

Кібербезпека та Кібергігієна: Основні тенденції

ЗМІСТ

Знайомство

Протидія кіберзлочинності в Україні

Проблеми правового регулювання

Кібербезпека. Кібергігієна

ОБСЕ Організація з безпеки та співробітництва в Європі
Координатор проектів в Україні



Протидія кіберзлочинності в Україні



Організація з безпеки та співробітництва в Європі
Координатор проектів в Україні

Про перелік, кількісний склад і предмети відання комітетів Верховної Ради України дев'ятого скликання

Документ **19-IX**, **чинний**, поточна редакція – **Редакція** від **18.12.2020**, підстава - **1127-IX**

 Інформація

 Зберегти

 Картка документа

 Зміст документа

 Пошук у тексті

 Текст для друку

 Поділитися ▾



18.12.2020 ▾



ПОСТАНОВА

Верховної Ради України

**Про перелік, кількісний склад і предмети відання комітетів
Верховної Ради України дев'ятого скликання**

(Відомості Верховної Ради (ВВР), 2019, № 35, ст.147)



17) Комітет з питань правоохоронної діяльності:

- формування стратегії функціонування правоохоронної системи України;
- кримінальне законодавство;
- кримінальне процесуальне законодавство;
- законодавство про адміністративні правопорушення;
- організація та діяльність органів прокуратури, поліції, Національної гвардії, прикордонної служби, Державного бюро розслідувань, інших правоохоронних органів;
- оперативно-розшукова діяльність;
- організація та діяльність органів досудового розслідування;
- протидія організованим злочинності і міжнародній злочинності, протидія кіберзлочинності;**
- протидія нелегальній (незаконній) міграції;
- запобігання злочинам та здійснення адміністративного нагляду за особами, звільненими з місць позбавлення волі;
- організація охорони громадської безпеки і порядку;
- охоронна і детективна діяльність;
- обіг зброї у цивільному обороті;
- державний захист учасників кримінального судочинства та державний захист суддів, працівників правоохоронних органів;
- соціальний захист працівників правоохоронних органів та членів їх сімей;
- міжнародне співробітництво та координація з питань правоохоронної діяльності;



Комітет цифрової
трансформації

23) Комітет з питань цифрової трансформації:

законодавчі засади цифровізації та цифрового суспільства в Україні;

Національна та державні програми інформатизації;

програми ЄС "Єдиний цифровий ринок" (Digital Single Market, EU4Digital) та інші програми цифрового співробітництва;

інновації у сфері цифрового підприємництва, розвиток екосистеми стартапів;

дослідницькі центри у сфері цифрових технологій;

цифрова індустрія та телекомунікації;

електронне урядування та публічні електронні послуги;

електронна демократія;

електронні довірчі послуги та цифрова ідентифікація;

державні інформаційно-аналітичні системи, електронний документообіг;

державні інформаційні ресурси, електронні реєстри та бази даних;

електронна комерція (електронна торгівля, електронний бізнес);

віртуальні активи, блокчейн та токенизація;

смарт-інфраструктура (міста, громади тощо);

розвиток сфери "відкритих даних";

радіочастотний ресурс;

розвиток орбітальної економіки;

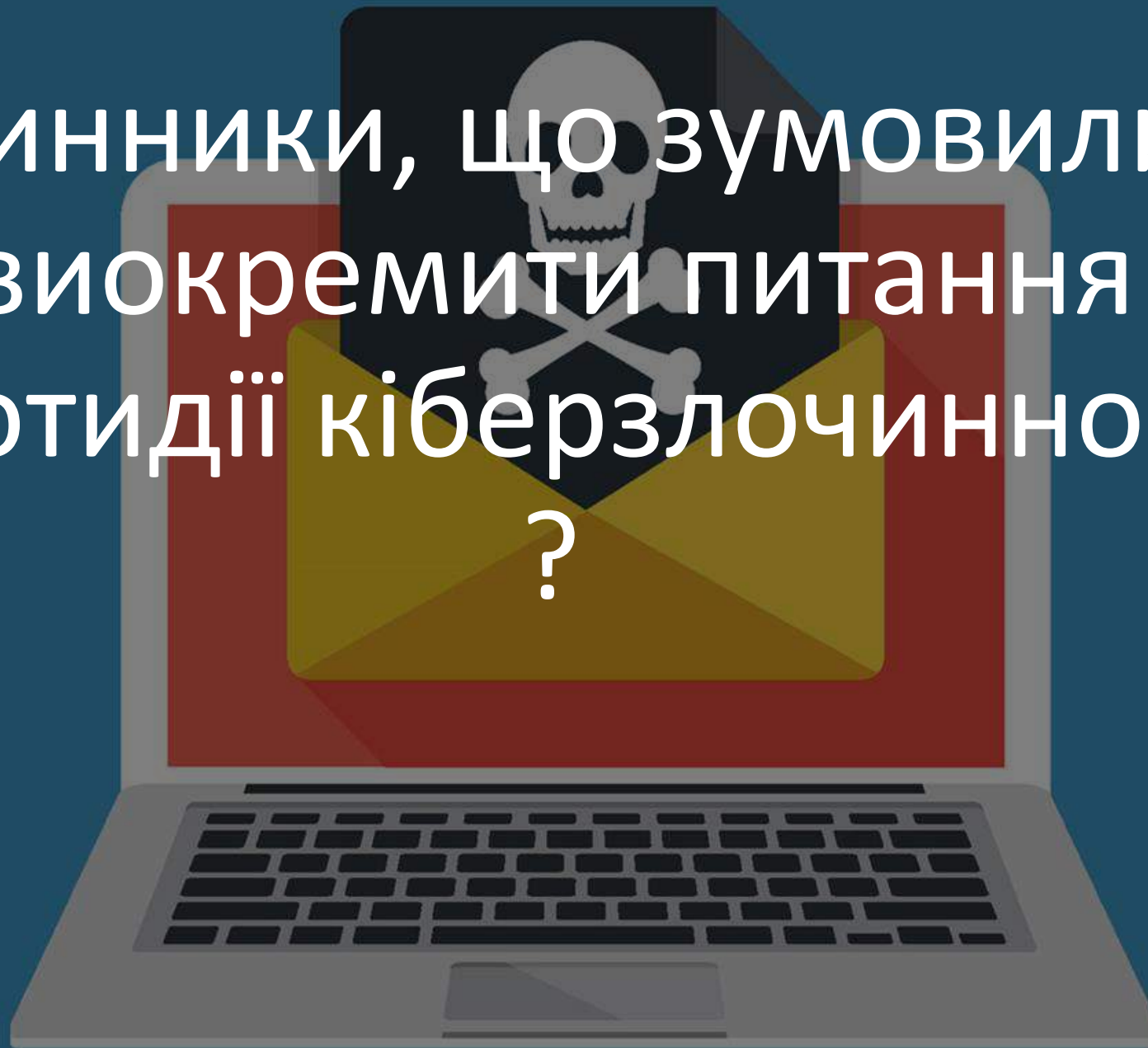
законодавчі засади адміністрування, функціонування та використання мережі Інтернет в Україні;

кібербезпека та кіберзахист, у тому числі у сфері критичної інфраструктури;

технічний та криптографічний захист інформації;

розвиток цифрових компетентностей, цифрові права.

Чинники, що зумовили виокремити питання протидії кіберзлочинності ?



Рівень кіберзлочинності

Проблеми правового регулювання



Недостатній рівень кібергігієни користувачів



Рівень  іноді

Проблеми  регулювання

I чинник Рівень кіберзлочинності

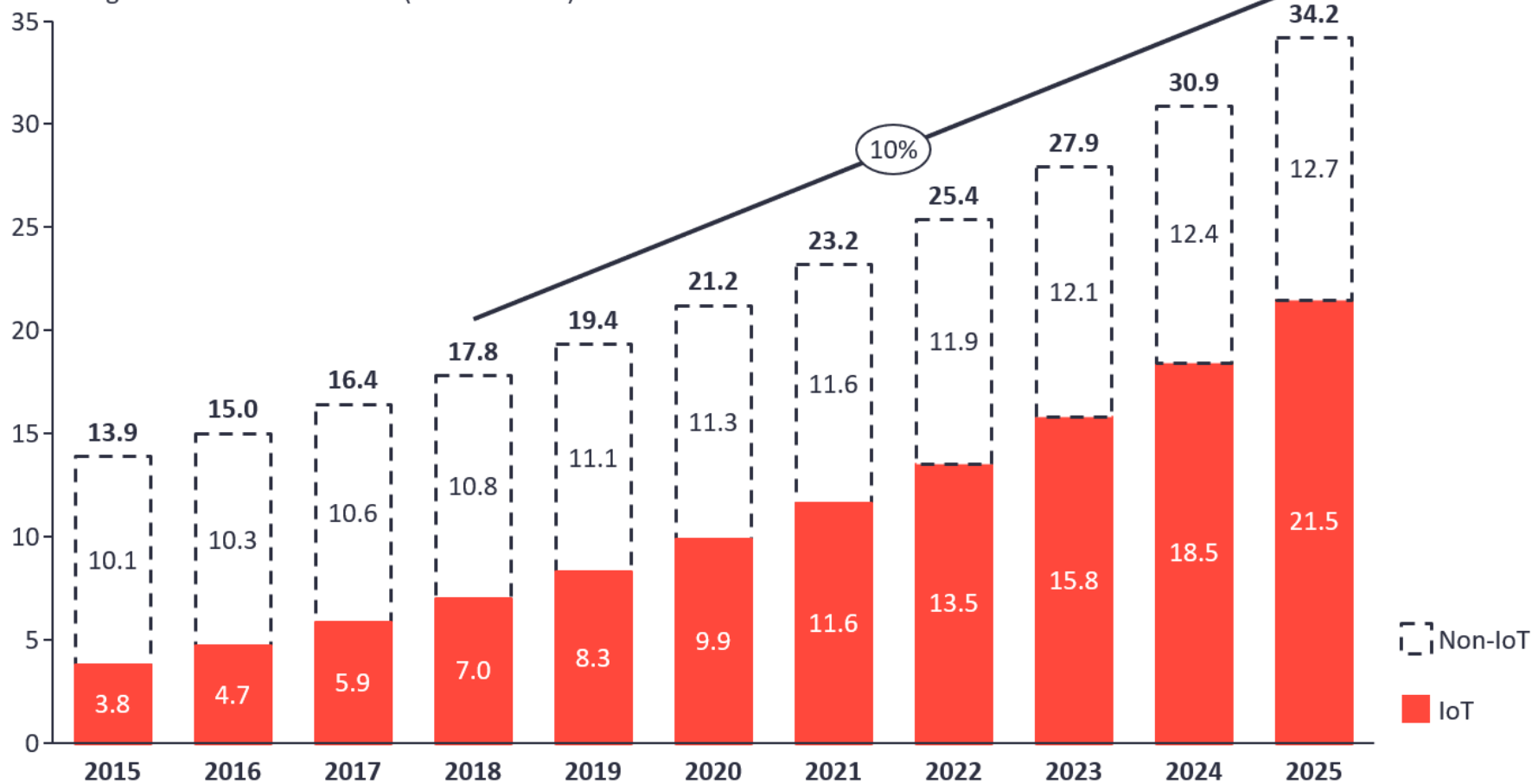


Інтернет речей та великі дані



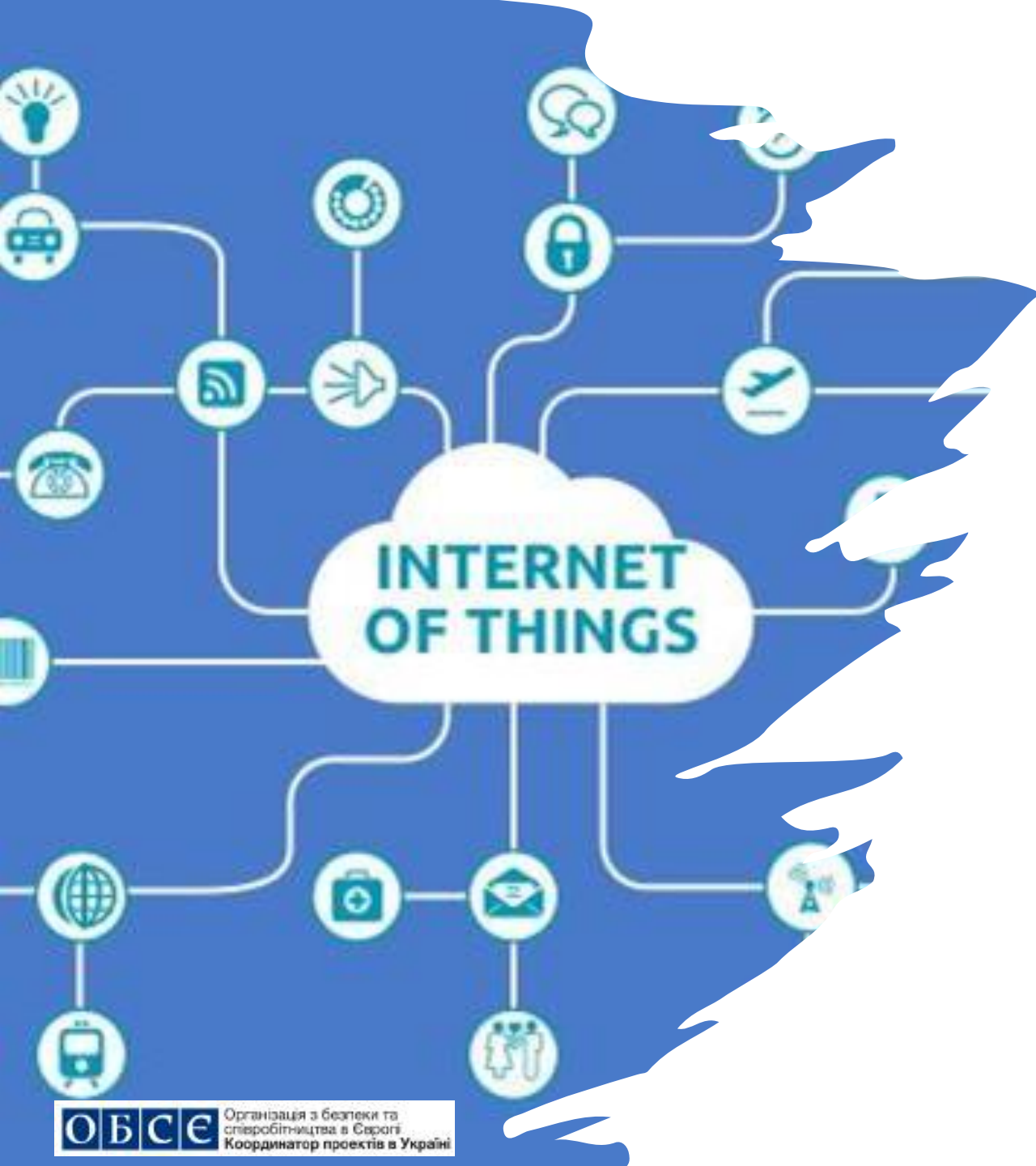
Total number of active device connections worldwide

Number of global active Connections (installed base) in Bn



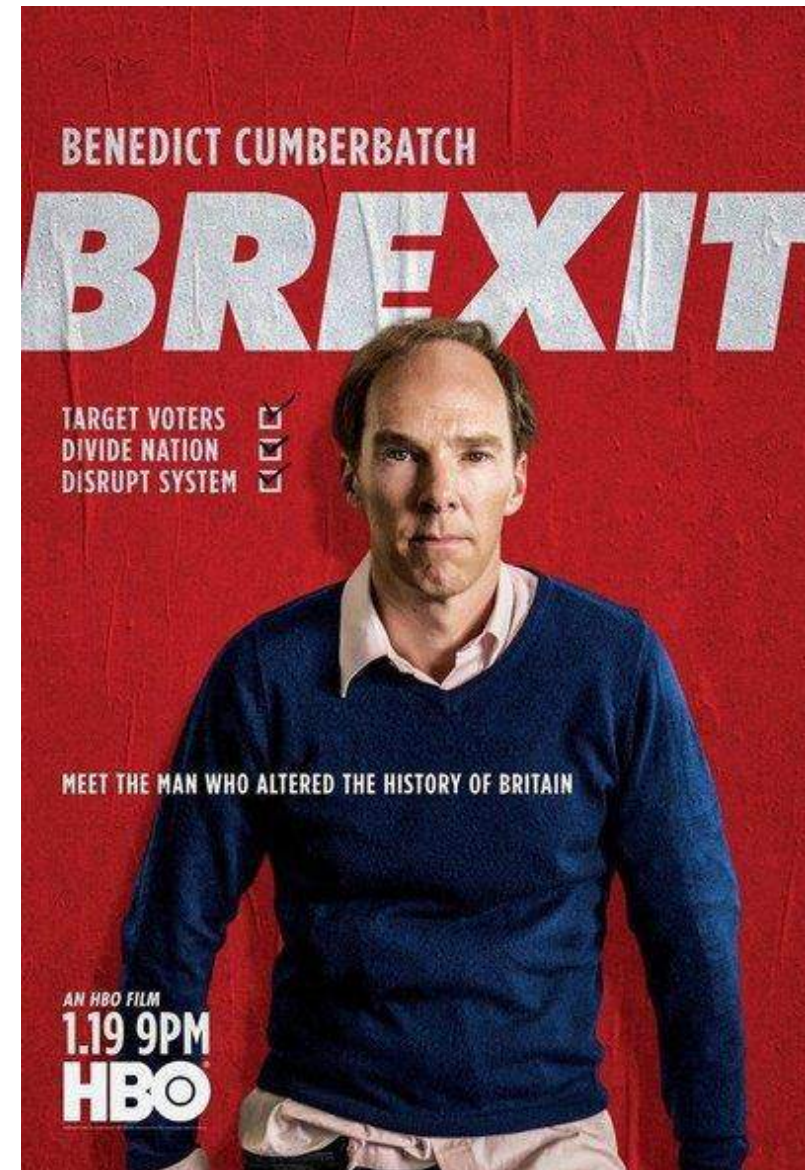
Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details
Source: IoT Analytics Research 2018

Кіберпростір



У 2025 році до Інтернету буде підключено 34 млрд. пристроїв

За рахунок підключення до мережі мікродатчиків звичайні речі з'єднуються між собою та стають інтелектуальними



■ Види кібернападників

- Хакери, що фінансуються державою



- Кіберзлочинці



- Хактивісти



Нестача спеціалістів з кібербезпеки до 2020 року досягне кількості 1,5 млн. людей відповідно до досліджень Frost & Sullivan and (ISC)²

Source: Harvard Business Review

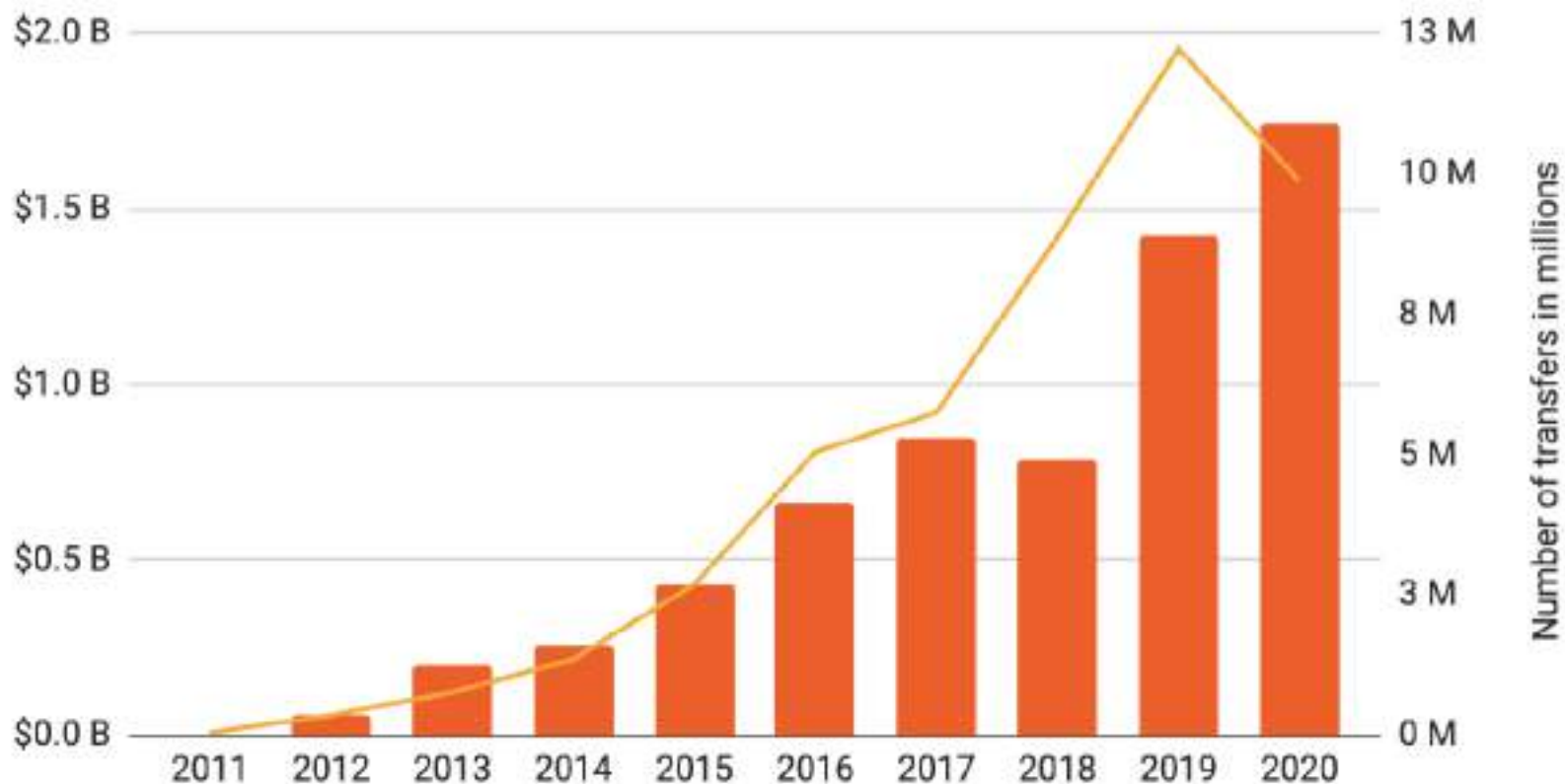
Кіберзлочинність завдасть
шкоди у розмірі 6 трильйонів
доларів до 2021 року

Source: Cybersecurity Ventures

- Продаж персональних даних
- Кібератаки як послуги
- Послуги ботненту
- Шкідливе програмне забезпечення
- Продаж аккаунтів



Darknet market revenue in billions of USD



Darknet market revenue

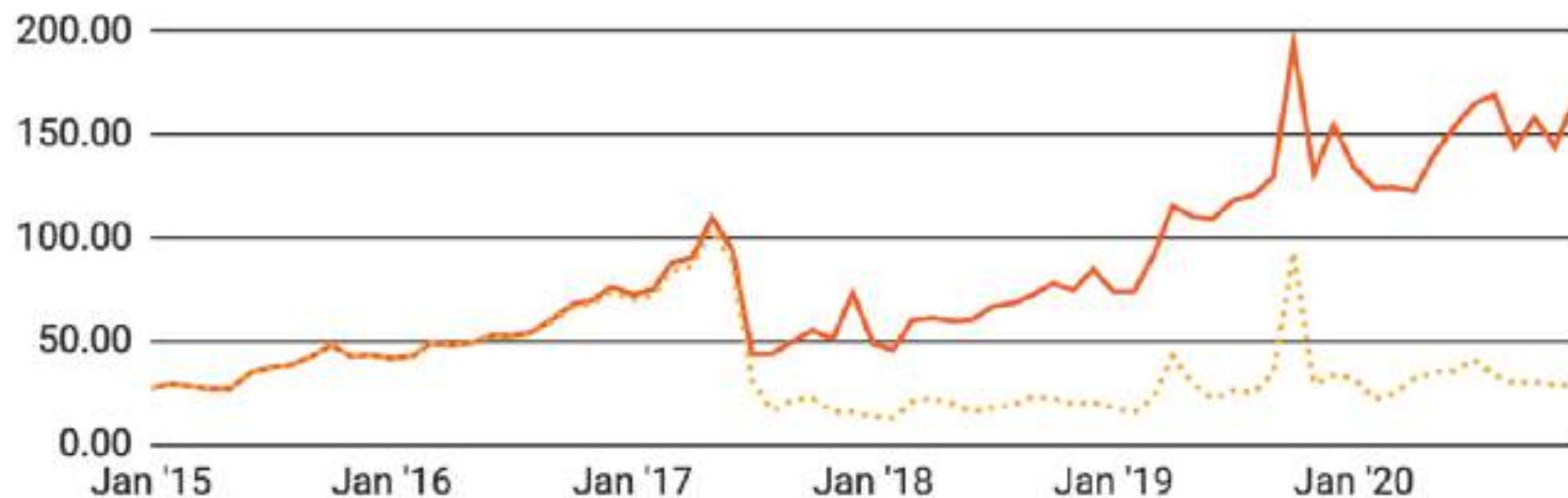
Number of transfers sent to darknet markets



Total revenue

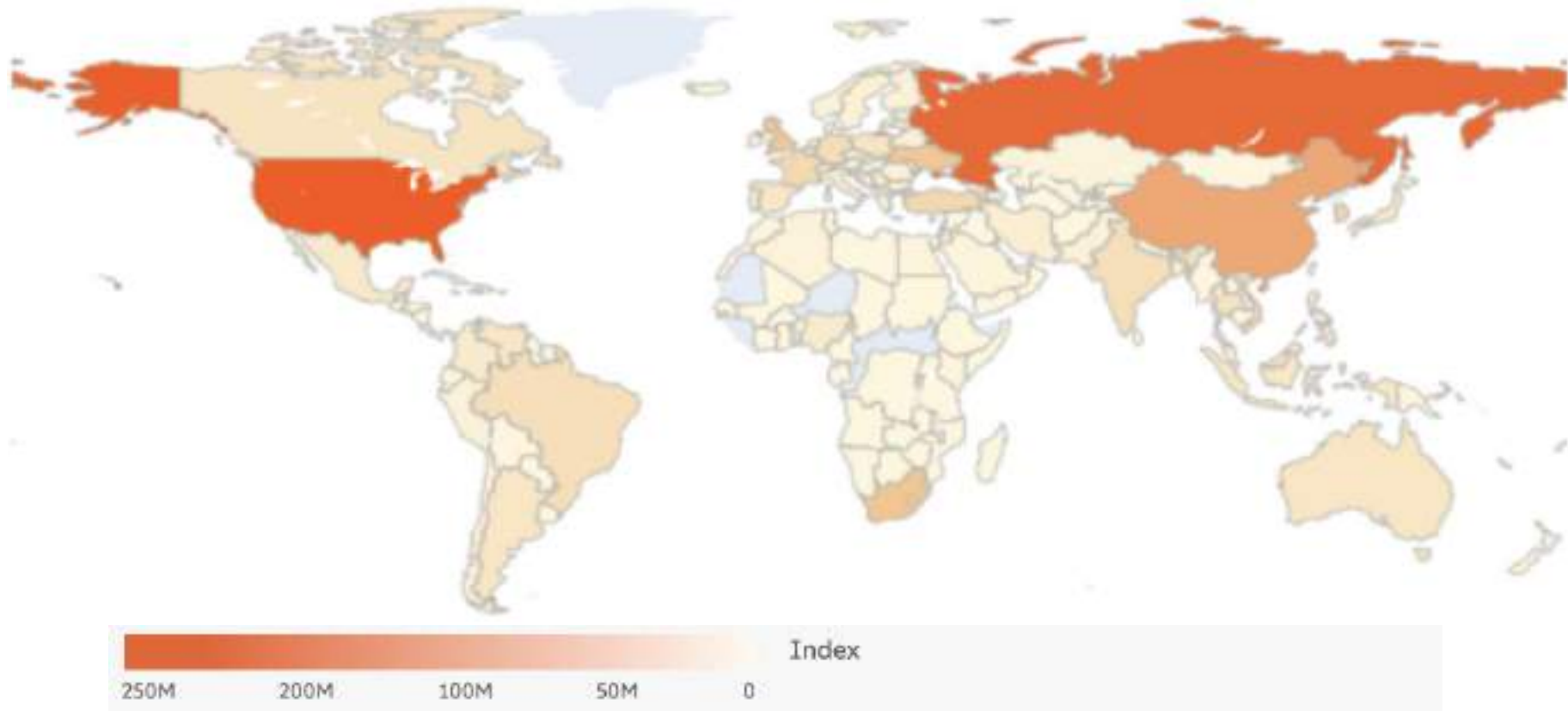
Total revenue excl. Hydra

Value in millions of USD

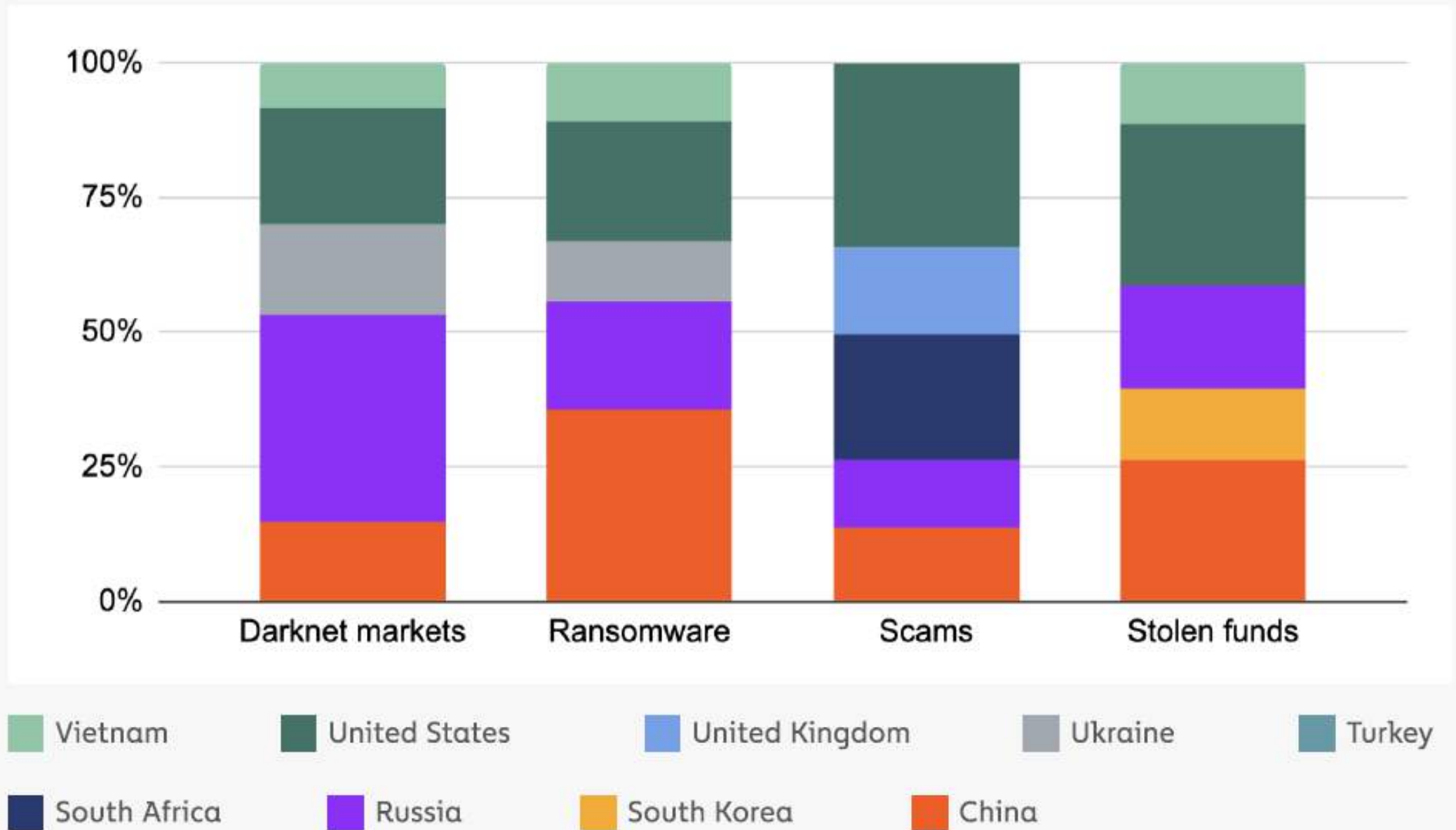


Країни, де зосереджено криптоактиви від незаконної діяльності

- United States
- Russia
- China
- South Africa
- United Kingdom
- Ukraine
- South Korea
- Vietnam
- Turkey
- France



Top 5 countries estimated to receive illicit funds by crime type | 2020



КЛЮЧОВІ РЕЗУЛЬТАТИ

Результати роботи кіберполіції по напрямку документування та розслідування злочинів у сфері високих технологій за 2020 рік



3 946
у банківській сфері

3 720
у сфері онлайн
шахрайства

11 621
супроводжуємо
розслідувань

802
у сфері
протиправного
контенту

3 153
у кіберсфері



Підозрілі події на об'єктах критичної інфраструктури

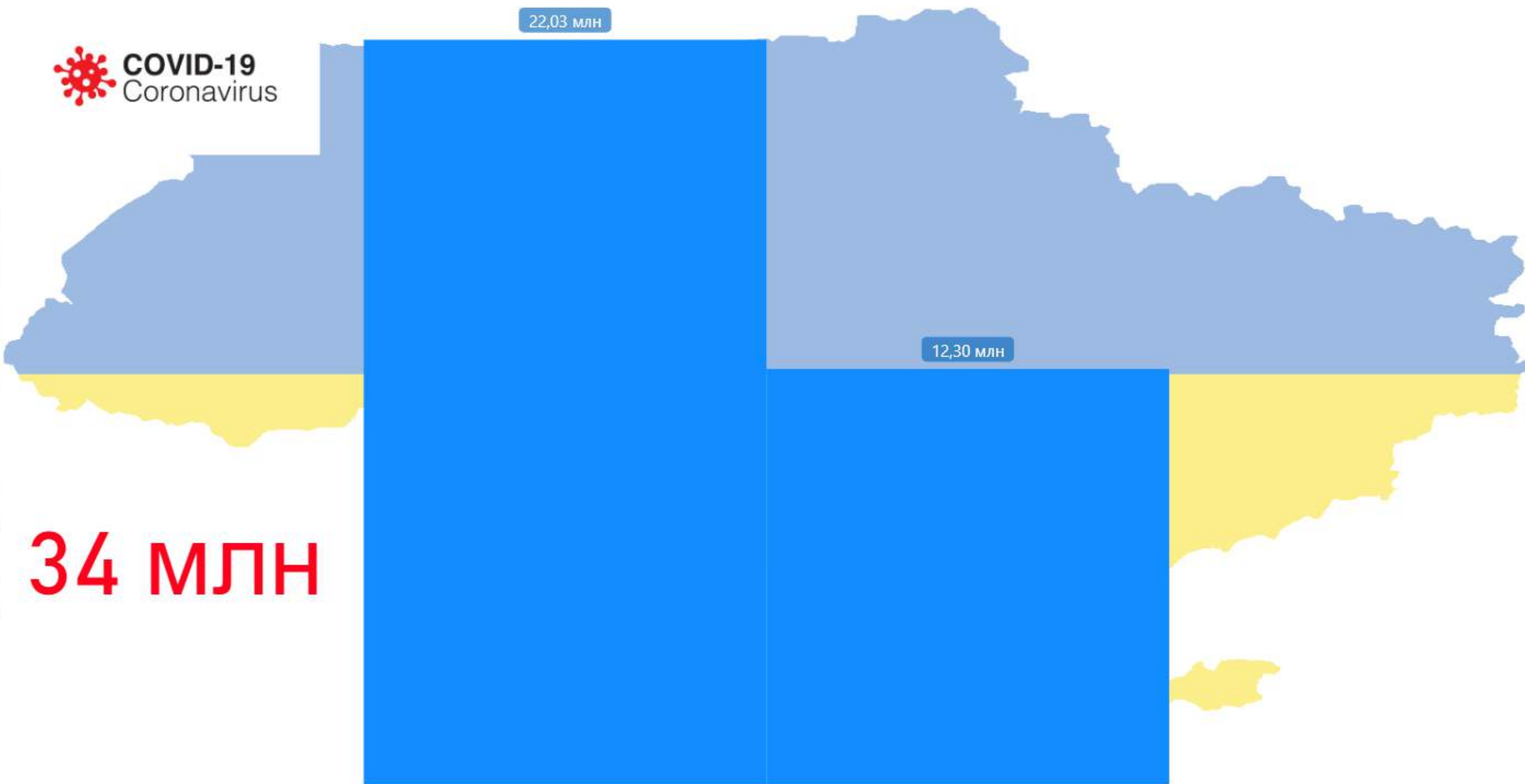
34 МЛН

22,03 МЛН

12,30 МЛН

2020

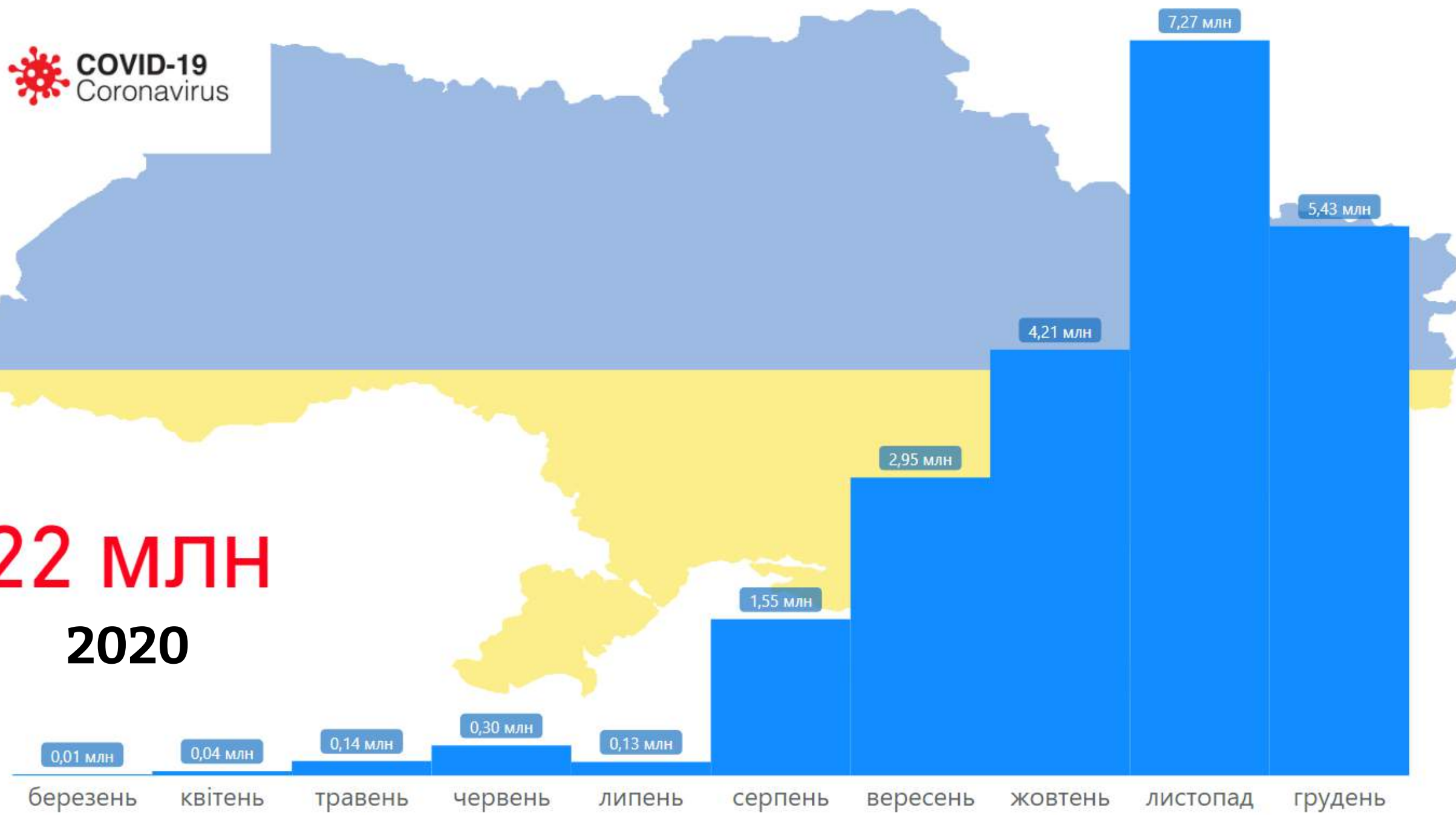
2021





Підозрілі події на об'єктах критичної інфраструктури

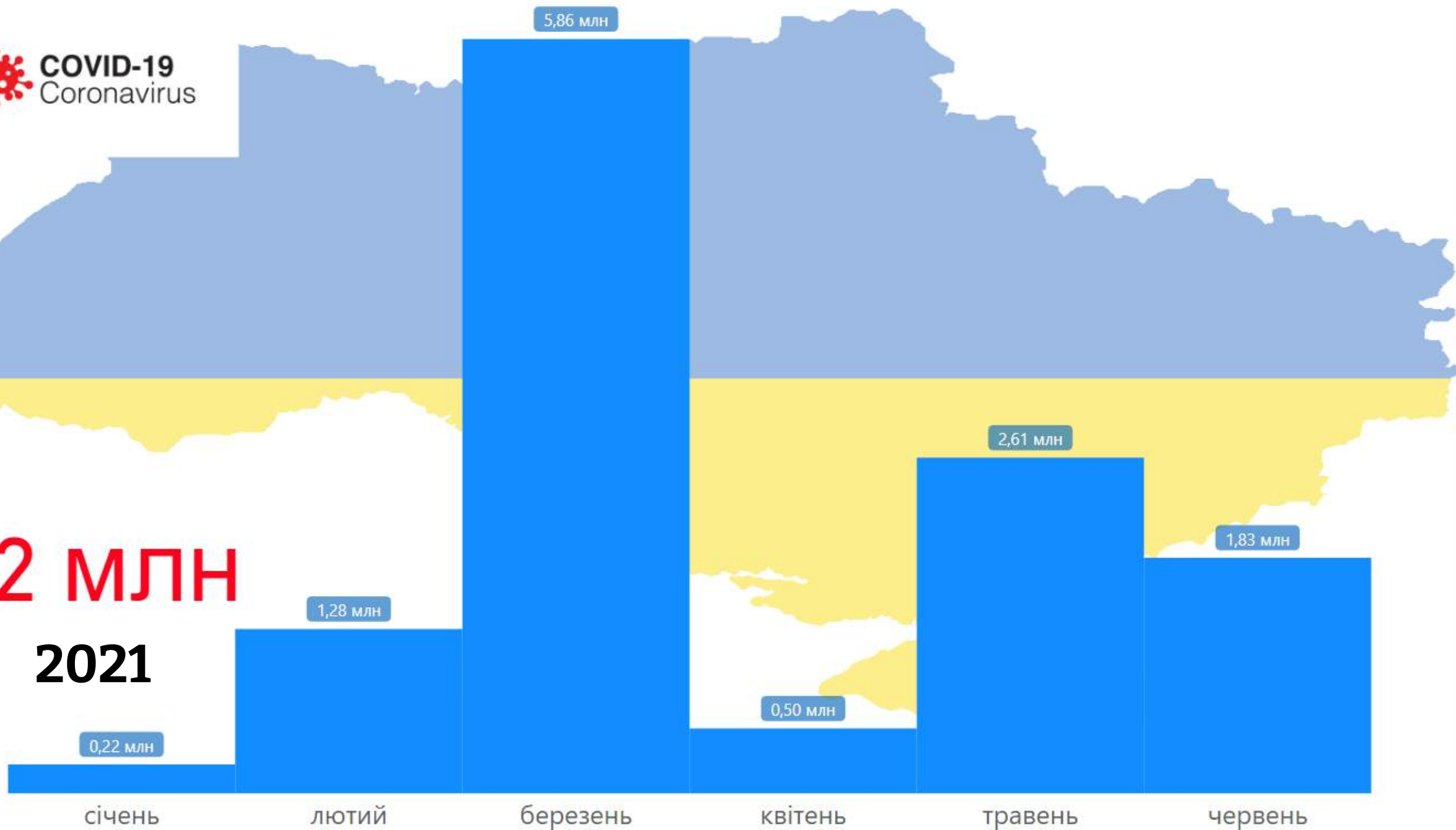
22 МЛН
2020





Підозрілі події на об'єктах критичної інфраструктури

12 МЛН
2021



II чинник

Проблеми правового регулювання





ВІТАЄМО НА ОФІЦІЙНОМУ САЙТІ КІБЕРПОЛІЦІЇ УКРАЇНИ

ДО ЗАВДАНЬ КІБЕРПОЛІЦІЇ ВХОДЯТЬ:

Реалізація державної політики в сфері протидії кіберзлочинності
Завчасне інформування населення про появу нових кіберзлочинців
Впровадження програмних засобів для систематизації кіберінцидентів
Реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів



**КІБЕР
ПОЛІЦІЯ**
НАЦІОНАЛЬНА ПОЛІЦІЯ
УКРАЇНИ

[Зворотний зв'язок](#) [Новини](#) [Рекомендації](#) [Стоп фрод](#) [No more ransom](#) [Контакти](#) [Вакансії](#) [Запобігання корупції](#) [Очищення влади](#)

Кіберполіція викрила злочинне угруповання, яке через ринок криптовалют легалізувало 42 мільйони доларів, здобутих злочинним шляхом

18 серпня 2020 р. 16:00

Співробітники кіберполіції в ході співпраці з міжнародними фахівцями у сфері цифрових валют, виявили трьох осіб, причетних до відмивання грошей.

На початку 2020 року Департамент кіберполіції розпочав співпрацю із однією з найбільших в світі бірж цифрових валют «Binance». Фахівці компанії використовують провідні в галузі алгоритми для аналізу і виявлення транзакцій, потенційно пов'язаних з фінансовими злочинами та шантажем.



Розділ XVI Кримінального кодексу України

«Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»

***статті 361, 361-1, 361-2, 362, 363, 363-1
в редакції Закону України № 2289-IV
від 23.12.2004 року***



Конвенція про кіберзлочинність

Дата підписання: 23.11.2001

Дата ратифікації: 07.09.2005

Дата набрання чинності: 01.07.2006

Норми Конвенції спрямовані на врегулювання трьох основних блоків питань:

- зближення кримінально-правової оцінки злочинів у сфері комп'ютерної інформації;
- зближення національних кримінально-процесуальних заходів, спрямованих на забезпечення збирання доказів при розслідуванні таких злочинів;
- міжнародне співробітництво в кримінально-процесуальній діяльності, спрямованої на збирання доказів вчинення таких злочинів за кордоном.

Законопроєкти

Проєкт Закону України № 4004 від 01.09.2020 року «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів»

http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=6977

1



Проєкт Закону України № 4003 від 01.09.2020 року «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам»



Висновки по чиннику № 1 та № 2



Все в наших руках!

**Не питаєте, що ваша країна
може зробити для Вас —
питаєте, що Ви можете
зробити для своєї країни**





**KEEP
SECURE
AND SAY
NO
TO CYBER CRIME**

III чинник

Недостатній рівень кібергігієни користувачів



Центральна виборча комісія	
	18.05.2014

СТБ, «5 канал», ICTV, ТРК «Україна», UBR и ATR	
	24.10.2015

АТ "Чернівціобленерго"	
	23.12.2015

АТ "Прикарпаттяобленерго"	
	23.12.2015

ПрАТ "Київобленерго"	
	23.12.2015

Аеропорт "Бориспіль"	
	17.01.2016

Укренерго	
	20.01.2016

Пенсійний фонд України	
	06.12.2016

Державна казначейська служба України	
	06.12.2016

Міністерство інфраструктури України	
	16.12.2016

Міністерство фінансів України	
	06.12.2016

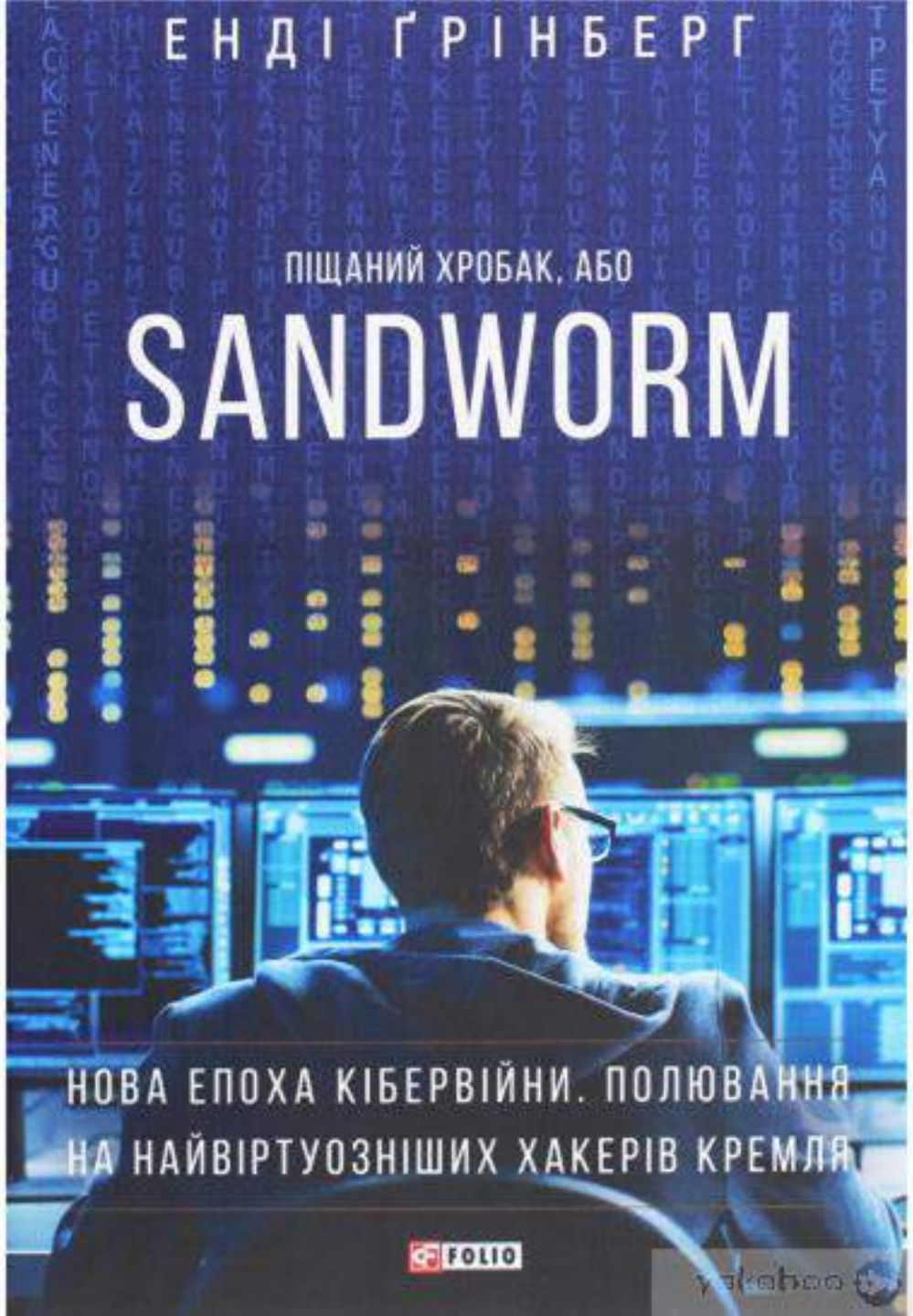
Укрзалізниця	
	15.12.2016

Укренерго	
	17.12.2016

Вірусна атака шифрувальника «XData»	
	17-22.05.2017

Всесвітня вірусна атака шифрувальника «WannaCry»	
	12-15.05.2017

Вірусна атака шифрувальника "Petya.A / Petya-Misha / ExPetr / Nyetya / NePetya"	
	27.06.2017



Книга
«Піщаний хробак, або
SANDWORM. Нова епоха
кібервійни. Полювання на
найвіртуозніших хакерів
Кремля»

Бачить кожен: Кульмінація кібератак

Від секунд до хвилини

Приховано:
захоплення

Вторгнення та

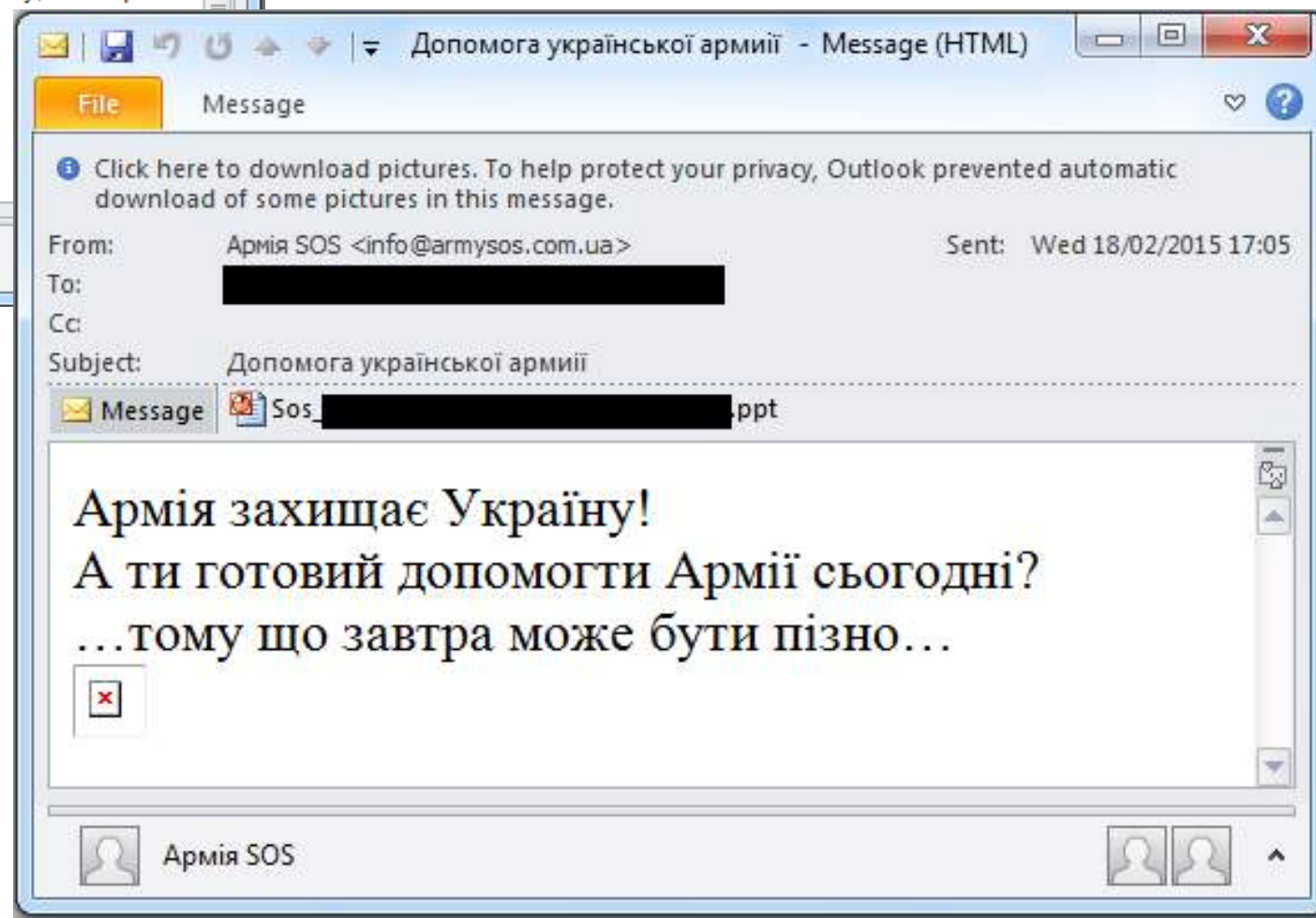
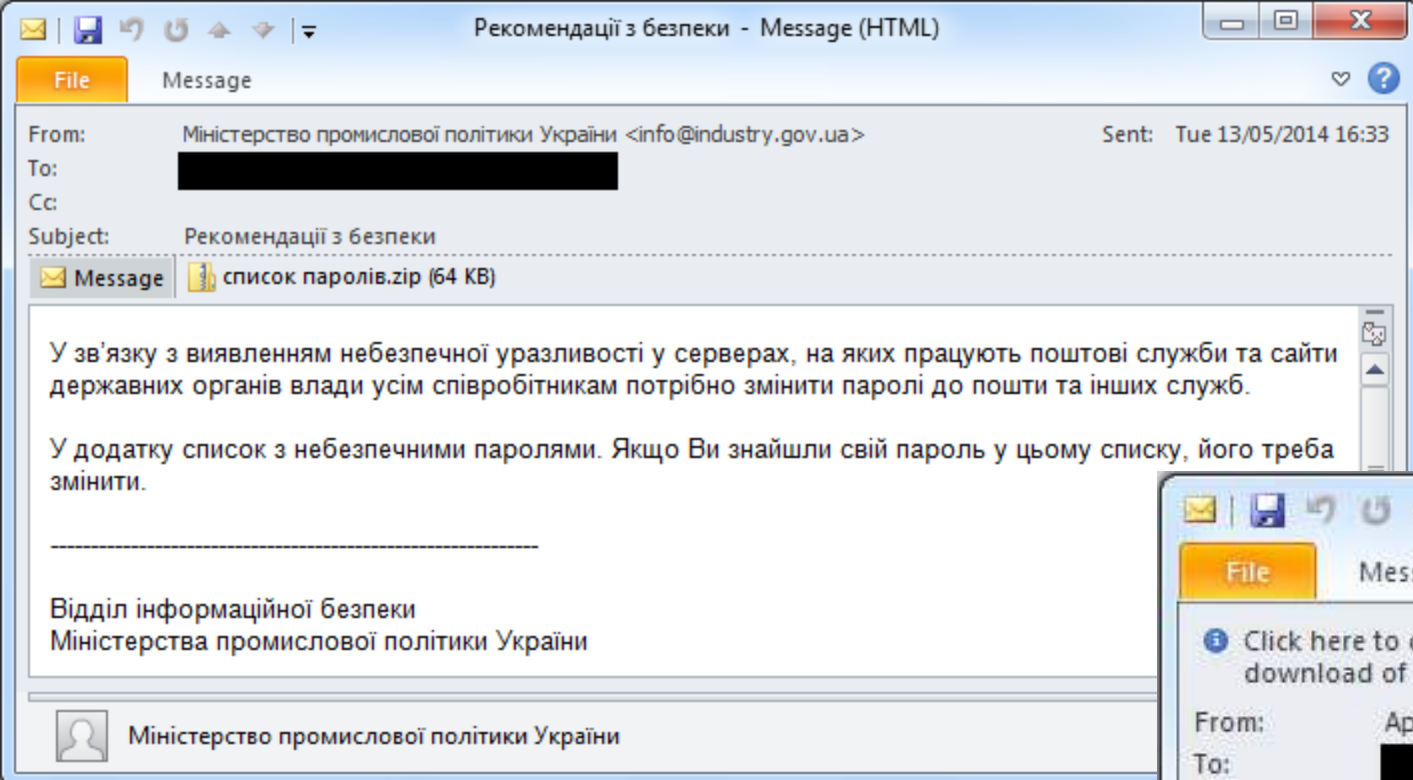
Від 1 місяця до декількох років
В середньому 4-6 місяців

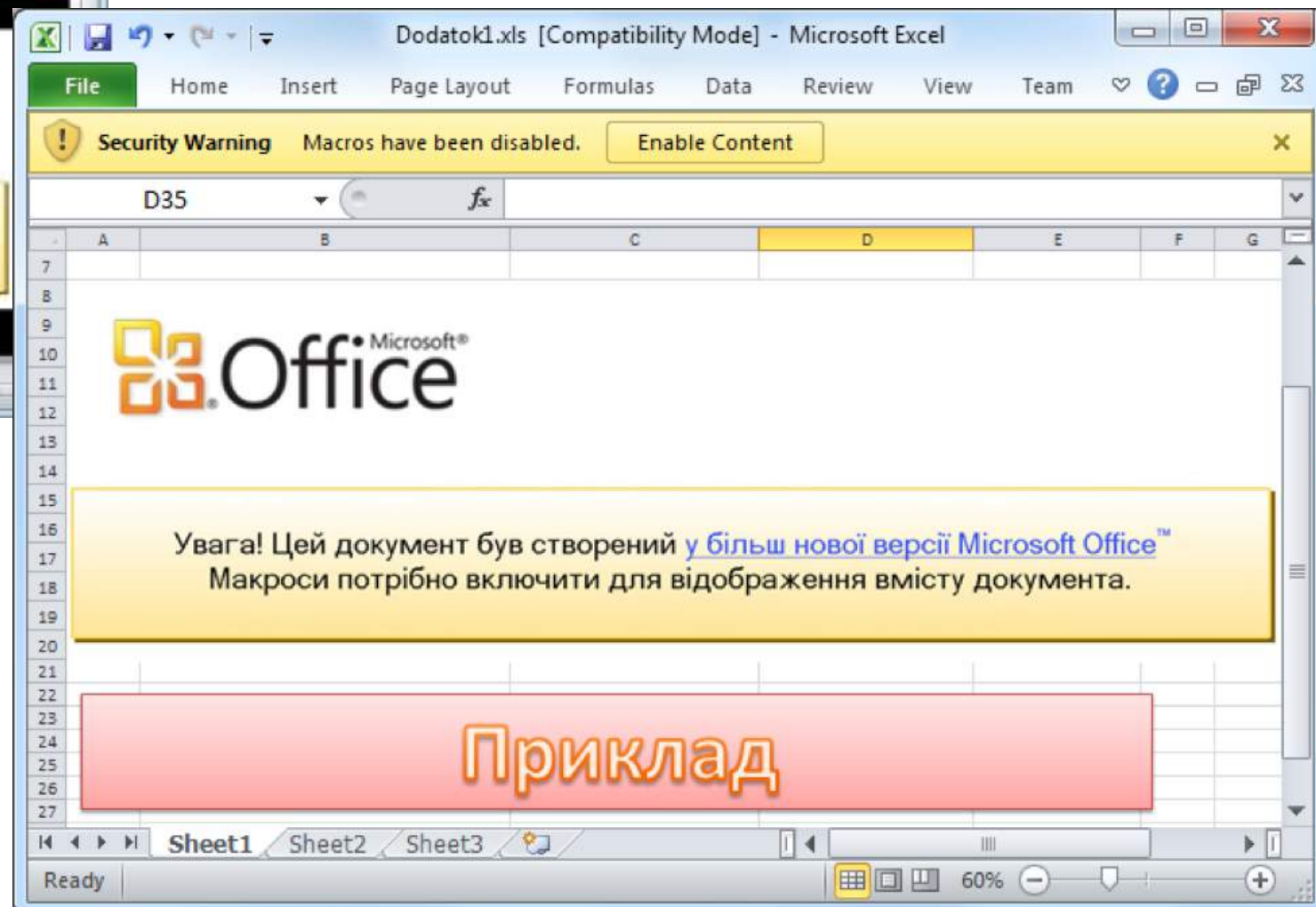
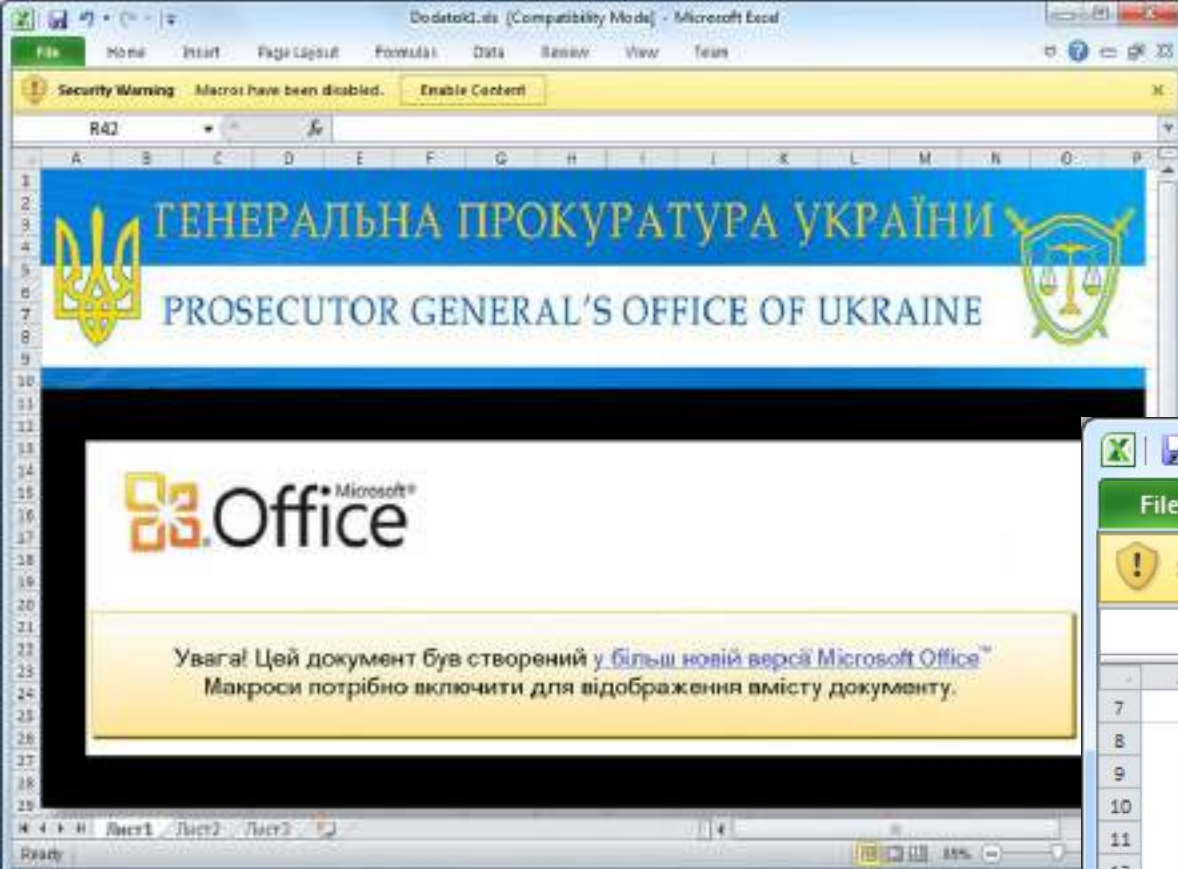
Глибинна та Темна мережа, де здійснюється підготовка до

- Проблема: недостатній рівень кібергігєни користувачів

**80% вторгнень
відбувається
завдяки успішній
фішинг-атаці**







Проблематичні питання кібергігієни держслужбовців



1. Безпечне використання Wi-Fi мереж
2. Працівники не забезпеченні VPN (віртуальною приватною мережею)
3. Використання однакових паролів для різних облікових записів
4. Проблема поводження з «чутливими паперовими даними»
5. Низька культура звернень до служби IT-підтримки
6. Проблема використання багатофакторної аутентифікації
7. Фішинг та соціальна інженерія
8. Нерозуміння негативних наслідків від публікації особистої інформації

Проблематичні питання кібергігієни держслужбовців



-
9. Безпечний «серфінг» в мережі Інтернет
 10. Шифрування даних. Безпечне використання USB-носіїв
 11. Використання персональних пристроїв для виконання робочих завдань
 12. Передача «чутливих даних» відкритим зв'язком
 13. Захист «чутливих даних» в громадських місцях
 14. Оновлення програмного забезпечення
 15. Резервне копіювання даних
 16. Використання хмарних технологій
-