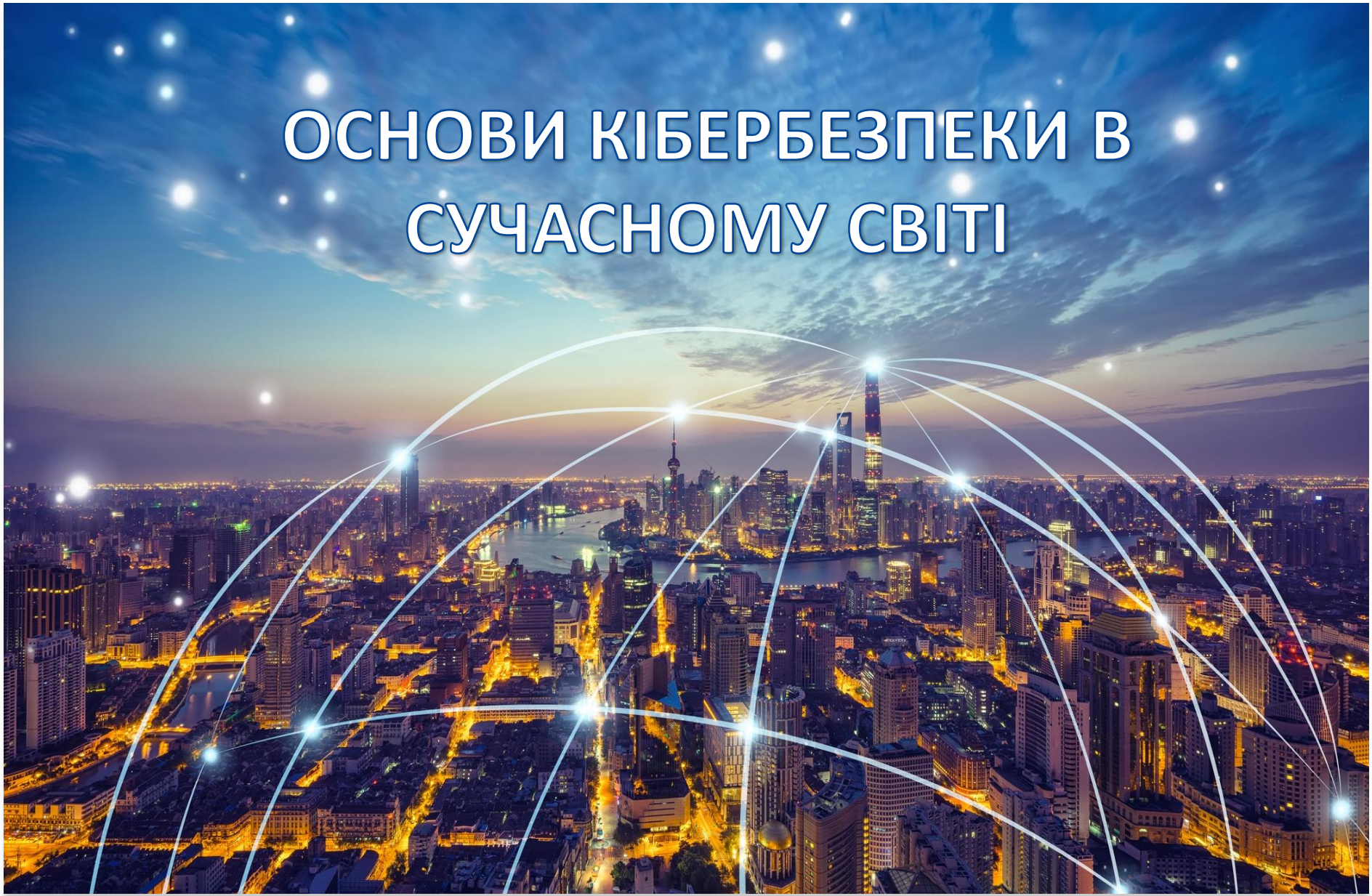
ОСНОВИ КІБЕРБЕЗПЕКИ В СУЧАСНОМУ СВІТІ



Що таке кібербезпека?

Кібербезпека – це набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до керування ризиками, дій, професійної підготовки страхування та технологій, які використовуються для захисту кіберсереди, ресурсів організацій та користувачів.

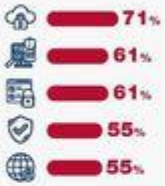
USAID ВІД АМЕРИКАНСЬКОГО НАРОДУ

НКЦК

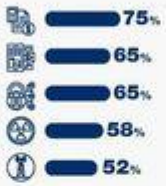
РИНОК КІБЕРБЕЗПЕКИ У 2022 РОЦІ. ПОГЛЯД МІЖНАРОДНИХ ЕКСПЕРТІВ

ТЕНДЕНЦІЇ СВІТОВОГО РИНКУ

СЕГМЕНТИ, ЯКІ НАЙІНТЕНСИВНІШЕ РОЗВИВАЮТЬСЯ У 2022



ГАЛУЗІ ІЗ ВИСОКИМ РІВНЕМ КІБЕРГОТОВНОСТІ



СВІТОВИЙ РИНОК КІБЕРБЕЗПЕКИ

- Безпека хмарних сервісів оцінена як сегмент із найбільшим потенціалом
- Фішинг - тип кібератаки, з яким найчастіше стикалися у 2022 році
- Росія визнана основною країною походження кібератак

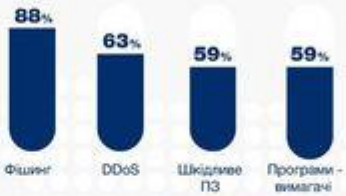
УКРАЇНСЬКИЙ РИНОК КІБЕРБЕЗПЕКИ

- Українські експерти мають найсильніші компетенції у пошуку та аналізі кіберзагроз
- 25% експертів обізнані про компанії українського походження
- 13% знають про продукти / послуги, що надаються українськими компаніями
- 47% обізнані про діяльність українських кіберволонтерів

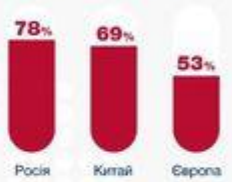
НАЙСИЛЬНІШІ КОМПЕТЕНЦІЇ УКРАЇНСЬКИХ КОМПАНІЙ ЗА СФЕРАМИ

НАЙЦІННІША ЕКСПЕРТИЗА УКРАЇНСЬКИХ КОМПАНІЙ ЗА ГАЛУЗЯМИ

НАЙБІЛЬШ ПОШИРЕНІ ВИДИ АТАК У 2022 РОЦІ

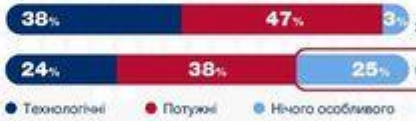


ОСНОВНІ РЕГІОНИ ПОХОДЖЕННЯ АТАК У 2022 РОЦІ



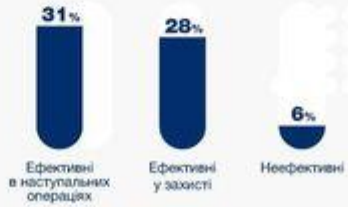
КІБЕРСТІЙКІСТЬ УКРАЇНИ ПРОТИ КІБЕРАГРЕСІЇ РОСІЇ

ЕКСПЕРТНА ОЦІНКА РОСІЙСЬКИХ КІБЕРАТАК



ОЦІНКА КІБЕРСТІЙКОСТІ УКРАЇНИ

ОЦІНКА ДІЯЛЬНОСТІ КІБЕРВОЛОНТЕРІВ

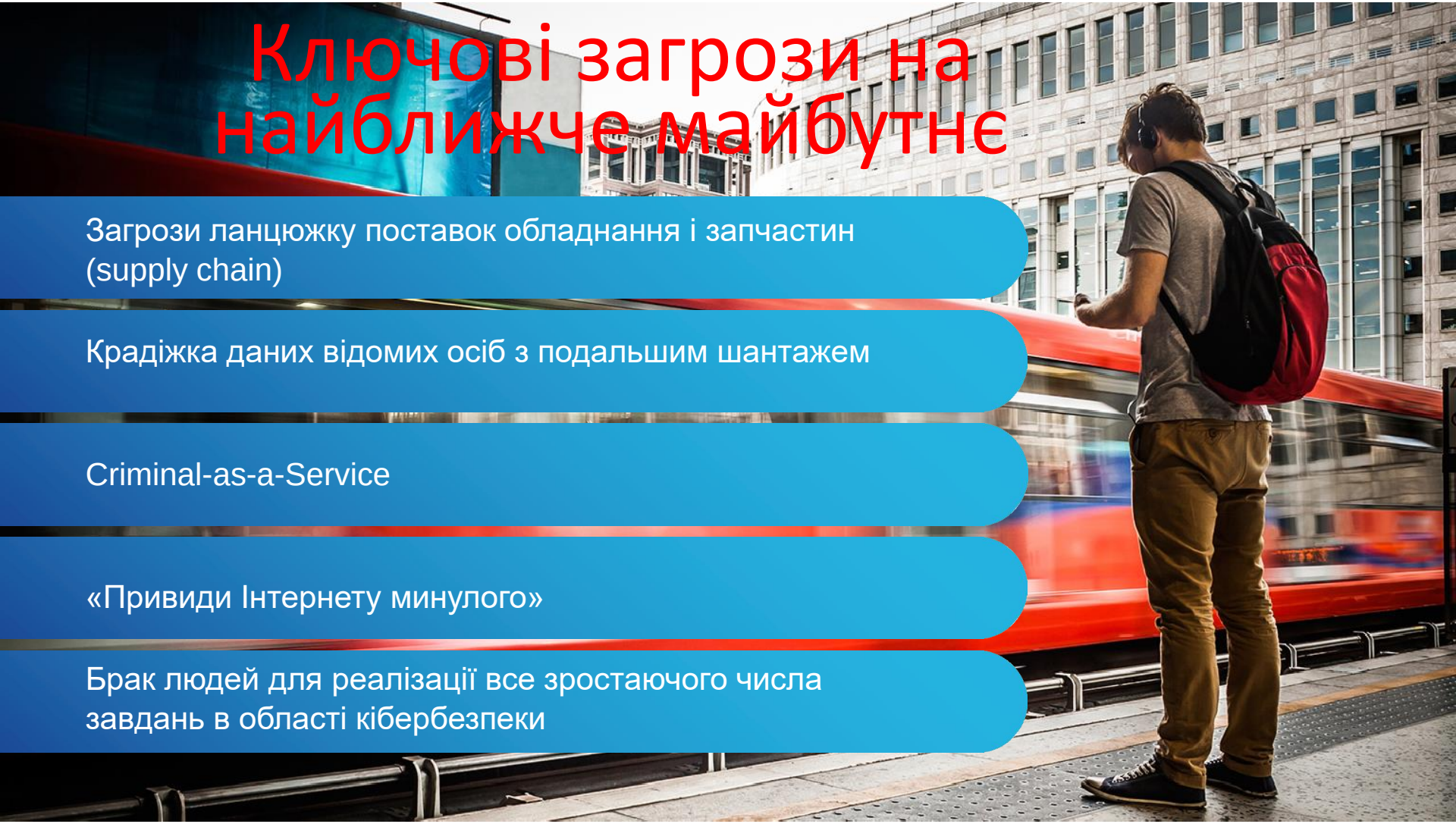


Вибірка: Опитано 50 експертів у 2022 році: з 21 країни, 5 континентів. Фахівці команд CERT та CSIRT, керівники відділів IT-безпеки та віцепрезиденти з кібербезпеки, блогери (візіонери) ринку кібербезпеки, учасники галузевих робочих груп

Ключові загрози на найближче майбутнє

- Пристрої «Всеохоплюючого Інтернету» (IoT) як майданчик для реалізації атак
- Мобільні додатки як розносники шкідливого ПО і «злодії» даних
- Програми вимагачі (ransomware або кріптолокери) і супутні їм технології (наприклад, фішинг)
- Використання протоколу DNS для приховування активності шкідливого ПЗ
- Цілеспрямовані загрози, що реалізують повний цикл "kill chain»

Ключові загрози на найближче майбутнє



- Загрози ланцюжку поставок обладнання і запчастин (supply chain)
- Крадіжка даних відомих осіб з подальшим шантажем
- Criminal-as-a-Service
- «Привиди Інтернету минулого»
- Брак людей для реалізації все зростаючого числа завдань в області кібербезпеки

Нові IT змінюють ландшафт кібербезпеки

Всеохоплюючий Інтернет підключає автомобілі, відеокамери, грошові мішки, банкомати, пропуску\

Хмарні технології вимагають забезпечення ІБ на що не належить організації платформі з нечітким місцем розташування

Мобільність розмиває периметр, збільшує площу атаки і перекладає частину завдань ІБ на недосвідчених користувачів

Програмовані мережі (SDN) і відсутність контролю за связностью Інтернет (BGP) відкриває можливість для перехоплення трафіку

Нові IT змінюють ландшафт кібербезпеки

- Соціальні мережі стають джерелом поширення негативної інформації про компанію, а також каналом проникнення
- Нове робоче місце працівника (динамічний, BYOD, BYOT) створює нові складності для забезпечення ІБ
- Аналіз Великих даних призводить до порушення законодавства про персональні дані
- Квантові обчислення привносять нові можливості в забезпечення конфіденційності переданих по каналах зв'язку даних
- Штучний інтелект (машинне навчання, нечітка логіка ...) дозволяє побачити невидиме (але незрозуміло як)

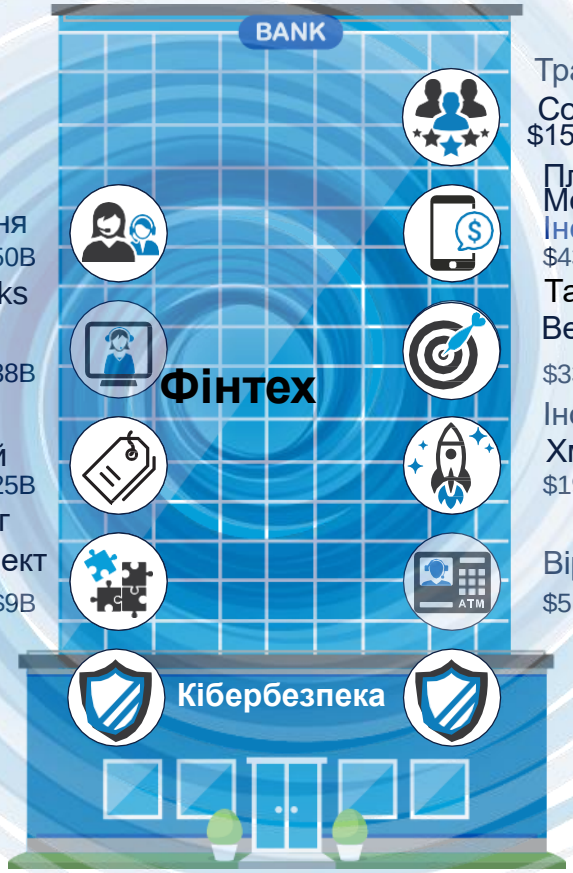
** Customer Experience Emerges as the Marketers' Next Battlefield, Jake Sorofman, Oct 2014

ОСНОВНІ НАПРЯМИ РЕАЛІЗАЦІЇ КІБЕРБЕЗПЕКИ

- Розвиток кіберпростору (системи/мережі е-комунікацій, ІТ-сфера, е-довірчі послуги)
- Боротьба з кібертероризмом (ОРД, розвідка, контррозвідка)
- Кібероборона (активний захист, міжнародна військова співпраця)
- Кіберзахист (базові вимоги захисту ІТС/КЗІ/ТЗІ, орг-тех модель, НТМ, виявлення, протидія, відновлення)
- Аудит інформаційної безпеки (ІТС критичної інфраструктури, ризик орієнтовані підходи, тестування вразливостей)
- Взаємодія, фахові і ресурсні спроможності, законодавче врегулювання, обмежувальні заходи
- Протидія кіберзлочинності (розслідування, притягнення до відповідальності)

Майже 80% дій і заходів – компетенції Держспецзв'язку

Що впливає на кібербезпеку?



APT

Працівники наступного покоління

$50B

Software Defined Networks

Відео-радники $38B

Брендовані послуги

Інтернет речей

$25B

Консталтинг

Штучний інтелект

$9B

Шахрайство

Трансформація продажів і послуг

Соціальні мережі

$152B

Платежі

Мобільність

Інсайдери

$43B

Таргетована реклама і маркетинг

Великі данні і аналітика

$33B

Іноваційні продукти

Хмарні технології

$19B

Віртуальні помічники

$5B

Законодавство

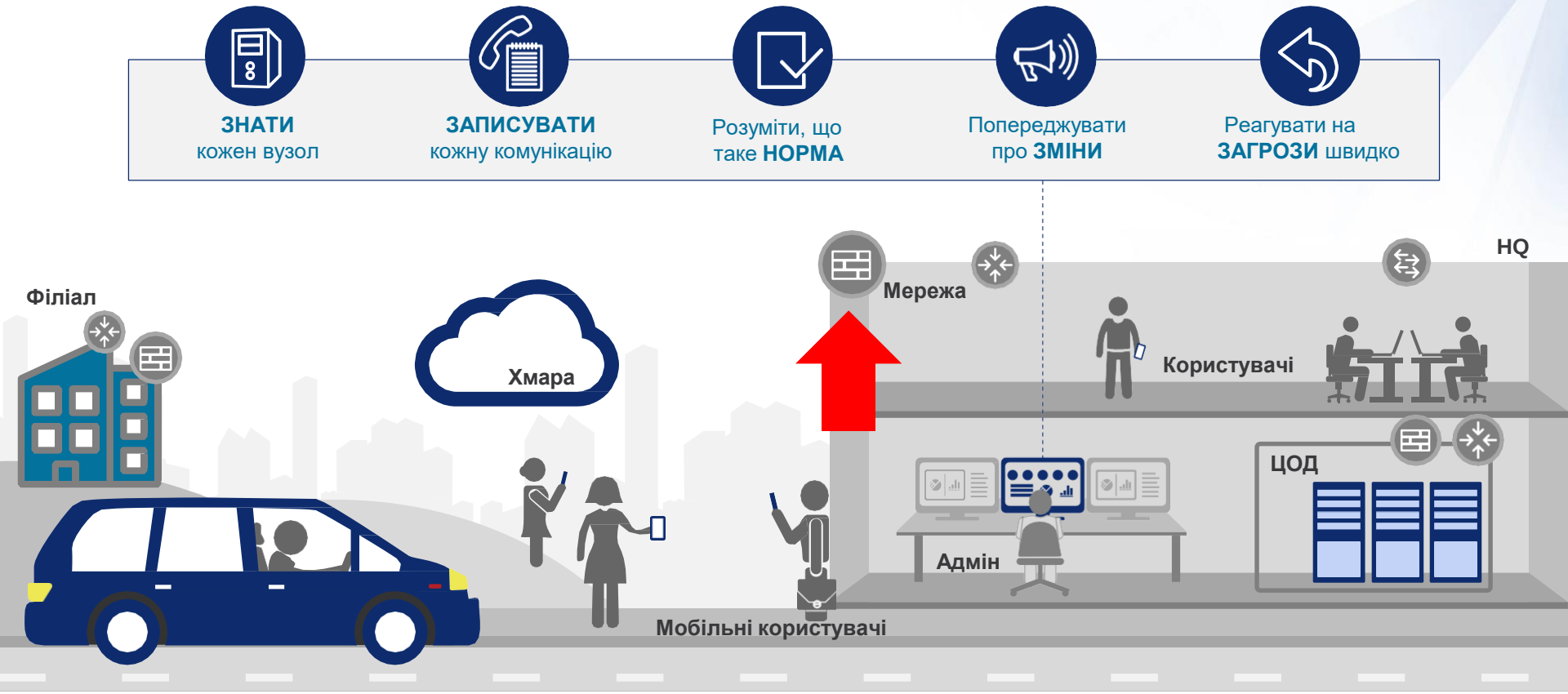
Магічні абревіатури

Що у вас є?

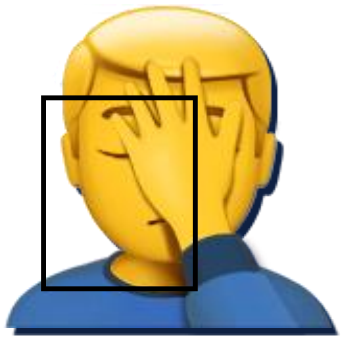
1. FW, IDS, IPS, AV, VM, DLP, PKI, SIEM, UTM, WAF, MDM, HIPS
2. NTA, EDR, SOC, UEBA, CASB, TI, EPP, NGAV, STAP, EVC, BDS, PAM, NFT, IRP, NAC, SAT, IAG, NGEP, AEP, AWL
3. SDS, SDP, DDP, MDR, SOAR

У затвердженому сьогодні плану заходів щодо ІБ в рамках «Цифрової економіки» є й інші абревіатури

Де/як ми зазвичай будуємо захист?

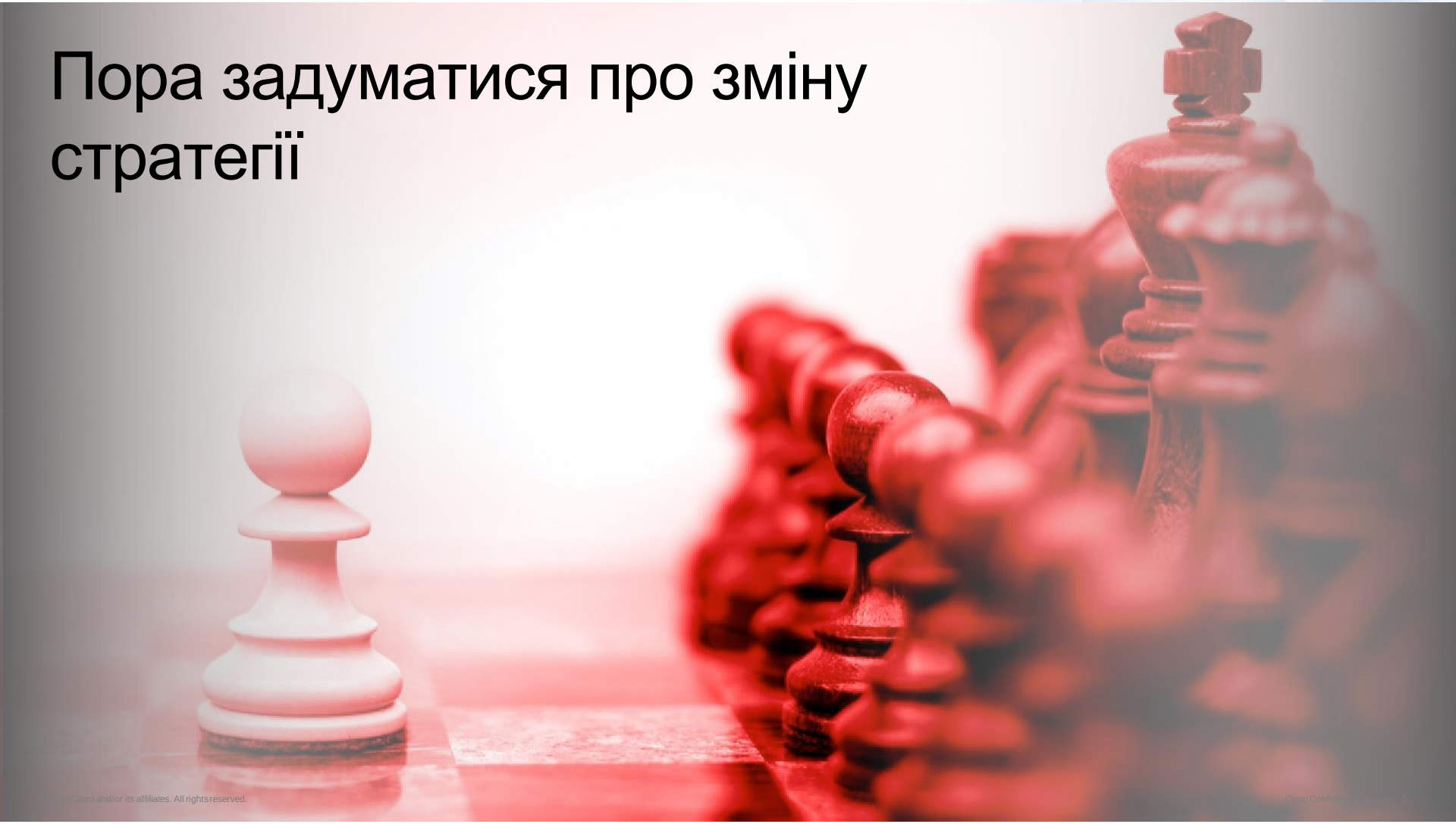


Навіть якщо ваш периметр захищений



- А що робити зі зростаючим обсягом зашифрованого трафіку (наприклад, TLS)?
- А як бути з технологіями типу pinning?
- А наш периметр готовий до переходу в хмари?
- А периметр враховує програмно-визначаючі мережі і сегментацію?

Пора задуматися про зміну стратегії



ПК залишаються основною точкою входу для інцидентів

70% інцидентів починаються на ПК

ЧОМУ?

Розрив в захисті

65%

організацій кажуть, що атаки обходять засоби запобігання

Помилки користувачів

48%

атакуючих обходять захист ПК через помилки користувачів

Розрив у видимості

55%

організацій не можуть визначити причину інциденту

100

ДНІВ

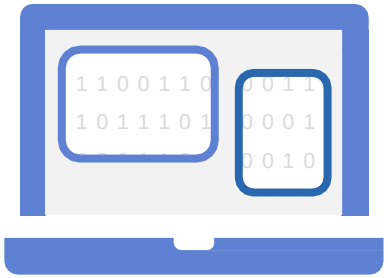
середній час виявлення в індустрії

Джерело: Cisco

З сучасних підходів до захисту ПК

Виявляти IOCs & аномалії в системній активності

може вимагати додаткової експертизи та ресурсів



Ізолювати додатки & дані в гіпервізора / контейнерах

може зажадати від користувачів зміни поведінки і може бути складним у впровадженні

Запобігати з'єднання в Інтернет активності

може забезпечити кращу видимість і блокування *** якщо *** є можливість блокувати з будь-якого порту, протоколу або додатка

Брак фахівців з безпеки

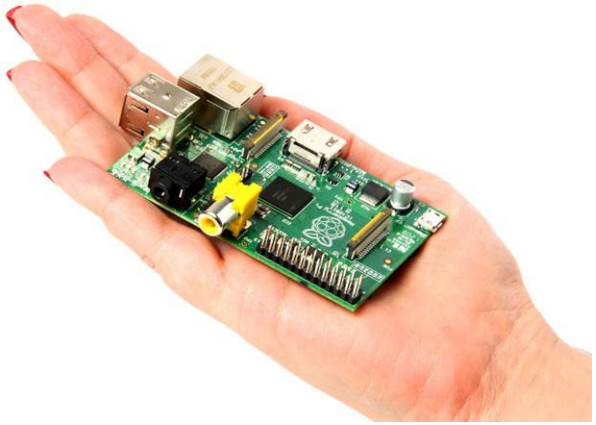
Світовий брак фахівців з кібербезпеки складе до 2020-го року 1 мільйон осіб

Брак фахівців з кібербезпеки в Росії становить близько 55-60 тисяч осіб, тоді як щорічна підготовці 25500 чоловік

Потреба у фахівцях з кібербезпеки в 12 разів вище, ніж в IT фахівцях

Компанії з браком фахівців, витрачають на боротьбу з наслідками атак в середньому в 5 разів більше

Загроза може проникнути минаючи периметр



Лобі і переговорки ...
Ви їх контролюєте?

Цікавість візьме верх чи ні?

СКЛАДОВІ СИСТЕМИ КІБЕРБЕЗПЕКИ

РНБО

Національний координаційний центр кібербезпеки

Організаційно-технічна складова кіберзахисту

організаційно-технічна модель кіберзахисту, система аудиту інформаційної безпеки

Оперативна складова кібербезпеки

розвідувальні, контррозвідувальні, оперативно-розшукові, правоохоронні заходи

ОБ ’ ЄКТИ

- Сектор профдіяльності (оператори, провайдери)
- ІТ-системи дежорганів
- Критична інфраструктура
- Приватний сектор

ОСНОВНІ СУБ’ЄКТИ

Захищеність *(ІТС, інформресурс)*	Активний захист *(реагування, протидія)*	Боротьба з кіберзлочинністю	Кіберрозвідка, протидія кібертероризм
Держспецзв'язку, НБУ	Держспецзв'язку, НБУ, МОУ, Генштаб ЗСУ	СБУ, Нацполіція	СБУ, СЗР, ГУР МО

КЛАСИФІКАЦІЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ПЕРСПЕКТИВНІ НАПРЯМИ РОЗВИТКУ СИСТЕМИ КІБЕРЗАХИСТУ

- Нормативно-правове врегулювання питань кіберзахисту та кібербезпеки
- Налагодження міжнародного співробітництва з питань кіберзахисту та кібербезпеки
- Дооснащення Команди реагування на комп’ютерні надзвичайні події України CERT-UA
- Побудова оперативного центру реагування на кіберінциденти
- Модернізація центрального сегменту Системи захищеного доступу державних органів до Інтернету
- Побудова Національної телекомунікаційної мережі