КІБЕРНАВЧАННЯ ТА ТРЕНІНГИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Вересень 2020. Кібернавчання для фахівців Центральної виборчої комісії та основних суб'єктів забезпечення кібербезпеки з метою відпрацювання заходів спільного реагування на випадок кібератак під час місцевих виборів 2020 року.
Листопад 2020. Кібернавчання в рамках проекту «Bug Bounty», який організовано спільно із Фондом цивільних досліджень та розвитку США. Наразі в рамках другого етапу реалізації проєкту здійснюється оцінка стану захищеності 22 об'єктів критичної інфраструктури.
Листопад 2020. Сертифікаційний тренінг CISSP для фахівців НКЦК.
Листопад-грудень 2020. Міжнародні навчання для фахівців НКЦК International Program on Cyber Security Studies (iPCSS) з питань планування, розробки та імплементації національної стратегії кібербезпеки.
Грудень 2020. Тренінг «Стратегічне планування та управління кібербезпекою», організовано спільно із Фондом цивільних досліджень та розвитку США для керівників ІТ та ІБ об'єктів критичної інфраструктури та основних суб'єктів забезпечення кібербезпеки.

ВЗАЄМОДІЯ З МІЖНАРОДНИМИ ПАРТНЕРАМИ ТА ПРИВАТНИМ СЕКТОРОМ

Німеччина: українo-німецька експертна зустріч з питань кібербезпеки з представниками Східного комітету – Східноєвропейської спілки німецької економіки.
Словенія: перший раунд двосторонніх міжвідомчих кіберконсультацій.
Естонія: третій раунд двосторонніх міжвідомчих кіберконсультацій.
Молдова: участь у тижні кібербезпеки Молдови.
Нідерланди: щорічне засідання платформи «Global Forum on Cyber Expertise» в рамках посилення двосторонньої співпраці в сфері кібербезпеки.
Афганістан: зустріч Секретаря РНБО України з Надзвичайним та Повноважним Послом Ісламської Республіки Афганістан в Україні з метою ознайомлення з можливостями НКЦК та розвитку співпраці, зокрема, у сфері кіберзахисту.
Норвегія: зустріч Секретаря РНБО України з Надзвичайним та Повноважним Послом Королівства Норвегія в Україні з метою ознайомлення з можливостями НКЦК та налагодження обміну інформацією про кіберзагрози.
Велика Британія: зустріч Секретаря РНБО України з Надзвичайним та Повноважним Послом Великої Британії в Україні з питань двостороннього співробітництва зокрема у сфері кібербезпеки, інформаційної безпеки, протидії гібридним загрозам.
Європейський Союз: здійснюється підготовка до проведення першого засідання Кібердіалогу Україна-ЄС.
В рамках місяця кібербезпеки в Україні взято участь у Третьому міжнародному форумі «Кібербезпека. Захистимо бізнес - захистимо державу», в рамках якого підписано Меморандум про співробітництво з ТПП в сфері кібербезпеки.
В ході реалізації проєкту USAID «Кібербезпека критично важливої інфраструктури» проведено опитування об'єктів критичної інфраструктури щодо вивчення потреб у підвищенні кваліфікації фахівців з кібербезпеки та оцінки стану комунікації, координації та взаємодії між суб'єктами національної системи кібербезпеки.

РАДА НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

СТАН НАЦІОНАЛЬНОЇ КІБЕРБЕЗПЕКИ

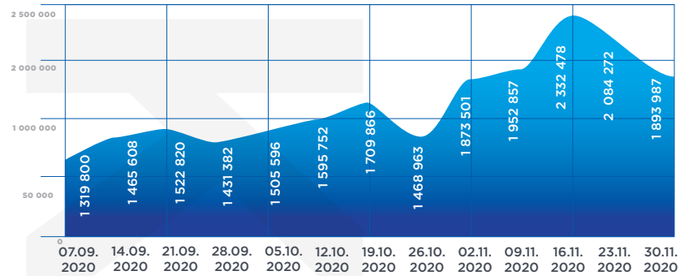
НКЦК

07вересня – 06 грудня 2020 року

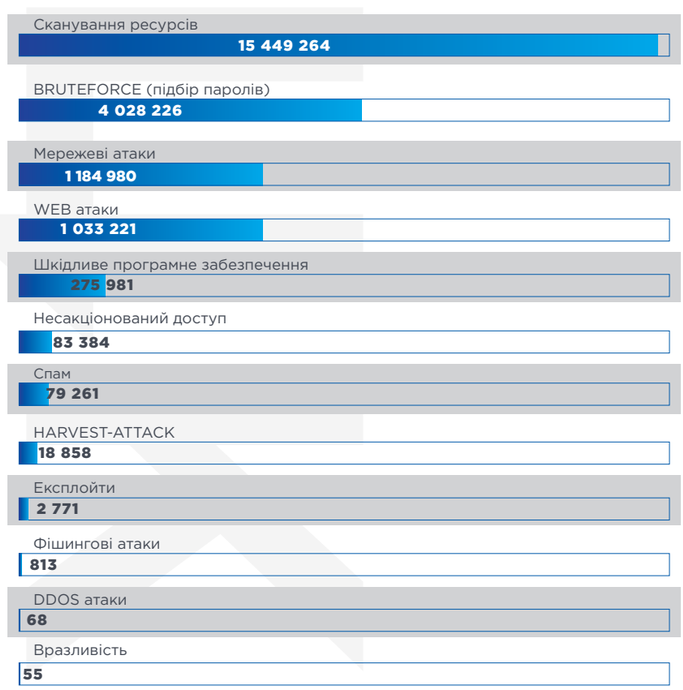
Індикатор рівня загрози

22 156 882 ЗАГАЛЬНА КІЛЬКІСТЬ ІНЦИДЕНТІВ ЗА ПЕРІОД

Динаміка



ТИПИ КІБЕРІНЦИДЕНТІВ



Основні суб`єкти кібербезпеки

	Кількість кіберінцидентів
	18 600 175

Кількість організацій, установ, підприємств, які регулярно надають інформацію щодо стану кібербезпеки — **10**

«Відповідно до ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» та абзац 5 п. 5 Положення про НКЦК до основних суб'єктів належать: Держспецзв'язку, Національна поліція, СБУ, Міноборони, розвідувальні органи, Генштаб ЗСУ, Нацбанк, Мінцифра»

Суб`єкти кібербезпеки
(у межах компетенції)

Суб'єкт кібербезпеки	Кількість кіберінцидентів
Приватний сектор	237 441
Критична інфраструктура	63 505
Державні органи	2 938 475

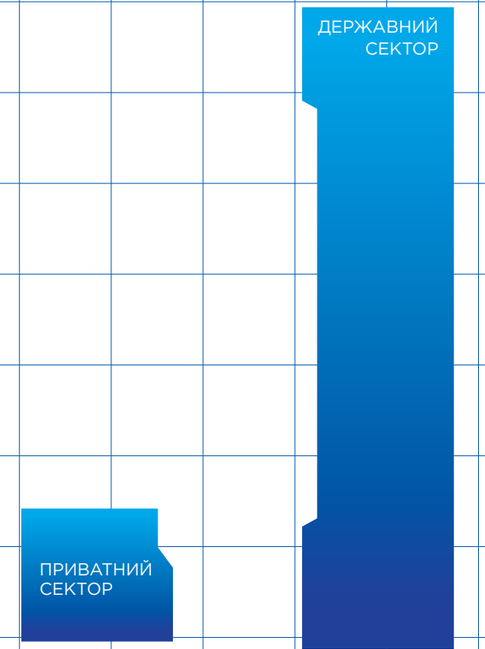
Кількість організацій, установ, підприємств, які регулярно надають інформацію щодо стану кібербезпеки — **31**

Міжнародні суб'єкти кібербезпеки

	Кількість кіберінцидентів
	317 286

Кількість організацій, установ, підприємств, які регулярно надають інформацію щодо стану кібербезпеки — **4**

Кібершкода



≈151,9 млн. грн

≈748,6 млн. грн

КРАЇНИ, З ЯКИХ ЗДІЙСНЮЄТЬСЯ НАЙБІЛЬШЕ АТАК

США 23.83%
Державний сектор **22,09%**
Приватний сектор **44,56%**

Франція 6.75%
Державний сектор **7,05%**
Приватний сектор **<2%**

Німеччина 3%
Державний сектор **<4%**
Приватний сектор **2,89%**

Інші 30.05%
Державний сектор **25,42%**
Приватний сектор **20,20%**

Росія* 6.03%
Державний сектор **7,18%**
Приватний сектор **9,79%**

Китай 29.44%
Державний сектор **31,22%**
Приватний сектор **7,49%**

Чехія 3.88%
Державний сектор **6,59%**
Приватний сектор **<1%**

Болгарія <1%
Державний сектор **<1%**
Приватний сектор **15,07%**

*Атакуючі використовують орендовані або скомпроментовані системи для приховування свого реального місця розташування, тому дані щодо кількості атак співвідносяться із розвитком IT інфраструктури (в тому числі кількістю та доступністю дата-центрів) у певній державі

Приватний сектор **1,35%** | Державний сектор **98,65%**

ТОП КІБЕРАТАК КРИТИЧНОГО ТА ВИСОКОГО РІВНЯ

Опис	Кількість	Суб'єкти реагування	Стан реагування
DDoS атаки на інфраструктуру Херсонської ОДА	**1**	НКЦК	**Забезпечено резервні канали зв'язку та збір індикаторів атаки**
Веб-шел на сайті Миколаївської РДА	**2**	Держспецзв'язку, СБУ	**Дані про загрозу надано CERT-UA та ДКІБ СБУ для реагування**
Фішингова атака на Офіс Президента України	**1**	НКЦК, ОПУ	**Атаку локалізовано. Виявлено скомпрометовані системи, реагування відповідно до протоколу**
Фішингові сторінки українських банків	**4**	Нацбанк, Держспецзв'язку	**Виявлені фішингові ресурси заблоковано**
Спрямована кібератака на інформаційні системи Міністерства оборони України	**1**	НКЦК, Міноборони	**Атаку локалізовано. Виявлено скомпрометовані системи, реагування відповідно до протоколу**
Фішингові розсилки з адрес державних органів	**2**	Держспецзв'язку, учасники платформи обміну індикаторами кіберзагроз НКЦК	**Дані про загрозу надано CERT-UA для реагування**
Спрямовані атаки на веб-ресурси органів державної	**28**	НКЦК	**Атаки попереджено. Здійснено збір індикаторів**
Атаки з використанням шкідливого програмного забезпечення – вимагача (ransomware)	**331**	НКЦК	**Атаки локалізовано. Здійснюється аналіз шкідливого коду.**
Атаки на українських користувачів, пов'язані з установкою шкідливого програмного забезпечення під виглядом антивірусу на пристрої Apple.	**1**	НКЦК	**Здійснюється аналіз шкідливого коду.**

Всього: **371**

ТОП ВИЯВЛЕНИХ ВРАЗЛИВОСТЕЙ

Опис	Кількість	Суб'єкти реагування	Стан реагування
Виявлено понад 12,5 тис. вразливих пристроїв (IoT), що використовувались для DDoS атак (UDP флуд)	**понад 2,5 тис. пристроїв**	Провайдери інтернет	**Інформування щодо скомпрометованих пристроїв**
Виявлено понад 5 тис. IP адрес, з яких здійснюється підбір паролів до інформаційних систем державного та приватного сектору	**понад 5 тис. IP адрес**	Учасники платформи обміну індикаторами кіберзагроз НКЦК	**Інформування**
Виявлено вразливий маршрутизатор на об'єкті критичної інфраструктури сектору оборони. При експлуатації вразливості наявний доступ до внутрішньої мережі об'єкту.	**1**	Держспецзв'язку	**Вразливість усунено**
У відкритому доступі виявлено облікові дані та сертифікати доступу до внутрішньої мережі регіонального органу	**3**	Міністерство юстиції	**Вразливість усунено**
Виявлено базу даних скомпрометованих облікових записів, що використовують електронну пошту в зоні GOV.UA (понад 1000 записів)	**понад 1000 записів**	Держспецзв'язку, органи влади	**Дані про скомпрометовані облікові записи надано CERT-UA. Здійснюється реагування.**
Виявлено близько 100 вразливих (CVE-2018-13379) пристроїв Fortinet в українському сегменті інтернет	**близько 100 пристроїв**	Держспецзв'язку, Нацбанк	**Дані про скомпрометовані пристрої надано CERT-UA. Здійснюється реагування.**

Всього: **>18604**