# 2022(Q1)

**ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ
ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ**


# ЗВІТ РОБОТИ
# СИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

TLP:WHITE

# СТАТИСТИКА

**ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

## ПІДСИСТЕМА ОПЕРАТИВНОГО ЦЕНТРУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

є складовою системи виявлення вразливостей і реагування на кіберінциденти та кібератаки і забезпечує:

- централізований збір та накопичення інформації про мережеві події інформаційної безпеки
- централізоване управління усіма підсистемами системи виявлення вразливостей і реагування на кіберінциденти та кібератаки
- проведення моніторингу та обробки в режимі реального часу кіберзагроз та кіберінцидентів

Підсистема оперативного центру реагування на кіберінциденти виявляє шкідливу активність, а також системні і мережеві аномалії на об'єктах кіберзахисту шляхом аналізу даних, отриманих з мережевих пристроїв (активні сенсори, міжмережеві екрани, сканери вразливостей), робочих та серверних станцій, систем авторизації, внутрішніх і зовнішніх джерел даних про кіберзагрози.

## КІЛЬКІСТЬ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

хостів **≈ 15.3 k**

FPS **≈ 20 k**

трафіку **≈ 50 Gbit/s**

об'єм вхідного трафіку SIEM

**≈ 70 Gb/d**

отримано вхідних даних (flow)

**≈ 13 млрд**

детектовано підозрілих подій ІБ

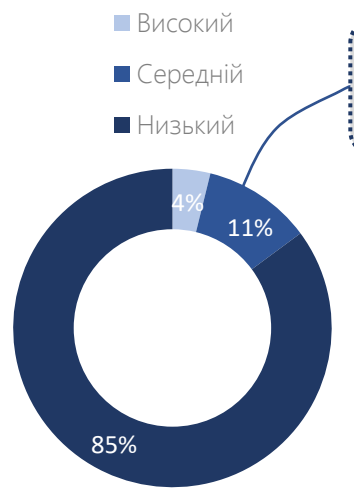
**≈ 14 млн**

опрацьовано критичних подій ІБ

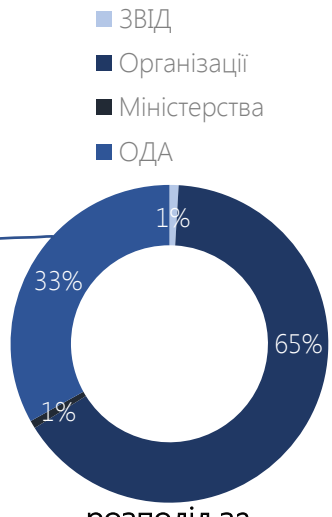
**≈ 78 000**

зареєстровано кіберінцидентів

**40**




розподіл за пріоритетом




розподіл за об'єктами моніторингу

# DATA SOURCES

ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ
ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ

## ОСНОВНІ ДЖЕРЕЛА ЗБОРУ ТА ЗБАГАЧЕННЯ КОНТЕКСТОМ ДАНИХ

- ВНУТРІШНІ ДЖЕРЕЛА ДАНИХ ПРО КІБЕРЗАГРОЗИ — 9%
- 15% — ЗОВНІШНІ ДЖЕРЕЛА ДАНИХ ПРО КІБЕРЗАГРОЗИ
- ДАНІ З РОБОЧИХ СТАНЦІЙ КОРИСТУВАЧІВ — 4%
- 6% — ДАНІ З СЕРВЕРНИХ СТАНЦІЙ
- СКАНЕРИ ВРАЗЛИВОСТЕЙ — 17%
- 5% — WEB & EMAIL ТРАФІК
- ДАНІ ПОВЕДІНКОВОГО МЕРЕЖЕВОГО АНАЛІЗУ — 6%
- 11% — ДАНІ АНАЛІЗУ МЕРЕЖЕВИХ ЗАГРОЗ
- ДАНІ СИСТЕМ ВИЯВЛЕННЯ ПРОНИКНЕНЬ — 18%
- 9% — ДАНІ СИСТЕМ ЗАПОБІГАННЯ ПРОНИКНЕННЮ

2022(Q1)

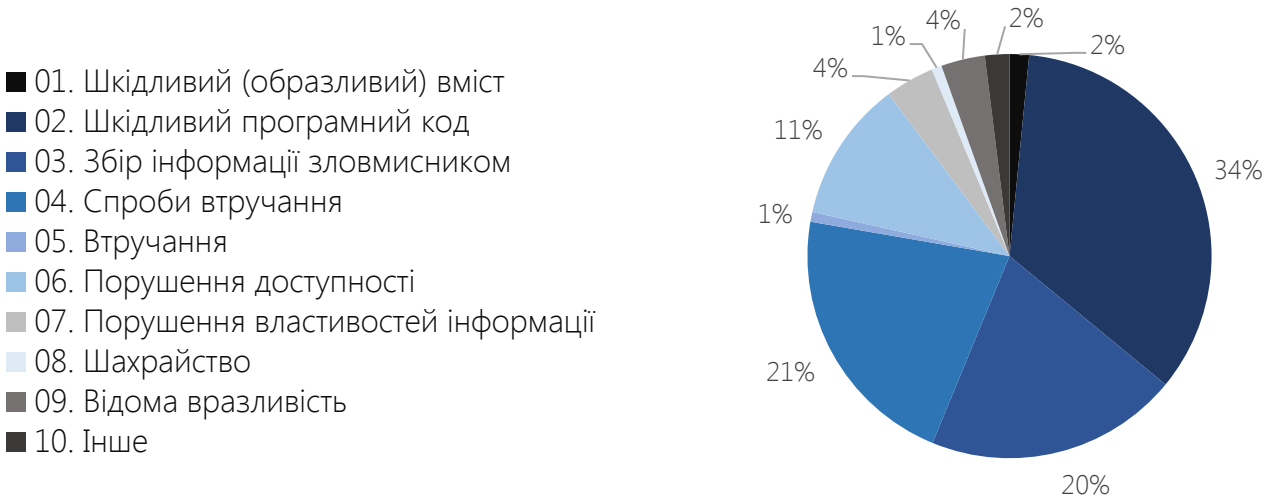
# СТАТИСТИКА

**ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

## СТАТИСТИКА ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

Представлена згідно Переліку категорій кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України (Протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021 (від 28.10.2021 № 16/320/21дск))

## КАТЕГОРІЇ ПОДІЙ ІБ




## ТИПИ ПОДІЙ ІБ

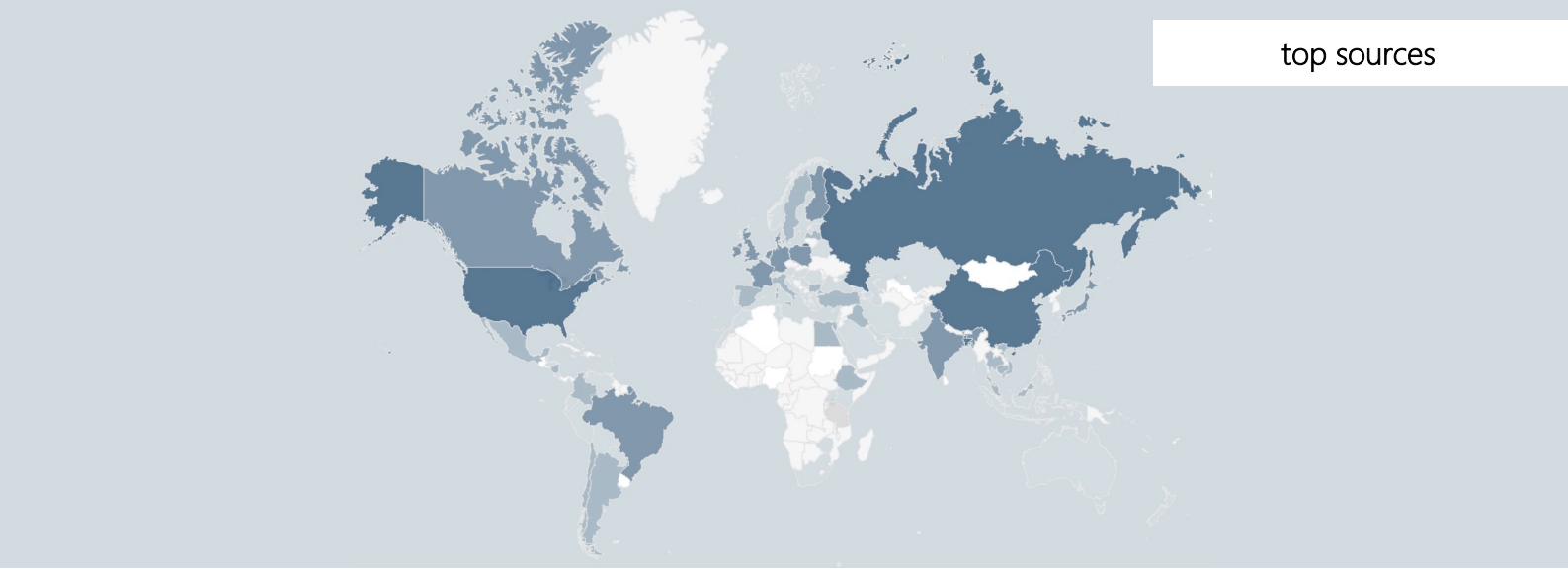
# СТАТИСТИКА

ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ
ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ

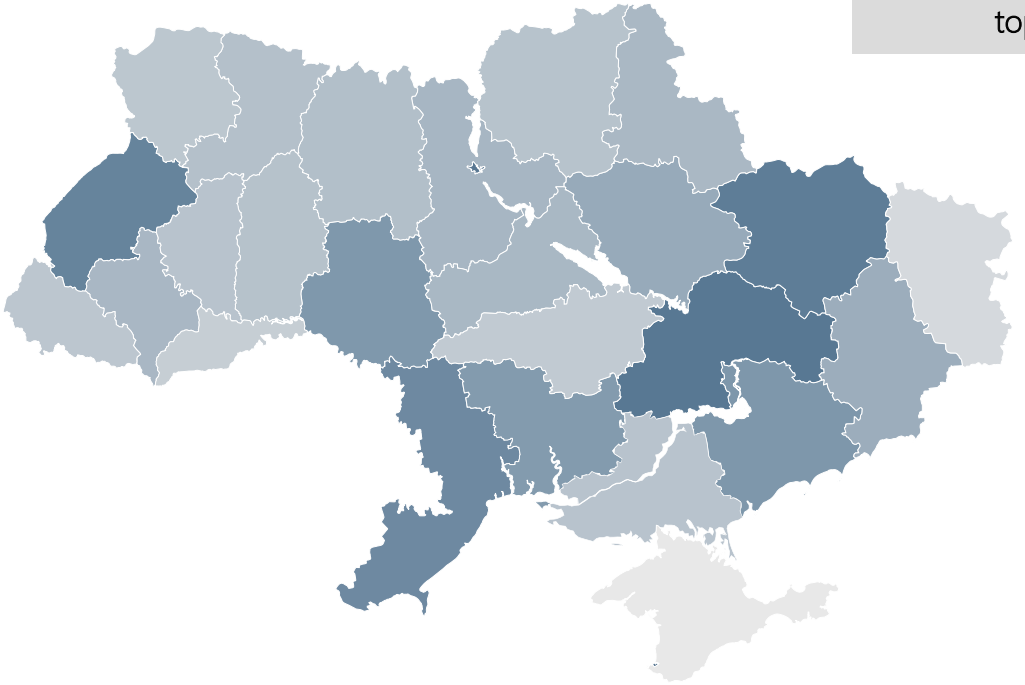
## ГЕОГРАФІЯ ДЕТЕКТУВАНЬ КРИТИЧНИХ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

на основі кількості спрацювань, таргетованих на регіони України, джерелом яких є IP адреси інших країн світу
(розташування IP у діапазоні делегування країни не завжди означає атрибуцію кібератаки до цієї країни)

top sources




top targets

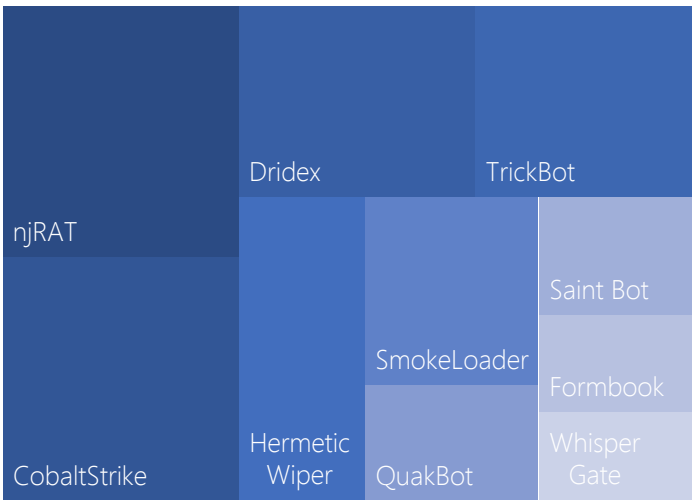


# TI

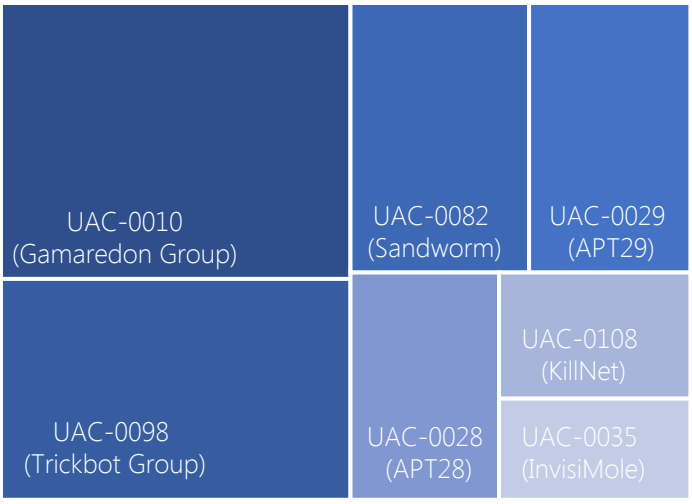
**ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ**
**ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ**
**ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ**



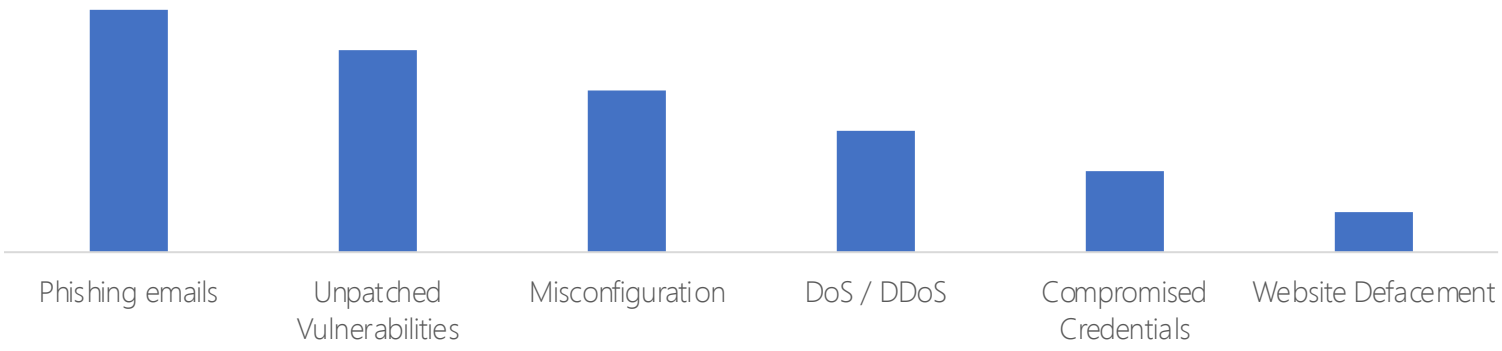
## Актуальне ШПЗ




## Актуальні хакерські угрупування




## Популярні вектори атак



# РЕКОМЕНДАЦІЇ

**ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

З метою попередження та зменшення наслідків впливу від реалізації популярних векторів кібератак, беручи до уваги найбільш таргетовані галузі кібербезпеки, рекомендуємо вживати наступних заходів для підвищення рівня захищеності:

## БЕЗПЕКА КІНЦЕВИХ ТОЧОК

- ✓ використовувати сучасне ліцензійне антивірусне програмне забезпечення, налаштовувати регулярну антивірусну перевірку;
- ✓ забезпечувати своєчасне встановлення оновлень безпеки (patching) операційної системи, браузерів та програмного забезпечення;
- ✓ здійснювати регулярно резервне копіювання та зберігати резервні копії на окремих сховищах даних, час від часу перевіряючи можливість відновлення даних із резервних копій;
- ✓ застосовувати принцип найменших привілеїв (Principle of Least Privilege), що передбачає надання найменших необхідних прав доступу.

## МЕРЕЖЕВА БЕЗПЕКА

- ✓ сегментувати мережу;
- ✓ забезпечувати захищений доступ до ресурсів, виключно для авторизованих користувачів і пристроїв через реалізацію принципів NAC (Network Access Control);
- ✓ використовувати сучасні технології та засоби для моніторингу та захисту від кібератак;
- ✓ керувати правами доступу користувачів через реалізацію принципів IAM (Identity and Access Management);
- ✓ попереджувати, виявляти і усувати вразливості, що уможливлюють доступ до мережевої інфраструктури.

## БЕЗПЕКА ОБЛІКОВИХ ЗАПИСІВ

- ✓ користуватися послугами довіреного third-party identity provider для автентифікації;
- ✓ налаштовувати багатофакторну автентифікацію (MFA);
- ✓ обмежувати кількість невдалих спроб автентифікації;
- ✓ використовувати паролі достатньої довжини і складності, періодично змінювати їх і не використовувати ідентичні паролі для декількох сайтів/сервісів;
- ✓ забезпечувати надійне збереження автентифікаційних даних.

# НОРМАТИВНО-ПРАВОВА БАЗА

- Закон України «Про основні засади забезпечення кібербезпеки України» , що визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

- Постанова Кабінету Міністрів України від 23.12.2020 №1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки», що визначає засади функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, які здійснюються щодо об'єктів кіберзахисту, визначених частиною другою статті 4 Закону України «Про основні засади забезпечення кібербезпеки України».

# КОНТАКТИ

Оперативний центр реагування на кіберінциденти
Державний центр кіберзахисту
Державна служба спеціального зв'язку
та захисту інформації України

04119, Україна, м. Київ, вул. Ю. Іллєнка, 83б
e-mail: soc@scpc.gov.ua
тел.: +38 (044) 281 87 37