2021

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

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 центральною 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 **≈ 3.5 k**

FPS **≈ 20 k**

трафіку **≈ 50 Gbit/s**

об'єм вхідного трафіку SIEM

≈ 70 Gb/d

отримано вхідних даних (flow)

≈ 650 млрд

детектовано підозрілих подій ІБ

≈ 41 млн

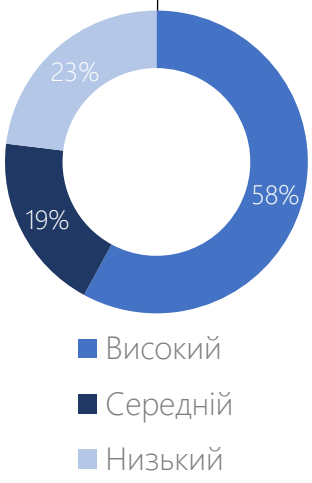
опрацьовано критичних подій ІБ

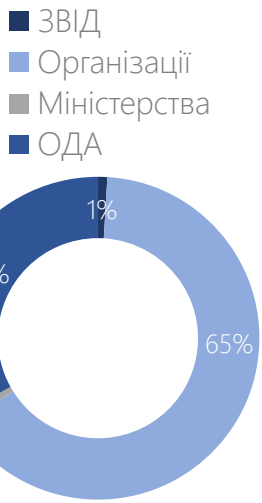
≈ 160 000

зареєстровано кіберінцидентів

147

розподіл за пріоритетом



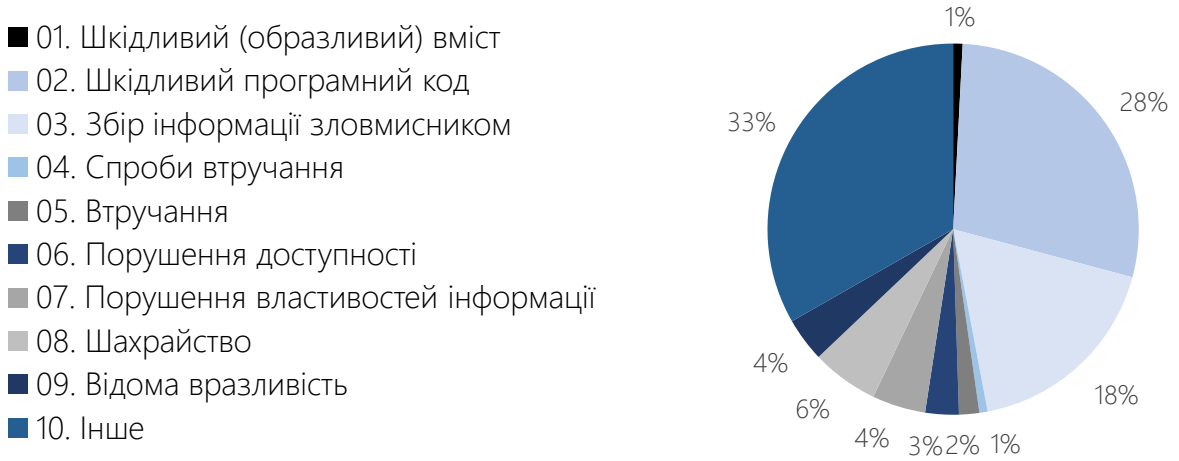


розподіл за об'єктами моніторингу

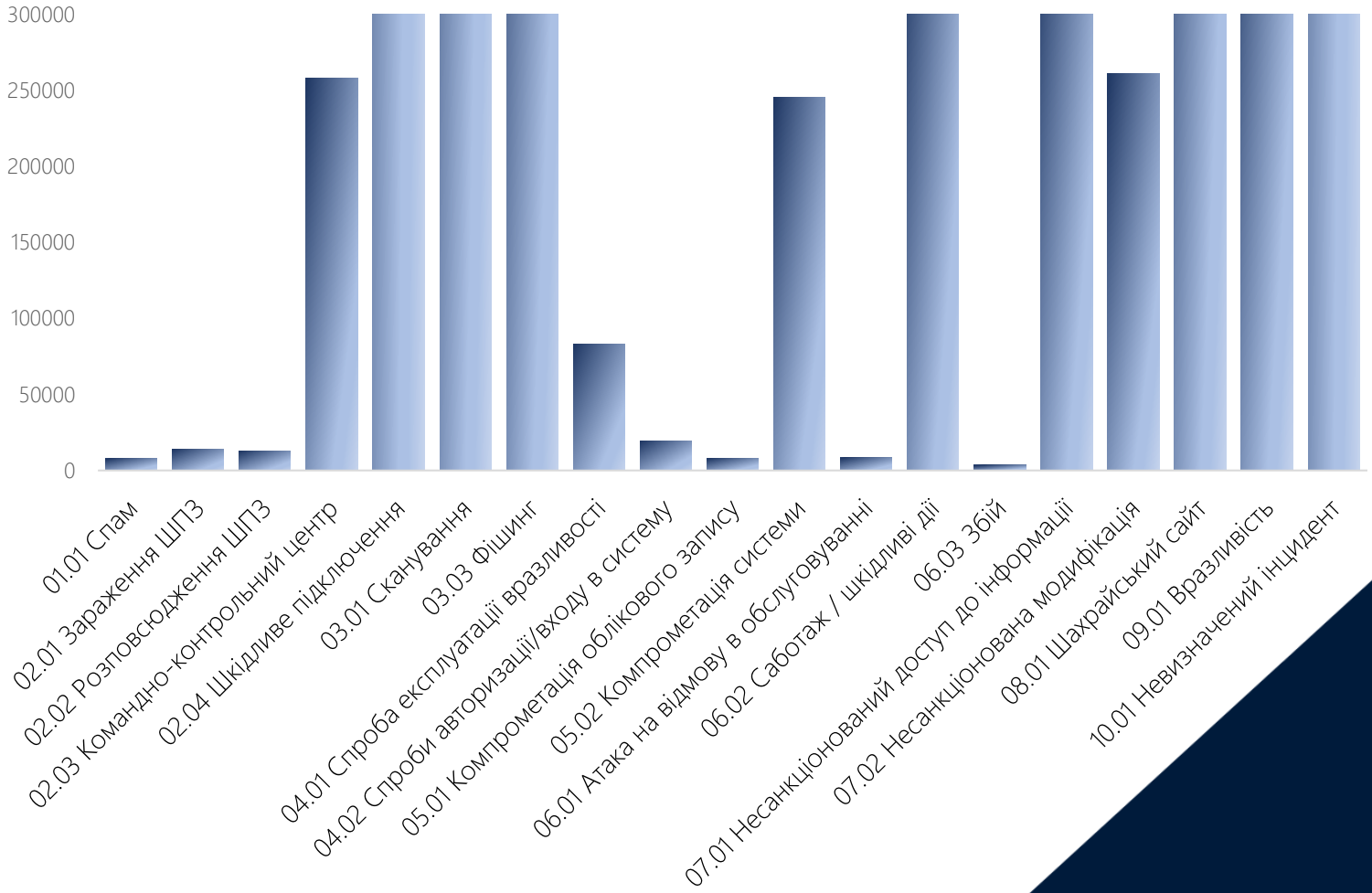
СТАТИСТИКА ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

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

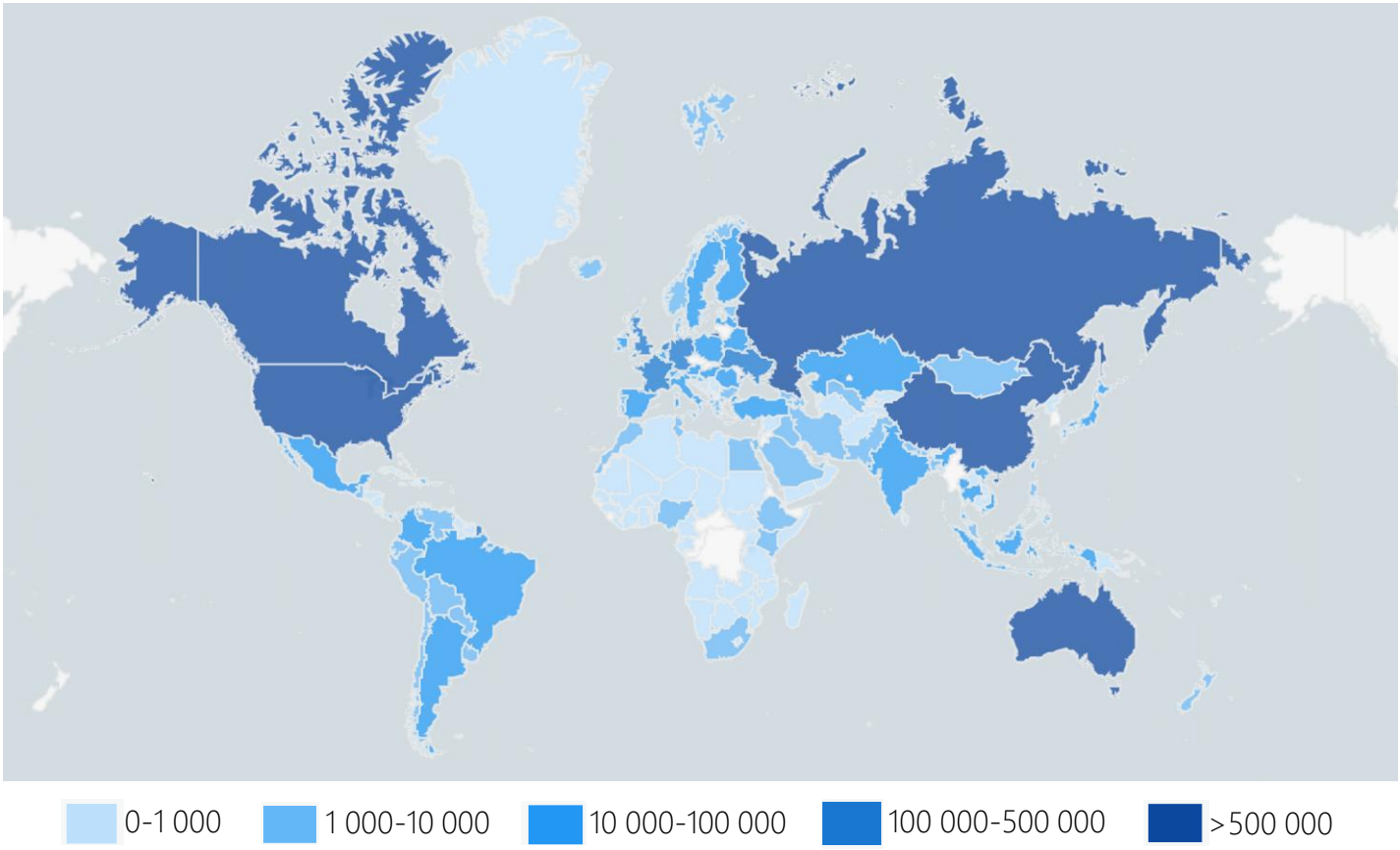


ТИПИ ПОДІЙ ІБ

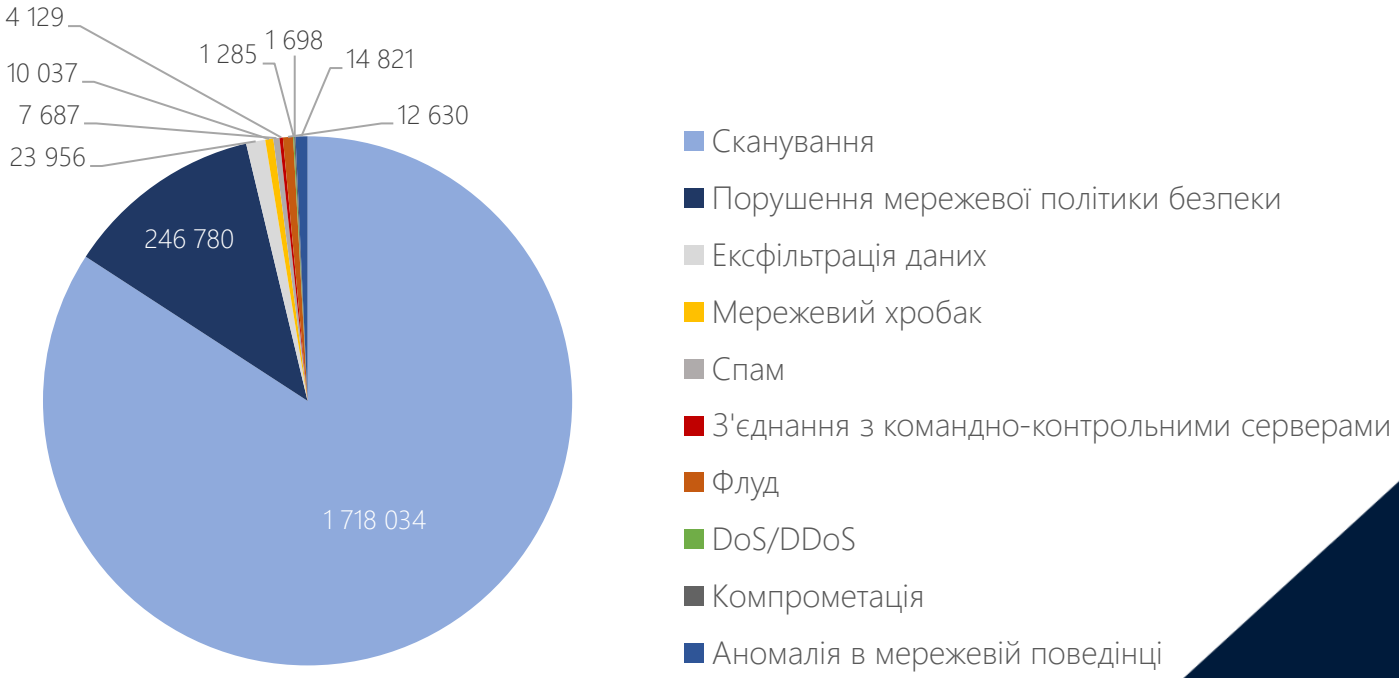


СТАТИСТИКА

ГЕОГРАФІЯ ДЕТЕКТУВАНЬ КРИТИЧНИХ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

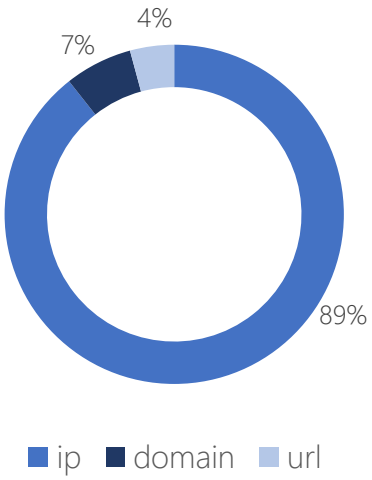


КАТЕГОРІЇ ДЕТЕКТУВАНЬ НА ОСНОВІ ПОВЕДІНКОВОГО АНАЛІЗУ

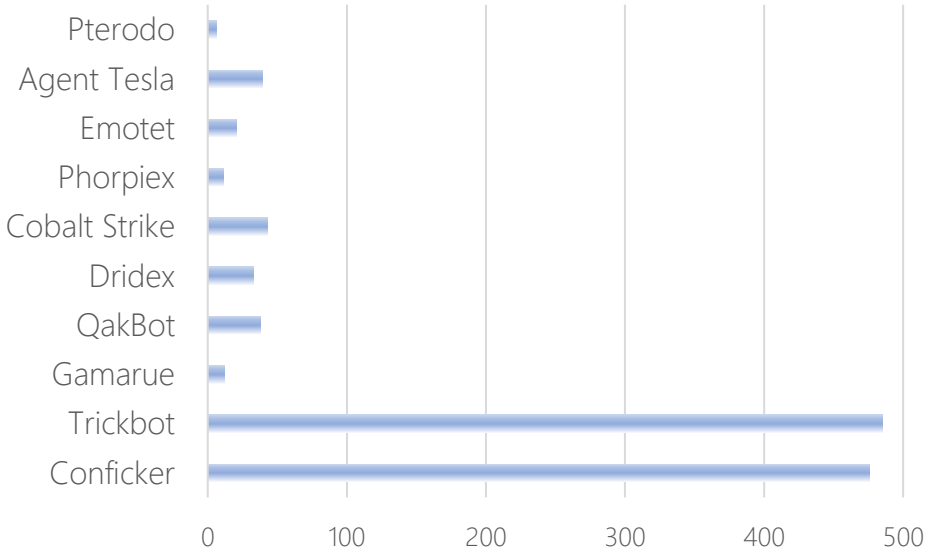


ВИЯВЛЕНО ТА ОБРОБЛЕНО 1 164 СПРАЦЮВАННЯ ЗА ІНДИКАТОРАМИ

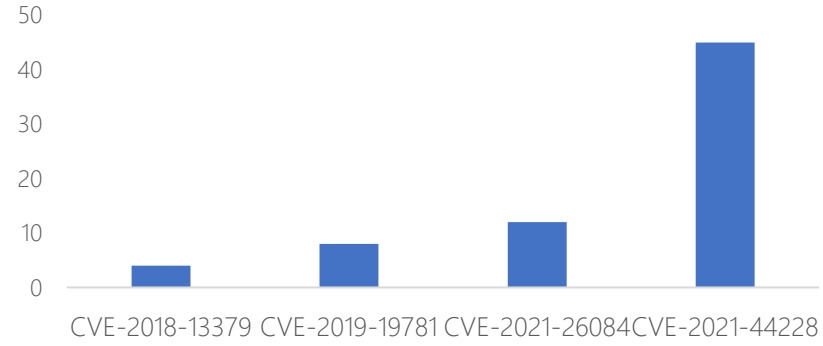
за типом індикаторів:

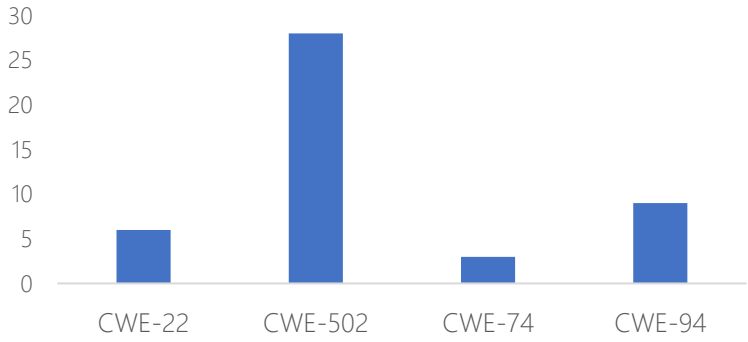


за типом сімейства ШПЗ:



СТАТИСТИКА ДЕТЕКТУВАНЬ ІНДИКАТОРІВ, ПОВ'ЯЗАНИХ ЗІ СПРОБАМИ ЕКСПЛУАТАЦІЇ CVE/CWE

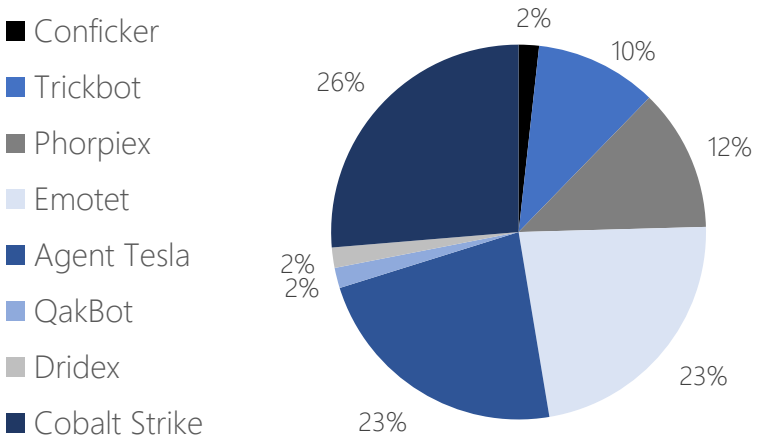




на основі виявлених та оброблених спрацювань за індикаторами

ЗАРЕЄСТРОВАНО 56 КІБЕРІНЦИДЕНТІВ

з яких за типом сімейства ШПЗ:



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 можливих спроб несанкціонованого втручання у роботу інформаційних систем РЕКОМЕНДУЄМО вживати наступних заходів:

- забезпечувати моніторинг подій інформаційної безпеки системними адміністраторами (адміністраторами безпеки);
- організувати всі можливі варіанти логування подій та забезпечити їх збереження на окремому дисковому сховищі;
- сформувати з фахівців IT (інформаційної безпеки) команду реагування на комп'ютерні надзвичайні події та визначити відповідальних осіб за виконання процесу та процедур реагування на кіберінциденти;
- проводити з усіма співробітниками, що мають доступ до інформаційних систем, інструктаж щодо дотримання політик інформаційної безпеки (правил кібергігієни) та приділяти увагу питанням використання Інтернет-ресурсів та електронної пошти, реагування на фішингові повідомлення;
- здійснювати регулярно резервне копіювання критичних (важливих) інформаційних ресурсів та зберігати їх резервні копії на окремих сховищах даних, час від часу перевіряючи можливість відновлення даних із резервних копій;
- використовувати ліцензійні/легалізовані операційні системи, інші програмні продукти, здійснювати ручне чи автоматизоване оновлення операційних систем, програм та мікропрограмного забезпечення, використовувати найновіші версії операційних систем та додатків;
- перевіряти та увімкнути антивірусний захист, здійснювати оновлення бази сигнатур антивірусного програмного забезпечення;
- проводити власними силами сканування на предмет вразливості інформаційних ресурсів, розміщених в Інтернеті або звернутися до Державного центру кіберзахисту;
- усувати вразливості в інформаційних системах;
- відключити віддалений доступ до інформаційних систем або переглянути коло співробітників, яким надано право віддаленого доступу до інформаційних систем, впроваджувати максимальні обмеження (фільтрація за IP, протоколами, часом доступу, користувачами тощо);
- застосовувати тільки надійно захищені методи віддаленого доступу та протоколи для адміністрування інформаційних систем та ресурсів, що мають належний рівень шифрування;
- використовувати стійкі паролі, налаштувати багатофакторну автентифікацію та забезпечити надійне збереження автентифікаційних даних.

Інші рекомендації:

- Основні правила кібергігієни
- Рекомендації щодо організації віддаленої роботи
- Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення
- Рекомендації CERT-UA з налаштувань програм MS Office
- Рекомендації CERT-UA з безпеки вебресурсів

Дивіться також:

- ПЕРЕЛІК категорій кіберінцидентів
- ПРАВИЛА обміну інформацією про кіберінциденти

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