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

2022 Q3

ЗВІТ ПРО РОБОТУ

СИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

TLP:WHITE

СИСТЕМА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

це сукупність програмних та програмно-апаратних засобів, які забезпечують проведення цілодобового моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об'єктах кіберзахисту і можуть мати негативний вплив на їх стале функціонування.

ПІДСИСТЕМА ОПЕРАТИВНОГО ЦЕНТРУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

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

- централізоване управління усіма підсистемами системи виявлення вразливостей і реагування на кіберінциденти та кібератаки;
- централізований збір та накопичення інформації про мережеві події інформаційної безпеки;
- проведення моніторингу та оброблення 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.

EXECUTIVE SUMMARY

Держспецзв'язку постійно фіксує зростання кількості кіберінцидентів та кібератак на державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури. Від початку війни тренд на зростання кількості кібератак зберігається.

Так, у ІІІ кварталі 2022 за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 24 млрд подій. Кількість зареєстрованих та опрацьованих кіберінцидентів зросла – від 64 до 115.

Основною метою хакерів є кібершпіонаж, порушення доступності державних інформаційних сервісів та навіть знищення інформаційних систем за допомогою програм-вайперів. У ІІІ кварталі 2022 року ми зафіксували істотне зростання активності хакерських груп щодо розповсюдження шкідливого програмного забезпечення, серед якого є як програми, що викрадають дані, так і ті, які спрямовані на знищення даних. Порівняно зі статистичними даними за ІІ квартал 2022 року, кількість подій ІБ з високим рівнем критичності зросла у 3,8 разів. Відповідно, кількість зареєстрованих кіберінцидентів з високим рівнем критичності зросла на 128%.

Порівняно з І та ІІ кварталами, у ІІІ кварталі 2022 року кількість критичних подій ІБ, джерелом яких є IP-адреси росії, зросла у 35 разів. Також, порівняно з ІІ кварталом 2022 року, майже вдвічі зросла кількість детектованих подій ІБ, пов'язаних із активним скануванням, джерелом яких є IP-адреси росії.
Саме з цих IP здійснювали кібератаки на українські інформаційні ресурси, розповсюджували фейкову інформацію, що стосується дискредитації державних органів під час російсько-української війни.

Наразі найбільша кількість критичних подій ІБ пов'язана з IP-адресами зі США. Проте автоматично визначена геолокація IP-адрес джерел необов'язково означає атрибуцію кібератак до ідентифікованого місцерозташування.

Втім, за атрибуцією абсолютна більшість кіберінцидентів пов'язана з хакерськими угрупуваннями, що фінансуються урядом рф. Зокрема, це UAC-0010 (Gamaredon) та інші.

У ІІІ кварталі 2022 року основною мішенню хакерів із російської федерації були фінансовий та комерційний сектори, а також українські державні та місцеві органи влади. Найбільшу частку подій інформаційної безпеки можна пов'язати з APT-угрупуваннями та хактивістами.

СТАТИСТИКА МОНІТОРИНГУ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

9 к
FPS

22.1 к
хостів

7 Tb
отримано вхідних даних

6 Gbit/s
швидкість вхідного трафіку сенсорної мережі

опрацьовано подій
отриманих за допомогою засобів моніторингу, аналізу та передання телеметричної інформації про кіберінциденти та кібератаки

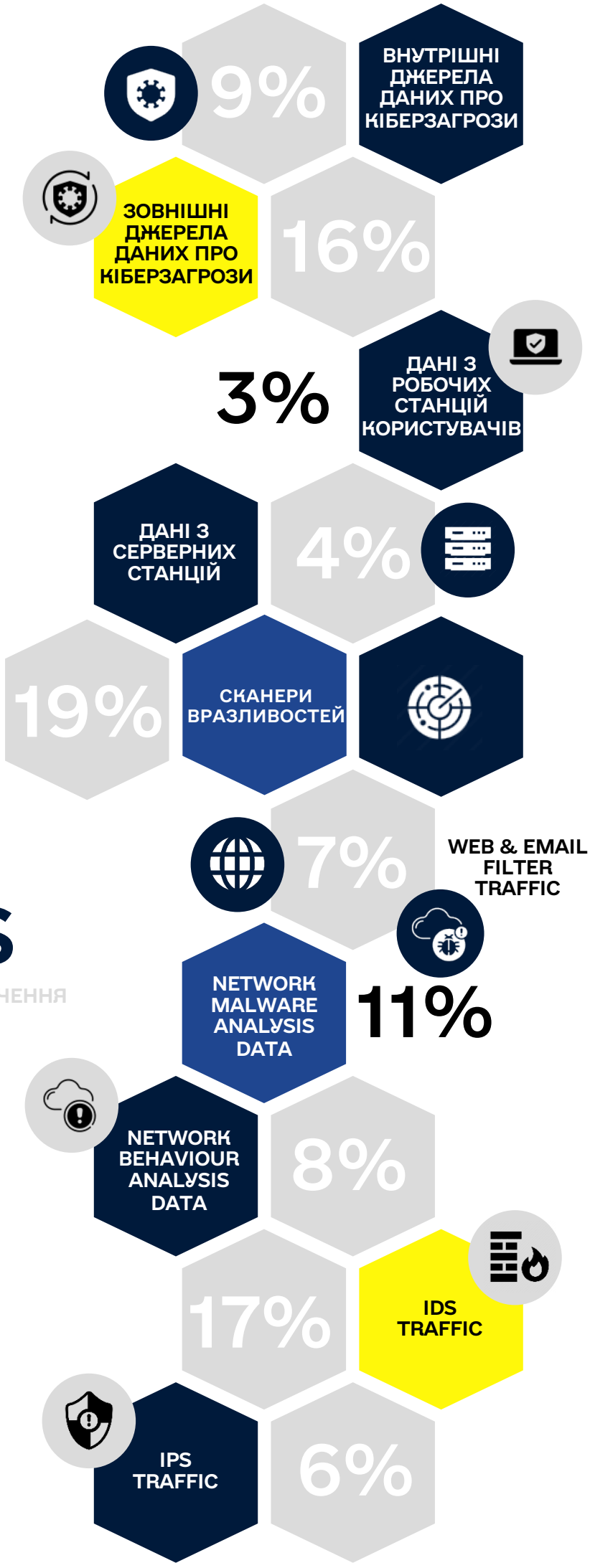
детектовано підозрілих подій ІБ
при первинному аналізі

опрацьовано критичних подій ІБ
потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу

зареєстровано кіберінцидентів
критичних подій ІБ, зафіксованих та оброблених безпосередньо аналітиками безпеки

DATA SOURCES

ОСНОВНІ ДЖЕРЕЛА ЗБОРУ ТА ЗБАГАЧЕННЯ КОНТЕКСТОМ ДАНИХ



2022(Q3)

СТАТИСТИКА ПОДІЙ ІБ

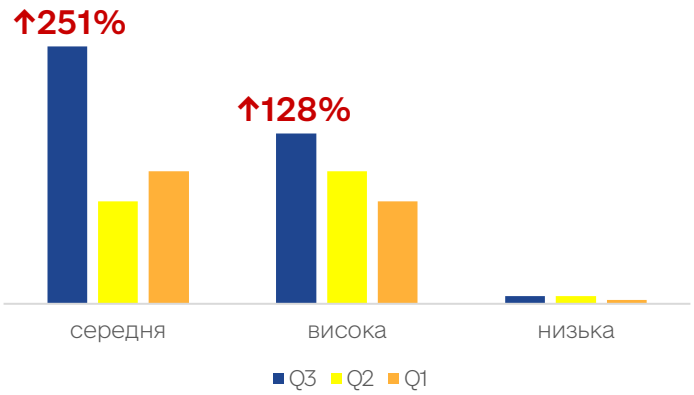
КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

представлена згідно **Переліку категорій кіберінцидентів** схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України

- 02 Шкідливий програмний код
- 01 Шкідливий (образливий) вміст
- 03 Збір інформації зловмисником
- 04 Спроби втручання
- 05 Втручання
- 06 Порушення доступності
- 07 Порушення властивостей інформації
- 08 Шахрайство
- 09 Відома вразливість
- 10 Інше

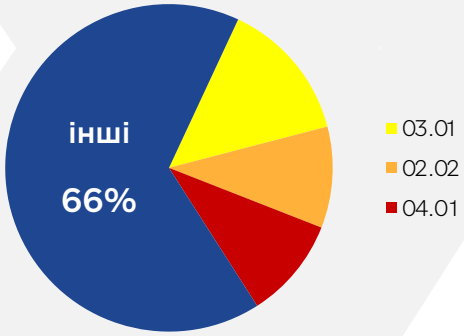
критичність кіберінцидентів

графік відображає статистичну інформацію за звітний період, отриману шляхом аналізу зареєстрованих інцидентів кібербезпеки згідно внутрішньої системи оцінювання рівня критичності, відповідно до якої інциденти можна класифікувати за цим параметром



статистика типів подій ІБ

які протягом III кварталу 2022 року домінують у відсотковому відношенні над іншими типами подій ІБ



14%

стільки у % відношенні становлять події ІБ цього типу порівняно із загальною кількістю детектувань активності, пов'язаної з типами інцидентів, описаних в Переліку категорій кіберінцидентів, за звітний період.

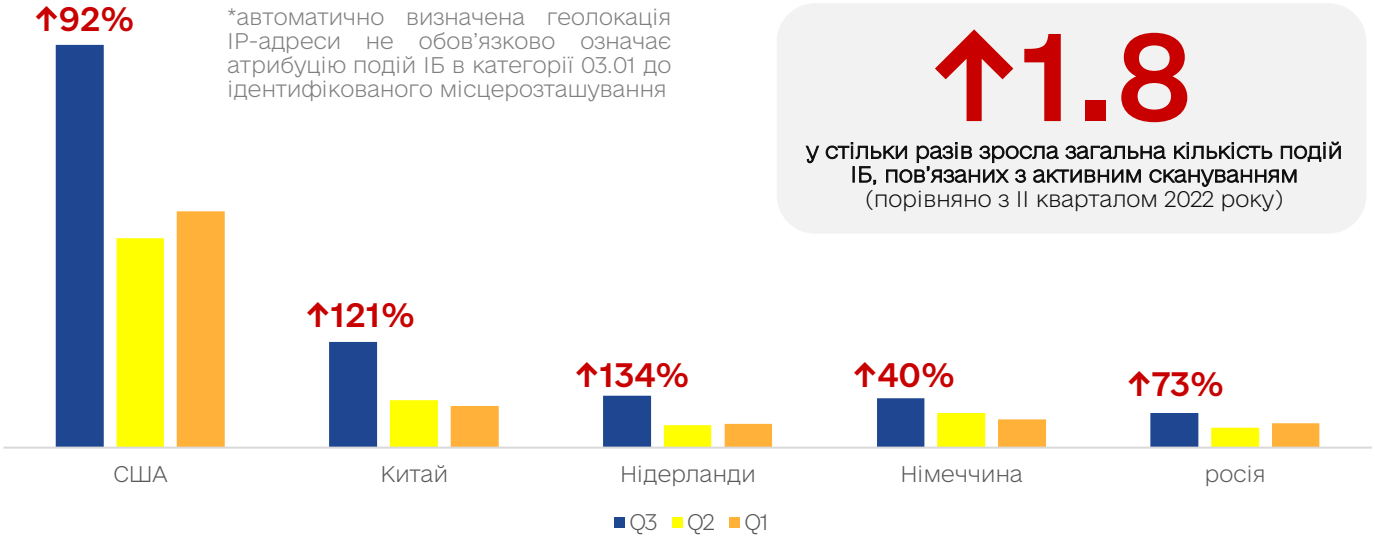
збір інформації про системи або мережі

за геолокацією* IP-адрес джерел

*автоматично визначена геолокація IP-адреси не обов'язково означає атрибуцію подій ІБ в категорії 03.01 до ідентифікованого місцерозташування

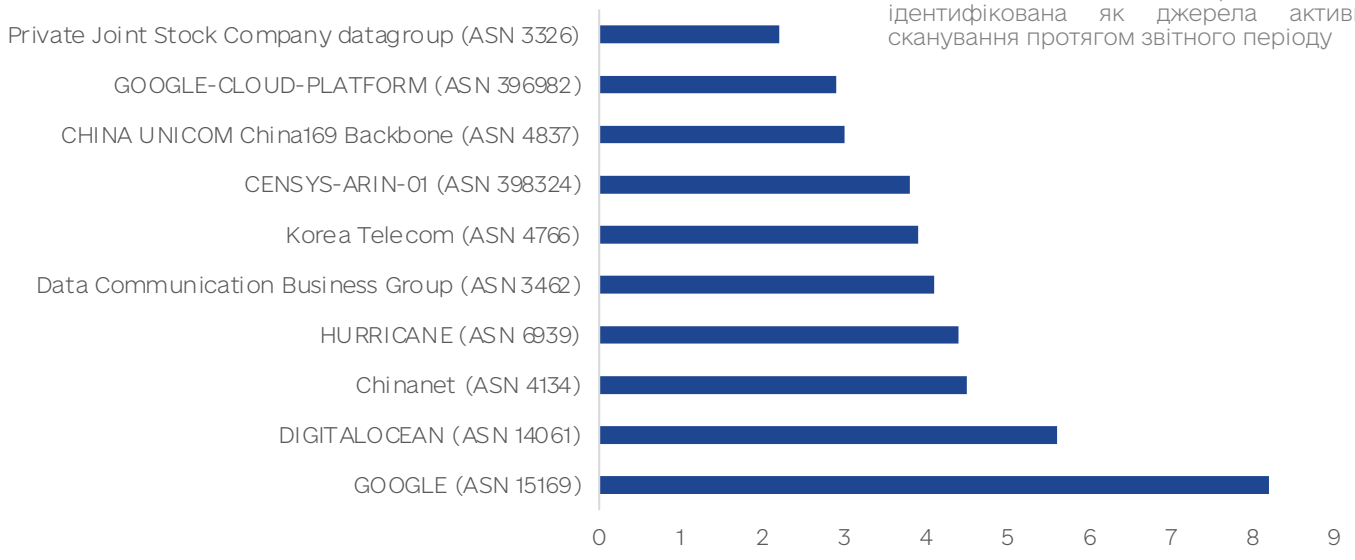
↑1.8

у стільки разів зросла загальна кількість подій ІБ, пов'язаних з активним скануванням (порівняно з II кварталом 2022 року)



за ASN IP-адрес джерел

графік відображає 10 ASN (у % відношенні), домінантна кількість IP-адрес яких була ідентифікована як джерела активного сканування протягом звітного періоду



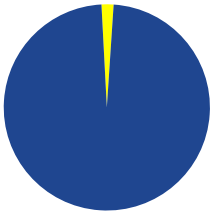
10%

стільки у % відношенні становлять події ІБ цього типу, порівняно із загальною кількістю детектувань активності, пов'язаної з типами інцидентів, описаних у Переліку категорій кіберінцидентів, за звітний період.

62 314

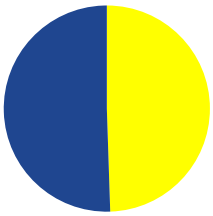
підозрілих унікальних файлів було детектовано в автоматичному режимі підсистемами, що належать до складу

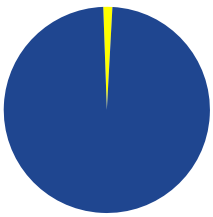
Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки



мережеві події з підсистеми збору телеметрії інформаційно-комунікаційних систем, що ідентифікують розповсюдження ШПЗ за протоколами HTTP, SMTP, POP3, IMAP

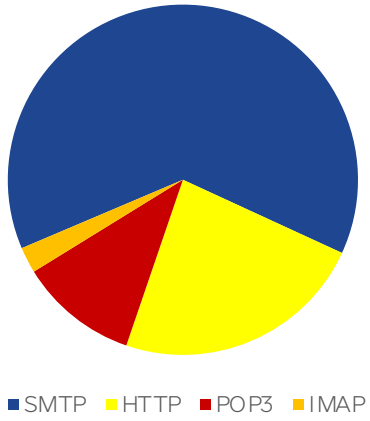
сповіщення з підсистеми виявлення та реагування на кібератаки на рівні робочих та серверних станцій (EDR) про виявлення шкідливої активності на них



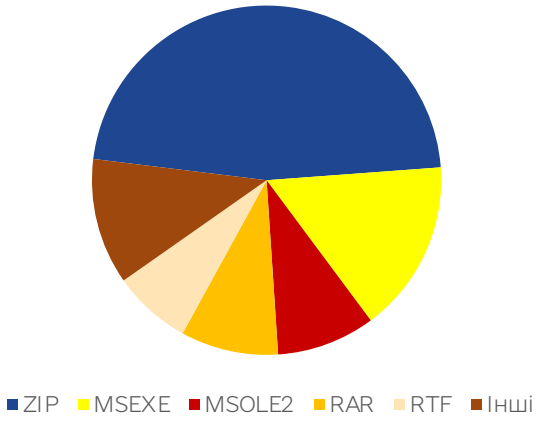


сповіщення з поштових шлюзів безпеки про пересилання шкідливого програмного забезпечення, ідентифікованого при фільтрації вхідного/вихідного трафіку

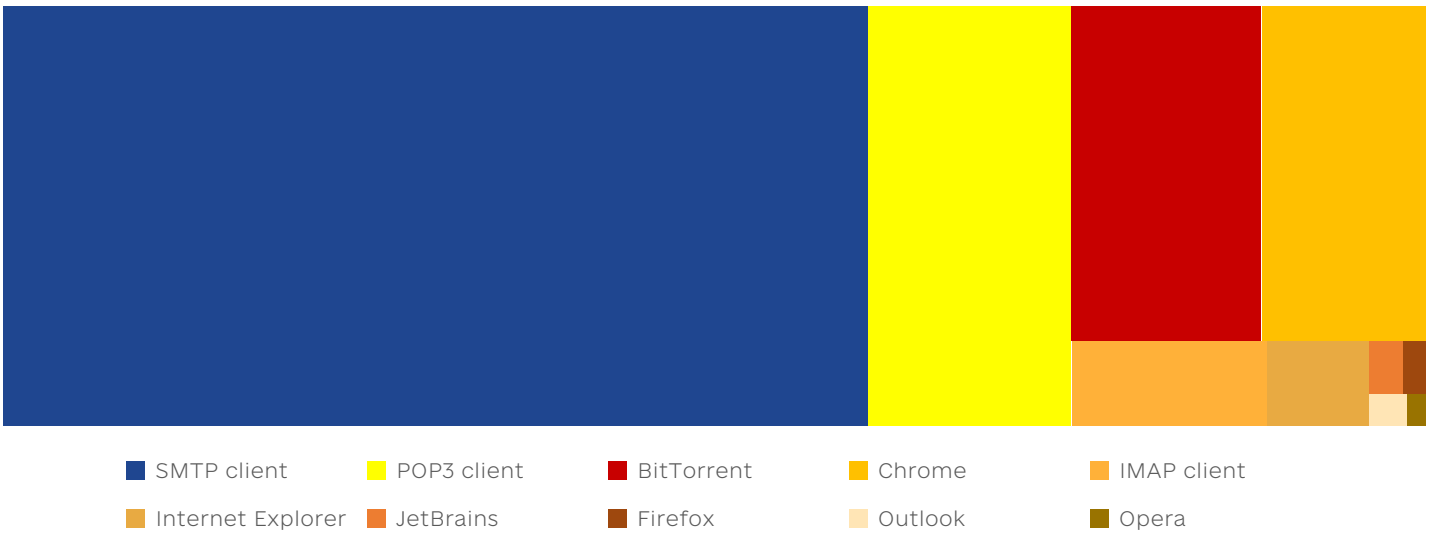
за протоколом розповсюдження ШПЗ



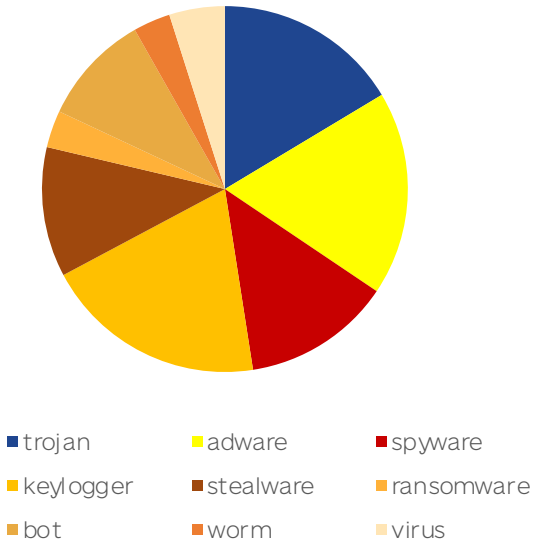
за форматом розповсюджуваного ШПЗ



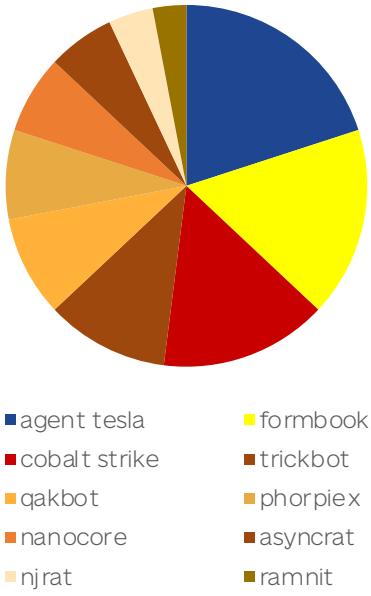
за асоційованим ПЗ клієнтів



за типом ШПЗ



за сімейством ШПЗ



10%

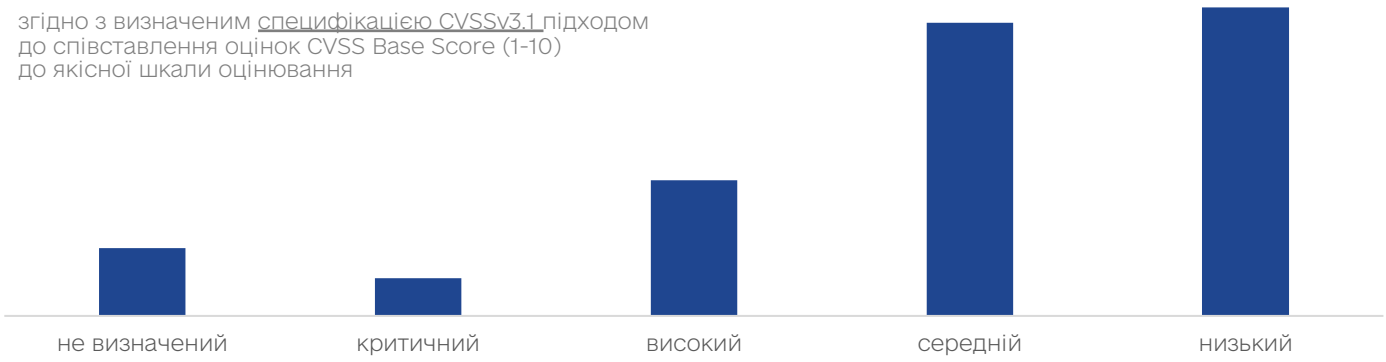
стільки у % відношенні становлять події ІБ цього типу порівняно із загальною кількістю детектувань активності, пов'язаної з типами інцидентів, описаних у Переліку категорій кіберінцидентів, за звітний період.

спроба вторгнення з використанням вразливості у системі, компоненті чи мережі

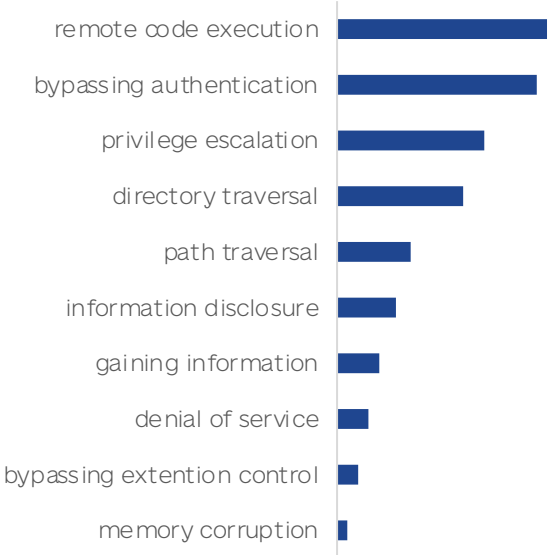
графіки відображають статистичну інформацію за звітний період, отриману шляхом аналізу подій ІБ, джерелом яких є спроби вторгнення до мереж об'єктів кіберзахисту і реалізація кіберзагроз із метою виявлення вразливостей у програмному забезпеченні, знаходження проблемних конфігурацій сервісів і активних мережевих пристроїв

якісна оцінка за CVSS Base Score

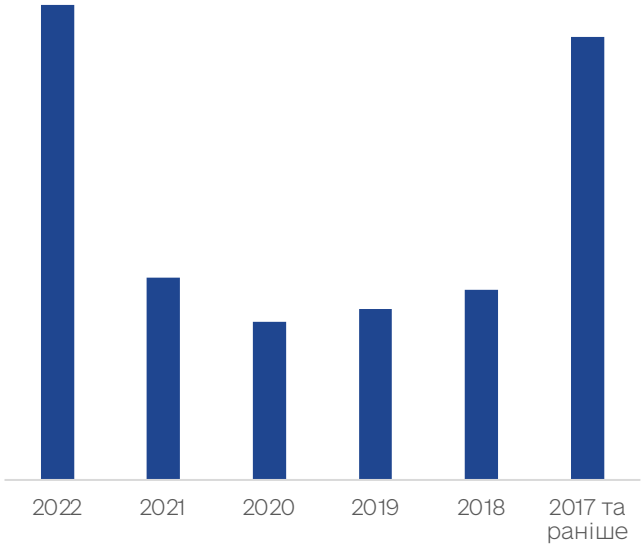
згідно з визначеним специфікацією CVSSv3.1 підходом до співставлення оцінок CVSS Base Score (1-10) до якісної шкали оцінювання



категорії експлуатованих CVE



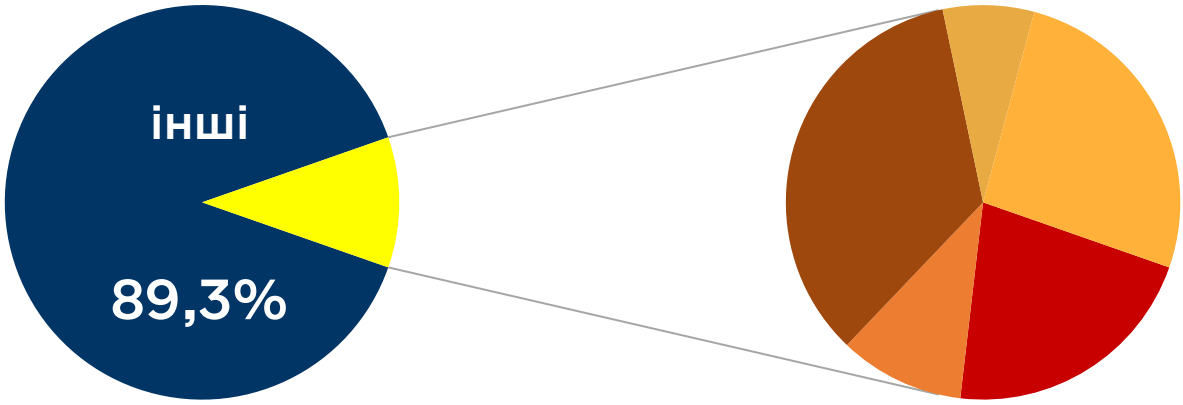
експлуатовані CVE за роком реєстрації



актуальні вразливості

Нижченаведений перелік актуальних вразливостей програмного забезпечення не є вичерпним та відображає CVE, що були задокументовані експертними групами кіберрозвідки і які продовжують активно експлуатуватись із метою отримання неавторизованого доступу або привілейованого контролю.

На графіку відображено % відношення виявленої активності в мережах клієнтів, потенційно пов'язаної з експлуатацією нижчеописаного переліку CVE, до загальної кількості детектувань активності, пов'язаної з усіма виявленими ідентифікаторами вразливостей за звітний період.



CVE-2022-33874

Вразливість компоненти *SSH Login Handler* у вразливих версіях продуктів Fortinet, може бути ініційована віддалено. Дозволяє реалізовувати **віддалене неавторизоване виконання довільного коду.**
CVSS: 9.8

CVE-2022-33872

Вразливість компоненти *Telnet Login Handler* у вразливих версіях продуктів Fortinet, може бути ініційована віддалено. Дозволяє реалізовувати **віддалене неавторизоване виконання довільного коду.**
CVSS: 9.8

CVE-2022-41352

Вразливість утиліти cpio у фільтрі контенту Amavis що належить до продукту Zimbra Collaboration, дозволяє реалізовувати **розміщення web-shell**.
CVSS: 9.8

CVE-2021-44228

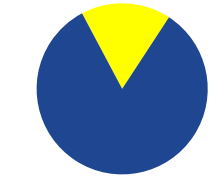
Вразливість має назву Log4Shell, пов'язана з бібліотекою Apache Log4j, яка дозволяє реалізовувати **віддалене неавторизоване виконання довільного коду.**
CVSS: 10

CVE-2022-30190

Вразливість у системі *Microsoft Support Diagnostic Tool (MSDT)* експлуатується за допомогою документів Microsoft Office. Дозволяє реалізовувати **віддалене неавторизоване виконання довільного коду.**
CVSS: 7.8

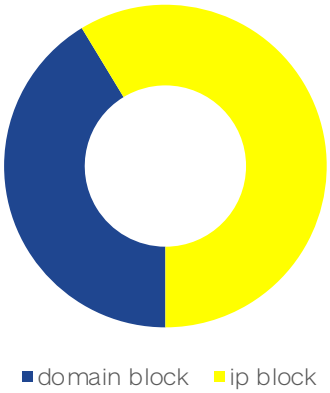
EMAIL SECURITY GATEWAY

з яких **83%**
заблокованих в автоматичному режимі



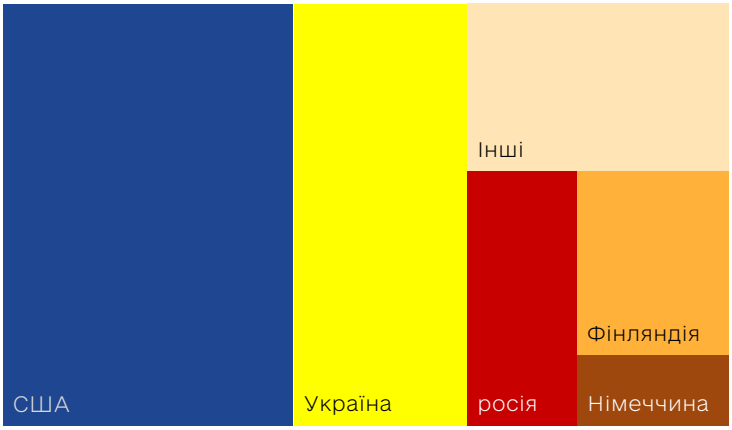
1.7mln
листів отримано та проаналізовано
за звітний період

Sender Validation failure reason

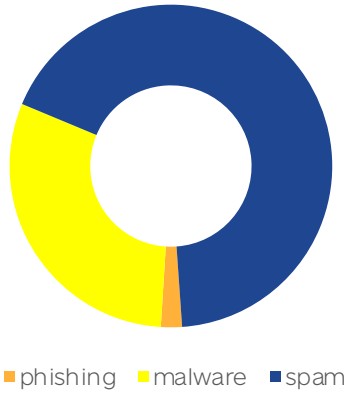


Sender Authentication failure reason

Sender Threat category (by country)



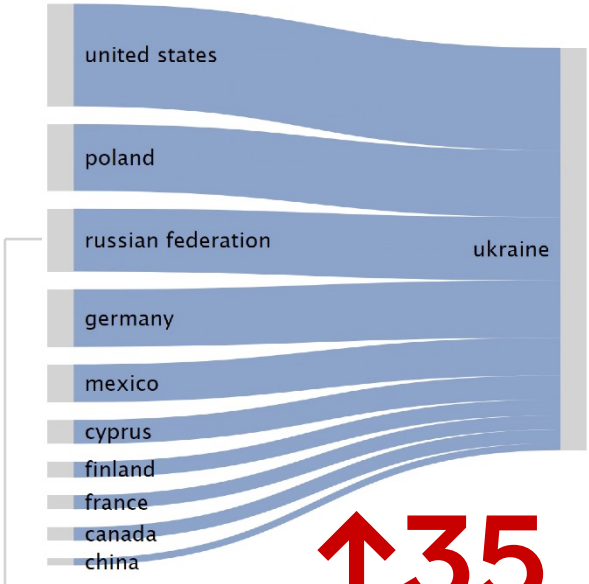
Sender Threat category

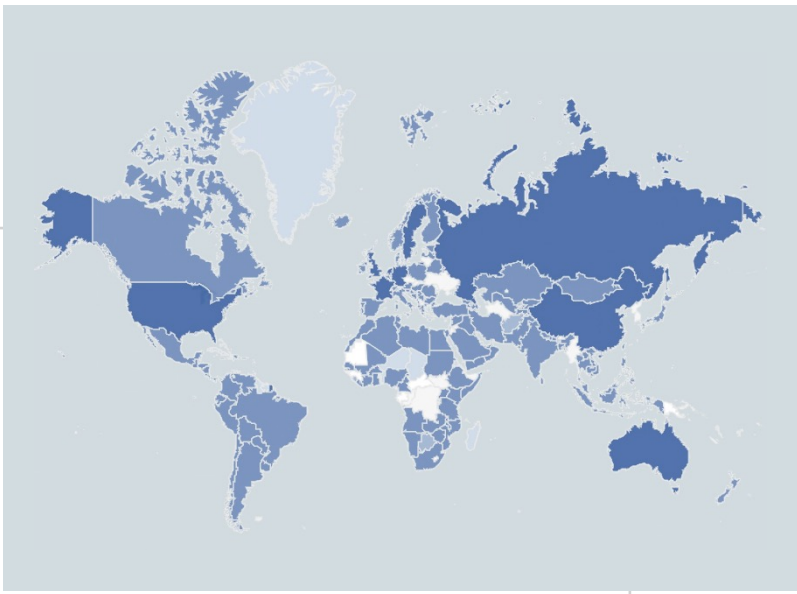


ГЕОГРАФІЯ ДЕТЕКТУВАНЬ

КРИТИЧНИХ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ*

*автоматично визначена геолокація IP-адрес джерел критичних подій ІБ не обов'язково означає їх атрибуцію до ідентифікованого місцерозташування





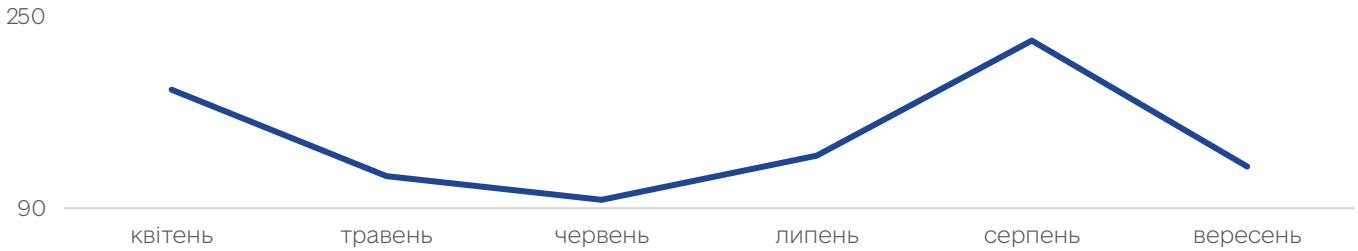
↑35

у стільки разів зросла кількість критичних подій ІБ, джерелом яких є IP-адреси росії (порівняно з двома попередніми кварталами 2022 року)

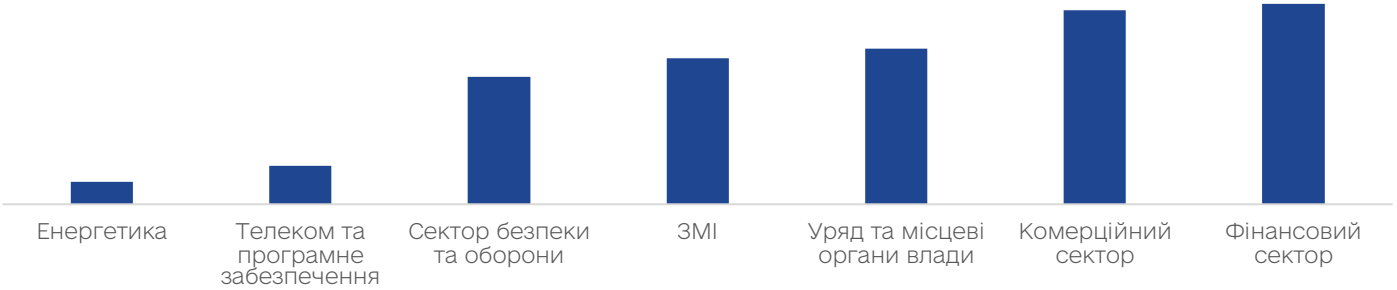
↑3,8

у стільки разів зросла загальна кількість критичних подій ІБ (порівняно з II кварталом 2022 року)

динаміка активності російських хакерських угрупувань протягом Q2, Q3



динаміка активності російських хакерських угрупувань за секторами



THREAT ACTORS ACTIVITY

нижченаведений перелік відображає актуальні хакерські угрупування, таргетовані на інформаційні ресурси України, ідентифікатори активності яких були детектовані в мережах об'єктів кіберзахисту за звітний період

UAC-0010

Related names: Gamaredon, Armageddon, PrimitiveBear
Category: Nation State Sponsored
Location: russia
First Reference: 2013-2014

Детальніше: Кібератаки групи UAC-0010 (CERT-UA#4634,4648)
Кібератака групи UAC-0010 (CERT-UA#4434)

UAC-0100

Related names: -
Potential Category: Financial Crime
Potential Location: -
First Reference: Apr, 2022

Детальніше: Кібератака групи UAC-0100 (CERT-UA#4964)

UAC-0056

Related names: Lorec53, SaintBear, GraphSteal, GrimPlant
Potential Category: Nation State Sponsored
Potential Location: russia
First Reference: Jul, 2021

Детальніше: Кібератака групи UAC-0056 (CERT-UA#4545)
Кібератака групи UAC-0056 (CERT-UA#4293)

UAC-0097

Related vulnerability: CVE-2018-6882
Threat Category: Cyber espionage
Potential Location: -
First Reference: Apr, 2022

Детальніше: Кібератака групи UAC-0097 (CERT-UA#4461)

UAC-0120

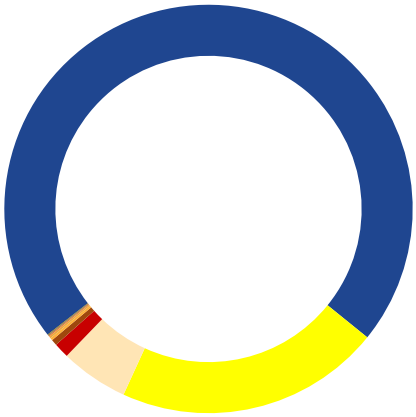
Related Malware: AgentTesla
Threat Category: Cyber espionage
Potential Location: -
First Reference: Aug, 2022

Детальніше: Атака з використанням AgentTesla (CERT-UA#5252)

MITRE ATT&CK MAPPING

attack surface

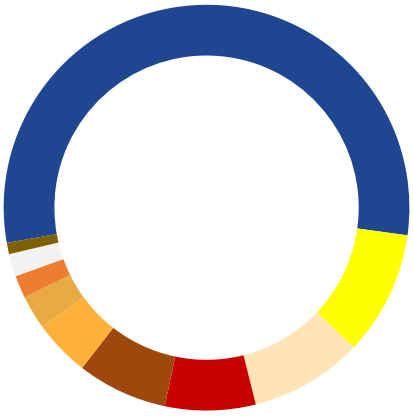
статистика детектованих тактик/технік (відповідно до бази знань MITRE ATT&CK), асоційованих із набором виявлених та оброблених індикаторів, що використовувались на різних етапах життєвого циклу атак, які відбувались протягом звітного періоду



- T1566 [Phishing]
- T1110 [Brute Force]
- T1090 [Proxy]
- T1498 [Network Denial of Service]
- T1568 [Dynamic Resolution]
- T1071 [Application Layer Protocol]
- T1584 [Compromise Infrastructure]
- T1583 [Acquire Infrastructure]
- T1190 [Exploit Public-Facing Application]
- T1210 [Exploitation of Remote Services]

detect surface

статистика детектованих тактик/технік (відповідно до бази знань MITRE ATT&CK), асоційованих із набором виявлених та оброблених індикаторів, що використовувались на різних етапах життєвого циклу атак, і за фактом яких були зареєстровані кіберінциденти протягом звітного періоду



- T1071 [Application Layer Protocol]
- T1204 [User Execution]
- E1133 [External Remote Services]
- T1566 [Phishing]
- T1598 [Phishing for information]
- T1498 [Network Denial of Service]
- T1190 [Exploit Public-Facing Application]
- T1078 [Valid Accounts]
- T1565 [Data Manipulation]
- T1110 [Brute Force]

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

ЩОДО ПІДВИЩЕННЯ РІВНЯ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури розроблені відповідно до підпункту 1 частини другої та пункту 3 частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України», абзацу другого частини першої статті 3, пунктів 85, 86 і 88 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», абзацу другого підпункту 1 пункту 3 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 3 вересня 2014 року № 411, та Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, з метою підвищення рівня кіберзахисту критичної інформаційної інфраструктури.

Рекомендації **розроблені з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity)**, виданої у 2014 році та оновленої у 2018 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology).

Рекомендації **не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і є добровільними для використання**.

Рекомендації **описують загальний підхід до забезпечення кібербезпеки**, що дозволяє:

- здійснити аналіз та надати характеристику поточного стану кібербезпеки ОКІІ;
- описати цільовий стан кібербезпеки ОКІІ;
- ідентифікувати та визначити пріоритети, рівень упровадження заходів кіберзахисту в контексті безперервного та повторюваного процесу управління ризиками у сфері кібербезпеки ОКІІ;
- оцінити прогрес у досягненні цільового стану кібербезпеки ОКІІ;
- забезпечити комунікацію між суб'єктами, які безпосередньо перебувають на ОКІ, та із суб'єктами, які є партнерами організації щодо управління ризиками у сфері кібербезпеки.

Рекомендації **складаються з трьох основних частин**:

- системи (таксономії) заходів кіберзахисту;
- рівнів упровадження заходів кіберзахисту;
- профілю кіберзахисту.

Підхід, що визначається у Рекомендаціях, **не є єдиним підходом для управління ризиком кібербезпеки**, оскільки ОКІ, що належать до різних секторів такої інфраструктури, можуть мати як однакові ризики, так і різні унікальні ризики – унікальні загрози, різні вразливості, різні допустимі рівні ризику. Підхід до забезпечення кібербезпеки залежить від того, яким чином організація впроваджуватиме заходи кіберзахисту, що наведені у цих Рекомендаціях.

Ознайомитись із Наказом Адміністрації Держспецзв'язку Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури

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

e-mail: soc@scpc.gov.ua
тел.: +38 (044) 281 87 37