Додаток

до Методичних рекомендацій щодо збору та обробки статистичних даних стосовно кібератак, кіберінцидентів і заходів протидії у Державній службі спеціального зв'язку та захисту інформації України

Показники кіберстатистики

Таблиця 1 – Показники кіберінцидентів (кібератак) CIA.

Показники кіберстатистики		
набір	показник	код
1	2	3
реєстраційні дані .REG.	сфера відповідальності	CIA.REG.SPH
	дата	CIA.REG.DATE
	час	CIA.REG.TIME
	номер	CIA.REG.NUM
	мітки (колір, рівень)	CIA.REG.TLP
	службові відомості	CIA.REG.SRV
	повідомлення	CIA.REG.LET
категорії .CTG.	категорія	CIA.CTG.CAT
	категорія (рівень критичності)	CIA.CTG.CRY
	назва (тип)	CIA.CTG.TYP
підтвердження реєстрації .VLD.	дата	CIA.VLD.DATE
	час	CIA.VLD.TIME
суб'єкти спостереження .SUB.	сектор	CIA.SUB.SEC
	регіон	CIA.SUB.RGN
	рівень мережі	CIA.SUB.NET
	персонал	CIA.SUB.HRQ
	назва	CIA.SUB.INM
	код	CIA.SUB.CODE
	доменна зона	CIA.SUB.URL
	IP-адреси	CIA.SUB.ADR
дані для закриття .CLS.	дата	CIA.CLS.DATE
	час	CIA.CLS.TIME
	службові відомості	CIA.CLS.SRV
	час застою	CIA.CLS.DOWN

1	2	3
	збитки	CIA.CLS.LOSS
	зв’язки	CIA.CLS.CON
	оцінка	CIA.CLS.EST

Таблиця 2 – Показники заходів протидії .PRC.

Показники кіберстатистики		
набір	показник	код
1	2	3
реєстраційні дані .REG.	сфера відповідальності	PRC.REG.SPH
	дата	PRC.REG.DATE
	час	PRC.REG.TIME
	номер	PRC.REG.NUM
	категорія	PRC.REG.CTR
	тип (назва)	PRC.REG.NAM
	документ	PRC.REG.DOC
	службові відомості	PRC.REG.SRV
	повідомлення	PRC.REG.LET
загальна таксономія (не для ОКІІ) .TXN.	НПА та регуляторні акти	PRC.TXN.NRM
	рекомендації та звіти	PRC.TXN.REC
	кримінальні провадження	PRC.TXN.CRM
	провадження в справах про адміністративні правопорушення	PRC.TXN.PNL
	діяльність адміністраторів (адміністраторів безпеки)	PRC.TXN.ADM
	діяльність служби реагуванняна надзвичайні події	PRC.TXN.ERT
	діяльність служби операційної безпеки	PRC.TXN.SOC
	підготовка персоналу	PRC.TXN.HRP
таксономія заходів кіберзахисту (для ОКІІ та ОТ/АСУ ТП) .TXM.	клас заходів кіберзахисту	PRC.TXM.CLA
	категорія заходів кіберзахисту	PRC.TXM.CTY
	рівень впровадження	PRC.TXM.LEV
	назва заходу кіберзахисту (тип)	PRC.TXM.TPP
	назва заходу кіберзахисту (власна)	PRC.TXM.NAZ
таксономія заходів огляду стану кіберзахисту (для уповноважених	орган виконавчої влади	PRC. REV.R0
	показник огляду № 1	PRC. REV.R1

1	2	3
органів) .REV.	показник огляду № 29 (табл. 2)	PRC. REV.R29
підтвердження реєстрації .VLD.	дата	PRC.VLD.DATE
	час	PRC.VLD.TIME
суб'єкти спостереження .SUB.	сектор	PRC.SUB.SEC
	регіон	PRC.SUB.RGN
	персонал	PRC.SUB.HRQ
	назва	PRC.SUB.INM
	код	PRC.SUB.CODE
дані для закриття .CLS.	дата	PRC.CLS.DATE
	час	PRC.CLS.TIME
	документ	PRC.CLS.DOC
	службові відомості	PRC.REG.SRV
	тривалість	CIA.CLS.DUR
	витрати на проведення	CIA.CLS.COST
	зв'язки	PRC.CLS.CON
	оцінка	PRC.CLS.EST

Опис і формат показників кіберстатистики:
ADM – характеристика залучення адміністраторів (адміністраторів безпеки), X/Y – участь у заході X (0 – захід без безпосередньої участіі поза межами компетенції адміністраторів (адміністраторів безпеки), 1 – захід з безпосередньою участю і в межах компетенції адміністраторів (адміністраторів безпеки)), Y – назва ресурсу або системи (ТЕКСТ), що адмініструється;
ADR – перелік IP-адрес (0 – приховано, 1 – надано; перелік через кому, якщо надано), конфіденційна інформація;
CAT – категорія відповідно до [1] (дві цифри 01, 02, 03, … 10);
CLA – клас заходів кіберзахисту відповідно до [2] (дві літери ID, PR, DE, RS, RC);
CODE XXX/YYYYYYYY – код (XXX – 3 цифри) відповідно до Класифікатора організаційно-правових форм господарювання ДК 002:2004[3] / код (YYYYYYYY – 8 цифр) відповідно до Єдиного державного реєстру

[1] Державна служба спеціального зв'язку та захисту інформації України, Перелік категорій кіберінцидентів, https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv.

[2] Наказ Адміністрації Держспецзв'язку від 06.10.2021 № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» (зі змінами), https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.

[3] Наказ Державного комітету України з питань технічного регулювання та споживчої політики від 28.05.2004 № 97 «Про затвердження національних стандартів України, державних класифікаторів України, національних змін до міждержавних стандартів, внесення зміни до наказу Держспоживстандарту України від 31 березня 2004 р. № 59 та скасування нормативних документів», https://zakon.rada.gov.ua/rada/show/v0097609-04#Text.

юридичних осіб, фізичних осіб-підприємців та громадських формувань, YYYYYYYY разом зі службовими відомостями – конфіденційна інформація;
CON – перелік кіберінцидентів (кібератак), заходів протидії, для яких існують зв'язки із цим кіберінцидентом (кібератакою), заходом протидії;
COST X/Y – джерела фінансування X (0 – не потребує окремого фінансування, 1 – державний бюджет, 2 – місцеві бюджети, 3 – кошти комерційних організацій, 4 – технічна допомога,41 – міжнародна технічна допомога, 5 – кошти приватних осіб) / обсяг витрат на організацію та проведення Y (тис. грн, одна або двізначущі цифри, 0 – не оцінювалося або менше 1 тис. грн), конфіденційна інформація;
CRM XXX/Y/Z – стаття Кримінального кодексу України XXX, за якою проводиться кримінальне провадження з переліку: 156^1, 190 (частина третя), 200, 301^1, 301^2, 359, 360, 361, 361^1, 361^2, 362, 363, 363^1, 376^1; стан розгляду кримінального провадження Y (1 – досудове розслідування, 2 – судовий розгляд, 3 – вирок: 31 – виправдувальний, 32 – звинувачувальний, 30 – не вступив в законну силу); встановлений розмір заподіяної шкоди Z (тис. грн, 2 значущі цифри, 0 – не встановлено або менше 1 тис. грн);
CRY – рівень критичності кіберінциденту (кібератаки) – колір COLOUR відповідно до [4] (BLACK, RED, AMBER, YELLOW, GREEN, WHITE);
CTR – категорія заходів протидії (1 – загальна таксономія, 2 – таксономія заходів кіберзахисту);
CTY – категорія заходів кіберзахисту відповідно до [5] XX.YY (XX – клас заходів кіберзахисту, YY – категорія заходів кіберзахисту);
DATE дата ДД.ММ.РРРР (ДД – 2 цифри день, ММ – 2 цифри місяць, РРРР – 4 цифри в рік);
DOC назва та реквізити документа – назва (ТЕКСТ), дата ДД.ММ.РРРР, номер (ЧИСЛО);
DOWN – час простою обладнання у робочих часах (одна значуща цифра, 0 – невідомо або не оцінювалося), конфіденційна інформація;
DUR тривалість заходу разом з підготовкою (1 – івент-подія, 2 – до 1 тижня, 3 – до 1 місяця, 4 – постійно на періодичній основі, 0 – невідомо);
ERT – характеристика діяльності служби (команди) реагування на комп'ютерні надзвичайні події, X/Y – участь у заході X (0 – захід безбезпосередньої участі і поза межами компетенції служби (команди) реагування, 1 – захід з безпосередньою участю і в межах компетенції служби (команди) реагування), Y – назва служби (команди) (ТЕКСТ);

[4] Наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570 «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі», https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori.

[5] Наказ Адміністрації Держспецзв'язку від 06.10.2021 № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» (зі змінами), https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.

EST – оцінка корисності SPH:X/Y/Z/W (від 1 до 10, SPH – оцінка суб'єкта збору та обробки даних кіберстатистики зі сферою відповідальності «SPH» з додатка 1, X – оцінка дотримання нормативних та процедурних вимог, Y – оцінка швидкості, Z – оцінка внеску реєстратора, W – оцінка ефективності впроваджених результатів, для інцидентів W=0); оцінювання обов'язково здійснюють CIP, MOU (у військовий час), рекомендовано для здійснення SSU і реєстратором інциденту (заходу); оцінювання виконується для завершеного (закритого) інциденту (заходу);
HRQ – показник кількості робітників X/Y/Z (X – загальна чисельність / Y – обов'язки, пов'язані з інформаційними технологіями / Z – обов'язки, пов'язані з інформаційною безпекою; 1 – більше ніж 1000 робітників, 2 – 101 – 1000 робітників, 3 – 11 – 100 робітників, 4 – 1 – 10 робітників, 0 – немає даних або робітників);
HRP характеристика заходу з підготовки персоналу X/Y/Z/W –складник системи освіти X (відповідно до ст. 10, п. 1 Закону України «Про освіту», 0 – не застосовується), рівень освіти Y (відповідно до ст. 10, п. 2 Закону України «Про освіту» , 0 – не застосовується), предметна область Z (1 – інформаційні технології (інформатизація);
2 – цифровізація (цифрова трансформація), 3 – інформаційна безпека, 4 – кібербезпека, 5 – кіберзахист, 6 – технічний захист інформації, 7 – захист персональних даних, 8 – кібергігієна, 0 – інші, витрачений час на підготовку W (0 – не оцінювалося, 1 – до 10 годин, 2 – 11 – 100 годин, 3 – більше ніж 100 годин);
INM – назва відповідно до Єдиного державного реєстру юридичних осіб, фізичних осіб-підприємців та громадських формувань разом зі службовими відомостями, конфіденційна інформація;
LET – повідомлення інших суб'єктів збору та обробки даних кіберстатистики відповідно до [6] (NOT – нікого не повідомлено, ALL – усі повідомлені, SPH – повідомлено суб'єкта збору та обробки даних кіберстатистики зі сферою відповідальності «XXX» з додатка 1, якщо повідомлено декілька – через кому);
LEV – рівень впровадження заходів кіберзахисту відповідно до [7] (1 частковий, 2 – ризик-орієнтований, 3 – повторюваний, 4 – адаптивний);
LOSS – розмір збитків (тис. грн, одна або дві значущі цифри, 0 – не оцінювалося або менше ніж 1 тис. грн), конфіденційна інформація;
NAM – назва (власна) заходу протидії ТЕКСТ;
NAZ – назва (власна) заходу кіберзахисту ТЕКСТ; плани заходів зазначаються як окремі заходи; окремі пункти планів заходів вказуються як окремі заходи із зазначенням зв'язків з планами;
NET – рівень мережі, де зареєстровано інцидент (1 – більше ніж 1000 кінцевих пристроїв, 2 – 101 – 1000 кінцевих пристроїв, 3 – 11 – 100 кінцевих пристроїв, 4 – до 10 кінцевих пристроїв, 0 – немає даних);
NRM – розроблені проєкти прийнятих нормативно-правових, нормативних або регуляторних актів, X/АКТ/Y/ Z – індикатор X (1 – нормативно-правовий акт, 2 – регуляторний акт), вид акта АКТ (ТЕКСТ) – Закон України, Указ Президента України, рішення Ради національної безпеки і оборони України, постанова Кабінету Міністрів України, розпорядження Кабінету Міністрів України, стандарт,

постанова органу, наказ органу; назва (ТЕКСТ), дата ДД.ММ.РРРР, номер (ЧИСЛО); предметна область Y (1 – інформаційні технології (інформатизація), 2 – цифровізація (цифрова трансформація), 3 – інформаційна безпека, 4 – кібербезпека, 5 – кіберзахист, 6 – технічний захист інформації, 7 – захист персональних даних, 8 – кібергігієна, 9 – захист критичної інфраструктури; 0 – інші); додаткові відомості Z (ТЕКСТ) із зазначенням нормативних підстав або акта-прототипу;

NUM – номер (число 1, 2, 3, …);

PNL XXX/Y/Z – стаття Кодексу України про адміністративні правопорушення XXX, за якою проводиться провадження у справі про адміністративне правопорушення (212[6] або інша за рішенням реєстратора); стан розгляду справи про адміністративне правопорушення Y (1 – справу порушено, триває адміністративне розслідування, 2 – справа розглядається, приймається рішення, 3 – рішення оскаржується, 4 – постанова про стягнення виконується, 5 – постанову про стягнення виконано); встановлений розмір заподіяної шкоди Z (тис. грн, одна або дві значущі цифри, 0 – не встановлено або менше ніж 1 тис. грн);

R0 – назва органу виконавчої влади (уповноваженого органу), використовується формат CIA.SUB.INM та CIA.SUB.CODE;

R1-29 – показники огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсівта інформації, вимога щодо захисту якої встановлена законом [8] (запитання опитувальної форми [11] Адміністрації Держспецзв’язку станом на 01.10.2023);

REC видано рекомендації та звіти S/X/Y/ Z – предметна область S (1 – інформаційні технології (інформатизація), 2 – цифровізація (цифрова трансформація), 3 – інформаційна безпека, 4 – кібербезпека, 5 – кіберзахист, 6 – технічний захист інформації, 7 – захист персональних даних, 8 – кібергігієна, 9 – захист критичної інфраструктури; 0 – інші); індикатор доступу X (0 – з обмеженим доступом, 1 – з відкритим доступом або публічний, 11 – оприлюднений у мережі Інтернет або у ЗМІ, 12 – поширений для фахівців); тип документа Y (1 – рекомендація, 2 – звіт, 3 – аналітичний звіт або доповідь, 0 – інше), періодичність Z (0 – невідомо або неперіодичний (разовий), 1 – 0 – 1 місяць, 2 – 6 місяців, 7 – 12 місяців);

[6] Порядок взаємодії суб’єктів забезпечення кібербезпеки під час реагування накіберінциденти/кібератаки https://www.rnbo.gov.ua/files/2022/NKCK/%D0%9F%D0%BE%D1%80%D1%8F%D0%B4%D0%BE%D0%BA_%D0%B2%D0%B7%D0%B0%D1%94%D0%BC%D0%BE%D0%B4%D1%96%D1%97.pdf.

[7] Наказ Адміністрації Держспецзв’язку від 06.10.2021 № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» (зі змінами), https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.

[8] Постанова Кабінету Міністрів України від 11.11.2020 № 1176 «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом», https://zakon.rada.gov.ua/laws/show/1176- 2020-п#Text.

RGN XX – позначення регіону (адміністративно-територіальної одиниці першого рівня) відповідно до Кодифікатора адміністративно-територіальних одиниць та територій територіальних громад (КАТОТТГ) відповідно до [9];
SEC – державний – GOV, недержавний – NGO, комерційний – BIZ, приватний – PRV сектори;
SOC – характеристика діяльності служби (центру) операційної безпеки, X/Y – участь у заході X (0 – захід без безпосередньої участі і поза межами компетенції служби (центру), 1 – захід з безпосередньою участю і в межах компетенції служби (центру)), Y – назва служби (центру) (ТЕКСТ);
SPH – сфера відповідальності «XXX» з додатка 1;
SRV – службові відомості X/ТЕКСТ (0 – немає, 1 – є в повному обсязі, 2 – є у достатньому обсязі, 3 – є і потребують уточнення, ТЕКСТ – текст повідомлення, яке розкриває зміст службових відомостей, конфіденційна інформація);
TIME – час ГГ:XX (ГГ – дві цифри години, XX – 2 цифри хвилини);
TLP COLOUR/X – колір відповідно до [10] (BLACK, RED, AMBER, YELLOW, GREEN, WHITE) та рівень відповідно до [11] (5, 4, 3, 2, 1, 0);
TPP – назва (тип) заходів кіберзахисту відповідно до [12] XX.YY-N (XX – клас заходів кіберзахисту, YY – категорія заходів кіберзахисту, N – номер заходу в категорії заходів);
TYP – тип код XX відповідно до [13] (назва ТЕКСТ відповідно до [14]);
URL – доменна зона (назва) (ТЕКСТ), разом зі службовими відомостями – інформація з обмеженим доступом.

[9] Наказ Міністерства розвитку громад та територій України 26.11.2020 № 290 «Про затвердження Кодифікатора адміністративно-територіальних одиниць та територій територіальних громад» (в редакції наказу Міністерства розвитку громад, територій та інфраструктури України від 19.01.2024 № 48), https://zakon.rada.gov.ua/rada/show/v0290914-20#n9.

[10] Загальні правила обміну інформацією про кіберінциденти, затверджені протоколом № 21 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 09.02.2023, https://cert.gov.ua/recommendation/4256181.

[11] Постанова Кабінету Міністрів України від 04.04.2023 № 299 «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі», https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text.

[12] Наказ Адміністрації Держспецзв'язку від 06.10.2021 № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури» (зі змінами), https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.

[13] Наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570 «Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі», https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori.

[14] Державна служба спеціального зв'язку та захисту інформації України, Перелік категорійкіберінцидентів, https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv.