ЗАТВЕРДЖЕНО
Наказ Міністерства охорони
здоров’я України
від 06 грудня № 2076

ПРОТОКОЛ КРИЗОВИХ КОМУНІКАЦІЙ ПІД ЧАС РЕАГУВАННЯ НА КІБЕРАТАКИ ТА КІБЕРІНЦИДЕНТИ

ЗМІСТ

І. СТИСЛИЙ ВИКЛАД

Цей документ надає шаблон та порядок інформаційного обміну, координації та спільних дій під час реагування на кіберінциденти та кібератаки в Міністерстві охорони здоров’я, Національній службі здоров'я України, Центрі громадського здоров'я України, Державному підприємстві «Електронне здоров’я».

ІІ. ВСТУП

Планом реалізації Стратегії кібербезпеки України для суб’єктів забезпечення кібербезпеки передбачено завдання зміцнювати довіру приватного сектору та громадян до цифрових послуг, які надаються державою, безумовно виконуючи вимоги щодо забезпечення кібербезпеки та кіберзахисту під час їх надання та інформуючи громадськість про їх безпечність та надійність, а також запровадити обов'язкове негайне, без невиправданої затримки, надання інформації про кіберзагрози, кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами кібербезпеки (кіберзахисту) до Національного координаційного центру кібербезпеки.

Порядок взаємодії суб’єктів забезпечення кібербезпеки під час реагування на кіберінциденти та кібератаки встановлює вимоги до інформаційного обміну, координації та спільних дій суб’єктів забезпечення кібербезпеки під час реагування на кіберінциденти та кібератаки.

Протокол засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 20 січня 2022 року № 19, вимагає від суб’єктів забезпечення кібербезпеки, невідкладно, не пізніше 30 хвилин з моменту виникнення, інформувати Національний координаційний центр кібербезпеки про виявлену кібератаку або кіберінцидент, що потенційно може мати критичні наслідки для кібербезпеки держави із зазначенням об’єкта кібератаки (кіберінциденту), часу її здійснення та іншої наявної інформації. Протягом 12 годин після виявлення такої кібератаки/кіберінцидента у встановленому порядку надавати Центру технічну інформацію, а також інформацію щодо можливого джерела, потенційних наслідків, додаткових обставин, вжитих та запланованих заходів реагування.

Мета цього документа полягає в наданні шаблонів і порядку дій відповідальних осіб по виконанню покладених на них обов’язків в частині інформаційного обміну, координації та спільних дій під час реагування на кіберінциденти та кібератаки.

ІІІ. ВИЗНАЧЕННЯ КІБЕРІНЦИДЕНТА ТА КІБЕРАТАКИ

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кіберінцидент та кібератака визначаються наступним чином:

Інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного,

помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

Кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту.

IV. РІВНІ КРИТИЧНОСТІ КІБЕРІНЦИДЕНТІВ ТА КІБЕРАТАК

Залежно від ступеня негативних наслідків, що можуть настати в результаті реалізації кіберінциденту/кібератаки, встановлюються такі рівні критичності кіберінцидентів/кібератак:

Некритичний (білий) – кіберінцидент/кібератака не загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів.

Низький (зелений) – кіберінцидент/кібератака безпосередньо загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів, інших об’єктів кіберзахисту, але не загрожує порушенню конфіденційності, цілісності та доступності державних інформаційних ресурсів або персональних даних громадян.

Середній (жовтий) – кіберінцидент/кібератака безпосередньо загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів, інших об’єктів кіберзахисту, внаслідок чого створюються передумови для порушення конфіденційності, цілісності та доступності державних інформаційних ресурсів або персональних даних громадян, виникають передумови для впливу на надання основних послуг населенню.

Високий (помаранчевий) – кіберінцидент/кібератака безпосередньо загрожує сталому функціонуванню системи електронних комунікацій, системи управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів, інших об'єктів кіберзахисту, внаслідок чого прогнозується помітній вплив на національну безпеку, обороноздатність, економічну безпеку, зовнішні відносини, основоположні свободи чи суспільну довіру або створюється потенційна загроза обмеження у наданні основних послуг населенню. Реагування на цьому рівні може потребувати залучення ресурсів більше ніж одного основного суб'єкта національної системи кібербезпеки.

Критичний (червоний) – кіберінцидент/кібератака безпосередньо загрожує сталому функціонуванню декількох систем електронних комунікацій, систем управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів, інших об'єктів кіберзахисту, внаслідок чого прогнозується значній вплив на національну безпеку, обороноздатність, економічну безпеку, зовнішні відносини, здоров'я чи безпеку громадян або створюється реальна загроза обмеження у наданні основних послуг населенню. Реагування на цьому рівні потребує залучення ресурсів усіх основних суб'єктів національної системи кібербезпеки.

Надзвичайний (чорний) – кіберінцидент/кібератака безпосередньо загрожує сталому функціонуванню значної кількості систем електронних комунікацій, систем управління технологічними процесами, безпеці (захищеності) електронних інформаційних ресурсів, інших об'єктів кіберзахисту, внаслідок чого відбувається невідворотній вплив на повноцінне функціонування держави або створюється загроза життю громадян України. Реагування на цьому рівні потребує максимальної державної участі, повного залучення всіх ресурсів основних та інших суб'єктів національної системи кібербезпеки.

Рівень критичності кіберінциденту/кібератаки попередньо визначається суб'єктом забезпечення кібербезпеки, який зафіксував кіберінцидент/кібератаку та обов'язково підтверджується (уточнюється за необхідності) суб'єктом, відповідальним за реагування на кіберінцидент/кібератаку, з урахуванням отримання додаткової інформації про кіберінцидент/кібератаку.

Категорія (рівень) критичності кіберінциденту/кібератаки визначається відповідно до трьох критеріїв критичності кіберінциденту/кібератаки:

А. Загроза порушення сталого, надійного та штатного режиму функціонування систем (системи):

А1. Загрози немає.

А2. Безпосередня загроза для сталого, надійного та штатного режиму функціонування систем (конкретної системи суб'єкта забезпечення кібербезпеки).

А3. Безпосередня загроза для сталого, надійного та штатного режиму функціонування декількох систем окремого суб'єкта забезпечення кібербезпеки.

А4. Безпосередня загроза для сталого, надійного та штатного режиму функціонування значної кількості систем декількох суб’єктів забезпечення кібербезпеки.

А5. Транскордонний вплив загрози порушення сталого, надійного та штатного режиму функціонування систем.

Б. Загроза порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в системах (системі):

Б1. Загрози немає.

Б2. Створені передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в системах (системі).

Б3. Порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в системах (системі).

В. Загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об’єктами критичної інфраструктури:

В1. Загрози немає;

В2. Передумови для припинення виконання функцій та/або надання послуг об’єктами критичної інфраструктури.

В3. Потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об’єктами критичної інфраструктури.

В4. Реальні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об’єктами критичної інфраструктури.

В5. Невідворотна загроза для повноцінного функціонування держави або загроза життю громадян України.

Суб’єкт забезпечення кібербезпеки, вибравши необхідні варіанти в трьох критеріях критичності кіберінциденту/кібератаки, визначає категорію (рівень) критичності кіберінциденту/кібератаки відповідно до Таблиці 1. Зіставлення критеріїв критичності кіберінциденту/кібератаки необхідно здійснювати послідовно від А до В.

Варіанти категорій (рівнів) критичності кіберінциденту/кібератаки враховуються відповідно до однакової важливості усіх критеріїв визначення категорії (рівня) критичності кіберінциденту/кібератаки та узгоджені між собою. Якщо для кіберінциденту/кібератаки можливі два варіанти категорії (рівня) критичності кіберінциденту/кібератаки (наприклад, середній (жовтий) та високий (помаранчевий)), рекомендовано обирати вищу категорію (рівень) критичності кіберінциденту/кібератаки (в зазначеному прикладі – високий (помаранчевий)).

Якщо не вдається визначити категорію (рівень) критичності кіберінциденту/кібератаки, необхідно перевизначити показники відповідно до критеріїв визначення категорії (рівня) критичності кіберінциденту/кібератакиабо повідомити ці показники суб'єкту, відповідальному за реагування на кіберінцидент/кібератаку, з урахуванням необхідності отримання додаткової інформації про кіберінцидент/кібератаку.

Варто враховувати, що кожен суб'єкт забезпечення кібербезпеки визначає наслідки впливу кіберінцидентів/кібератаки відповідно до власних бізнес-процесів, особливостей функціонування, надання послуг, ресурсів, організаційно-штатної структури та інших чинників. У разі потреби суб'єкт забезпечення кібербезпеки може звернутися за допомогою у пріоритетизації кіберінцидентів/кібератак до CERT-UA, команд реагування на комп'ютерні надзвичайні події, підрозділи (групи, команди, служби) захисту інформації, підприємства, установи та організації незалежно від форми власності, які провадять діяльність та/або надають послуги, пов'язані з кіберзахистом.

Критерії визначення категорії (рівня) критичності												Категорія (рівень) критичності, що визначається
А					Б			В				
А1	А2	А3	А4	А5	Б1	Б2	Б3	В1	В2	В3	В4	В5	
●					●			●					0, некритичний (білий)
	●				●			●					1, низький (зелений)
	●				●				●				1, низький (зелений)
		●			●			●					1, низький (зелений)
		●				●		●					1, низький (зелений)
	●					●		●					2, середній (жовтий)
	●					●			●				2, середній (жовтий)
		●				●		●					2, середній (жовтий)
	●						●	●					3, високий(помаранчевий)
	●						●		●				3, високий(помаранчевий)
	●						●			●			3, високий(помаранчевий)
	●						●				●		4, критичний (червоний)
		●					●				●		4, критичний (червоний)
		●					●					●	5, надзвичайний (чорний)
			●				●					●	5, надзвичайний (чорний)
				●			●				●		5, надзвичайний (чорний)
				●			●					●	5, надзвичайний (чорний)

Таблиця 1. Визначення категорії (рівня) критичності кіберінциденту/кібератаки

V. ПІДГОТОВКА ТА ПЛАНУВАННЯ

Групи реагування на кіберінциденти та кібератаки формуються заздалегідь і включають в свій склад відповідних фахівців, які засвоїли та відпрацювали порядок взаємодії шляхом проведення спільних навчань.

Група реагування на кіберінциденти та кібератаки (CSIRT) відповідає за реалізацію технічного плану виявлення та реагування, інформаційний обмін, координацію та спільні дії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти та кібератаки.

Група кризової комунікації відповідає за внутрішні і зовнішні комунікації з метою загального управління кризовою ситуацією відповідно до Плану кризових комунікацій.

1. СКЛАД ГРУПИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ (CSIRT)

Керівник групи: ПІБ, контакти, зручний канал швидкої комунікації
Заступник керівника групи: ПІБ, контакти, зручний канал швидкої комунікації
Член групи: ПІБ, контакти, зручний канал швидкої комунікації

2. СКЛАД ГРУПИ КРИЗОВОЇ КОМУНІКАЦІЇ

Керівник групи: ПІБ, контакти, зручний канал швидкої комунікації
Заступник керівника групи: ПІБ, контакти, зручний канал швидкої комунікації
Член групи: ПІБ, контакти, зручний канал швидкої комунікації

VI. ОТРИМАННЯ ІНФОРМАЦІЇ ПРО КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

Керівник групи реагування на кіберінциденти та кібератаки отримує інформацію про події кібербезпеки з наступних джерел:

1. Основні суб'єкти національної системи кібербезпеки власними силами і засобами в автоматизованому режимі виявляють події кібербезпеки в системі електронних комунікацій або системі управління технологічними процесами суб'єкта забезпечення кібербезпеки, які містять ознаки кіберінциденту/кібератаки і повідомляють про це керівника групи реагування на кіберінциденти та кібератаки.
2. Відомчий або галузевий (секторальний) центр кіберзахисту та інші джерела інформації (іноземні партнери, юридичні або фізичні особи тощо).
3. Власні технічні засоби моніторінгу.
4. Користувачі.

З метою своєчасного отримання інформації про кіберінциденти та кібератаки, керівник групи реагування відповідає за:

1. Встановлення та підтримання постійного зв'язку та обміну інформацією із суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, інших сил кіберзахисту, партнерів, відкритих джерел і підприємств та організацій усіх форм власності, в обов'язковому порядку – з фахівцями урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA;
2. Запровадження активного відстеження сповіщень про кіберзагрози чи вразливості від суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, інших сил кіберзахисту, партнерів, відкритих джерел, підприємств та організацій усіх форм власності. Крім цього, застосовуються індикатори кіберзагроз та усі (за можливості) наявні джерела інформації про кіберзагрози (загрози інформаційній безпеці), а також використані інші можливості захисту для виявлення та блокування підозрілої поведінки.

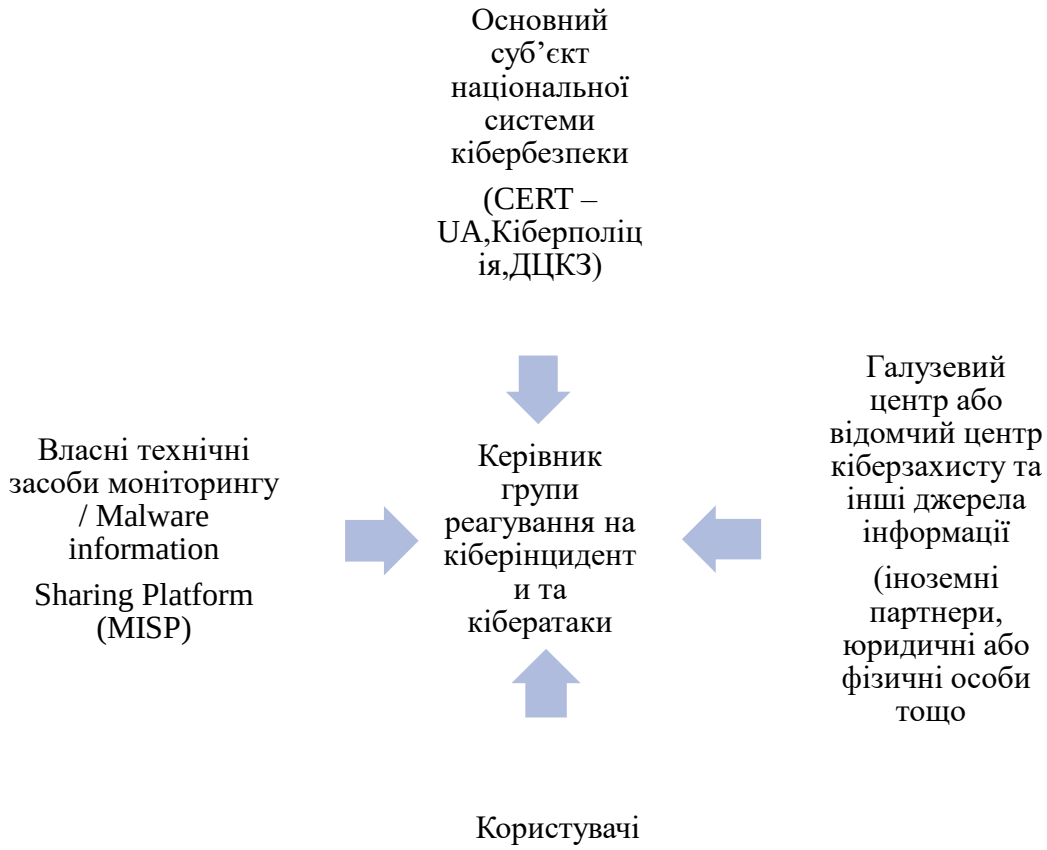

Схема 1. Джерела отримання інформації про кіберінциденти та кібератаки.

VII. РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

Порядок дій керівника групи реагування на кіберінциденти та кібератаки показано на *Схемі 2*.

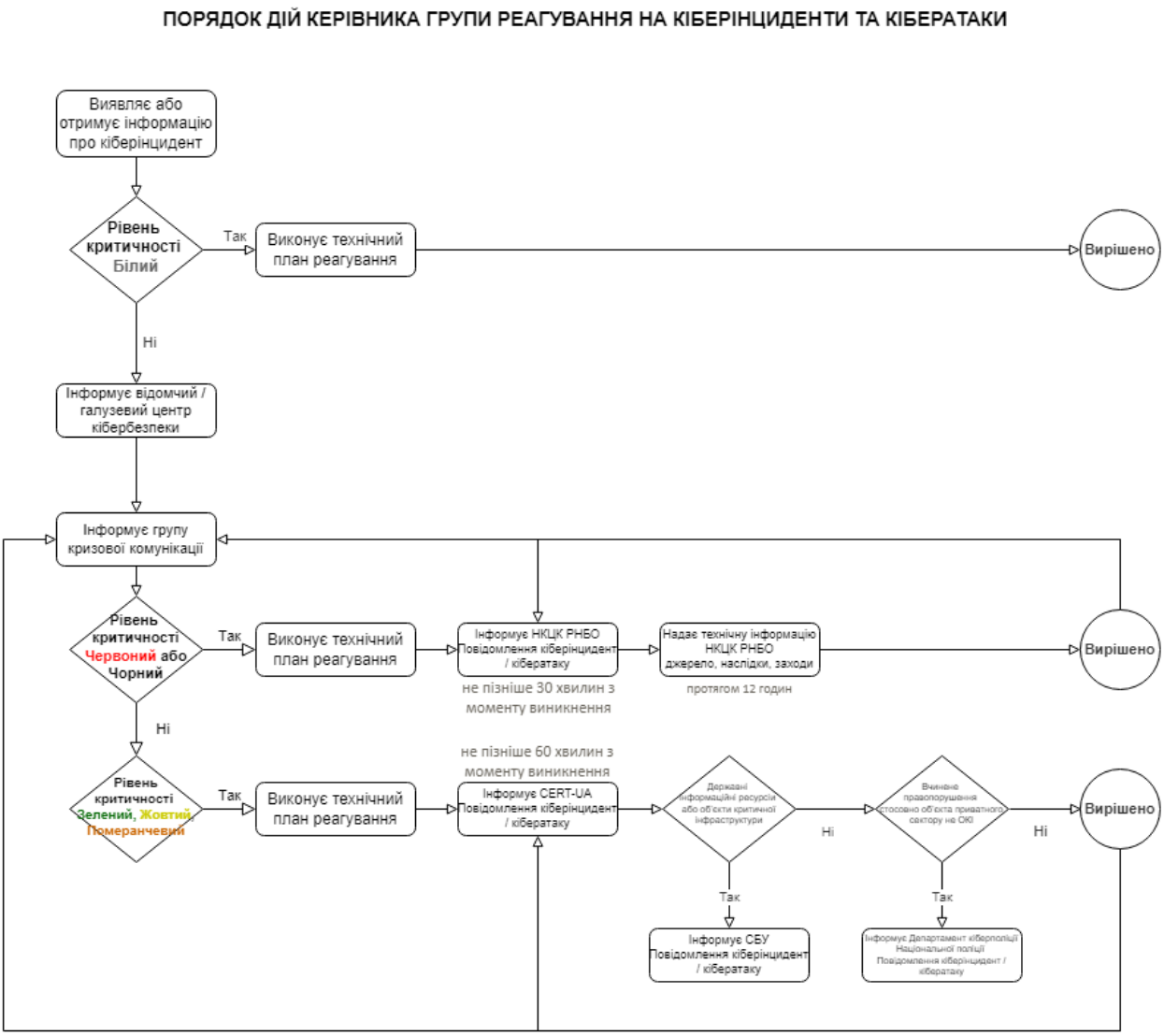

Схема 2. Порядок дій керівника групи реагування на кіберінциденти та кібератаки.

Порядок виконання дій під час реагування на кіберінциденти та кібератаки

Відповідальний	Дії
КЕРІВНИК ГРУПИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ (CSIRT)	Виявляє кіберінцидент або отримує від іншого джерела або суб'єкта національної системи кібербезпеки інформацію про кіберінцидент в системі електронних комунікацій або системі управління технологічними процесами.
	Визначає рівень критичності кіберінциденту залежно від ступеня негативних наслідків, що можуть настати в результаті реалізації кіберінциденту/кібератаки (білий, зелений, жовтий, помаранчевий, червоний, чорний).
	У разі, якщо рівень критичності кіберінциденту відрізняється від «білого», інформує про кіберінцидент/кібератаку Групу кризової комунікації з використанням шаблону *Помилка! Джерело посилання н*

	е знайдено. (Додаток 2). У разі наявності відповідного відомчого або галузевого (секторального) центру кібербезпеки (кіберзахисту), до сфери відповідальності якого належить заклад, здійснює інформування, передбачене пунктом 4 розділу ІІ Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти / кібератаки. При наявності, такий алгоритм взаємодії (інформування) додатково врегулюється відомчим розпорядчим документом.
	Виконує технічний план реагування на кіберінциденти/кібератаки.
	У разі, якщо рівень критичності кіберінциденту визначено як «чорний» або «червоний», невідкладно, не пізніше 30 хвилин з моменту виникнення, інформує Національний координаційний центр кібербезпеки через офіційну електронну поштову скриньку report@ncscc.gov.ua про виявлену кібератаку або кіберінцидент з використанням шаблону ***Помилка! Д жерело посилання не знайдено.*** (Додаток 1). Протягом 12 годин після виявлення такої кібератаки/кіберінциденту надавати Національному координаційному центру кібербезпеки через офіційну електронну поштову скриньку report@ncscc.gov.ua технічну інформацію, а також інформацію щодо можливого джерела, потенційних наслідків, додаткових обставин, вжитих та запланованих заходів реагування. Інформує Національний координаційний центр кібербезпеки через офіційну електронну поштову скриньку report@ncscc.gov.ua та Групу кризової комунікації про вирішення кіберінциденту.
	У разі, якщо рівень критичності кіберінциденту визначено як «зелений», «жовтий» або «помаранчевий», невідкладно, не пізніше 60 хвилин з моменту виникнення, інформує **Урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA** через офіційну електронну поштову скриньку incidents@cert.gov.ua або по телефону. З Понеділка по Четвер, з 8:00 - 17:00, П'ятниця: 8:00 - 15:45: +38 (044) 281-88-25; +38 (044) 281-88-05 Вихідні та святкові дні (цілодобово): +38 (044) 281-88-01

	Службу безпеки України – обов'язково, через офіційну електронну поштову скриньку cyber_security@dis.gov.ua, якщо кіберінцидент/кібератака відбувається стосовно державних електронних інформаційних ресурсів або об'єктів критичної інфраструктури; **Департамент кіберполіції Національної поліції України** – через офіційний сайт https://ticket.cyberpolice.gov.ua, у випадку вчинення правопорушення стосовно об'єкта приватного сектору, який не належить до об'єктів критичної інфраструктури; про виявлену кібератаку або кіберінцидент з використанням шаблону ***Помилка! Джерело посилання не знайдено.*** (Додаток 1). Забезпечує унеможливлення порушення цілісності доказової бази. Вживає заходів щодо виконання рекомендацій, наданих національними суб'єктами забезпечення кібербезпеки, що здійснювали реагування на кіберінцидент/кібератаку. Інформує Урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA через офіційну електронну поштову скриньку incidents@cert.gov.ua та Групу кризової комунікації про вирішення кіберінциденту.
ГРУПА КРИЗОВОЇ КОМУНІКАЦІЇ	Виконує внутрішні і зовнішні комунікації з метою загального управління кризовою ситуацією згідно з *Планом кризових комунікацій* з урахуванням того, що, відповідно до Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінци-денти та кібератаки [2]: - Національний координаційний центр кібербезпеки, CERT-UA та СБУ відповідають за інформування громадськості про кіберінцидент/кібератаку. - Оприлюднення відповідної інформації здійснюється з урахуванням інтересів суб'єкта забезпечення кібербезпеки (атакованого об'єкта) та, у визначених законом випадках, після отримання дозволу слідчого (прокурора). - У разі необхідності таке інформування може здійснюватись іншими суб'єктами забезпечення кібербезпеки (як самостійно, так і додатково) за погодженням із суб'єктом, який є відповідальним за

	реагування на кіберінцидент/кібератаку та/або Національним координаційним центром кібербезпеки.

VIII. ЗАБОРОНЕНО ПІД ЧАС РЕАГУВАННЯ

1. Розголошення даних щодо постраждалої сторони.
2. Оприлюднення інформації, у визначених законом випадках, без отримання дозволу слідчого (прокурора).
3. Порушення цілісності доказової бази.

IX. НОРМАТИВНІ ПОСИЛАННЯ

1. План реалізації Стратегії кібербезпеки України, схвалений рішенням Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України", уведеним в дію Указом Президента України від 01.02.2022 №37/2022.
2. Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти та кібератаки, затверджений на засіданні Національного координаційного центру кібербезпеки 22 вересня 2022 року.
3. Протокол засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 20 січня 2022 року № 19
4. Закон України «Про основні засади забезпечення кібербезпеки України».
5. Перелік категорій кіберінцидентів схвалений 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))
6. Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджений постановою Кабінету Міністрів України від 04.04.2023 № 299

ДОДАТКИ

ДОДАТОК 1. Картка інформування про кіберінцидент/кібератаку

Примітка: *1. Для позначення потрібних варіантів підкреслити (обвести, виділити кольором) обраний варіант.* *2. Намагатися вказати якомога більше інформації, заповнивши відповідні поля.*				
TLP				
RED	AMBER	AMBER + STRICT	GREEN	CLEAR
Дата та час виявлення кіберінциденту/кібератаки:	___..___._____ ___:___:___ GMT ____			

Заявник			
ПІБ:		Електронна адреса:	
Посада:		Номер телефону:	
Суб'єкт забезпечення кібербезпеки:			

Джерело виявлення кіберінциденту/кібератаки			
Адміністратор	Користувач	Антивірусне ПЗ	EDR
IDS/IPS	Інше(вказати): _____		

Запропонована категорія (рівень) критичності кіберінцидент/кібератаки	
0, некритичний (білий)	1, низький (зелений)
2, середній (жовтий)	3, високий (помаранчевий)
4, критичний (червоний)	5, надзвичайний (чорний)
Не вдалося визначити	

Отримана інформація
_____
_____
_____
_____
_____
_____
_____
_____
_____

Постраждалий суб'єкт забезпечення кібербезпеки	
Юридична назва:	
Адреса:	

Електронна адреса:		Номер телефону:	
Контактна особа 1			
ПІБ:		Електронна адреса:	
Посада:		Номер телефону:	
Контактна особа 2			
ПІБ:		Електронна адреса:	
Посада:		Номер телефону:	

Сектор (галузь) атакованого об'єкта			
Сектор безпеки і оборони	Органи державної влади	Органи місцевого самоврядування	Енергетичний сектор
Сфера електронних комунікаційних послуг	IT сектор	Транспортна галузь	Фінансовий сектор
Підприємства та організації відповідної форми власності	Засоби масової інформації	Інші критичні організації	Інше (вказати): _____ _____

Доменна зона			
UAGOV Український державний	UACOM Український недержавний	FGOV Закордонний державний	FCOM Закордонний недержавний

Відношення України до кіберінциденту/кібератаки			
Україна – об'єкт атаки	Україна – джерело атаки	Україна – елемент механізму атаки	не стосується території України
Інше(вказати): _____			

Категорія та тип кіберінциденту (відповідно до Переліку категорій та типів кіберінцидентів)

Код	*Категорія кіберінциденту*	*Код*	*Тип кіберінциденту*
01	Шкідливий (образливий) вміст (Abusive content)	01	Спам
02	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (ШПЗ)
		02	Розповсюдження ШПЗ
		03	Командно-контрольний центр (С2)
		04	Шкідливе підключення
03	Збір інформації зловмисником (Information Gathering)	01	Сканування
		02	Сніфінг
		03	Фішинг
04	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості
		02	Спроби авторизації/входу в систему
05	Втручання (Intrusion)	01	Компрометація облікового запису
		02	Компрометація системи

06	Порушення доступності (Availability)	01	Атака на відмову в обслуговуванні
		02	Саботаж/шкідливі дії
		03	Збій
07	Порушення властивостей інформації (Information Content Security)	01	Несанкціонований доступ до інформації
		02	Несанкціонована модифікація
08	Шахрайство (Fraud)	01	Шахрайський сайт
09	Відома вразливість (Vulnerable)	01	Вразливість
		03	Некоректна конфігурація
10	Інше (Other)	01	Невизначений інцидент

Дата та час початку кіберінциденту/кібератаки:	___.___._____ ___:___:___ GMT____

Чи пов'язаний цей (ця) кіберінцидент/кібератака з попередніми?			
ТАК	НІ	ID пов'язаного кіберінциденту/кібератаки: _____	Невідомо

Короткий опис кіберінциденту/кібератаки
_____
_____
_____
_____
_____
_____
_____

Вплив на функціонування систем/мереж, сервіси (послуги)	
Немає впливу взагалі	Немає впливу на сервіси (послуги)
Мінімальний вплив на некритичні сервіси (послуги)	Мінімальний вплив на критичні сервіси (послуги)
Значний вплив на некритичні сервіси (послуги)	Значний вплив на некритичні сервіси (послуги)
Втрата доступності некритичних сервісів (послуг)	Втрата доступності критичних сервісів (послуг)

Кількість скомпрометованих систем/мереж (ЕОМ)			
1-10	10-50	Інше (вказати):_____	Невідомо

Тип скомпрометованої системи/мережі за функціоналом			
Робочі станції	Сервер(и) додатків	Сервер(и) баз даних	Вебсервер(и)
Сервери доменних імен	Поштовий сервер	Брандмауер(и)	Мережеве обладнання
Інше(вказати):			

Об'єкт кібератаки	
Тип (модель):	
Ім'я:	

Операційна система:			
Дата встановлення ОС:			
Часова зона:			
Мережеві налаштування:			
Облікові записи:			
CVE:	CVE-____-____	CVE-____-____	CVE-____-____
Висновок:			

Тип (модель):			
Ім'я:			
Операційна система:			
Дата встановлення ОС:			
Часова зона:			
Мережеві налаштування:			
Облікові записи:			
CVE:	CVE-____-____	CVE-____-____	CVE-____-____
Висновок:			

Чи вирішено кіберінцидент/кібератаку?		**Чи потрібна допомога CERT-UA?**	
Так	Ні	Так	Ні

Чи повідомлялося про кіберінцидент/кібератаку іншим основним суб'єктам забезпечення кібербезпеки? Яким саме?		
Так		Ні
Служба безпеки України	Міністерство оборони України та Генеральний штаб Збройних Сил України	Розвідувальні органи
Національний банк України	Національна поліція України	Національний

		координаційний центр кібербезпеки при РНБО України
Департамент кіберполіції Національної поліції України	Коментар: _____ _____	

Чи залучалися сторонні організації до вирішення кіберінциденту/кібератаки?

Так		Ні	
Інший CERT, CSIRT, SOC	Антивірусні компанії	Обслуговуюча компанія, інтегратор, представник вендора	Інше (вказати): _____ _____

Коментар:
_____
_____
_____
_____

Результат впливу

Витік даних	Злам (компрометація) системи	Втрата функціональності систем/сервісів	Інше (вказати): _____ _____

Від потенційного впливу кіберінциденту/кібератаки на державному рівні під загрозою

Національна безпека	Сталість економіки	Національний імідж	Функціонування Уряду
Безпека персональних даних громадян	Інше: _____		

Індикатори компрометації

Мережеві:

IP/домен/URL/User Agent	Коментар

Хостові:

Шлях/команда/сервіс/заплановане завдання/гілка реєстру	Коментар

Файлові:

Хешсума файлу	Назва файлу	Коментар
MD5(приклад): [хешсума]		

Перелік отриманих даних		
Хешсума файлу	Назва файлу	Коментар
MD5(приклад): [хешсума]		

ДОДАТОК 2. ІНФОРМАЦІЯ ВІД CSIRT для ГРУПИ КРИЗОВОЇ КОМУНІКАЦІЇ

1. Назва події (інциденту)
2. Рівень критичності
3. Мета комунікації
4. Що трапилось
5. Коли це трапилось
6. Як це трапилось
7. Що відбувається прямо зараз
8. Хто постраждав
9. Хто втягнутий (залучений)
10. Які рекомендації потрібно додати до повідомлення

ДОДАТОК 3. Перелік категорій і типів кіберінцидентів.

1. Перелік категорій кіберінцидентів розроблений на основі 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)).

2. Перелік призначений для впровадження таксономії як інструменту для обміну інформацією щодо кіберінцидентів.

3. Перелік має регулярно переглядатися з урахуванням практики його застосування, появи нових категорій і типів кіберінцидентів, а також інформації, отриманої від суб'єктів забезпечення кібербезпеки.

Код xx	**Категорія інциденту**	**Код xx**	**Тип інциденту**	**Тип інциденту англійською**	**Опис типу інциденту**
01.	Шкідливий (образливий) вміст	01	Спам	Spam	Надсилання небажаних повідомлень або великої кількості повідомлень (флуд)

	(Abusive content)				
02.	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (далі – ШПЗ)	Malware infection	У системі виявлено ШПЗ.
		02	Розповсюдження ШПЗ	Malware distribution	Розповсюдження ШПЗ, наприклад шляхом розсилки повідомлень електронної пошти, що містятять вкладення з шпз або посилання на його завантаження.
		03	Командно-контрольний центр (C2)	Command & Control (C2)	Система, яка використовується як точка керування та управління ботнетом та/або служить точкою для збору інформації, викраденої ботнетами.
		04	Шкідливе підключення	Malicious connection	Спроби з’єднання від/до IP/URL - адреси, пов'язаної з відомим ШПЗ, наприклад C2C або ресурсом розповсюдження компонентів, пов’язаних із активністю певної бот-мережі.
03.	Збір інформації зловмисником (Information Gathering)	01	Сканування	Scanning	Збір інформації про системи або мережі.
		02	Сніфінг	Sniffing	Несанкціоноване перехоплення (логічне або фізичне) та аналіз мережевого трафіку. Несанкціонований моніторинг та зчитування мережевого трафіку.

		03	Фішинг	Phishing	Спроба збору інформації про користувача чи систему за допомогою методів соціальної інженерії (масова розсилка електронною поштою спрямована на збір даних, може містити посилання на фішингові сайти)
04.	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості	Vulnerability exploitation attempt	Спроба вторгнення з використанням вразливості у системі, компоненті чи мережі
		02	Спроби авторизації/входу в систему	Login attempts	Спроба входу до служб або механізмів автентифікації / доступу. Невдала спроба підбору автентифікаційних даних чи використання раніше скомпрометованих вже не актуальних даних.
05.	Втручання (Intrusion)	01	Компрометація облікового запису	Account compromise	Фактичне вторгнення в систему, компонент або мережу шляхом компрометації облікового запису користувача або адміністратора
		02	Компрометація системи	System compromise	Фактичне вторгнення в систему чи її компоненту, сервісу, застосунку через використання вразливості в компоненті або мережі. Несанкціонований доступ до системи або компоненту в обхід

					системи контролю доступу.
06.	Порушення доступності (Availability)	01	Атака на відмову в обслуговуванні	DoS/DDoS	Вплив на нормальне функціонування системи чи сервісу що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів.
		02	Саботаж / шкідливі дії	Sabotage	Дії (навмисні або ненавмисні), спрямовані на пошкодження системи, переривання процесів, зміну або видалення інформації тощо.
		03	Збій	Outage, no malice	Збій в роботі системи чи її компоненту без зловмисного втручання.
07.	Порушення властивостей інформації (Information Content Security)	01	Несанкціонований доступ до інформації	Unauthorised access to information	Несанкціонований доступ до інформації. Несанкціонований обмін конкретним набором інформації.
		02	Несанкціонована модифікація	Unauthorised modification of info	Несанкціонована зміна або видалення певного набору інформації.
08.	Шахрайство (Fraud)	01	Шахрайський сайт	Fraudulent site	Створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів. Використання ресурсів установи для цілей, відмінних від передбачуваних.

09.	Відома вразливість (Vulnerable)	01	Вразливість	Vulnerability	Наявність в системі чи її компонентах відомих вразливостей, відкритих для експлуатації
		02	Некоректна конфігурація	Misconfiguration	Недоліки в налаштуваннях, що можуть бути використані зловмисником (налаштування за замовчуванням тощо)
10.	Інше (Other)	01	Невизначений інцидент	Undetermined incident	Недостатньо даних для обробки інциденту

Директор Департаменту цифрових трансформацій в охороні здоров'я **В'ячеслав ДІДКІВСЬКИЙ**