Порядок захисту персональних даних

Назва Закладу **Політика інформаційної безпеки**	
Назва: Порядок захисту персональних даних	**Для ЗОЗ 1 і 2 категорії**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Затверджено: ПІБ керівника ЗОЗ**

Розроблено в рамках проекту HRS (Health Reform Support).

Порядок захисту персональних даних

НАЗВА ЗОЗ

ДАТА ОСТАНЬОЇ РЕДАКЦІЇ

25.04.2023

ДОКУМЕНТ ЗАТВЕРДЖЕНО

Прізвище ім’я та по батькові керівника ЗОЗ

Підпис

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Визначення

Відповідно до Закону України «Про інформацію», інформація з обмеженим доступом класифікується, як конфіденційна, таємна та службова. **Персональні дані** відносяться до класу конфіденційної інформації з обмеженим доступом і включають у себе відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Прикладом персональних даних у ЗОЗ є усі особисті дані про стан здоров'я фізичної особи, а також дані, які чітко та тісно пов'язані з даними про стан здоров'я і генетичними даними.

В свою чергу дані про стан здоров'я особи є **медичною інформацією** про особу, що містить не лише свідчення про стан здоров'я, а й про історію її хвороби, про запропоновані дослідження і лікувальні заходи, прогноз можливого розвитку захворювання, в тому числі і про наявність ризику для життя і здоров'я.

Лікарська таємниця – це таємниця про стан здоров'я особи; факт звернення за медичною допомогою; діагноз; інші відомості, одержані при медичному обстеженні особи.

МІ – медична інформація.

Актив – матеріальні та нематеріальні об'єкти або інформація, що мають цінність для ЗОЗ.

ВІБ – відповідальний за інформаційну безпеку, призначена особа, яка відповідає за впровадження та дотримання Політики інформаційної безпеки в закладі охорони здоров'я. У разі неможливості призначити окремого відповідального за інформаційну безпеку, його функцію виконує керівник закладу.

ЗОЗ – заклад охорони здоров'я.

Зовнішні носії інформації – компакт-диски, DVD-диски, дискети, флешки, USB, флеш-накопичувачі, касети та інші.

ІБ - Інформаційна безпека, це процес, який забезпечує збереження визначених Політикою безпеки властивостей інформації та спрямований на запобігання несанкціонованим діям в інформаційній системі, що включає сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи інформаційної системи.

Керівник – керівник закладу охорони здоров'я.

Користувач - будь-яка особа зі складу персоналу ЗОЗ, уповноважена на доступ до певного інформаційного ресурсу.

ПД – персональні дані.

ПІБ – Політика інформаційної безпеки, це центральний, програмний документ, який визначає основні засади забезпечення належного рівня інформаційної безпеки закладу охорони здоров'я.

Персонал – всі працівники ЗОЗ, які використовують інформаційні ресурси закладу, комп'ютерне, телекомунікаційне і офісне обладнання відповідно до своїх посадових обов’язків.

Інші терміни, що вживаються у цьому Порядку, застосовуються в значеннях, визначених чинним законодавством України.

1.2. Затвердження та застосування документу

Цей документ визначає порядок обробки персональних даних в *[Назва ЗОЗ]*. Порядок затверджується керівником ЗОЗ та зберігається у відповідального за інформаційну безпеку ЗОЗ. У разі неможливості призначити окремого відповідального за обробку ПД, функцію відповідального за порядок роботи з персональними даними виконує призначена особа зі складу персоналу ЗОЗ.

З цим документом повинні бути ознайомлені та дотримуватися його всі штатні та тимчасові працівники в усіх місцях (на робочому місці, в будівлі ЗОЗ чи працюючи віддалено), які є працюють з ПД в ЗОЗ, а також підрядники – постачальники послуг, які працюють з ПД в ЗОЗ.

2. ПЕРСОНАЛЬНІ ДАНІ У ЗАКЛАДАХ ОХОРОНИ ЗДОРОВ’Я

2.1. Мета та підстави для обробки даних

I. Обробка ПД здійснюється в цілях охорони здоров’я з метою:

1) встановлення медичного діагнозу,
2) забезпечення піклування чи лікування або надання медичних послуг,
3) моніторингу відповідності встановленим умовам надання таких послуг (у тому числі умовам договорів про медичне обслуговування населення та договорів про реімбурсацію за програмою медичних гарантій),
4) функціонування електронної системи охорони здоров’я.

Обов’язковою умовою обробки ПД в зазначених цілях є те, що такі дані обробляються медичним працівником, фахівцем з реабілітації або іншою особою закладу охорони здоров’я, реабілітаційного закладу чи фізичною особою - підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов’язки щодо забезпечення захисту персональних даних та поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, працівниками закладу, що здійснює державний санітарно-епідеміологічний нагляд та діяльність у галузі громадського здоров’я, який одержав ліцензію на провадження господарської діяльності з медичної практики, на яких покладено обов’язки щодо забезпечення захисту персональних даних.

II. Обробка ПД для цілей інших, ніж передбачені у п. I вище, (наприклад, маркетинг, розсилка, пропонування додаткових послуг або поширення даних з фармацевтичними компаніями, тощо) повинна здійснюватися на інших підставах, передбачених Законом України «Про захист персональних даних». Наприклад, за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних. Приклад такої Згоди наведено у Додатку 1 цього документу.

III. Обробка ПД може також здійснюватися і на інших підставах, передбачених статтями 7 та 11 Закону України «Про захист персональних даних».

2.2. Категорії суб’єктів ПД

Суб’єктом ПД - є фізична особа, персональні дані якої обробляються.

Для мети визначеній у цьому порядку, ЗОЗ здійснює обробку ПД пацієнтів - осіб, які звернулись за медичною та/або реабілітаційною допомогою або медичною послугою та/або яким така допомога або послуга надається.

2.3. Склад ПД

Перелік ПД, які обробляє медичний працівник:

1) паспортні дані;
2) індивідуальний податковий номер;
3) контактний телефон;
4) адреса електронної пошти;
5) адреса реєстрації та фактичного проживання;
6) історія відвідування медичних працівників ЗОЗ:
7) історія хвороби пацієнта.

Перелік ПД, які використовуються у МІС:

1) -
2) -

2.4. Використання персональних даних

Використання персональних даних передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта персональних даних чи відповідно до закону.

Обробка персональних даних, це будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних у тому числі з використанням інформаційних (автоматизованих) систем.

Використання персональних даних медичними працівниками ЗОЗ, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених ст. 10 Закону України «Про захист персональних даних. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, встановлених законом.

2.5. Відповідальність за обробку ПД в рамках ЗОЗ

Відповідно до закону України «Про захист персональних даних» порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом. Відповідальність за впровадження процедури роботи з персональними даними у *[Назва ЗОЗ]* несе керівник закладу. Контроль за дотриманням персоналом порядку ПД покладається на відповідального за ІБ або призначену особу зі складу персоналу *[Назва ЗОЗ]*. Особисту відповідальність за обробку, зберігання персональних даних пацієнта несе медичний працівник закладу охорони здоров’я, який безпосередньо здійснює обробку персональних даних.

3. ПОРЯДОК ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. Порядок доступу до ПД осіб, які здійснюють обробку

Відповідно до Законодавства України встановлено обмеження щодо того, хто і в яких випадках може обробляти дані, що стосуються здоров'я. Лише медичні працівники, фахівці з реабілітації або інші працівники ЗОЗ, реабілітаційного закладу на яких покладено обов'язки щодо забезпечення захисту персональних даних та поширюється дія законодавства про лікарську таємницю, та якщо обробка таких даних про здоров'я пацієнта необхідна для мети, передбаченої у п. 2.1 цього документу.

3.2. Вимоги при обробці ПД

Основною вимогою до всіх осіб, які здійснюють обробку персональних даних - є забезпечення належного захисту персональних даних з метою виключення можливості отримання ПД третіми особами, які не мають мати доступ до персональних даних, не отримали такі дані та персональні дані не були знищені або втрачені. Вимоги захисту персональних даних наведено у 4 розділі цього Порядку.

I.3. Спосіб збору, накопичення ПД

Збір ПД пацієнтів здійснюється шляхом підписання декларації про вибір лікаря, який надає первинну медичну допомогу, з пацієнтом.

I.4. Строк та умови зберігання ПД

Персональні дані пацієнтів ЗОЗ обробляються, зберігаються, передаються та у разі потреби знищуються безпечним способом відповідно до вимог Закону «Про захист інформації в інформаційно-телекомунікаційних системах».

Строк зберігання ПД та медичної інформації пацієнта визначається визначаються відповідно до законодавства, наданої згоди на обробку ПД, але відповідні дані не можуть зберігатися більше 75 років відповідно з Переліком документів з кадрових питань, затвердженим наказом Мін'юсту від 12.04.2012 р. №578/5 та не перевищує строк, необхідний для реалізації мети обробки та строк, визначений законодавством України у сфері архівної справи та діловодства..

I.5. Умови та процедура зміни, видалення або знищення ПД

Зміна ПД здійснюється за наступних підстав:

1) за вмотивованою вимогою пацієнта;
2) зі згоди пацієнта;
3) за приписом Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини;
4) за рішенням суду, що набрало законної сили;

5) інших підстав, передбачених законодавством України.

Зміна персональних даних, які не відповідають дійсності, проводиться невідкладно з моменту встановлення невідповідності.

Видалення або знищення ПД вчиняється у разі:

1) закінчення строку зберігання даних;
2) видання відповідного припису Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини;
3) набрання законної сили рішенням суду щодо видалення або знищення персональних даних.
4) інших підстав, передбачених законодавством України.

I.6. Умови та процедура передачі ПД третім особам

Товариство не передає ПД третім особам, за винятком випадків, передбачених законодавством України.

Порядок та умови надання доступу до ПД третім особам регулюються статтями 16 та 17 Закону України «Про захист персональних даних».

I.7. Процедура збереження інформації про операції, пов'язані з обробкою ПД та доступом до них

ЗОЗ веде облік операцій, пов'язаних з обробкою ПД суб'єкта та доступом до них, згідно до вимог чинного законодавства.

ЗОЗ самостійно визначає процедуру збереження інформації про операції, пов'язані з обробкою ПД пацієнтів та доступом до них. У випадку обробки ПД за допомогою автоматизованої системи така система автоматично фіксує вказану інформацію.

I.8. Права суб'єкта ПД

ЗОЗ забезпечує дотримання прав суб'єкта персональних даних, передбачених статтею 8 Закону України «Про захист персональних даних», а саме:

1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) власника чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;
2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються Ваші персональні дані;
3) на доступ до своїх персональних даних;
4) отримувати не пізніш як за тридцять календарних днів (30) з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються Ваші персональні дані, а також отримувати зміст таких персональних даних;

5) пред’являти вмотивовану вимогу власнику персональних даних із запереченням проти обробки своїх персональних даних;
6) пред’являти вмотивовану вимогу щодо зміни або видалення своїх персональних даних будь-яким власником та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
7) на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв’язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;
8) звертатися із скаргами на обробку своїх персональних даних до Уповноваженого Верховної Ради України з прав людини або до суду;
9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;
10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;
11) відкликати згоду на обробку персональних даних;
12) знати механізм автоматичної обробки персональних даних;
13) на захист від автоматизованого рішення, яке має для нього правові наслідки.

4. ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Захист персональних даних – це комплекс заходів, спрямованих на запобігання випадкової втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Персональні дані залежно від способу їх відтворення/відображення/зберігання (паперові або електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

Володілець та розпорядник ПД зобов’язані вживати заходів, щоб забезпечити захист ПД на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів, а також самостійно визначати перелік і склад заходів, спрямованих на безпеку обробки ПД, з урахуванням вимог законодавства у сферах захисту ПД та інформаційної безпеки.

4.1. Заходи захисту ПД:

Для забезпечення безпеки обробки ПД виконуються наступні заходи з захисту ПД:

- забезпечення порядку видачі, контролю та відчуження доступу до персональних даних та медичної інформації відповідно до п. 4-9 затвердженої *Політики контролю доступу* Назва ЗОЗ;
- виконання заходів безпеки з обмеження фізичного доступу до ПД та МІ визначені в розділі “ФІЗИЧНА БЕЗПЕКА” *Політики інформаційної безпеки* Назва ЗОЗ;
- доступ та дії, що пов’язані з обробкою ПД, записуються в журнал обліку подій (логування) та забезпечуються засобами МІС;
- ПД та МІ при обробці та передачі засобами поза МІС шифруються відповідно до *Політики криптографічного захисту* Назва ЗОЗ;
- під час роботи з ПД та МІС обов'язково використовуються ресурси мережі Назва ЗОЗ, що застосовуються відповідно до *Політики використання мереж і послуг мережі* та *Процедури управління віддаленим доступом* Назва ЗОЗ;
- проводиться регулярне навчання співробітників, які працюють з персональними даними, раз на квартал.

4.2. Порядок дій на випадок надзвичайних подій з ПД

Порядок дій працівників Назва ЗОЗ на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій.

У випадку **виявлення ознак несанкціонованого доступу до персональних даних**:

- припинити обробку персональних даних;
- змінити пароль доступу до облікового запису.
- відключити комп’ютер від мережі Інтернет;
- звернутися до ІБ з метою блокування доступу до облікового запису;
- повідомити безпосереднього керівника, відповідальну особу, що організує роботу, пов’язану із захистом ПД у Назва ЗОЗ;

У випадку **зараження програмного забезпечення та носіїв інформації комп’ютерними вірусами**:

- негайно припинити обробку персональних даних;
- відключити комп'ютер від мережі Інтернет та ІТ мережі Назва ЗОЗ;
- повідомити ІБ про подію;
- повідомити безпосереднього керівника.

У випадку **вчинення випадкових та/або помилкових дій, що можуть призвести до втрати, зміни, поширення, розголошення ПД та МІ тощо**:

- припинити обробку персональних даних;
- повідомити ІБ про подію;
- повідомити безпосереднього керівника.

У випадку **відмови та/або збою програмного забезпечення, за допомогою якого здійснюється обробка ПД та МІ**:

- припинити обробку персональних даних;
- повідомити ІБ про подію;
- повідомити безпосереднього керівника.

У випадку **виявлення пошкодження, втрати, викрадення документа або іншого носія ПД та МІ**:

- припинити обробку персональних даних;
- повідомити ІБ про подію;
  повідомити безпосереднього керівника.

4.3. Порядок дій відповідального за ІБ у разі отримання повідомлення про інцидент ІБ з ПД

Порядок дій відповідального за ІБ у разі отримання повідомлення про інцидент ІБ з ПД визначається Порядком взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти / кібератаки та складається з наступних етапів:

1. 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.
2. Визначає рівень критичності кіберінциденту залежно від ступеня негативних наслідків, що можуть настати в результаті реалізації кіберінциденту/кібератаки (білий, зелений, жовтий, помаранчевий, червоний, чорний).
3. У разі наявності відповідного відомчого або галузевого (секторального) центру кібербезпеки (кіберзахисту), до сфери відповідальності якого належить заклад, здійснює інформування, передбачене пунктом 4 розділу II Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти / кібератаки. При наявності, такий алгоритм взаємодії (інформування) додатково врегулюється відомчим розпорядчим документом.
4. Виконує технічний план реагування на кіберінциденти/кібератаки.
5. 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 ПОВІДОМЛЕННЯ ПРО КІБЕРІНЦИДЕНТ/КІБЕРАТАКУ (Додаток 3).

6. 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.
7. Інформує Національний координаційний центр кібербезпеки через офіційну електронну поштову скриньку report@ncscc.gov.ua та Групу кризової комунікації про вирішення кіберінциденту.
8. 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 ПОВІДОМЛЕННЯ ПРО КІБЕРІНЦИДЕНТ/КІБЕРАТАКУ (Додаток 3).

9. Забезпечує унеможливлення порушення цілісності доказової бази.
10. 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.

ДОДАТОК 1

ЗГОДА

На обробку персональних даних

Я, _____, народився (-лась)_____, паспорт серія ____ № _____, виданий _____ _____(ким, коли) як суб'єкт персональних даних (далі – Суб'єкт персональних даних, Пацієнт), шляхом підписання цього тексту, відповідно до Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI (далі – Закон), надаю згоду [*Назва ЗОЗ, адреса ЗОЗ, ідентифікаційний код юридичної особи, контактний номер телефону ЗОЗ*] (далі - ЗОЗ), на обробку персональних даних Пацієнта, що містять як загальні дані про особу (перелік загальних даних включає: прізвище, ім'я, по батькові, стать, дата народження, паспортні дані, адреса місця реєстрації, адреса місця проживання та контактні номери телефонів), так і чутливі дані, тобто такі, що стосуються стану здоров'я особи, цей перелік включає: медична інформація про особу, що містить не лише свідчення про стан здоров'я, а й про історію хвороби, запропоновані дослідження і лікувальні заходи, прогноз можливого розвитку захворювання, наявність ризику для життя і здоров'я, що включаються до Бази персональних даних ЗОЗ, яка збирається, зберігається, передається, обробляється, розповсюджується та відображається в інформаційно-телекомунікаційних системах [*Назва ЗОЗ*].

Метою обробки персональних даних є [*вказати необхідну мету*].

Розпорядником персональних даних є *[вказати необхідну інформацію: назва та адреса розпорядника персональних даних]*.

[Персональні дані передаватимуться (назва та адреса третьої особи) з метою _____.]

Згода дається на строк, необхідний для досягнення мети, зазначеної в цій згоді, і може бути відкликана за заявою, направленою володільцю персональних даних.

Обробка персональних даних на підставі цієї згоди передбачатиме такі дії, як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем розпорядником даних від імені володільця даних відповідно до Закону «Про захист персональних даних» у часових рамках, що передбачені цією згодою.

Я повідомлений(-а) та ознайомлений(-а) з моїми правами як суб'єкта персональних даних, передбаченими ст. 8 Закону України «Про захист персональних даних» та правом на відкликання цієї згоди.

_____ 202_ _____

(підпис)

ДОДАТОК 2

ПЕРЕЛІК ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІКС ДЛЯ ОБРОБКИ ПД

Нижче наведений перелік затвердженого для використання програмного забезпечення та інформаційно-комунікаційних систем, що визначені Назва ЗОЗ, як такі у яких дозволяється обробляти, зберігати та передавати ПД пацієнта.

Використання не затвердженого програмного забезпечення або інформаційно-комунікаційних систем для обробки ПЗ заборонено.

ПЗ/ІКС	Версія	Затверджено	Дата	Опис/Коментарі

ДОДАТОК 3

ПОВІДОМЛЕННЯ ПРО КІБЕРІНЦИДЕНТ/КІБЕРАТАКУ

1. Тип кіберінциденту/кібератаки (відповідно до таксономії кіберінцидентів).
2. Рівень критичності кіберінциденту/кібератаки.
3. Короткий опис (контекст).
4. Попередня оцінка: кібератака чи кіберінцидент?
5. Хто виявив (підрозділ, посадова особа, контактні дані)?
6. Перелік суб’єктів, яких поінформовано про кіберінцидент/кібератаку.
7. Позначка «Потрібна допомога в реагуванні» або «Допомога в реагуванні не потрібна».