ОПИТУВАЛЬНА АНКЕТА

_____

назва заявника

для оцінки діючої в організації системи управління інформаційною безпекою на відповідність вимогам стандарту ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги»

1. Керівний склад: вище керівництво, відповідальний за систему управління інформаційною безпекою

Посада	Прізвище, ім'я та по-батькові	Телефон

3. Кількість змін: _____

4. Дні та часи роботи:_____

5. Кількість видів діяльності за КВЕД:

_____

6. Кількість персоналу задіяні у виробництві/наданні послуг:_____

7. Сфера застосування системи управління інформаційною безпекою:

_____

8. Дата останнього аналізування системи управління інформаційною безпекою з боку вищого керівництва:_____

9. Дата останнього внутрішнього аудиту: _____

10 Відомості за останній рік про наявність та кількість скарг, претензій чи рекламацій замовників і споживачів та недотримання законодавчих і нормативних вимог:_____

11. Документи системи управління інформаційною безпекою, які додаються:

_____

12. Інформація на відповідність системи управління інформаційною безпекою вимогам стандарту ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT):

Номер пункту стандарту ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT)	Вказати номер та пункт документу, який реалізує вимогу стандарту
4 КОНТЕКСТ ОРГАНІЗАЦІЇ	
4.1 Розуміння організації та її контексту	
Організація повинна визначити зовнішні та внутрішні чинники, які мають відношення до мети її діяльності та впливають на її здатність досягти наміченого результату (результатів) її системи управління інформаційною безпекою. *ПРИМІТКА Визначення цих питань, які стосуються встановлення зовнішнього та внутрішнього контексту організації розглядається в пункті 5.4.1 ISO 31000:2018*	
4.2 Розуміння потреб та очікувань зацікавлених сторін	
Організація повинна визначити: a) зацікавлені сторони, які мають відношення до системи управління інформаційною безпекою; b) відповідні вимоги цих зацікавлених сторін; c) які з цих вимог будуть вирішені через систему управління інформаційною безпекою. *ПРИМІТКА. Вимоги зацікавлених сторін можуть включати правові та нормативні вимоги та договірні зобов'язання.*	
4.3 Визначення сфери застосування системи управління інформаційною безпекою	
Організація повинна визначити межі та застосовність системи управління інформаційною безпекою, щоб встановити сферу її застосування. Визначаючи цей обсяг, організація повинна враховувати: a) зовнішні та внутрішні питання, зазначені в 4.1; b) вимоги, зазначені в 4.2; c) інтерфейси та залежності між діяльністю, що виконується організацією, та діяльністю, що виконується іншими організаціями. Обсяг має бути доступним як документована інформація.	
4.4 Система управління інформаційною безпекою	
Організація повинна створити, запровадити, підтримувати та постійно вдосконалювати систему управління інформаційною безпекою, включаючи необхідні процеси та їх взаємодію, відповідно до вимог цього стандарту.	
5 КЕРІВНИЦТВО	
5.1 Лідерство та відданість справі	
Найвище керівництво має продемонструвати лідерство та відданість системі управління інформаційною безпекою шляхом: a) забезпечення впровадження політики інформаційної безпеки та цілей інформаційної безпеки та їх сумісності зі стратегічним напрямком організації; b) забезпечення інтеграції вимог системи управління інформаційною безпекою в процеси організації; c) забезпечення наявності ресурсів, необхідних для системи управління інформаційною безпекою;	

d) інформування про важливість ефективного управління інформаційною безпекою та дотримання вимог системи управління інформаційною безпекою; e) забезпечення того, що система управління інформаційною безпекою досягає запланованих результатів; f) спрямування та підтримка осіб для сприяння ефективності системи управління інформаційною безпекою; g) сприяння постійному вдосконаленню; і h) підтримка інших відповідних управлінських ролей, щоб продемонструвати їхнє лідерство, оскільки це стосується їхніх сфер відповідальності. *ПРИМІТКА. Посилання на «бізнес» у цьому документі можна тлумачити широко як означати ту діяльність, яка є основою для цілей існування організації.*	
5.2 Політика	
Найвище керівництво має встановити політику інформаційної безпеки, яка: a) відповідає меті організації; b) включає цілі інформаційної безпеки (див 6.2) або забезпечує основу для встановлення цілей інформаційної безпеки; c) містить зобов'язання задовольнити застосовні вимоги щодо інформаційної безпеки; d) містить зобов'язання щодо постійного вдосконалення системи управління інформаційною безпекою. Політика інформаційної безпеки: a) бути доступною як документована інформація; b) комунікувати всередині організації; c) бути доступним для зацікавлених сторін, якщо це доречно.	
5.3 Організаційні ролі, відповідальності та повноваження	
Найвище керівництво має гарантувати, що відповідальність і повноваження для ролей, пов'язаних з інформаційною безпекою, розподіляються та повідомляються в організації. Найвище керівництво призначає відповідальність і повноваження для: a) забезпечення відповідності системи управління інформаційною безпекою вимогам цього документа; b) звітування про ефективність системи управління інформаційною безпекою перед вищим керівництвом. *ПРИМІТКА. Найвище керівництво також може призначати відповідальність і повноваження для звітування про ефективність системи управління інформаційною безпекою в організації.*	
Примітка. Вище керівництво може також призначити відповідальності та повноваження для звітування щодо результативності системи управління інформаційною безпекою в межах організації	
6 ПЛАНУВАННЯ	
6.1 Дії щодо ризиків та можливостей	
6.1.1 Загальні положення	

Під час планування системи управління інформаційною безпекою організація повинна враховувати питання, зазначені в 4.1 та вимоги, зазначені в 4.2 і визначте ризики та можливості, на які необхідно звернути увагу: a) гарантувати, що система управління інформаційною безпекою може досягти запланованих результатів; b) запобігання або зменшення небажаних ефектів; c) досягти постійного вдосконалення. Організація планує: d) дії щодо усунення цих ризиків і можливостей; e) як 1) інтегрувати та впроваджувати дії в процеси системи управління інформаційною безпекою; і 2) оцінити ефективність цих дій.	
6.1.2 Оцінка ризиків інформаційної безпеки	
Організація повинна визначити та застосувати процес оцінки ризиків інформаційної безпеки, який: a) встановлює та підтримує критерії ризику інформаційної безпеки, які включають: 1) критерії прийнятності ризику; і 2) критерії виконання оцінки ризиків інформаційної безпеки; b) гарантує, що повторні оцінки ризиків інформаційної безпеки дають узгоджені, достовірні та порівнювані результати; c) визначає ризики інформаційної безпеки: 1) застосовувати процес оцінки ризиків інформаційної безпеки для виявлення ризиків, пов'язаних із втратою конфіденційності, цілісності та доступності інформації в межах системи управління інформаційною безпекою; і 2) визначити власників ризиків; d) аналізує ризики інформаційної безпеки: 1) оцінити можливі наслідки, які можуть виникнути, якщо виявлені ризики в 6.1.2 в) 1) мали матеріалізуватися; 2) оцінити реалістичну ймовірність виникнення ризиків, визначених у 6.1.2 в) 1); і 3) визначити рівні ризику; e) оцінює ризики інформаційної безпеки: 1) порівняти результати аналізу ризику з критеріями ризику, встановленими в 6.1.2 а); і 2) визначити пріоритетність проаналізованих ризиків для лікування ризиків. Організація повинна зберігати задокументовану інформацію про процес оцінки ризиків інформаційної безпеки.	
6.1.3 Керування ризиками інформаційної безпеки	
Організація повинна визначити та застосувати процес обробки ризиків інформаційної безпеки для: a) вибрати відповідні варіанти управління ризиками інформаційної	

безпеки з урахуванням результатів оцінки ризиків; b) визначити всі засоби контролю, необхідні для реалізації вибраного варіанта(ів) обробки ризиків інформаційної безпеки; ПРИМІТКА 1. Організації можуть розробляти засоби контролю за потребою або ідентифікувати їх із будь-якого джерела. c) порівняти елементи керування, визначені в 6.1.3 б) вище з тими в Додаток А і перевірити, чи не було пропущено жодного необхідного контролю; ПРИМІТКА 2 Додаток А містить список можливих заходів безпеки інформації. Користувачі цього документа спрямовані на Додаток А щоб гарантувати, що жодні необхідні засоби контролю інформаційної безпеки не будуть упущені. ПРИМІТКА 3. Засоби керування інформаційною безпекою, перелічені в Додаток А не є вичерпними, і за потреби можна включити додаткові засоби контролю безпеки інформації. d) підготувати заяву про застосовність, яка містить: - необхідні засоби контролю (див 6.1.3 б) і в)); - обґрунтування їх включення; - чи впроваджено необхідні засоби контролю чи ні; і - обґрунтування виключення будь-якого з Додаток А елементи керування. e) сформулювати план обробки ризиків інформаційної безпеки; і f) отримати схвалення власників бізнес процесів ризиків щодо плану обробки ризиків інформаційної безпеки та прийняття залишкових ризиків інформаційної безпеки. Організація повинна зберігати задокументовану інформацію про процес обробки ризиків інформаційної безпеки. *ПРИМІТКА 4. Оцінка ризику інформаційної безпеки та процес обробки в цьому документі узгоджується з принципами та загальними рекомендаціями, наданими в ISO 31000*	
6.2 Цілі інформаційної безпеки та планування їх досягнення	
Організація повинна встановити цілі інформаційної безпеки на відповідних функціях і рівнях. Цілі інформаційної безпеки: a) відповідати політиці інформаційної безпеки; b) бути вимірюваною (якщо можливо); c) брати до уваги застосовні вимоги до інформаційної безпеки та результати оцінки та обробки ризиків; d) підлягати моніторингу; e) бути в комунікації; f) оновлюватися відповідно; g) документована інформація має бути доступною Організація повинна зберігати задокументовану інформацію про цілі інформаційної безпеки. Плануючи, як досягти цілей інформаційної безпеки, організація повинна визначити: h) що буде зроблено;	

i) які ресурси будуть потрібні; j) хто відповідатиме; k) коли він буде завершений; і l) як будуть оцінюватися результати.	
6.3 Планування змін	
Коли організація визначає необхідність внесення змін до системи управління інформаційною безпекою, зміни повинні проводитися в плановому порядку.	
7 ПІДТРИМКА	
7.1 Ресурси	
Організація повинна визначити та забезпечити ресурси, необхідні для створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою.	
7.2 Компетентність	
Організація повинна: a) визначити необхідну компетенцію особи (осіб), яка виконує роботу під його контролем, що впливає на ефективність його інформаційної безпеки; b) забезпечити, щоб ці особи були компетентними на основі відповідної освіти, підготовки або досвіду; c) у відповідних випадках вживати заходів для набуття необхідної компетентності та оцінювати ефективність вжитих дій; і d) зберігати відповідну задокументовану інформацію як доказ компетентності. *ПРИМІТКА. Застосовні дії можуть включати, наприклад: забезпечення навчання, наставництво або перепризначення поточних працівників; або найм або контракт з компетентними особами.*	
7.3 Обізнаність	
Особи, які виконують роботу під контролем організації, повинні знати: a) політика інформаційної безпеки; b) їхній внесок в ефективність системи управління інформаційною безпекою, включаючи переваги покращених характеристик інформаційної безпеки; і c) наслідки невідповідності вимогам системи управління інформаційною безпекою.	
7.4 Комунікація	
Організація повинна визначити потребу у внутрішніх і зовнішніх комунікаціях, що стосуються системи управління інформаційною безпекою, включаючи: a) про що спілкуватися; b) коли спілкуватися; c) з ким спілкуватися; d) як спілкуватися.	
7.5 Документально підтверджена інформація	
7.5.1 Загальні положення	

Система управління інформаційною безпекою організації повинна включати: a) документально підтверджену інформацію, яка вимагається цим стандартом; і b) документовану інформацію, визначену організацією як необхідна для ефективності системи управління інформаційною безпекою. *ПРИМІТКА Обсяг документованої інформації для системи управління інформаційною безпекою може відрізнятися від однієї організації до іншої через:* *1) розмір організації та тип її діяльності, процеси, продукти та послуги;* *2) складність процесів та їх взаємодії; і* *3) компетентність осіб.*	
7.5.2 Створення та оновлення	
Під час створення та оновлення документованої інформації організація повинна забезпечити належне: a) ідентифікація та опис (наприклад, назва, дата, автор або номер посилання); b) формат (наприклад, мова, версія програмного забезпечення, графіка) та носії (наприклад, папір, електронний); і c) перевірка та затвердження на придатність та адекватність.	
7.5.3 Контроль документованої інформації	
Задокументована інформація, яка вимагається системою управління інформаційною безпекою та цим документом, контролюється для забезпечення: a) він доступний і придатний для використання, де і коли це необхідно; і b) він належним чином захищений (наприклад, від втрати конфіденційності, неналежного використання або втрати цілісності). Для контролю за задокументованою інформацією організація повинна здійснювати наступні види діяльності, у відповідних випадках: c) поширення, доступ, пошук і використання; d) зберігання та збереження, включаючи збереження розбірливості; e) контроль змін (наприклад, контроль версій); і f) утримання та розпорядження. Задокументована інформація зовнішнього походження, визначена організацією як необхідна для планування та функціонування системи управління інформаційною безпекою, має ідентифікуватися як відповідна та контролюватися. *ПРИМІТКА Доступ може означати рішення щодо дозволу переглядати лише задокументовану інформацію або дозвіл і повноваження переглядати та змінювати задокументовану інформацію тощо.*	
8 ФУНКЦІОНУВАННЯ	
8.1 Оперативне планування та контроль	

Організація повинна планувати, впроваджувати та контролювати процеси, необхідні для виконання вимог, а також для виконання дій, визначених у розділі 6, шляхом: — встановлення критеріїв для процесів; — здійснення контролю процесів відповідно до критеріїв. Задокументована інформація має бути доступною в обсязі, необхідному для впевненості в тому, що процеси виконувалися за планом. Організація повинна контролювати заплановані зміни та переглядати наслідки ненавмисних змін, у разі потреби вживаючи заходів для пом'якшення будь-яких негативних наслідків. Організація повинна забезпечити контроль процесів, продуктів або послуг, що надаються зовні, які мають відношення до системи управління інформаційною безпекою.	
8.2 Оцінювання ризиків інформаційної безпеки	
Організація повинна виконувати оцінювання ризиків інформаційної безпеки через заплановані проміжки часу або коли пропонуються або відбуваються значні зміни, беручи до уваги критерії, встановлені в 6.1.2 a). Організація повинна зберігати задокументовану інформацію про результати оцінювання ризиків інформаційної безпеки.	
8.3 Оброблення ризиків інформаційної безпеки	
Організація повинна впровадити план оброблення ризиків інформаційної безпеки. Організація повинна зберігати задокументовану інформацію стосовно результатів оброблення ризиків інформаційної безпеки.	
9 ОЦІНЮВАННЯ РЕЗУЛЬТАТИВНОСТІ	
9.1 Моніторинг, вимірювання, аналіз та оцінювання	
Організація повинна визначити: a) що потрібно контролювати та вимірювати, включаючи процеси та засоби контролю інформаційної безпеки; b) методи моніторингу, вимірювання, аналізу та оцінки, якщо це застосовно, для забезпечення дійсних результатів. Вибрані методи повинні давати порівнювані та відтворювані результати, щоб вважатися дійсними; c) коли буде здійснюватися моніторинг та вимірювання; d) хто буде контролювати та вимірювати; e) коли результати моніторингу та вимірювання повинні бути проаналізовані та оцінені; f) який має проаналізувати та оцінити ці результати. Задокументована інформація має бути доступною як доказ результатів. Організація повинна оцінити ефективність інформаційної безпеки та ефективність системи управління інформаційною безпекою.	
9.2 Внутрішній аудит	
9.2.1 Загальні положення	

Організація повинна проводити внутрішні аудити через заплановані проміжки часу, щоб надати інформацію про те, чи система управління інформаційною безпекою: a) відповідає 1) власні вимоги організації до її системи управління інформаційною безпекою; 2) вимоги цього документа; b) ефективно впроваджується та підтримується.	
9.2.2 Програма внутрішнього аудиту	
Організація повинна планувати, створювати, впроваджувати та підтримувати програму(и) аудиту, включаючи частоту, методи, відповідальність, вимоги до планування та звітність. Розробляючи програму(и) внутрішнього аудиту, організація повинна враховувати важливість відповідних процесів і результати попередніх аудитів. Організація повинна: a) визначити критерії аудиту та обсяг для кожного аудиту; b) відбирати аудиторів і проводити аудити, які забезпечують об'єктивність і неупередженість процесу аудиту; c) забезпечити донесення до відповідного керівництва результатів аудитів; Задокументована інформація має бути доступною як доказ виконання програми(ів) аудиту та результатів аудиту.	
9.3 Перегляд з боку керівництва	
9.3.1 Загальні положення	
Найвище керівництво повинно переглядати систему управління інформаційною безпекою організації через заплановані проміжки часу, щоб переконатися в її постійній придатності, адекватності та ефективності.	
9.3.2 Вхідні дані для аналізу керівництва	
Аналіз керівництва повинен включати розгляд: a) статус дій з попередніх оглядів керівництва; b) зміни зовнішніх і внутрішніх питань, які мають відношення до системи управління інформаційною безпекою; c) зміни в потребах та очікуваннях зацікавлених сторін, що мають відношення до системи управління інформаційною безпекою; d) відгуки про ефективність інформаційної безпеки, включаючи тенденції в: 1) невідповідності та коригувальні дії; 2) результати моніторингу та вимірювань; 3) результати аудиту; 4) виконання завдань інформаційної безпеки; e) відгуки зацікавлених сторін; f) результати оцінки ризику та статус плану лікування ризику; g) можливості для постійного вдосконалення.	
10 ПОЛІПШЕННЯ	

10.1 Постійне вдосконалення	
Організація повинна постійно покращувати придатність, адекватність та ефективність системи управління інформаційною безпекою.	
10.2 Невідповідність і коригувальні дії	
Якщо виникає невідповідність, організація повинна: a) реагувати на невідповідність і, якщо це застосовно: 1) вживати заходів щодо контролю та її виправлення; 2) боротися з наслідками; b) оцінити потребу в діях для усунення причин невідповідності, щоб вона не повторилася або виникла деінде, шляхом: 1) розгляд невідповідності; 2) визначення причин невідповідності; і 3) визначення наявності подібних невідповідностей або потенційної можливості їх виникнення; c) здійснювати будь-які необхідні дії; d) переглядати ефективність будь-яких вжитих коригувальних заходів; і e) у разі необхідності вносити зміни до системи управління інформаційною безпекою. Коригувальні дії повинні відповідати наслідкам виявлених невідповідностей. Задокументована інформація повинна бути доступна як доказ: f) характер невідповідностей та будь-які подальші вжиті дії, g) результати будь-яких коригувальних дій.	

Відповідальний за систему управління інформаційною безпекою

_____ _____

підпис Прізвище та ініціали

Керівник організації

_____ _____

підпис Прізвище та ініціали

М.П.