**Анкета щодо проведення експертизи**

| **№ з/п** | **Питання** | **Примітка** |
| --- | --- | --- |
|  | Наявність документації згідно ЕСПД (ГОСТ 19.201) |  |
|  | Наявність Політики безпеки інформації, яка повинна бути реалізована в об'єктом експертизи (ПЗ, засіб технічного захисту інформації) |  |
|  | Чи задокументовані всі етапи кожної стадії життєвого циклу ПЗ і їх граничні вимоги щодо розробки, впровадження і підтримки в роботі  |  |
|  | Наявність документованої методики щодо керування конфігураціями ПЗ на всіх стадіях її життєвого циклу |  |
|  | Наявність функціональної специфікації ПЗ, що реалізовані відповідно до політики безпеки. Конкретний опис функціонування кожного механізму, що входить до загального ПЗ, який виконує питання захисту/безпеки  |  |
|  | Наявність проекту архітектури ПЗ/ системи |  |
|  | Який вид інформації планується оброблятися в системі |  |
|  | За якими параметрами планується здійснювати захищати інформацію (конфіденційність, цілісність, доступність) |  |
|  | Яким чином реалізовано розмежування доступу до інформації (механізми) |  |
| 10. | Перелік протоколів, які використовується під час передачі інформації |  |
| 11. | Територіальне розміщення компонентів системи, їх функціональне призначення |  |
| 12.  | Які засоби криптографічного захисту інформації використовується в системі |  |
| 13. | Наявність функції самотестування в системі на предмет цілісності ядра, системних файлів, файлів конфігурацій системи |  |
| 14. | Наявність осіб відповідальних за підтримку, безпеку |  |
| 15. | Перелік платформ або наявність описаної архітектури ПЗ. (Компоненти версії, мова програмування, база даних) |  |

**Вимоги щодо отримання Експертного висновку за рівнем гарантії Г-2**

(НД ТЗІ 2.5-004-99)

1. **Архітектура**

Вимоги до архітектури забезпечують гарантії того, що КЗЗ (комплекс засобів захисту) у змозі повністю реалізувати політику безпеки:

* *КЗЗ повинен реалізовувати політику безпеки. Всі його компоненти повинні бути чітко визначені;*
1. **Середовище розробки**

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки і супроводження оцінюваної КС (комп’ютерної системи) є повністю керованими з боку Розробника.

Процес розробки

* *Розробник повинен визначити всі стадії життєвого циклу КС, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги;*

Керування конфігурацією

* *Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією КС на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми ПЗП (постійний запам'ятовуючий пристрій), вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ;*
1. **Послідовність розробки**/Функціональна специфікація
* *Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією КС на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ;*

Функціональні специфікації (модель політики безпеки)

* *Функціональні специфікації повинні включати модель політики безпеки неформалізована;*

Проект архітектури

* *На стадії розробки ескізного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення неформалізована*

Детальний проект

* *На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ неформалізована.*
1. **Середовище функціонування**

Вимоги до середовища функціонування забезпечують гарантії того, що КС поставляється Замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється Замовником так, як це передбачається Розробником:

* *Розробник повинен представити засоби інсталяції, генерації і запуску КС, які гарантують, що експлуатація КС починається з безпечного стану. Розробник повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску.*
1. **Документація**

Вимоги до документації є загальними для всіх рівнів гарантій.

У вигляді окремих документів або розділів (підрозділів) інших документів Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратору щодо послуг безпеки, настанови користувача щодо послуг безпеки.

В описі функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ оцінюваної КС, а також самі послуги.

Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску КС, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску КС, опис властивостей КС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує КС.

Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Назва документів (розділів) не регламентується. Опис послуг безпеки може відрізнятися для користувача і адміністратора. Настанови адміністратору і настанови користувачу можуть бути об'єднані в настанови з встановлення і експлуатації.