



АГЕНЦИЯ ЗА ИНФОРМАЦИОННА БЕЗОПАСНОСТ И
РАЗУЗНАВАНЕ

ПРОТОКОЛ ЗА ТЕХНИЧЕСКО КОНТРАНАБЛЮДЕНИЕ

AIBR-TSCM-P · ПУБЛИЧНА ВЕРСИЯ

Методология за физическа и електронна инспекция при откриване на скрито
наблюдателно оборудване

Издател: АИБР

Версия 1.0 · 2 септември 2026 г.

ПУБЛИЧЕН ДОКУМЕНТ · ADBIR.EU

01 · ВЪВЕДЕНИЕ

Защо съществува този стандарт

За разлика от останалите стандарти на АИБР, TSCM областта няма единен признат публичен стандарт, върху който да стъпим — тя разчита на индустриална практика и фирмена методология. AIBR-TSCM-P формализира тази практика в проверим протокол.

Различен вид документ

Докато AIBR-IVS, AIBR-MAS и AIBR-CFS оценяват **достоверността на информация**, AIBR-TSCM-P описва **процедура за физическа инспекция** — резултатът е не степен на увереност, а потвърдено наличие или отсъствие на устройство, плюс степен на покритие на самата проверка.

Стандартен обхват на индустрията

Протоколът следва утвърдената в сектора четиристепенна структура — визуална физическа инспекция, честотен анализ на радиоспектъра (обичайно 10 kHz - 24 GHz), проверка на комуникационни системи (телефонни линии, мрежа) и детекция на нелинейни възли (NLJD) за устройства в режим на изчакване.

02 · ФАЗИ НА ПРОВЕРКАТА

Шест фази на един пълен sweep

- 1 Предварителен брифинг и оценка на риска**
Определяне на зоните с приоритет и предполагаемия тип заплаха.
- 2 Физическа инспекция**
Ръчен визуален оглед на помещения, мебели, ел. фитинги и контакти.
- 3 Честотен анализ на радиоспектъра**
Сканиране за активно предаващи устройства със спектър анализатор.
- 4 Проверка на комуникационни системи**
Телефонни линии, мрежова инфраструктура, видеоконферентни системи.
- 5 Детекция на нелинейни възли (NLJD)**
Откриване на устройства дори когато са изключени или в режим на изчакване.
- 6 Доклад и предаване**
Писмен доклад с констатациите и степента на покритие на проверката.

03 · КЛАСИФИКАЦИЯ НА РЕЗУЛТАТА

Кодове на находка и покритие

КОД	НАХОДКА
F-0	Не е открито устройство
F-1	Установена аномалия, неубедителна — изисква допълнителна проверка
F-2	Потвърдено устройство — активно
F-3	Потвърдено устройство — в режим на изчакване (открито чрез NLJD)

КОД	ПОКРИТИЕ НА ПРОВЕРКАТА
S-F	Пълен sweep — всички фази изпълнени, пълен достъп
S-P	Частичен sweep — една или повече зони недостъпни
S-R	Ограничен sweep — намален обхват по искане на клиента

Защо покритието е отделен код

Резултат F-0 при ограничен sweep (S-R) не е равносилен на F-0 при пълен sweep (S-F) — прозрачността за реалния обхват на проверката е част от честността на доклада.

04 · ПРИЛОЖЕНИЕ НА ПРОТОКОЛА

Пример за маркировка и спешна реакция

S-F [Фази 1-6] F-2

Пълен sweep, всички фази изпълнени · потвърдено активно устройство

Спешна реакция при F-2/F-3

За разлика от останалите стандарти на АИБР, при потвърдено устройство клиентът се уведомява незабавно, устно — не се изчаква писмен доклад. Активно наблюдателно устройство е текущо събитие за сигурност, не архивна констатация.

За кого е предназначен протоколът

AIBR-TSCM-P се прилага при всяка проверка от услугата TSCM на АИБР. Пълните вътрешни процедури, включително оборудване и техники за верификация, са достъпни за партньори и клиенти при заявка.

Отсъствието на устройство никога не се представя като абсолютна гаранция — само като резултат от проверка с конкретно, документирано покритие.