SYSTEMY ZABEZPIECZEŃ PRZECIWINWIGILACYJNYCH

Transfarm Sp. z o.o., ul. Puławska 370, 02-819 Warszawa
tel.: +48 22 550 47 11, fax: +48 22 550 47 90, e-mail: office@transfarm.pl, nasza strona: www.transfarm.pl

XXI wiek, to wiek w którym szczególnego znaczenia nabiera bezpieczeństwo informacji. Jednocześnie jest to czas, gdy technologie zdobywania informacji rozwijają się niezwykle dynamicznie pokonując kolejne bariery miniaturyzacji oraz stosowanych metod inwigilacji elektronicznej. Urządzenia podsłuchowe, do transmisji radiowej oraz służące nagrywaniu (rejestracji) dźwięków i obrazów są z każdym dniem coraz bardziej nowoczesne i wyrafinowane. Jak więc chronić to, co w każdej instytucji jest najważniejsze? Szczególnie gdy informacja jest przekazywana w czasie spotkań z najważniejszymi współpracownikami czy klientami?

W załączeniu mamy przyjemność przedłożyć Państwu szczegółową ofertę systemów zabezpieczeń przeciwinwigilacyjnych. Nasza oferta obejmuje wykonanie kompleksowych zabezpieczeń w oparciu o najnowocześniejsze rozwiązania techniczne, a także doradztwo w dostosowaniu poszczególnych elementów zabezpieczających do indywidualnych potrzeb klienta oraz pakiet usług towarzyszących.

Spółka **TRANSFARM** jest polskim przedsiębiorstwem istniejącym nieprzerwanie od stycznia 1990 r. Siedzibą Spółki jest Warszawa. Działalność TRANSFARM Sp. z o.o. polega na zaopatrywaniu w materiały i sprzęt kryminalistyczny specjalistycznych państwowych służb zajmujących się ochroną bezpieczeństwa i porządku publicznego. TRANSFARM jest dostawcą materiałów i sprzętu kryminalistycznego m.in. dla Komendy Głównej Policji, komend wojewódzkich Policji, Straży Granicznej, Żandarmerii Wojskowej i innych służb mundurowych w Polsce oraz zagranicą. Firma współpracuje również z ośrodkami akademickimi, specjalistycznymi szkołami oraz firmami zainteresowanymi ofertą TRANSFARM. Specjalistyczne przygotowanie pracowników TRANSFARM umożliwia realizację szkoleń w określonej tematyce dla uczestników konferencji, seminariów, sympozjów oraz innych form wymiany wiedzy i doświadczeń. Osobnym działem naszej działalności są usługi związane wykrywaniem urządzeń inwigilacyjnych, zabezpieczaniem pomieszczeń oraz wykrywaniem oprogramowania szpiegowskiego na nośnikach danych i w telefonach.

Naszym klientom oferujemy:

NAJWYŻSZĄ JAKOŚĆ PRODUKTÓW renomowanych firm amerykańskich, izraelskich i europejskich, w tym polskich. Jakość oferowanych produktów została potwierdzona wieloletnim ich wykorzystaniem przez struktury kryminalistyczne oraz służby odpowiedzialne za ochronę informacji wrażliwych na całym świecie.

RZETELNOŚĆ DOSTAW realizowanych w 100% zgodnie z zamówieniem i oczekiwaniami odbiorców.

PROFESJONALNE DORADZTWO TECHNICZNE w doborze produktów najlepiej spełniających oczekiwania odbiorców. Jest ono realizowane przez wyspecjalizowany zespół TRANSFARM posiadający wieloletnie doświadczenie zawodowe z zakresu stosowania oferowanych produktów i usług. Naszą misję w biznesie rozumiemy bowiem w ten sposób, że „drożej" nie musi oznaczać „lepiej", a „lepiej" nie zawsze znaczy „więcej".

OBSŁUGĘ KLIENTA realizowaną przez wysoko wyspecjalizowany zespół pracowników TRANSFARM. Działalność zespołu jest wspomagana przez ekspertów różnych specjalności, w tym byłych funkcjonariuszy policji posiadających wieloletnie doświadczenie zawodowe.

BIEŻĄCE MONITOROWANIE JAKOŚCI OFEROWANYCH PRODUKTÓW poprzez okresowe badanie zadowolenia klientów z otrzymanych produktów. Wyniki badań służą do utrzymania w ofercie określonych produktów lub decyzji o ich wycofaniu, a tym samym do profilowania polityki handlowej TRANSFARM.

STAŁY DOSTĘP KLIENTÓW DO NOWOŚCI Z DZIEDZINY KRYMINALISTYKI dzięki bieżącemu monitoringowi nowości pojawiających się na rynku kryminalistycznym na całym świecie. Przed rekomendacją tych produktów dla klientów zostają one przebadane przez specjalistów TRANSFARM i współpracujących ekspertów kryminalistyki.

Dlatego pozostajemy w nadziei, że prezentowana oferta spotka się z Państwa zainteresowaniem.

Zespół Transfarm Sp. z o.o.

I.
SYSTEMY ZABEZPIECZENIA PRZECIWINWIGILACYJNEGO

Założenia funkcjonalne:

Oferowane Systemy Zabezpieczenia Przeciwinwigilacyjnego chroni pomieszczenie przed możliwością inwigilacji prowadzonej przy pomocy technicznych środków podsłuchowych zarówno z zewnątrz jaki i z wewnątrz. System zabezpiecza przed następującymi formami inwigilacji:

1) podsłuchowi bezpośredniemu prowadzonemu przez pracowników lub osoby postronne przez ściany, sufit, podłogę lub drzwi pomieszczenia;
2) działaniu urządzeń podsłuchowych realizujących transmisję radiową zarówno analogową jak i cyfrową, w tym z użyciem telefonów komórkowych i innych środków transmisji GPS, DECT, Wi-Fi, itp.;
3) podsłuchowi linii elektrycznych, niskoprądowych instalacji sygnałowych oraz sieci logicznych;
4) podsłuchowi prowadzonemu za pomocą stetoskopów zwykłych, stetoskopów elektronicznych, a także mikrofonów przewodowych, kontaktowych, kierunkowych i optycznych, w tym laserowych;
5) nagrywaniu rozmów z użyciem środków audio (dyktafony, magnetofony) oraz za pomocą urządzeń do rejestracji video.

Działanie oferowanych systemów nie jest widoczne i słyszalne dla osób przebywających w zabezpieczonym pomieszczeniu.

Działanie systemów:

Oferowane systemy przeznaczony są do zabezpieczenia przeciwinwigilacyjnego i integrują następujące formy zabezpieczeń:

1) **System zabezpieczenia wibroakustycznego** w zakresie aktywnego tłumienia sygnałem wibroakustycznym w postaci losowo zmiennego białego szumu generowanego bezpośrednio w elementy infrastruktury zabezpieczanego pomieszczenia na poziomie sygnału do 60 dB.

   Podsłuchiwanie mowy ludzkiej:

   Mowa ludzka jest jednym z najstarszych i najbardziej rozpowszechnionym sposobem wymiany informacji między ludźmi. Dlatego już w czasach antycznych stosowano systemy podsłuchiwania łączących w formie kanałów dźwiękowych prowadzonych w podłogach i ścianach np. apartamenty gościnne z pomieszczeniami dostępnymi dla gospodarzy. Osiągnięcia nowoczesnej techniki, pozwalają obecnie na stosowanie szerokiego wachlarza urządzeń do prowadzenia niejawnej inwigilacji poufnych rozmów z zewnątrz pomieszczenia, w którym się ona odbywa. W szczególności zastosowanie w tym zakresie mają następujące grupy urządzeń: mikrofony laserowe, mikrofony działające w podczerwieni, mikrofony kontaktowe itp.

Przechwycona informacja głosowa, szczególnie tzw. sygnał pierwotny (głos ludzki nie poddany obróbce) jest jak dokumentem opatrzony własnoręcznym podpisem, ponieważ współczesne metody analizy mowy pozwalają na jednoznaczną identyfikację tożsamości osoby mówiącej.

Stąd wyjątkowa wartość mowy ludzkiej, a w konsekwencji duże zainteresowanie potencjalnego przeciwnika jej przechwyceniem. Dlatego pomieszczenia, w których następuje wymiana poufnej informacji za pomocą mowy ludzkiej powinny być specjalnie zabezpieczone.

Możliwość nieuprawnionego przechwytywania informacji głosowej i jej jakość określa się stosunkiem (relacją) sygnału do szum w miejscach potencjalnej instalacji urządzeń podsłuchowych. Poziom sygnału, który może być przechwycony jest uzależniony od specyficznych cech architektoniczno-konstrukcyjnych budynku lub wydzielonego pomieszczenia (grubość otaczających konstrukcji budowlanych, zastosowane materiały, jakość wykończenia). Odbiór sygnałów wibracyjnych i akustycznych zawsze przebiega w tle zakłóceń mających swe pochodzenie naturalne lub ze sztucznego źródła.

Minimalny poziom zabezpieczenia informacji głosowej zostaje spełniony gdy w czasie odsłuchiwania fonogramu (zapisu dźwięku), nie jest możliwe odtworzenie sensu przekazywanej wiadomości. Nazywane jest to zerową zrozumiałością sensu. Zjawisko to zachodzi wtedy, kiedy poziom zakłócenia jest w przybliżeniu 3 razy wyższy od poziomu sygnału, w całym zakresie częstotliwości, to jest wtedy, kiedy stosunek sygnał / szum wynosi minus 10dB.

Maksymalny poziom ochrony, odpowiada takiej sytuacji, kiedy w ogóle nie można stwierdzić samego faktu prowadzenia rozmowy, lub występowania mowy w sygnale. Osiągnięcie tego stanu rzeczy jest możliwe poprzez sztuczne wprowadzenie w przegrody techniczne losowo zmiennego sygnału białego szumu akustycznego o poziomie sygnału gwarantującym zagłuszenie prowadzonej rozmowy w zabezpieczanym pomieszczeniu. Sygnał ten powinien spełnić możliwość redukcji sygnału prowadzonej rozmowy o 60 dB.

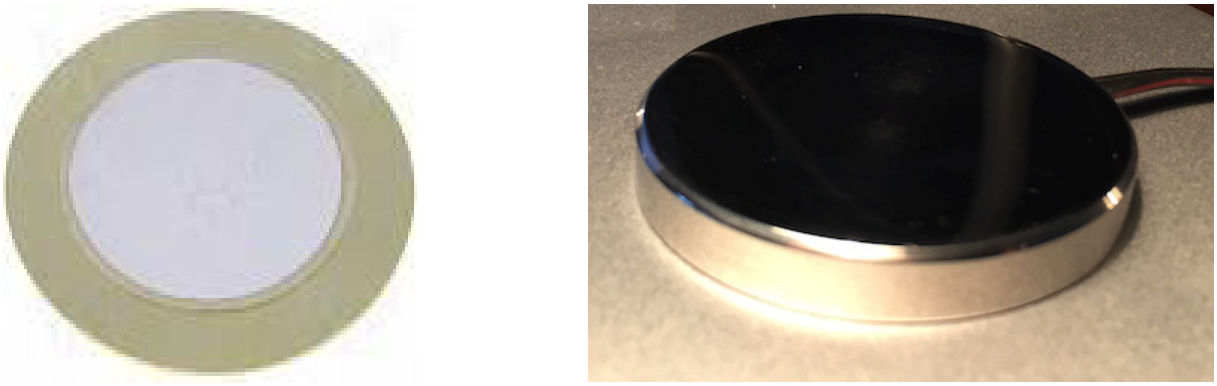
System zabezpieczenia wibroakustycznego uniemożliwia prowadzenie działań inwigilacyjnych z zewnątrz zabezpieczanego pomieszczenia za pomocą środków technicznych takich jak akustyczne mikrofony kontaktowe, mikrofony laserowe, stetoskopy, itp. System zabezpiecza również przed podsłuchem prowadzonym poprzez centralne instalacje wentylacyjne i klimatyzacyjne.

Piezoemitery

Zabezpieczenie wibroakustyczne realizowane jest za pomocą szeregowej niskoprądowej sieci elektrycznej 12V DC integrującej obwody przetworników wibroakustycznych „PIEZO”. Są to urządzenia przetwarzające energię elektryczną w energię sprężystych drgań wibroakustycznych.

Przetworniki PIEZO montowane są do przegród budowlanych lub bezpośrednio do ścian, a także do sufitów, podłogi, szyb okiennych oraz drzwi z rozmieszczeniem zapewniającym uzyskanie jednolitej bariery wibroakustycznej o poziomie tłumienia nie mniejszym niż 60 dB. Poprzez odpowiednie ugięcie przetwornika można go również zamontować na rurach i grzejnikach.

Jeden przetwornik wibroakustyczny „PIEZO" zabezpiecza swoim zasięgiem powierzchnię do 1 m^2. Kanały wentylacyjne zabezpieczone są za pomocą zainstalowanych w ich wnętrzu głośników akustycznych typ Velleman 616002.



przetworniki PIEZO

Przetworniki PIEZO (piezoemitery) - dane techniczne:

- impedancja: 8 Ω,
- zakres częstotliwości: 10 ÷ 10.000 Hz,
- zasilanie: 5,6 V DC,
- wymiary: ∅ 36 x 0,5 mm,
- masa: 10 g.

sposób montażu przetworników PIEZO na różnych podłożach

W wejściach i wyjściach kanałów instalacji wentylacyjnej lub klimatyzacyjnej w pomieszczeniach izolowanych wibroakustycznie montowane są dedykowane emitery zakłócające.

Generator szumu wibroakustycznego:

Przetworniki PIEZO oraz emitery zakłócające współpracują z cyfrowym generatorem szumu wibroakustycznego, z którym tworzą system zabezpieczenia wibroakustycznego chroniącego sygnały akustyczne rozmów odbywających się w zabezpieczanym pomieszczeniu przed możliwością zewnętrznego podsłuchu akustycznego lub prowadzonego za pomocą mikrofonu laserowego. Barierę stanowi losowo emitowany zmienny biały szum w zakresie częstotliwości 10 - 10.000 Hz, który poprzez współpracujące przetworniki PIEZO przekazywany jest bezpośrednio w elementy konstrukcyjne zabezpieczanego pomieszczenia. W ten sposób generowana jest bariera akustyczna na poziomie tłumienia dźwięku ΔRw o wartościach nie niższych niż 60dB. Taka izolacja jest adekwatna do poziomu sygnału, który podlega zagłuszeniu. Poziom sygnału (szumu) jest kontrolowany automatycznie przez układ mikroprocesora generatora, jednak może też być regulowany manualnie, jeżeli jest to determinowane akustyką zabezpieczanego pomieszczenia lub wymaganym wyższym poziomem tłumienia.

Generator szumu wibroakustycznego - dane techniczne:

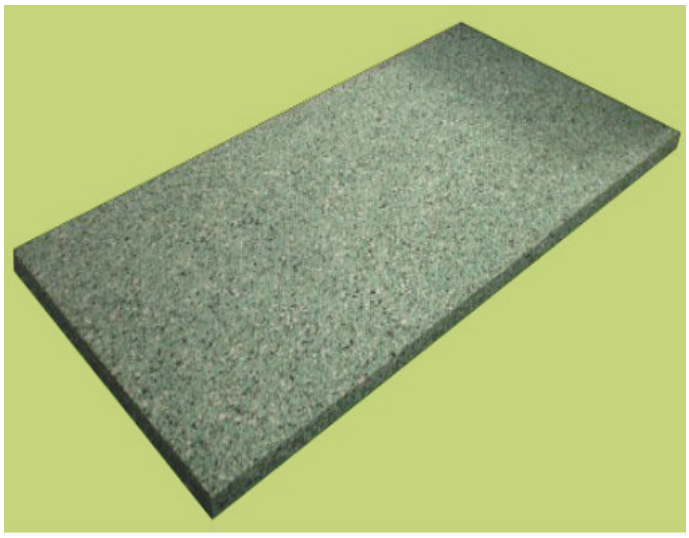
- zakres generowanych częstotliwości: 10 ÷ 10.0000 Hz,
- liczba kanałów: 2,
- poziom sygnału szumu wibroakustycznego: 12 dB,
- moc wyjściowa: 2 x 7W / na kanał,
- obsługa do 100 przetworników,
- wymiary: 118 x 58 x 187 mm,
- masa: 400 g,
- zasilanie: 13,8 V DC lub 220/230 V 50 Hz,
- temperatura środowiska pracy: 0° ÷ 40° C
- wilgotność względna: do 85%

Włączanie systemu wibroakustycznego następuje za pomocą centralki alarmowej z klawiaturą numeryczną lub zdalnie za pomocą dedykowanego pilota podczerwieni. Zainstalowana centrala alarmowa będzie jednocześnie sterować **Autonomicznym Systemem Kontroli Dostępu oraz Sygnalizacji Włamania** do zabezpieczanego pomieszczenia.

2) **System izolacji akustycznej** w zakresie tłumienia akustycznego w następujących częstotliwościach oktawowych:

częstotliwość:	250 Hz	500 Hz	1000 Hz	2000 Hz	4000 Hz
tłumienność:	50 dB	58 dB	60 dB	70 dB	70 dB

System izolacji akustycznej wykonany jest z paneli ekranowania akustycznego HDS 50. Panele wykonane są z izolacji akustycznej składającej się z prasowanej pianki technicznej T3037SG. Panele zachowują pełną efektywność tłumienia w paśmie 10 - 20.0000 Hz dla wartości współczynnika Rw > 55 dB. Panele są elastyczne i odporne na uderzenia i wykruszanie.



panel akustyczny HDS 50 i sposób jego montażu

Pianka T3037SG posiada atest do stosowania w pomieszczeniach biurowych (palność: trudno zapalny - atest TZ/PN1021/209/2013). Dzięki gęstości 180 - 200kg/m^3 warstwa izolacyjna wykonana z paneli na podłodze może przyjmować obciążenie maksymalnie do 5.000 kg/m2.

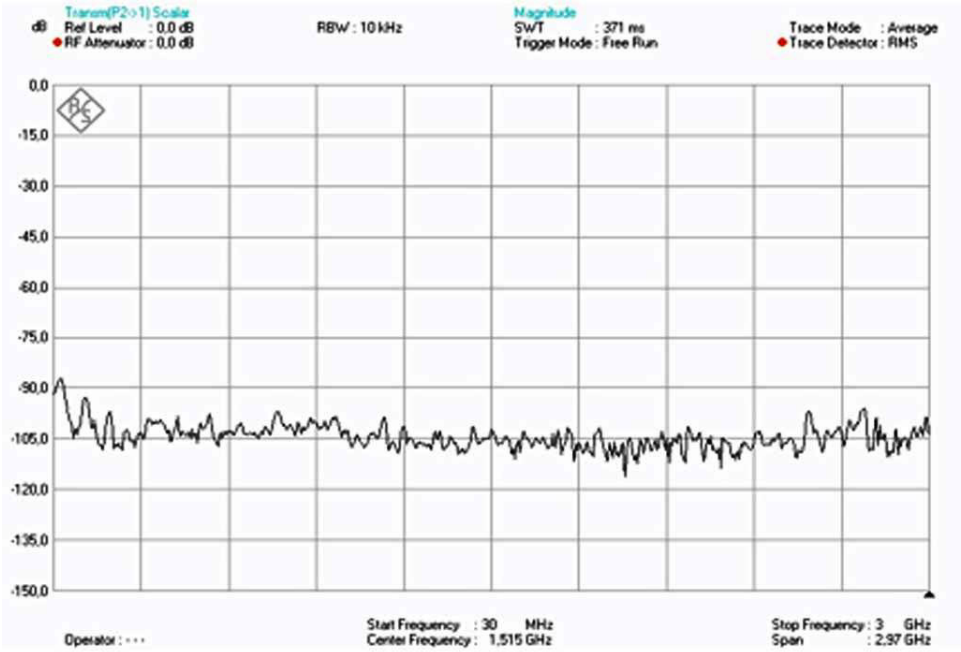
W zabezpieczanym pomieszczeniu po jednej stronie śluzy elektromagnetycznej montowane są drzwi izolowane akustycznie.

W wejściach i wyjściach kanałów instalacji wentylacyjnej lub klimatyzacyjnej w pomieszczeniach izolowanych akustycznie montowane są dedykowane tłumiki akustyczne.

3) **System zabezpieczenia elektromagnetycznego**, który uniemożliwia prowadzenie działań inwigilacyjnych za pomocą nadajników radiowych oraz innych technicznych środków transmisji telekomunikacyjnej.

Zabezpieczenie elektromagnetyczne realizowane jest za pomocą szczelnej klatki Faradaya gwarantującej odpowiednią tłumienność elektromagnetyczną. System tworzą następujące elementy:
- ekran elektromagnetyczny,
- ekranowane drzwi wejściowe,
- ekranowane otwory okienne,
- system dedykowanego uziemienia.

Ekran elektromagnetyczny tworzy włóknina ekranująca nakładana w postaci „tapety" pokrywającej powierzchnie wewnętrzne pomieszczenia (ściany, sufit i podłogę) „na zakładkę". Warstwy ekranujące włókniny uziemione są przy pomocy dedykowanego zestawu uziemiającego (linki miedzianej) do szyny RED uziomu bezpieczeństwa emisji lub uziemienia ogólno budynkowego. Oferowana włóknina zapewnia tłumienność elektromagnetyczną 90-105 dB od 30 MHz do 1.5 GHz oraz 105 dB od 1.5 GHz do 3.0 GHz.



charakterystyka tłumienia elektromagnetycznego włókniny ekranującej EMI/RFI RASKCUEXNI w zakresie częstotliwości od 30 MHz do 3 GHz

Włóknina przeznaczona jest do ekranowania pomieszczeń przed działaniem pól elektrycznych niskich częstotliwości, pól elektromagnetycznych wysokich częstotliwości oraz sygnałów radiowych i telekomunikacyjnych.

<u>przykładowa włóknina ekranująca: EMI/RFI RASKCUEXNI, dane techniczne:</u>

a) materiał: tkanina z Polieterosulfonu (PES) platerowana miedzią i niklem
b) typ splotu: spadochronowy
c) średnia rezystancja powierzchniowa: 0,01 Ohm/m2
d) tłumienność: 90-105 dB od 30 MHz do 1,5 GHz, 105 dB od 1,5 do 3,0 GHz
e) szerokość na rolce: 133 cm ± 3 cm.

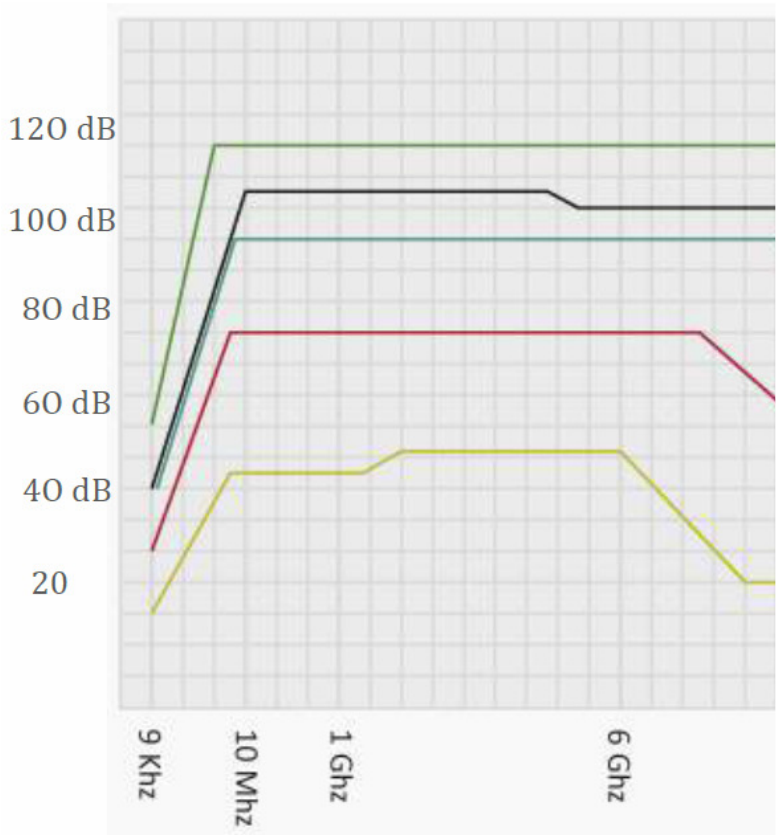
sposób montażu włókniny ekranującej

W pomieszczeniach objętych ekranowaniem elektromagnetycznym montowane są jako drugie w śluzie elektromagnetycznej drzwi ekranowane elektromagnetycznie zapewniające ciągłość powierzchni ekranującej pomieszczenia.

przykładowe drzwi ekranowane elektromagnetycznie

Drzwi ekranowane mogą zostać zamontowane jako jedno lub dwuskrzydłowe oraz dodatkowo być:
- dźwiękoszczelne,
- ogniotrwałe,
- gazoszczelne.

W zależności od indywidualnych potrzeb naszych klientów oferujemy drzwi ekranowane z różnym poziomem tłumienności. Naszą ofertę w tym zakresie ilustruje poniższy wykres:



- ekranowane drzwi drewniane - tłumienność do 50dB
- standardowe drzwi ekranowane, metalowe – tłumienność do 80 dB
- drzwi metalowe, ekranowane – tłumienność do 100 dB
- drzwi metalowe, ekranowane – tłumienność do 115 dB
- drzwi metalowe, ekranowane – tłumienność do 120 dB

Ponadto w pomieszczeniach objętych ekranowaniem elektromagnetycznym ekranowania wymagają również otwory okienne.

Ekran na oknie tworzy panel w postaci otwieranego okna z szybami ekranowanymi włókniną z przewodzącej siatki niklowej o średniej tłumienności 60dB i następujących szczegółowych parametrach technicznych:

a) ekranowanie: promieniowanie wysokiej częstotliwości oraz pole elektryczne niskiej częstotliwości
b) zakres częstotliwości: 14 kHz do 10 GHz
c) tłumienność:
   - w zakresie 1 MHz ÷ 4 GHz: 70 dB,
   - w zakresie 4 GHz ÷ 10 GHz: 46 dB,
d) poziom tłumienia: 99,9999999% we wszystkich zakresach
e) profil ekranu: stal nierdzewna

szyba zabezpieczona włókniną z siatki niklowej

Wejścia i wyjścia kanałów instalacji wentylacyjnej lub klimatyzacyjnej w pomieszczeniach objętych ekranowaniem elektromagnetycznym są zabezpieczone dedykowanymi falowodami typu HineyComb.

4) **Autonomiczną instalację uziemienia** o impedancji nie wyższej niż 5 Ohm przy częstotliwości 100 kHz, która stanowi dopełnienie systemu zabezpieczenia elektromagnetycznego. Główna szyna uziemiająca uziemienia ochronnego (ST/Zn 25x4) zlokalizowana będzie w zabezpieczonym pomieszczeniu i może być traktowana jako uziemienie bezpieczeństwa emisji. Punkt przyłączenia dedykowanego uziomu bezpieczeństwa emisji do szyny (ST/Zn25x4) zostanie wykonany w skrzynce metalowej zamykanej na klucz i doprowadzony zostanie do szyny „RED" zlokalizowanej w skrzynce z filtrami SRF z zastosowaniem linki 35 mm^2 izolowanej na całej długości.

5) **Separację linii elektrycznych i sygnałowych** w obrębie zabezpieczanego pomieszczenia - linie elektryczne i sygnałowe znajdujące się w obrębie zabezpieczanego pomieszczenia chroni się przy pomocy filtrów separacyjnych. Filtry zakładane są oddzielnie dla każdej linii elektrycznej i sygnałowej.

skrzynka z zainstalowanymi filtrami separacyjnymi

Alternatywnie może być również wykonane mniej wydajne, ale korzystniejsze cenowo zabezpieczenie przewodów linii elektrycznych 230V za pomocą filtrów ferrytowych typu STRAG GAP o impedancji 190Ω przy 100MHz.. Filtry STRAG GAP są przeznaczone do ekranowania przewodów elektrycznych w zakresie częstotliwości 100MHz – 2,5GHz. Filtry instaluje się na przewodach linii elektrycznych na wejściu do zabezpieczanego pomieszczenia oraz na odcinkach eksploatacyjnych.

filtr typu STRAG GAP

6) **System Protektor** w zakresie blokowania emitowanym białym zmiennym losowo szumem akustycznym mikrofonów urządzeń elektronicznych służących rejestracji lub transmisji audio.

Urządzenia Systemu Protektor przeznaczone są do zabezpieczania pomieszczeń (sal konferencyjnych, gabinetów itp.) przed podsłuchem realizowanym za pomocą technicznych środków zapisu i transmisji audio. Generatory urządzeń emitują barierę w postaci białego szumu w paśmie bliskich ultradźwięków, który skutecznie zakłóca mikrofony urządzeń elektronicznych takich jak dyktafony, telefony komórkowe, mikronadajniki radiowe, itp.

przenośne urządzenie systemu Protektor

Urządzenia Systemu Protektor emitują sygnał w wycinkowych wąskich pasmach dźwięku akustycznego i ponadakustycznego. Składowe emitowanego sygnału są zmiksowane losowo zmiennie przy pomocy specjalnie opracowanego algorytmu. Sygnał ten zakłóca mikrofony wywołując ich rezonans i uniemożliwiając w ten sposób czytelne zapisywanie oraz odsłuchanie wszelkiego rodzaju odbieranych sygnałów akustycznych. Emitowany sygnał zakłócający ma charakter dookólny (330°) z gwarantowaną skutecznością zagłuszania w promieniu 1,5 metra od urządzenia.

wykres sygnału rozmowy niezabezpieczonej

wykres sygnału rozmowy zabezpieczonej

Urządzenie Protektor - dane techniczne:

- zakres generowanych częstotliwości: 25,5 - 26,5 kHz,
- poziom sygnału: 117 dB,
- zasięg: 330° w promieniu 1,5 m,
- zasilanie AC 230 V, 50 Hz lub 12V DC,
- maksymalny czas ciągłej pracy przy zasilaniu z akumulatora do 2 godzin
- dopuszczalny czas ciągłej pracy przy zasilaniu 230V AC – 5 godzin
- temperatura pracy: 0° ÷ 40° C,
- wilgotność względna: do 85%.
- wymiary: średnica - 230 mm, wysokość - 110 mm
- waga: 5 kg

Alternatywne rozwiązanie dla urządzeń przenośnych stanowi zestaw 4 emiterów „Protektor Long" montowanych na stałe na ścianach zabezpieczanego pomieszczenia. Istotną różnicę w działaniu urządzeń typu „Long" w stosunku do urządzenia przenośnego, stanowi szerszy zakres emisji białego szumu, która jest realizowana w ich przypadku zarówno w paśmie bliskich ultradźwięków, jak i w paśmie słyszalnym przez człowieka. Dzięki temu urządzenia typu „Long" wytwarzają jeszcze skuteczniejszą ochronę zabezpieczającą przed możliwością podsłuchu za pomocą technicznych środków rejestracji i transmisji dźwięku, jednak jest to osiągane kosztem komfortu osób uczestniczących w zabezpieczanej wymianie informacji.

Typowa rozmowa w miejscu publicznym prowadzona jest na poziomie ok. 60dB. Tak rozmawiamy w przeciętnej restauracji, czy na zwykłej ulicy. Głośna rozmowa ma poziom ok. 70dB i jest charakterystyczna dla ruchliwej ulicy, albo dużej restauracji, np. stołówki akademickiej. Urządzenia typu „Long" generują szum na poziomie 50-55dB. Oznacza to że, urządzenia te, choć są bardzo skuteczne, to zauważalnie (odczuwalnie dla uczestników) utrudniają prowadzenie rozmowy.

system Protektor - urządzenia typu „Long"

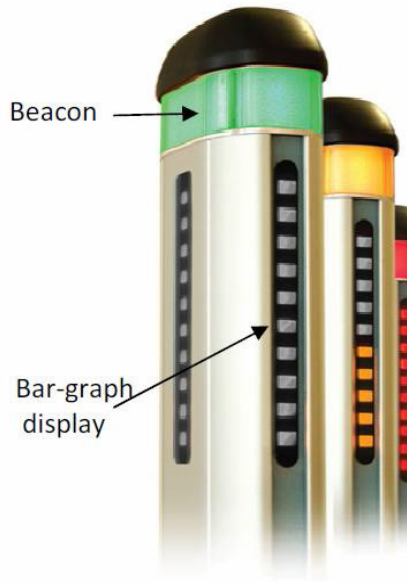
Działanie systemu Protektor

7) Uruchamianą przed najważniejszymi spotkaniami przy wejściu do zabezpieczanego pomieszczenia **strefę depozytu i kontroli** wyposażoną w depozytor na urządzenia elektroniczne oraz w detektor przedmiotów ferromagnetycznych i urządzeń elektronicznych posiadanych przez osoby wchodzące do zabezpieczonego pomieszczenia (przechodzące przez strefę kontroli).

Detektor FG

Detektor przeznaczony jest do wykrywania urządzeń elektronicznych: telefonów komórkowych, dyktafonów, mikronadajników radiowych, kamer video itp., które są wnoszone przez osoby wchodzące do ochranianej strefy (pomieszczenia). Jednocześnie detektor nie wykrywa metali nieferromagnetycznych takich jak biżuteria.

W przypadku wykrycia urządzeń niedozwolonych, osoba wchodząca obowiązana jest zdeponować je w depozytorze w indywidualnie przypisanej skrytce.



detektor FG zamontowany na stałe w strefie depozytu i kontroli

Detektor FG został opracowany na podstawie wieloletnich doświadczeń prowadzonych w amerykańskich ośrodkach penitencjarnych zmierzających do skutecznego wykrywania wnoszonych zabronionych przedmiotów takich jak : telefony komórkowe, mikronadajniki i odbiorniki radiowe, dyktafony, tablety, notebooki, itp. Dodatkowo detektor może wykrywać przedmioty ferromagnetyczne, broń palną, broń białą, itp. Możliwości detekcyjne urządzenia FG są zdecydowanie większe od konwencjonalnych detektorów metali.

Detektor wykrywa zabronione przedmioty nawet jeżeli są one przenoszone wewnątrz ciała kontrolowanej osoby. Detektor FG automatycznie dostosowuje się do właściwości elektro i ferromagnetycznych otoczenia, kompensuje zewnętrzne zakłócenia pochodzące od urządzeń elektrycznych i mechanicznych, takich jak oświetlenie, drzwi, metalowe kraty i elementy konstrukcyjne budynków.

Obsługa urządzenia jest wyjątkowo prosta, może ono być montowany trwale np. do ściany lub pracować jako urządzenie przenośne z zasilaniem wewnętrzną baterią gwarantującą 7 godzin ciągłej pracy.

Detektor umożliwia skanowanie do 40 osób na minutę. W przeciwieństwie jednak do konwencjonalnych detektorów metali, detektor FG jest całkowicie pasywny, nie emituje pola elektromagnetycznego, nie ma wpływu na urządzenia elektroniczne, nie zagraża zdrowiu i jest nieszkodliwy (bezpieczny) dla kobiet w ciąży.

Detektor FG - zasada działania

Działanie Detektora FG opiera się na wykrywaniu zmian w polu magnetycznym spowodowanych ruchem obiektu ferromagnetycznego w bezpośrednim otoczeniu detektora. Pole magnetyczne otoczenia jest sumą własnego pola magnetycznego detektora, pola magnetycznego Ziemi oraz pól magnetycznych pobliskich stacjonarnych obiektów żelaznych. Naturalne pole magnetyczne w otoczeniu detektora jest stałe i nie zmienne w czasie, cechy te umożliwiają detektorowi ich pasywny odbiór jako stałej, która może być zmieniona (zakłócona) tylko ruchem obiektów ferromagnetycznych. Stałe obiekty ferromagnetyczne (żelazne kraty, stalowe drzwi, urządzenia elektryczne) nie powodują działania detekcyjnego detektora. Detektor FG posiada również regulację poziomu czułości.

Praca detektora w trybie niskiej czułości może być wykorzystywana w aplikacjach bezpieczeństwa do wykrywania broni palnej, noży itp., z pominięciem detekcji większość innych na co dzień używanych przedmiotów noszonych przez ludzi (np. telefony komórkowe). Praca w trybie wysokiej czułości może być stosowana do szczegółowej kontroli osób i pozwoli wykrywać obecność nawet bardzo drobnych przedmiotów z określonych metali.

W urządzeniu FG do procesów detekcji zastosowane są detektory magnetometryczne. Detektory te są całkowicie pasywne i jak zostało to już wskazane nie narażają kontrolowanych osób na działanie aktywnych pól elektromagnetycznych.

Pole magnetyczne emitowane przez ferromagnetyki jest aktywne stale i nawet w przypadku stosowania osłon, umieszczenie obiektu wewnątrz innego obiektu, odzieży lub wewnątrz ciała ludzkiego, jest zawsze wykrywane przez detektor FG. Odbiór zakłóceń pola magnetycznego powodowanych poprzez ruch ferromagnetyków nie ma charakteru kierunkowego - detektor wykrywa obiekty niezależnie od kierunku ich przemieszczania w strefie detekcyjnej urządzenia.

Przenoszony przez kontrolowaną osobę przedmiot ferromagnetyczny skutkuje zakłóceniem pola.

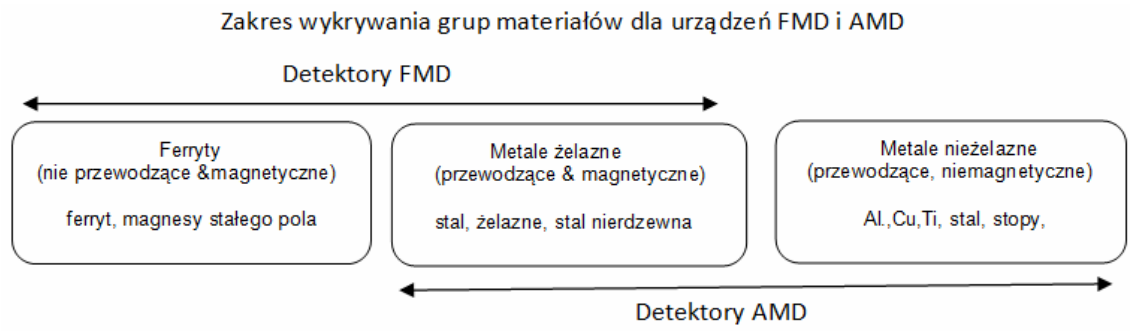
detektor FG - zasada działania

Urządzenia wykrywające ferromagnetyki (FMD) są często mylone z konwencjonalnymi detektorami metali (AMD). Ich działanie jednak istotnie się różni.

Detekcja AMD opiera się na wywołaniu zmiennego pola magnetycznego, które może być polem pulsacyjnym lub ciągłym polem sinusoidalnym emitowanym z jednej strony detektora. Metalowe obiekty generują pole wtórne, które jest wykrywane i przechwytywane przez cewki detektora po przeciwnej jego stronie. Podstawowym mechanizmem reakcji detektora jest wytworzenie prądów wirowych w wykrytym metalu. To z kolei prowadzi do powstania pola wtórnego. Drugi mechanizm pojawia się w materiałach ferromagnetycznych przy czym indukowane pole magnetyczne powoduje powstanie pola wtórnego, które zazwyczaj jest znacznie mniejsze niż reakcja prądów wirowych tego samego obiektu. Reakcje te mogą być uważane za indukowane momenty magnetyczne dla przedmiotów metalowych, a ich wielkość i kierunek jest proporcjonalny do wielkości i kierunku pola nadawanego w jego lokalizacji. Urządzenia AMD wykrywają głównie przewodność elektryczną kontrolowanych obiektów, cecha ta umożliwia im wykrywanie wszystkich rodzajów metali (żelazne i nieżelazne). Jednak obiekty o słabej przewodności niezależnie od tego, czy posiadają one potencjał magnetyczny, nie są wykrywane.

Urządzenia FMD nie emitują pół magnetycznych - ich działanie jest całkowicie pasywne. Wykrywają one bowiem zakłócenia naturalnego pola magnetycznego spowodowane przemieszczającymi się obiektami ferromagnetycznymi. Główne czynniki detekcji w działaniu detektorów FMD to:
- poziom stałego namagnesowania obiektu,
- względna przenikalność magnetyczna,
- wielkość i kształt
- wielkość stałego naturalnego pola magnetycznego w otoczeniu detektora

Urządzenia FMD nie są więc wrażliwe na cechy przewodnictwa elektrycznego kontrolowanych obiektów. Głównym czynnikiem detekcyjnym jest magnetyzm. Dzięki tej funkcji detekcyjnej są one w stanie wykrywać obiekty o słabej przewodności lub obiekty nie mających w ogóle cech przewodności elektrycznej takie jak ferryt i niektóre stopy magnetyczne czy stal nierdzewna.



Detektor FG - dane techniczne:

- strefa wykrywania: do 2m,
- zakres detekcji: 360°,
- przepustowość: do 40 osób na minutę,
- alarm: świetlny i dźwiękowy o regulowanej głośności,
- zasilanie: 230 V 50/60 Hz AC lub 12 V, 4,5 Ah DC,
- czas pracy na akumulatorze: 7 godzin,
- posiadane certyfikaty: CE,
- wymiary: 188 cm (wysokość) x 13 cm (szerokość) x 8 cm (głębokość),
- waga urządzenia: 9 kg,
- waga urządzenia z podstawą: 18 kg.

detektor FG w wersji stacjonarnej

Ekranowana komora depozytowa na urządzenia elektroniczne

Oferowana komora depozytowa na urządzenia elektroniczne zapewnia wysoką izolację akustyczną oraz elektromagnetyczną (stanowi tzw. klatkę Faradaya).

Komora jest przeznaczona do deponowania urządzeń elektronicznych, takich jak telefony komórkowe, dyktafony, tablety, komputery przenośne, które mogą służyć do pozyskiwania informacji chronionych. Oferowana komora jest ekranowana zarówno elektromagnetycznie, jak i akustycznie. Zastosowany ekran elektromagnetyczny blokuje dostęp do sieci GSM. Dźwiękoszczelny ekran akustyczny uniemożliwia zaś ewentualną rejestrację audio.

dane techniczne komory depozytowej:

- zakres szczelności elektromagnetycznej: 800 MHz – 6 GHz;
- poziom ekranowania elektromagnetycznego: 75 dB dla 2,4 GHz; 70 dB dla 5,8 GHz (średnio 70 dB);
- poziom ekranowania akustycznego: średnio 50 dB w zakresie od 300 do 6000 Hz;
- wymiary zewnętrzne: 430 x 430 x 280 mm.;
- wymiary wewnętrzne: 390 x 390 x 240 mm.;
- waga: 10 kg.

Alternatywę dla przenośnej komory depozytowej stanowi depozytor wykonany w postaci stacjonarnej lub mobilnej szafki meblowej z indywidualnymi skrytkami do deponowania urządzeń elektronicznych (telefony komórkowe, dyktafony, tablety, notebooki, itp.), których wniesienie do zabezpieczonego pomieszczenia jest niedozwolone.

Depozytor jest dostarczony w wykończeniu w kolorze wskazanym przez klienta. Skrytki zgodnie z wytycznymi klienta wykonywane są w różnych rozmiarach: małe do deponowania drobnych urządzeń elektronicznych (telefony, dyktafony, itp.) oraz większe do deponowania notebooków i tabletów.

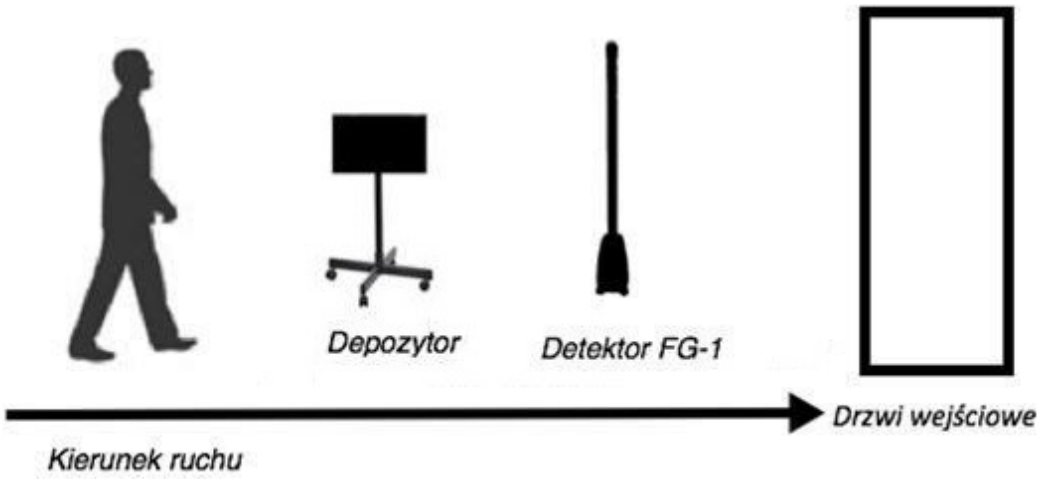
W przypadku depozytora na podstawie mobilnej ze względu na stabilność szafki sugerowany jest następujący podział skrytek: 6 lub 8 przedziałów na małe urządzenia elektroniczne (telefony i tablety) oraz odpowiednio 3 lub 4 na większe urządzenia takie jak komputery przenośne).

Wszystkie skrytki w oferowanych depozytorach (zarówno stacjonarnych, jak i mobilnych) zamykane są w systemie Master-Key.

sala konferencyjna - zewnętrzna przenośna strefa depozytu i kontroli z mobilnym depozytorem i detektorem FG

stacjonarny depozytor zamontowany na stałe
na ścianie w strefie depozytu i kontroli

Strefa kontroli i depozytu powinna być zorganizowana w ciągu komunikacyjnym znajdującym się przed drzwiami wejściowymi do zabezpieczanego pomieszczenia w następującym układzie:



Odległość pomiędzy detektorem FG, a depozytorem powinna wynosić minimum 1,5 m. Osoba wchodząca w strefę kontroli i depozytu powinna najpierw zdeponować urządzenia niedozwolone w depozytorze, a następnie przejść przed detektorem FG w odległości ok. 1 m. od detektora. Jeżeli detektor nie zasygnalizuje faktu przenoszenia urządzeń elektronicznych, kontrolowana osoba powinna zostać skierowana bezpośrednio do wejścia do zabezpieczanego pomieszczenia. Jeżeli detektor zasygnalizuje fakt przenoszenia urządzenia elektronicznego kontrolowana osoba ponownie powinna zostać poproszona o zdeponowanie urządzeń niedozwolonych w depozytorze, a następnie poddana ponownej kontroli. W przypadku wyjścia z sali konferencyjnej osoby, która była wcześniej kontrolowana, przed jej powrotem na salę osoba taka powinna być poddana nowej kontroli.

8) **Autonomiczny system kontroli dostępu i sygnalizacji włamania** do zabezpieczonego pomieszczenia. Zabezpieczone pomieszczenie powinno stanowić wydzielony zasób, do którego dostęp jest limitowany i kontrolowany. Dlatego realizując usługę kompleksowego zabezpieczenia przeciwinwigilacyjnego wyposażamy chronione pomieszczenie w Autonomiczny system kontroli dostępu oraz sygnalizacji włamania obejmujący także sygnalizację pożarową oraz przycisk awaryjnego otwierania drzwi.

W przypadku zabezpieczania pomieszczeń już wyposażonych w taką sygnalizację oferujemy montaż systemu kontroli dostępu realizowanej za pomocą zamków elektronicznych rejestrujących kolejne operacje otwarcia / zamknięcia w zadanym okresie czasu lub aż do całkowitego zapełnienia dostępnej pamięci zamka.

Opisany zamek elektroniczny może być również zainstalowany na drzwiach wejściowych do pomieszczenia poprzedzającego zabezpieczoną salę, stanowiącego recepcję w którym zlokalizowana jest strefa depozytu i kontroli.

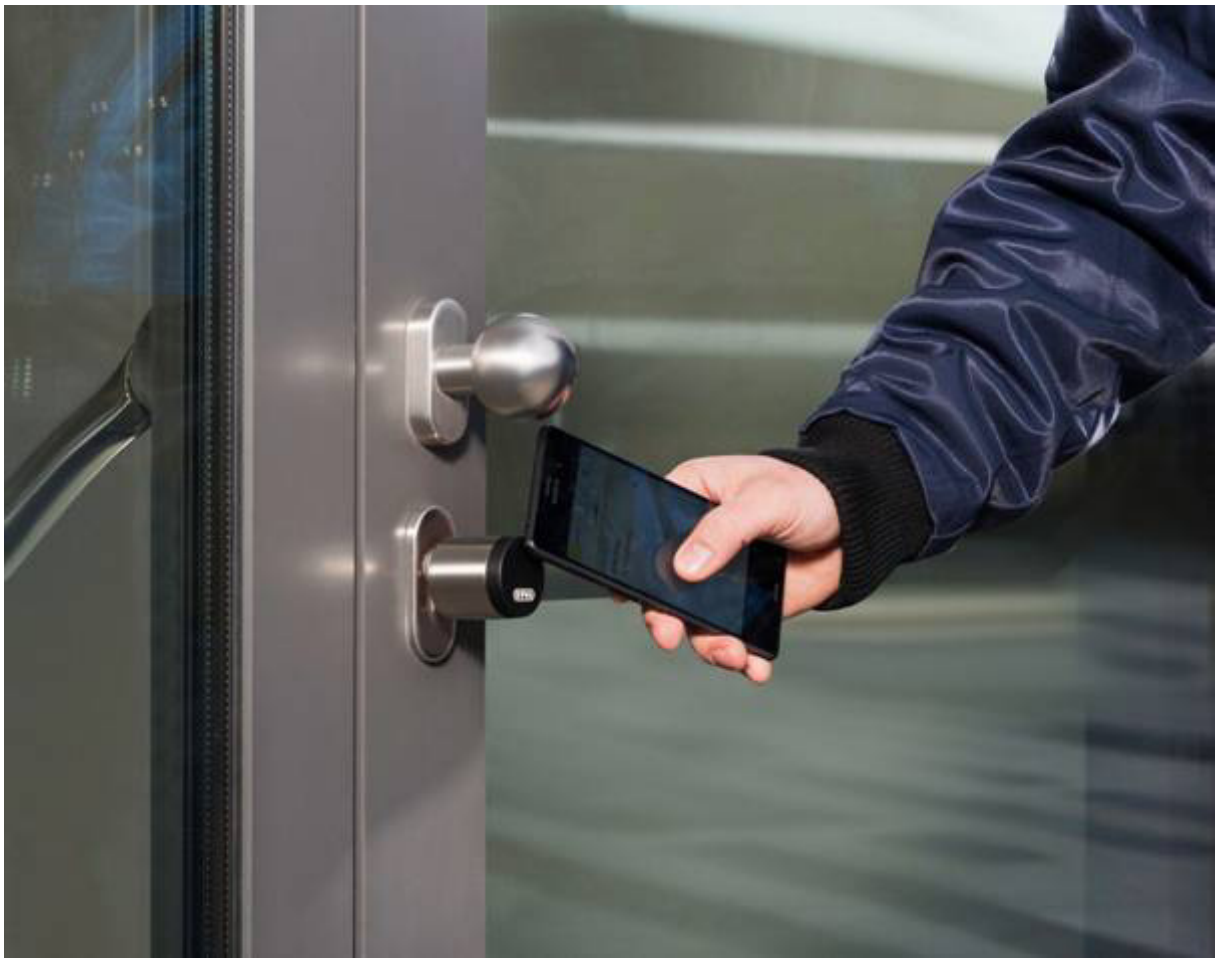
<u>Zamek elektroniczny Yale YDG313 Shine do drzwi szklanych bezramowych</u>

Oferowany zamek posiada lustrzane wykończenie panelu, cyfry na panelu pojawiają się dopiero po dotknięciu dłonią. Wewnętrzna kaseta zamka wyposażona jest w pokrętło. Odblokowywanie zamka następuje za pomocą kodu PIN lub karty zbliżeniowej. W celu ochrony przed możliwością podejrzenia kodu przez osoby trzecie zamek można tak zaprogramować, aby przed i po faktycznym kodzie wprowadzać dodatkowo dowolną sekwencję fałszywych cyfr.

zamek Yale YDG313

Zamek elektroniczny EVVA AIRKEY do drzwi ramowych

Zamek EVVA AIRKEY jest wyposażony w zabezpieczenie przed rozwierceniem, zabezpieczenie przed wyjęciem rdzenia, hamulec rotacyjny i miejsce kontrolowanego uszkodzenia w razie próby wyłamania zamka. Zamek jest sterowany za pomocą dedykowanej aplikacji AirKey, która współpracuje z telefonami komórkowymi z systemem operacyjnym Android oraz iOS.



odblokowywanie zamka EVVA AIRKEY
za pomocą aplikacji zainstalowanej w telefonie komórkowym

Komunikacja telefonu z czytnikiem zamka odbywa się za pomocą technologii NFC lub - według wyboru użytkownika - technologii Bluetooth, które spełniają identyczne standardy bezpieczeństwa. Użytkownik może we własnym zakresie wybrać, którą funkcję chce stosować w telefonie z systemem Android (wybór technologii Bluetooth wymaga wersji systemu Android 4.0 lub nowszej, a wybór technologii NFC wersji systemu Android 6.0 lub nowszej). W przypadku iPhone'a dostępna jest tylko opcja Bluetooth (wymagana jest wersja iOS 10 lub nowsza).

Wszystkie przesyłane dane są zabezpieczone od początku do końca zgodnie z najnowszymi standardami szyfrowania ECDSA i AES. W ten sam sposób są zabezpieczone wszystkie dane użytkowników. Dzięki użyciu certyfikowanych elementów zabezpieczających (modułów pamięci, które dokonują aktywnego szyfrowania i odszyfrowania) we wkładce, system AirKey wyznacza nowy standard bezpieczeństwa w zakresie elektronicznych systemów zamknięć. Protokołowanie 1.000 ostatnich zdarzeń zapewnia możliwość pełnej identyfikowalności wejść.

Bateria zainstalowana we wkładce zapewnia okres eksploatacji do 30.000 cykli ryglowania. W razie niskiego poziomu naładowania baterii wkładka generuje migający, czerwony sygnał optyczny. Wówczas należy wymienić baterię. Stan baterii jest także wskazywany w module zarządzania online i w razie potrzeby prezentowany jako zadanie konserwacyjne.

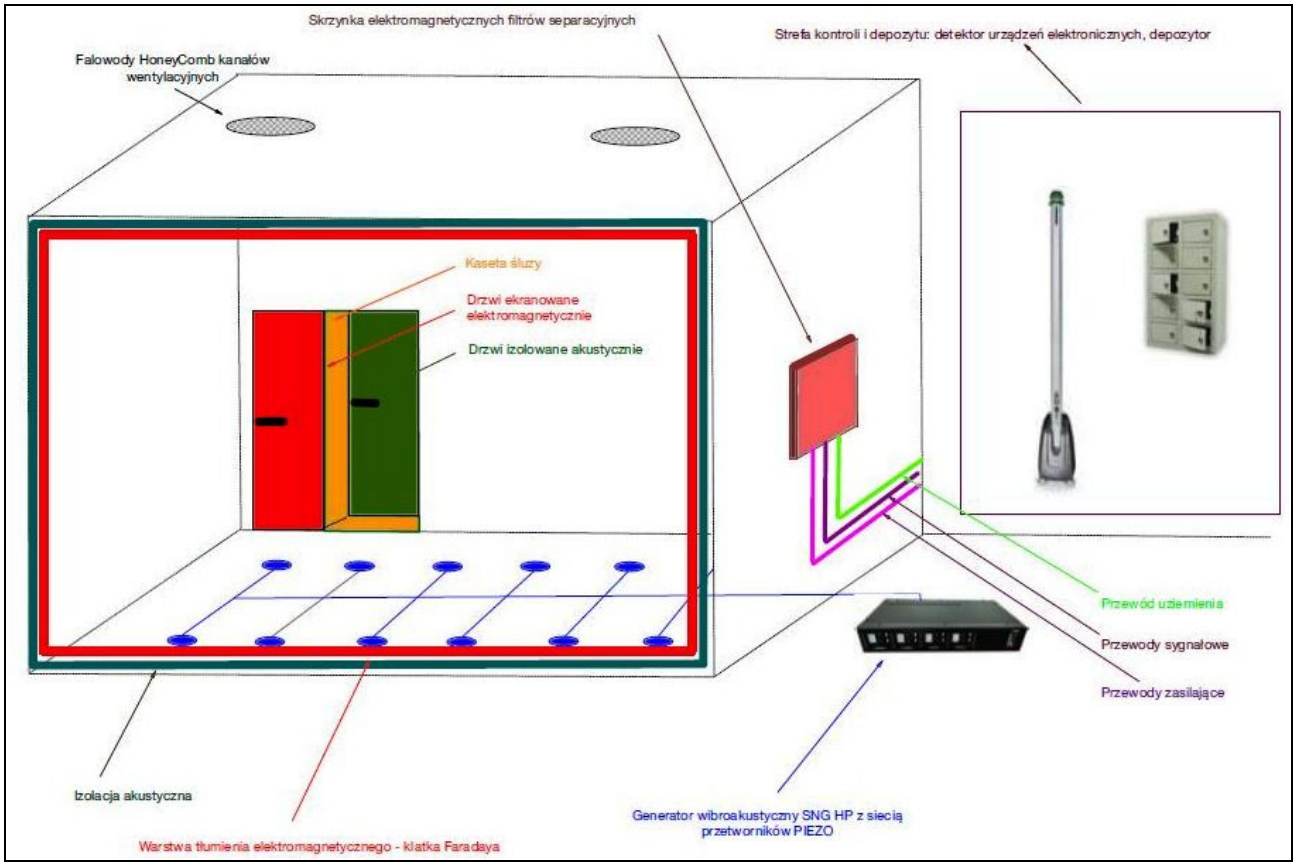
Aplikacja administratora kluczy spełnia wymagania dotyczące ochrony danych osobowych zgodnie z przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000) oraz z przepisami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Aplikację mobilną w telefonie można zabezpieczyć indywidualnym kodem PIN, a w przypadku utraty telefonu można natychmiast skasować udzielone uprawnienia dostępu i przydzielić uprawnienia do nowego telefonu.

Do utworzenia uprawnień dostępu (kluczy elektronicznych) potrzebne są jednostki „KeyCredit". Bieżąca eksploatacja nie wymaga dalszych jednostek KeyCredit i jest bezpłatna. Wraz z oferowanym zamkiem dostarczana jest karta z jednostkami „KeyCredit" uprawniającymi do utworzenia kluczy elektronicznych dla 10 różnych osób / urządzeń.

9) **Dedykowane wyposażenie konferencyjne zabezpieczonego pomieszczenia** w stół z przezroczystym blatem, komplet bezobiciowych foteli oraz ewentualną szafkę biurową. Prezentowane wzory oraz kolorystyka są przykładowe i każdorazowo są dostosowywane do indywidualnych oczekiwań klienta.

przykładowe wyposażenie konferencyjne zabezpieczanego pomieszczenia



schemat Zintegrowanych Systemów Zabezpieczenia Przeciwinwigilacyjnego

II.
WPŁYW NA ZDROWIE CZŁOWIEKA

Oferowane przez nas systemy zabezpieczeń nie mają jakiegokolwiek negatywnego wpływu na zdrowie człowieka, w tym w szczególności są one całkowicie bezpieczne dla osób z wszczepionym rozrusznikiem serca.

Aby prawidłowo działać, rozruszniki nieustannie monitorują pracę serca analizując jego aktywność elektryczną wynoszącą ok. 0,01 V. Tylko w bezpośrednim sąsiedztwie silnego pola elektrycznego lub magnetycznego może zostać wytworzony indukowany impuls elektryczny, który rozrusznik mylnie oceni jako sygnał z serca. Wtedy taki sygnał (stanowiący zakłócenie) mógłby zostać zinterpretowany jako aktywność własna serca, w wyniku czego rozrusznik przestałby dostarczać impulsy stymulujące. Ponieważ jednak w otoczeniu człowieka pojawia się coraz więcej urządzeń elektrycznych, rozruszniki serca są wyposażone w system chroniący pracę urządzenia przed tego typu zakłóceniami. Jest to tak zwany „*Noise Reversion Mode*" i polega on na tym, że w przypadku wykrycia nadmiernej „aktywności elektrycznej" (pochodzącej z zewnętrz, jednak interpretowanej jak aktywność własna serca) rozrusznik przełącza się w asynchroniczny tryb stymulowania serca - podejmuje stałą stymulację ignorując sygnały bezpośrednie.

Dzięki trybowi „*Noise Reversion*" urządzenia domowe takie jak sprzęt RTV i AGD, włącznie z kuchenkami mikrofalowymi, golarkami elektrycznymi, suszarkami do włosów, wiertarkami, a nawet grzewczymi płytami indukcyjnymi i spawarkami do 400A, są bezpieczne dla osób z wszczepionym rozrusznikiem serca.

Dopiero bardzo silne pole, którego nie są w stanie wytworzyć otaczające nas na co dzień przedmioty (tylko urządzenia o wielkiej mocy, np. siłownie energetyczne, stacje transformatorowe czy maszyny przemysłowe), może indukować znacznie większe prądy, które będą podgrzewać wszczepione urządzenie i końcówkę elektrody umieszczoną w sercu. W takim przypadku może dojść do poparzenia tkanki wokół metalowych części rozrusznika. Potencjalnie istnieje też wtedy ryzyko uszkodzenia elektroniki urządzenia lub zawieszenie jego programu.

Żaden z naszych systemów zabezpieczających nie jest wyposażony w silnik elektryczny, a ich pracy może towarzyszyć jedynie śladowe pole elektromagnetyczne. Dlatego, wszystkie oferowane przez nas zabezpieczenia są całkowicie obojętne dla osób z wszczepionym rozrusznikiem serca.

III.
ZGODNOŚĆ TECHNICZNA

Oferowane systemy zabezpieczenia przeciwinwigilacyjnego oraz ich poszczególne komponenty są zgodne zaleceniami Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego w zakresie budowy specjalnych stref ochronnych służących ochronie informacji niejawnych, a także są zgodne w odpowiednim zakresie z następującymi normami, o których mowa w Załączniku nr 1 do rozporządzenia Ministra Infrastruktury z dnia 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. z 2019 r. poz. 1065):

1) PN-EN 62305-1:2011 Ochrona odgromowa - Część 1: Zasady ogólne;
2) PN-EN 62305-2:2008 Ochrona odgromowa - Część 2: Zarządzanie ryzykiem;
3) PN-HD 60364-4-41:2009 Instalacje elektryczne niskiego napięcia - Część 4-41: Ochrona dla zapewnienia bezpieczeństwa - Ochrona przed porażeniem elektrycznym;
4) PN-EN 12464-1:2012 Światło i oświetlenie - Oświetlenie miejsc pracy - Część 1: Miejsca pracy we wnętrzach;
5) PN-HD 60364-4-43:2012 Instalacje elektryczne niskiego napięcia - Część 4-43: Ochrona dla zapewnienia bezpieczeństwa - Ochrona przed prądem przetężeniowym;
6) PN-IEC 60364-4-442:1999 Instalacje elektryczne w obiektach budowlanych - Ochrona;
7) dla zapewnienia bezpieczeństwa - Ochrona przed przepięciami - Ochrona instalacji niskiego napięcia przed przejściowymi przepięciami i uszkodzeniami przy doziemieniach w sieciach wysokiego napięcia;
8) PN-HD 60364-4-443:2016 Instalacje elektryczne w obiektach budowlanych - Ochrona dla zapewnienia bezpieczeństwa - Ochrona przed przepięciami - Ochrona przed przepięciami atmosferycznymi lub łączeniowymi;
9) PN-HD 60364-4-444:2012 Instalacje elektryczne niskiego napięcia - Część 4-444: Ochrona dla zapewnienia bezpieczeństwa - Ochrona przed zakłóceniami napięciowymi i zaburzeniami elektromagnetycznymi;
10) PN-HD 60364-5-51:2011 Instalacje elektryczne w obiektach budowlanych - Część 5-51: Dobor i montaż wyposażenia elektrycznego - Postanowienia ogólne;

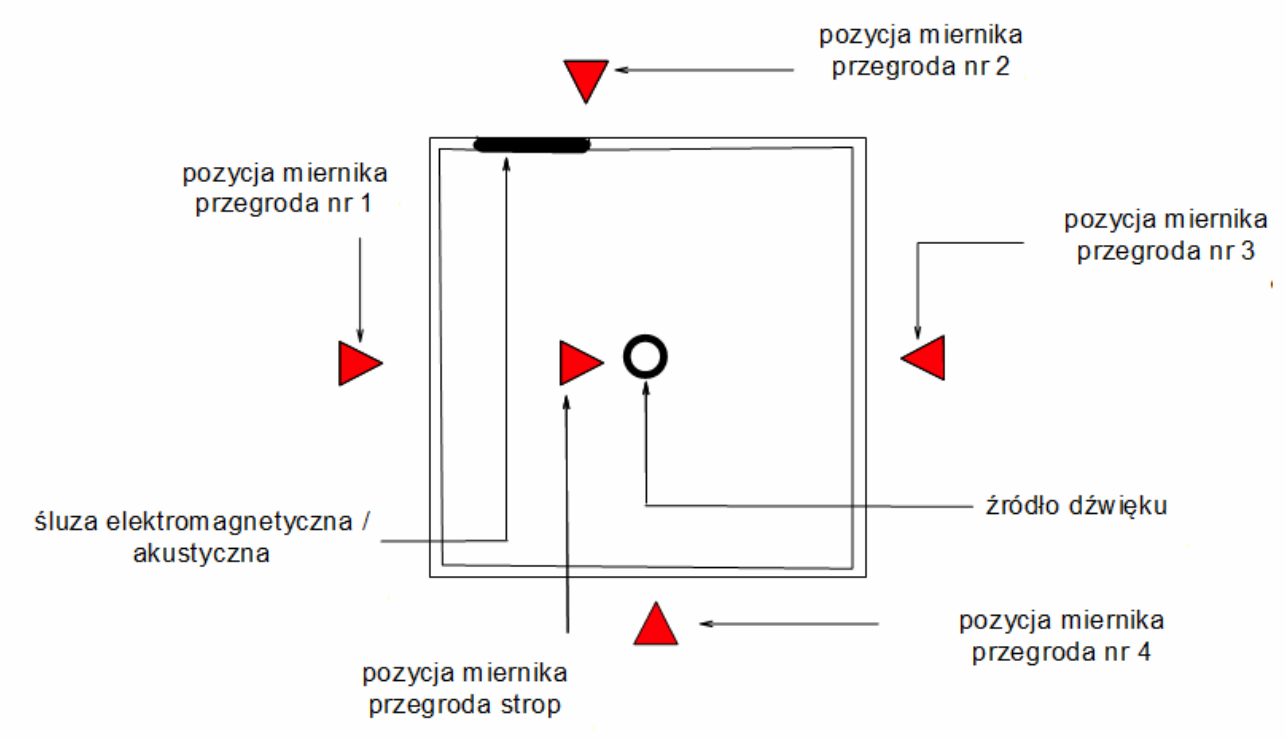
11) PN-IEC 60364-5-52:2011 Instalacje elektryczne niskiego napięcia - Część 5-52: Dobór i montaż wyposażenia elektrycznego - Oprzewodowanie;
12) PN-IEC 60364-5-53:2016 Instalacje elektryczne niskiego napięcia - Część 5-53: Dobór i montaż wyposażenia elektrycznego - Aparatura rozdzielcza i sterownicza;
13) PN-HD 60364-5-534:2016 Instalacje elektryczne niskiego napięcia - Część 5-534: Dobór i montaż wyposażenia elektrycznego - Odłączanie izolacyjne, łączenie i sterowanie - Urządzenia do ochrony przed przejściowymi przepięciami;
14) PN-IEC 60364-5-537:1999 Instalacje elektryczne w obiektach budowlanych - Dobór i montaż wyposażenia elektrycznego - Aparatura rozdzielcza i sterownicza - Urządzenia do odłączania izolacyjnego i łączenia;
15) PN-HD 60364-5-54:2011 Instalacje elektryczne niskiego napięcia - Część 5-54: Dobór i montaż wyposażenia elektrycznego - Układy uziemiające i przewody ochronne;
16) PN-HD 60364-5-56:2010 Instalacje elektryczne niskiego napięcia - Część 5-56: Dobór i montaż wyposażenia elektrycznego - Instalacje bezpieczeństwa;
17) PN-HD 60364-6:2008 Instalacje elektryczne niskiego napięcia - Część 6: Sprawdzanie;
18) PN-E-05204:1994 Ochrona przed elektrycznością statyczną - Ochrona obiektów, instalacji i urządzeń - Wymagania;
19) PN-E-05010:1991 Zakresy napięciowe instalacji elektrycznych w obiektach budowlanych;
20) PN-EN 50310:2012 Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym;
21) PN-HD 60364-1:2010 Instalacje elektryczne niskiego napięcia - Część 1: Wymagania;
22) podstawowe, ustalanie ogólnych charakterystyk, definicje;
23) PN-IEC 60364-4-443:1999 Instalacje elektryczne w obiektach budowlanych - Ochrona dla zapewnienia bezpieczeństwa - Ochrona przed przepięciami - Ochrona przed przepięciami atmosferycznymi lub łączeniowymi;
24) PN-IEC 60364-4-45:1999 Instalacje elektryczne w obiektach budowlanych - Ochrona dla zapewnienia bezpieczeństwa - Ochrona przed obniżeniem napięcia;
25) PN-IEC 60364-4-473:1999 Instalacje elektryczne w obiektach budowlanych - Ochrona dla zapewnienia bezpieczeństwa - Stosowanie środków ochrony zapewniających bezpieczeństwo - Środki ochrony przed prądem przetężeniowym;
26) PN-IEC 60364-5-52:2002 Instalacje elektryczne w obiektach budowlanych - Dobór i montaż wyposażenia elektrycznego - Oprzewodowanie;
27) PN-IEC 60364-5-523:2001 Instalacje elektryczne w obiektach budowlanych - Dobór i montaż wyposażenia elektrycznego - Obciążalność prądowa długotrwała przewodów;
28) PN-IEC 60364-5-53:2000 Instalacje elektryczne w obiektach budowlanych - Dobór i montaż wyposażenia elektrycznego - Aparatura rozdzielcza i sterownicza;
29) PN-HD 60364-5-534:2012 Instalacje elektryczne niskiego napięcia - Część 5-53: Dobór i montaż wyposażenia elektrycznego - Odłączanie izolacyjne, łączenie i sterowanie - Sekcja 534: Urządzenia do ochrony przed przepięciami;
30) PN-IEC 60364-5-56:2010 Instalacje elektryczne niskiego napięcia - Część 5-56: Dobór i montaż wyposażenia elektrycznego - Instalacje bezpieczeństwa;
31) PN-EN 61140:2005/AI:2008 Ochrona przed porażeniem prądem elektrycznym - Wspólne aspekty instalacji i urządzeń;
32) PN-EN 62305-4:2011 Ochrona odgromowa - Część 4: Urządzenia elektryczne i elektroniczne w obiektach;
33) PN-EN 1363-1:2012 Badania odporności ogniowej - Część 1: Wymagania ogólne;
34) PN-EN 50200:2003 Metoda badania palności cienkich przewodów i kabli bez ochrony specjalnej stosowanych w obwodach zabezpieczających;
35) PN-EN 50174-2:2010/Ap1:2016-12 Technika Informatyczna - Instalacje okablowania - Część 2: Planowanie i wykonywanie instalacji wewnątrz budynków;

36) PN-EN 1021-1:2007 Meble - Ocena zapalności mebli tapicerowanych - Część 1: Źródło zapłonu: tlący się papieros;
37) PN-EN 1021-2:2007 Meble - Ocena zapalności mebli tapicerowanych - Część 2: Źródło zapłonu: równoważnik płomienia zapałki;
38) PN-B-02852:2001 Ochrona przeciwpożarowa budynków - Obliczanie gęstości obciążenia ogniowego oraz wyznaczanie względnego czasu trwania pożaru (w zakresie części dotyczącej gęstości obciążenia ogniowego - pkt 2);
39) PN-B-02855:1988 Ochrona przeciwpożarowa budynków - Metoda badania wydzielania toksycznych produktów rozkładu i spalania materiałów;
40) PN-EN ISO 6940:2005 Wyroby włókiennicze - Zachowanie się podczas palenia - Wyznaczanie zapalności pionowo umieszczonych próbek;
41) PN-EN ISO 6941:2005 Wyroby włókiennicze - Zachowanie się podczas palenia - Pomiar właściwości rozprzestrzeniania się płomienia na pionowo umieszczonych próbkach;
42) PN-EN 13501-1 Klasyfikacja ogniowa wyrobów budowlanych i elementów budynków - Część 1: Klasyfikacja na podstawie badań reakcji na ogień;
43) PN-EN 13501-2 Klasyfikacja ogniowa wyrobów budowlanych i elementów budynków - Część 2: Klasyfikacja na podstawie badań odporności ogniowej, z wyłączeniem instalacji wentylacyjnej;
44) PN-EN 13501-4 Klasyfikacja ogniowa wyrobów budowlanych i elementów budynków - Część 4: Klasyfikacja na podstawie wyników badań odporności ogniowej elementów systemów kontroli rozprzestrzeniania dymu;
45) PN-B-02151-3:2015-10 Akustyka budowlana - Ochrona przed hałasem w budynkach - Część 3: Wymagania dotyczące izolacyjności akustycznej przegród w budynkach i elementów budowlanych;
46) PN-B-02151-02:1987/Ap1:2015-05 Akustyka budowlana - Ochrona przed hałasem pomieszczeń w budynkach - Dopuszczalne wartości poziomu dźwięku w pomieszczeniach;
47) PN-B-02156:1987 Akustyka budowlana - Metody pomiaru dźwięku w budynkach.

IV.
POMIARY POWYKONAWCZE
I PRZECIWINWIGILACYJNE BADANIE ZABEZPIECZONEGO POMIESZCZENIA

Po zakończeniu prac zabezpieczających przeprowadzimy udokumentowane pomiary izolacyjności akustycznej przegród z wyłączonym i z aktywnym systemem wibroakustycznym oraz poziomu tłumienności elektromagnetycznej.

Pomiary izolacyjności akustycznej zostaną przeprowadzone osobno dla każdej z przegród zgodnie z następującym schematem.



schemat powykonawczych czynności pomiarowych

Analogicznie przeprowadzamy pomiar tłumienności elektromagnetycznej.

Po zakończeniu prac zabezpieczających przeprowadzimy również badanie objętego usługą pomieszczenia w celu identyfikacji i neutralizacji ukrytych urządzeń do pozyskiwania informacji. Badanie będzie polegać na wykonaniu kompleksowego sprawdzenia sali, w tym: jego ścian, sufitu, podłogi, drzwi oraz wszystkich elementów jego wyposażenia w następującym zakresie:

- wykrywanie i lokalizacja cyfrowych i analogowych elektronicznych systemów emisji radiowej, telewizyjnej, elektromagnetycznej oraz telefonii komórkowej,
- wykrywanie i lokalizacja środków zapisu audio (dyktafony, magnetofony analogowe i cyfrowe),
- wykrywanie ukrytych mikrofonów przewodowych,
- pomiar poziomu tła elektromagnetycznego i jego odchyleń,
- wykrywanie i identyfikacja podsłuchów laserowych i podsłuchów w podczerwieni,
- wykrywanie i lokalizacja obiektywów optycznych (ukrytych kamer video),
- sprawdzenie linii i urządzeń elektrycznych,
- sprawdzenie elementów sieci informatycznej,
- sprawdzenie linii telefonicznych.

Badanie przeprowadzą nasi specjaliści, którzy posiadają wieloletnie doświadczenie zawodowe w tej dziedzinie oraz posługują się profesjonalnym, specjalnie do tego celu dedykowanym najnowocześniejszym sprzętem.

Do badań wykorzystujemy miedzy innymi:

- skaner spektrum radiowego OSCOR do wykrywania i identyfikacji sygnałów analogowej i cyfrowej transmisji radiowej w zakresie do 34MHz do 24GHz;

- detektor złącz nieliniowych NR 900V oraz detektor ORION przeznaczony do wykrywania i lokalizacji aktywnych i nieaktywnych urządzeń elektronicznych typu mikronadajniki radiowe, dyktafony itp.

- multidetektor MDS4002 przeznaczony do wykrywania źródeł transmisji radiowej, wykrywania mikrofonów laserowych, mikrofonów przewodowych, a także sprawdzania linii telefonicznych i elektrycznych;

- system monitorowania transmisji radiowych składający się jednostki centralnej współpracującej z komputerem przenośnym oraz modułów czułych selektywnych analizatorów częstotliwości MRA5Q służących do skanowania i wykrywania aktywnych sygnałów analogowej i cyfrowej transmisji radiowej w zakresie częstotliwości od 34 MHz do 5,9 GHz.

Systemy, na których pracujemy wykrywają i informują o wszelkich sygnałach w nadzorowanym paśmie częstotliwości 34 MHz - 24 GHz. W przypadku wykrycia emisji radiowej przez analizator MRA5Q jest ona identyfikowana i wraz z sygnałem alarmowym w oknie dialogowym użytkownika wyświetlane są informacje dotyczące poziomu sygnału wraz z protokołem transmisji oraz wykresem spektralnym

Należy jednak wskazać, iż utrzymywanie stałego poziomu bezpieczeństwa wymaga okresowego powtarzania wyżej opisanego badania raz na kwartał lub raz na 6 miesięcy, ewentualnie także przed każdym szczególnie ważnym spotkaniem. W celu zaś zapewnienia najwyższego poziomu zabezpieczenia, pomieszczenie które wcześniej podlegało sprawdzeniu, a w którym planowane jest odbycie szczególnie istotnego spotkania, możemy także objąć dyżurem przeciwinwigilacyjnym.

W czasie dyżuru przy pomocy specjalistycznych urządzeń dyskretnie sprawdzamy w celu identyfikacji i neutralizacji nieformalnych urządzeń do pozyskiwania informacji, wszystkie wchodzące osoby (np. osoby obsługi kelnerskiej) oraz wszelkie przedmioty wnoszone do zabezpieczanego pomieszczenia.

Na życzenie możemy też dokonać perlustracji innych miejsc i pomieszczeń takich jak sale restauracyjne, pokoje hotelowe, domy i mieszkania, czy środki transportu.

V.
USŁUGI TOWARZYSZĄCE, GWARANCJA

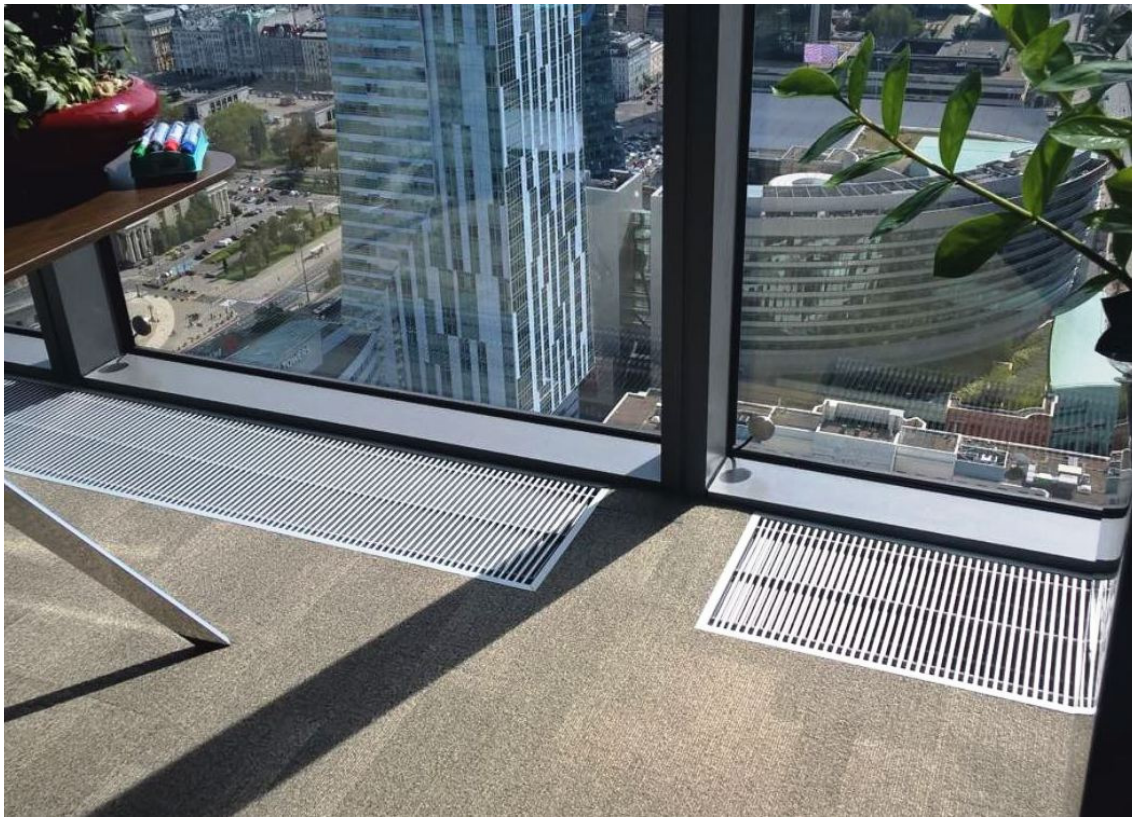
Po wykonaniu usługi przeprowadzamy szkolenie z obsługi poszczególnych komponentów zainstalowanych zabezpieczeń oraz przekazujemy Zleceniodawcy kompletną techniczną dokumentację wykonawczą i powykonawczą obejmującą w szczególności:

- dokumentację fotograficzną elementów przykrytych;
- pisemny raport z wykonanych pomiarów izolacyjności akustycznej przegród z wyłączonym i z aktywnym systemem wibroakustycznym;
- pisemny raport z wykonanych pomiarów tłumienności elektromagnetycznej;
- pisemny protokół z poświadczeniem poziomu zagrożenia stwierdzonego w czasie badania objętego usługą pomieszczenia mającego na celu identyfikację i neutralizację ukrytych urządzeń do pozyskiwania informacji, które zostanie przeprowadzone zgodnie z pkt IV oferty;
- instrukcje obsługi, procedury eksploatacji, monitorowania i kontroli zainstalowanych systemów, oraz zakres obowiązków administratora zabezpieczonego pomieszczenia,
- certyfikaty i gwarancje.

Ponadto przeprowadzimy kompleksowe szkolenie wskazanych pracowników Zleceniodawcy z obsługi wszystkich zainstalowanych systemów i dostarczonych urządzeń.

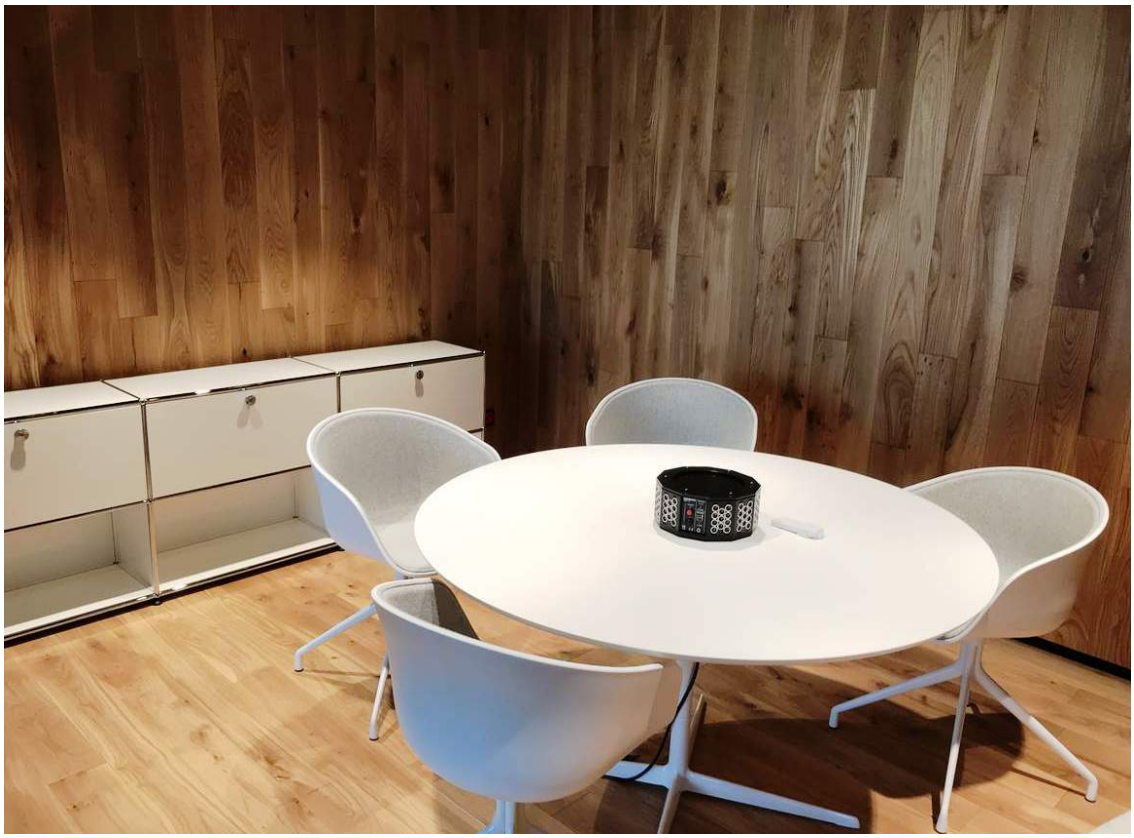
Na wszystkie wykonane systemy oraz dostarczone urządzenia udzielimy dwuletniej gwarancji.

VI.
PRZYKŁADOWE REALIZACJE



gabinet - system wibroakustyczny

sala konferencyjna Zarządu - system wibroakustyczny, ekranowanie akustyczne



sala konferencyjna - zintegrowany system zabezpieczenia przeciwinwigilacyjnego, system Protektor

strefa specjalna - system wibroakustyczny, ekranowanie akustyczne, ekranowanie elektromagnetyczne, strefa kontroli z detektorem ferromagnetycznym, depozyt, system kontroli dostępu

Jeżeli niniejsza oferta spotkała się z Państwa zainteresowaniem, to nasz zespół jest do Państwa dyspozycji. W celu uzyskania dodatkowych szczegółów oraz informacji o naszej firmie i warunkach współpracy prosimy o kontakt:

tel.: (+48) 22 550 47 11
fax: (+48) 22 550 47 90

e-mail 1: zabezpieczenia@transfarm.pl
e-mail 2: biuro@transfarm.pl

Nasza strona internetowa: www.transfarm.pl