

Приватне акціонерне товариство «Вищий навчальний заклад»
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»

ЗАТВЕРДЖУЮ

Форма навчання – денна
Термін навчання: 0,5 міс.– 90 год.

Т.в.о. ректора ПрАТ «ВНЗ «МАУП»

Михайло ГОНЧАРЕНКО

«21» липня 2025 р.

РОБОЧИЙ НАВЧАЛЬНИЙ ПЛАН З ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ
відповідно до ліцензії з напрямку (спеціальності)
256 «Національна безпека»
за програмою
«Технічні системи захисту інформації»

№	Назва дисципліни	Кількість годин						Кредити ЄКТС
		Теоретичних	Практичних	Залік	Екзамен	Всього	Самостійна робота	
1.	Загальна характеристика технічних каналів витоку інформації	2	0			2		
2.	Вібро-акустичний та параметричний канали витоку інформації	2	4			6		
3.	Електричний, електромагнітний та оптично-електронний канали витоку інформації	2	4			6		
4.	Основи методів технічного захисту інформації	4	0	2		6	9	
5.	Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами	4	4			8		
6.	Методи пошуку і блокування засобів негласного отримання інформації	4	4			8	7	
7.	Методи технічного захисту інформації від витоку вібро-акустичними та параметричними каналами	4	4			8	7	
8.	Методи технічного захисту інформації від витоку електричними, електромагнітними та оптично-електронними каналами	4	4			8	7	
9.	Системи відеоспостереження, охоронних сигналізацій, контролю доступу	4	2		2	8		
Всього:		30	26	2	2	60	30	3

Директор Інституту безпеки

Сергій ЛИСЕНКО

Директор Інституту освіти дорослих

Юлія КУЗЬМІНСЬКА

**Приватне акціонерне товариство «Вищий навчальний заклад»
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»**

ЗАТВЕРДЖУЮ

Форма навчання – денна

Термін навчання: 0,5 міс.– 90 год.

Т. в. о. ректора ПрАТ «ВНЗ «МАУП»



Михайло ГОНЧАРЕНКО

«21» липня 2025 р.

**РОБОЧА НАВЧАЛЬНА ПРОГРАМА
З ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ
відповідно до ліцензії з напрямку (спеціальності)
256 «Національна безпека»
за програмою
«Технічні системи захисту інформації»**

Київ 2025 рік

ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Загальна характеристика технічних каналів витоку інформації

Поняття технічного каналу витоку інформації. Класифікація технічних каналів витоку: акустичні, віброакустичні, електромагнітні, оптичні, електроживильні, комбіновані. Джерела технічного витоку інформації в організаціях та об'єктах критичної інфраструктури. Основні методи перехоплення інформації: побічні випромінювання, наведення, використання шкідливих технічних засобів. Акустичний витік: механізми формування, методи виявлення та захисту. Електромагнітне випромінювання як канал витоку: особливості генерації та поширення, засоби контролю. Оптичні канали витоку: використання відбитого світла, лазерних мікрофонів, оптичних сенсорів. Технічні пристрої для несанкціонованого отримання інформації: диктофони, мікрокамери, закладні пристрої, SDR-монітори, інші спеціальні технічні засоби розвідки (СТЗР). Методи виявлення ТКВІ: радіоконтроль, аналіз спектру, технічне обстеження, неруйнівний контроль середовища. Основи технічного захисту інформації: екранування, акустична ізоляція, фільтрація каналів живлення, використання перешкод і глушіння.

Системи захисту від витоку інформації: організаційні, інженерно-технічні, програмно-апаратні заходи. Нормативно-правова база захисту інформації в Україні: Закон України «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», стандарти та технічні регламенти. Міжнародні стандарти і підходи до технічного захисту інформації. Оцінка ризиків технічного витоку інформації: фактори, що впливають на ймовірність та шкоду, методи моделювання загроз. Особливості організації безпечного інформаційного простору в умовах гібридної війни та кібершпигунства.

Тема 2. Вібро-акустичний та параметричний канали витоку інформації

Вібро-акустичний канал витоку інформації. Механізми утворення вібро-акустичних сигналів у результаті мовлення, роботи техніки, вібрацій конструкцій приміщення. Передача інформації через конструктивні елементи будівель, системи вентиляції, труби, меблі, елементи освітлення. Методи знімання інформації за допомогою контактних і безконтактних вібродатчиків, лазерних віброметрів, акселерометрів. Приклади практичного використання вібро-акустичних каналів у шпигунських технологіях. Засоби виявлення та блокування вібро-акустичних каналів: демпфування, антивібраційна ізоляція, шумогенерація, конструктивні рішення приміщень.

Параметричні канали витоку інформації як результат функціонування інформаційно-технічних систем. Основні фізичні параметри, що можуть бути змінені під впливом обробки інформації — струм, напруга, температура, електромагнітне поле, споживана потужність. Принципи побудови параметричних каналів — виявлення інформації за непрямыми ознаками. Канали витоку через фонові випромінювання пристроїв, зміну параметрів навколишнього середовища, споживання енергії. Методи аналізу електроживлення. Засоби захисту: екранування, стабілізація

енергоспоживання, фізичне розмежування, використання криптографічно стійких апаратних рішень.

Тема 3. Електричний, електромагнітний та оптично-електронний канали витоку інформації

Виток інформації в технічних системах. Загальні характеристики та класифікація каналів технічного витоку. Електричні канали витоку інформації: особливості формування побічних електричних сигналів; механізми проникнення інформації в мережі електроживлення та заземлення; основні методи перехоплення інформації через параметри споживаної потужності. Способи зняття інформації з силових мереж: наведення, контактні підключення, електричний аналіз. Засоби протидії електричному витоку: фільтрація, стабілізація напруги, розподіл мереж живлення.

Електромагнітні канали витоку інформації: класифікація побічних електромагнітних випромінювань; особливості поширення побічних сигналів у просторовому середовищі; вплив типу обладнання та середовища експлуатації. Джерела ЕМ-випромінювань: комп'ютери, монітори, мережеві пристрої, периферія. Методи електромагнітного перехоплення інформації, сучасні технічні засоби зчитування. Створення безпечних зон: екранування, заземлення, глушіння. Нормативна база забезпечення електромагнітної сумісності та захисту в Україні та світі.

Оптично-електронні канали витоку інформації: поняття та класифікація; принципи витоку інформації через світлові та оптичні випромінювання. Джерела: світлодіодні індикатори, дисплеї, екрани, відбиття з поверхонь, лазерні сигнали. Методи зняття інформації: аналіз оптичних змін, відеоспостереження, зчитування відбиттів, лазерні мікрофони. Загрози, пов'язані з віддаленим оптичним моніторингом. Технічні засоби виявлення оптичного витоку. Методи протидії: затемнення, маскування, структурне розмежування, блокування оптичного поля огляду.

Комплексна оцінка ризиків технічного витоку інформації. Взаємозв'язок електричних, електромагнітних та оптично-електронних каналів у комбінованих загрозах. Впровадження організаційно-технічних заходів захисту інформації на об'єктах критичної інформаційної інфраструктури. Сучасні стандарти, нормативні документи та перспективні технології забезпечення технічної інформаційної безпеки.

Тема 4. Основи методів технічного захисту інформації

Поняття технічного захисту інформації. Класифікація інформації з обмеженим доступом. Законодавче та нормативне забезпечення у сфері технічного захисту інформації (ТЗІ). Основні поняття та терміни в галузі ТЗІ. Суб'єкти забезпечення технічного захисту інформації. Методи і засоби забезпечення конфіденційності, цілісності, доступності інформації в технічних системах. Основи аналізу загроз витоку інформації. Канали технічного витоку інформації: електромагнітні, електричні, віброакустичні, оптичні, параметричні. Механізми реалізації загроз і приклади витоку інформації в практиці діяльності державних органів, підприємств і організацій.

Захисні бар'єри та організаційно-технічні заходи запобігання витоку інформації: екранування, заземлення, фільтрація, блокування каналів, маскування інформаційних сигналів. Основи побудови захищених приміщень та зон обмеженого доступу. Методи контролю та виявлення каналів витоку: активні та пасивні засоби технічного контролю, моніторинг електромагнітної обстановки. Основи сертифікації технічних засобів на відповідність вимогам захисту інформації. Принципи створення систем технічного захисту інформації в автоматизованих системах. Структура комплексної системи захисту інформації. Основні етапи та методики проведення атестації об'єктів інформаційної діяльності.

Методи захисту інформації в каналах зв'язку: екранування та шифрування сигналів, криптографічні та стеганографічні методи. Засоби обмеження несанкціонованого доступу: системи контролю доступу, фізичний захист інформаційних носіїв, облік і зберігання технічних засобів. Практичні аспекти впровадження ТЗІ: проектування, аудит, технічна експертиза. Новітні тенденції в розвитку методів технічного захисту інформації, кіберфізичні загрози, бездротові канали витоку, захист IoT-пристроїв. Інтеграція ТЗІ в загальну систему управління інформаційною безпекою на підприємстві чи в установі.

Тема 5. Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами

Теоретичні основи технічного захисту інформації: поняття про побічні випромінювання та наведення, інформаційні сигнали та їх уразливість. Сутність і характеристика пасивних методів захисту: екранування технічних засобів, фільтрація сигналів, заземлення, застосування поглинаючих матеріалів, просторове розмежування, фізичне блокування каналів витоку. Створення захищених приміщень, зон контролю доступу, структурована організація робочих місць. Системи електроживлення та їх роль у захисті інформації.

Активні методи протидії витоку інформації: генератори шумових перешкод, створення маскуючих сигналів, вплив на засоби несанкціонованого зняття інформації. Технічні засоби активного захисту: активні завади, блокатори акустичних хвиль, пристрої локалізації побічних сигналів. Особливості застосування активного захисту в автоматизованих системах, обмеження і ризики використання активних засобів у реальних умовах. Системи моніторингу технічної безпеки: виявлення закладних пристроїв, зчитування побічних сигналів, контроль електромагнітного фону. Засоби виявлення небезпечних технічних пристроїв, аудити ТЗІ.

Оцінювання ефективності захисних заходів, порівняльний аналіз методів, вибір оптимальної стратегії захисту. Комплексне застосування пасивних та активних засобів у структурі технічної системи безпеки. Нормативно-правове забезпечення в галузі технічного захисту інформації. Стандарти і вимоги до пасивних і активних засобів захисту, сертифікація та атестація засобів. Перспективи розвитку активних та пасивних технологій захисту в умовах швидкого розвитку інформаційних технологій, зокрема

бездротових і мобільних комунікацій, штучного інтелекту та квантових технологій.

Тема 6. Методи пошуку і блокування засобів негласного отримання інформації

Засоби негласного отримання інформації (ЗНОІ). Класифікація ЗНОІ: електронні пристрої прихованого аудіо та відеоконтролю, радіозакладки, лазерні та акустичні системи зняття інформації, мікрофони спрямованої дії, GSM/Wi-Fi-жучки, оптико-електронні системи спостереження. Правові та нормативні засади протидії засобам несанкціонованого отримання інформації в Україні. Технічні принципи роботи ЗНОІ: види випромінювань, принципи активації, механізми передачі інформації. Особливості їх маскування в об'єктах інформаційної діяльності.

Методи пошуку закладних пристроїв: радіочастотний моніторинг, аналіз електромагнітного середовища, нелінійна локація, тепловізійний контроль, виявлення паразитних сигналів у лініях живлення та комунікації. Використання аналізаторів спектра, нелінійних локаторів, інфрачервоних детекторів, засобів пошуку активних і пасивних пристроїв. Професійне інструментальне сканування приміщень та каналів витoku. Методики перевірки електроживлення, заземлення, вентиляційних та кабельних трас, корпусів технічних засобів, предметів обстановки. Оцінка сигнатур ЗНОІ.

Методи блокування засобів негласного зняття інформації: створення електромагнітних та акустичних завад, застосування генераторів шуму, екранування, організація захищених приміщень, активне глушіння каналів передачі даних. Інженерно-технічне моделювання приміщень для зниження ризику установки ЗНОІ. Організація режиму безпеки, фізичний контроль доступу, заходи персональної інформаційної гігієни, розробка маршрутів обходу та регулярного контролю зон підвищеної уваги.

Комплексні системи технічного захисту від ЗНОІ: інтеграція систем виявлення, нейтралізації, ізоляції та моніторингу в загальну структуру інформаційної безпеки. Особливості захисту мобільних і тимчасових об'єктів. Актуальні тенденції: мініатюризація, бездротові технології, керування через Інтернет речей (IoT). Стандарти технічного контролю та процедур пошуку в умовах цифрового середовища. Практичні тренінги з виявлення засобів ЗНОІ. Перспективи розвитку систем активного захисту від негласного отримання інформації.

Тема 7. Методи технічного захисту інформації від витoku вібро-акустичними та параметричними каналами

Вібро-акустичний та параметричний канал витoku інформації. Фізичні основи утворення побічних вібро-акустичних випромінювань та коливань: механічні коливання конструкцій, резонансні явища, акустичні хвилі, перетворення мовного сигналу у вторинні акустичні поля. Класифікація джерел вібро-акустичних випромінювань: голос людини, вібрації обладнання, технічні засоби комунікації. Основні механізми витoku інформації параметричними каналами: зміна характеристик електричних параметрів унаслідок мовлення або іншої активності, модуляція сигналів. Оцінка зон

ризикі та рівнів загроз при роботі в закритих приміщеннях і на відкритому просторі.

Методи виявлення вібро-акустичних каналів витоку: аналіз спектру коливань, вимірювання акустичного фону, використання датчиків тиску та прискорення, акустичних аналізаторів, лазерних мікрофонів. Підходи до моделювання шляхів поширення вібрацій. Технічні засоби оцінки ефективності шумоізоляції та віброзахисту. Ідентифікація параметричних каналів за зміною вхідних і вихідних сигналів у проводових і безпроводових системах.

Пасивні методи захисту інформації: звукопоглинаючі матеріали, вібропоглиначі, антивібраційні конструкції, розрив механічного зв'язку між джерелом інформації та елементами конструкцій, герметизація приміщень, багатошарова структура стін, вікон, дверей. Архітектурно-будівельні рішення для мінімізації поширення вібрацій. Екранування та механічна ізоляція джерел коливань. Методи дезактивації небезпечних об'єктів.

Активні методи протидії: генерація завад і шумів у віброакустичному діапазоні, інфразвукове або ультразвукове маскування мовних сигналів, активне гасіння вібрацій. Пристрої генерації шуму, створення контрольованого звукового поля в приміщенні. Системи блокування параметричних каналів: стабілізація електричних параметрів, електричне екранування, фільтрація сигналів у мережах живлення, захист від індуктивних наведень.

Організаційно-технічні заходи із запобігання витоку: регламент доступу до приміщень, часова синхронізація мовної активності, розділення простору на зони, періодична перевірка приміщень засобами технічного контролю. Оцінювання ефективності реалізованих заходів. Регламентуюча база, стандарти та нормативні документи щодо захисту інформації від віброакустичних і параметричних каналів. Розвиток інноваційних засобів технічного захисту в умовах застосування високочутливих сенсорів і технологій дистанційного спостереження.

Тема 8. Методи технічного захисту інформації від витоку електричними, електромагнітними та оптично-електронними каналами

Технічні канали витоку інформації, їх класифікація за фізичними принципами. Природа електричних, електромагнітних і оптично-електронних каналів витоку інформації. Джерела електричних сигналів, які можуть стати об'єктами технічної розвідки. Витік інформації через лінії живлення, заземлення, інформаційні кабелі, електричні схеми апаратури. Електромагнітне випромінювання як наслідок роботи електронних пристроїв: монітори, процесори, мережеві інтерфейси. Побічні електромагнітні поля, наведення, ретрансляція сигналів. Основи теорії побічного електромагнітного випромінювання (ПЕМВ) та компрометувальних сигналів (КС). Оптично-електронні засоби спостереження: лазерна прослушка, телескопічні та інфрачервоні системи, оптичне зчитування з елементів індикації та відбитків світла.

Методи виявлення каналів витоку: аналіз електричних та магнітних параметрів систем, вимірювання рівня ПЕМВ, виявлення електромагнітного

фону, перевірка елементів кабельної інфраструктури, виявлення нелегітимних джерел оптичного випромінювання. Використання спектроаналізаторів, осцилографів, нелінійних локаторів, тепловізорів, фотомультіплікаторів, детекторів лазерного випромінювання. Методи моделювання поширення сигналів у середовищі та виявлення слабких місць у структурі систем зв'язку.

Пасивні методи захисту: використання екранів з електропровідних матеріалів (металевих шаф, сіток, фольги), заземлення, фільтрація вхідних та вихідних сигналів, просторове рознесення елементів систем, сегментація інфраструктури, ізоляція кабелів, впровадження захисних оболонок. Використання оптичного волокна замість електропровідних середовищ для передавання інформації.

Активні методи: генерація електромагнітних завад, активне маскування корисного сигналу, застосування генераторів шуму у відповідних частотних діапазонах, періодичне змінення параметрів сигналів, цифрове шифрування з паралельним фізичним захистом каналів передавання. Методи «білого шуму», глушіння активних каналів витоку, використання засобів контролю цілісності каналів передавання.

Організаційні заходи захисту: зонування приміщень за рівнями електромагнітної безпеки, створення контрольованих зон, обмеження використання електронних пристроїв, режимно-пропускні заходи. Проведення регулярних вимірювань ПЕМВ та електричного фону. Розробка комплексної системи технічного захисту інформації (КСТЗІ), яка поєднує технічні, інженерні та процедурні рішення. Вимоги міжнародних стандартів (Tempest, ISO/IEC 11801, ISO/IEC 27001), нормативно-правова база України щодо електромагнітної безпеки та захисту інформації.

Тема 9. Системи відеоспостереження, охоронних сигналізацій, контролю доступу

Поняття, призначення та класифікація технічних засобів охорони. Основи побудови інтегрованих систем безпеки об'єктів. Складові системи фізичної безпеки. Загальна характеристика систем відеоспостереження: типи камер (аналогові, цифрові, IP-камери), параметри відеозображення, методи обробки відеопотоку, архівація даних. Побудова локальних і віддалених систем відеоконтролю. Використання штучного інтелекту у відеоаналітиці: виявлення облич, трекінг руху, аналіз поведінки. Принципи побудови структурованих систем відеоспостереження для підприємств, державних установ, стратегічних об'єктів.

Системи охоронної сигналізації: класифікація засобів (об'ємні, периметральні, точкові), принцип дії датчиків руху, розбиття скла, вібрації, відкривання. Підключення та взаємодія датчиків з центральним блоком управління. Програмне забезпечення для моніторингу та реагування. Технології дротової і бездротової сигналізації. Методи дублювання каналів зв'язку. Підключення до пультів централізованого спостереження.

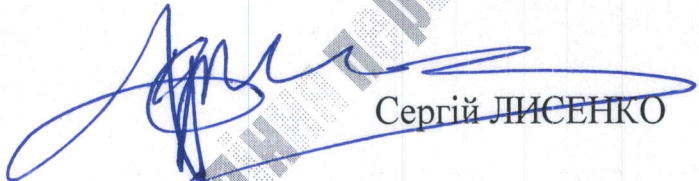
Системи контролю та управління доступом (СКУД): функціональні можливості, архітектура, апаратні та програмні компоненти. Ідентифікація користувачів: карти доступу, кодові клавіатури, біометричні параметри

(відбитки пальців, райдужна оболонка ока, розпізнавання облич). Принципи обліку та обмеження доступу до приміщень і ресурсів. Журнали подій, звітність, інтеграція з системами обліку робочого часу. Побудова розподілених СКУД у великих організаціях.

Інтеграція систем відеоспостереження, сигналізації та контролю доступу в єдину інформаційно-аналітичну платформу. Вимоги до електроживлення та резервування систем безпеки. Мережеві інтерфейси, канали зв'язку, стандарти обміну даними. Захист інформації в межах технічних систем безпеки: шифрування, автентифікація, цифровий журнал подій. Аудит безпеки та виявлення інцидентів. Нормативно-правова база України щодо експлуатації систем охоронного призначення.

Планування, проектування та впровадження комплексної системи безпеки для об'єктів різної категорії захисту. Особливості захисту критичної інфраструктури. Підготовка персоналу для експлуатації та обслуговування технічних засобів охорони.

Директор Інституту безпеки


Сергій ЛИСЕНКО

Директор Інституту освіти дорослих


Юлія КУЗЬМІНСЬКА

Міжвузівська Академія