„СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ”

Кафедра компютерної інженерії та кібербезпеки

ЛЕКЦІЯ №1
з навчальної дисципліни
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

- **Тема 1. Передумови утворення каналів витоку інформації**
- **Заняття № 1. Введення в дисципліну. Загальна характеристика методів розвідки. Канали поширення інформації та способи несанкціонованого доступу до інформації**

- **1 питання. Предмет і завдання навчальної дисципліни. Література.**
- **2 питання. Канали поширення інформації та способи несанкціонованого доступу до інформації**

Література

1. Поповський В.В., Персіков А.В. Захист інформації в телекомунікаційних системах. Том 1, Том 2.-Харків 2008.
2. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 № 1229.
3. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
4. НД ТЗІ 1.6-003-04 Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.
5. https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf
6. https://nni1.naiau.kiev.ua/files/KIT/pidruchnik.doc
7. http://bit.nau.edu.ua/vydannya/pidruchnyky/2935
8. http://bit.nau.edu.ua/vydannya/pidruchnyky/3312

Питання 2. Канали поширення інформації та способи несанкціонованого доступу до інформації

- **Поняття *промислове шпигунство*** виникло разом з появою промисловості і є невід'ємною часткою стосунків в країнах, де на ряду з державною існують і інші форми власності.
- ***Суть промислового шпигунства*** *– це прагнення до опанування секретів конкурентів з метою отримання максимальної комерційної вигоди.*

- **Основні способи ведення розвідувальних (шпигунських) дій можуть бути представлені у вигляді трьох основних груп:**
  - **• на основі відкритих джерел;**
  - **• шляхом використання суб'єктів – носіїв інформації;**
  - **• через технічні канали.**

відкриті джерела

- **До використання *відкритих джерел* відносяться способи добування інформації, що реалізуються шляхом:**
  - **аналізу газет**
  - **книг**
  - **наукових і технічних видань**
  - **офіційних звітів**
  - **рекламних матеріалів.**
- **Основна робота покладається на спеціально підготовлених аналітиків, які відсівають і накопичують необхідну інформацію.**

відкриті джерела

- **Головними напрямами отримання відкритого доступу до конфіденційної інформації у відкритих джерелах є:**
  - **• доповіді на конференціях, симпозіумах і інших зборах;**
  - **• питання, що обережно задаються фахівцями;**
  - **• спроби запросити на роботу співробітників конкуруючої фірми і заповнення ними при цьому спеціальних анкет;**
  - **• прийом на роботу, як правило з різким збільшенням окладу, службовця конкуруючої фірми (свого роду законний підкуп);**
  - **• вивчення виставкових зразків;**
  - **• надумані переговори з конкурентами про придбання ліцензії або спільної діяльності та інші.**

відкриті джерела

- **Головне правило – завжди потрібно пам'ятати про властивість інформації поступово накопичуватися.**
  - **Коли ви даєте проводити зовнішню рекламу або надаєте інтерв'ю, посилаєте звіт або робите доповідь, завжди зіставляйте їх вміст з раніше «опублікованими» матеріалами.**
  - **У поєднанні з ними Ваші напрацювання можуть мати зовсім інше значення.**
- **Збирати відкриту інформацію достатньо легко, але вона може бути і дезінформацією.**

Використання суб'єктів – носіїв інформації

- У ряді джерел конфіденційної інформації люди займають особливе місце, бо здатні виступати не лише володарями відомостей, але і суб'єктами зловмисних дій.
- На відміну від технічного пристрою їх можна:
  - підкупити,
  - шантажувати
  - просто обдурити.
- Будь-який фахівець- носій інформації, може її аналізувати, узагальнювати і робити висновки.
- За певних умов люди здатні приховувати, красти, продавати інформацію і здійснювати інші кримінальні дії аж до вступу до стійких злочинних зв'язків із зловмисниками.

Використання суб'єктів – носіїв інформації

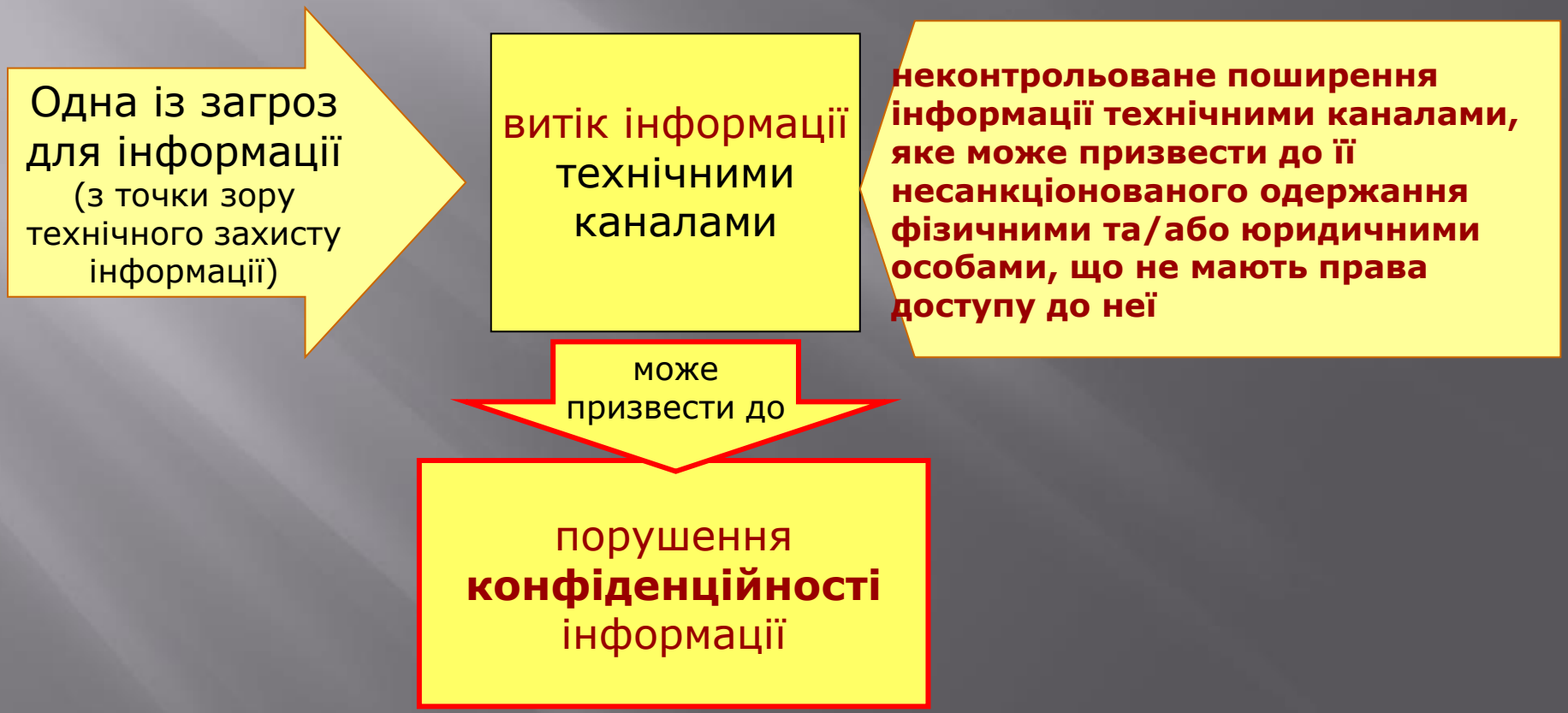
- **Процес виявлення кандидата в агенти є досить складним.**
- **На початку проводиться оцінка і розробка кандидата, тобто вивчення його особистих якостей і здібностей, а також дослідження способів його найбільш эффективного вербування і використання.**
- **Далі проводиться саме вербування шляхом**
  - **шантажу**
  - **підкупу**
  - **ідейних міркувань**
  - **особистого несприйняття керівника компанії і так далі**

Використання суб єктів – носіїв інформації

- **Для обмеження діяльності агентів необхідно, перш за все, визначити строгий порядок і виділити спеціально обладнані приміщення для ведення ділових бесід, щоб виключити навіть короткочасну «випадкову» присутність сторонніх, у тому числі і зі своїх співробітників.**
  - **Організувати максимально жорсткий облік і строго регламентувати роботи з діловими документами.**
  - **Узаконити коло осіб, що допускаються до тих або інших внутрішньофірмових секретів, заборонити співробітникам вести службові переговори з домашніх телефонів.**
  - **При сторонніх не можна називати прізвище, ім'я, по батькові співбесідника.**
  - **Призначаючи місце зустрічі, треба переходити на умовності і так далі.**

Технічні канали

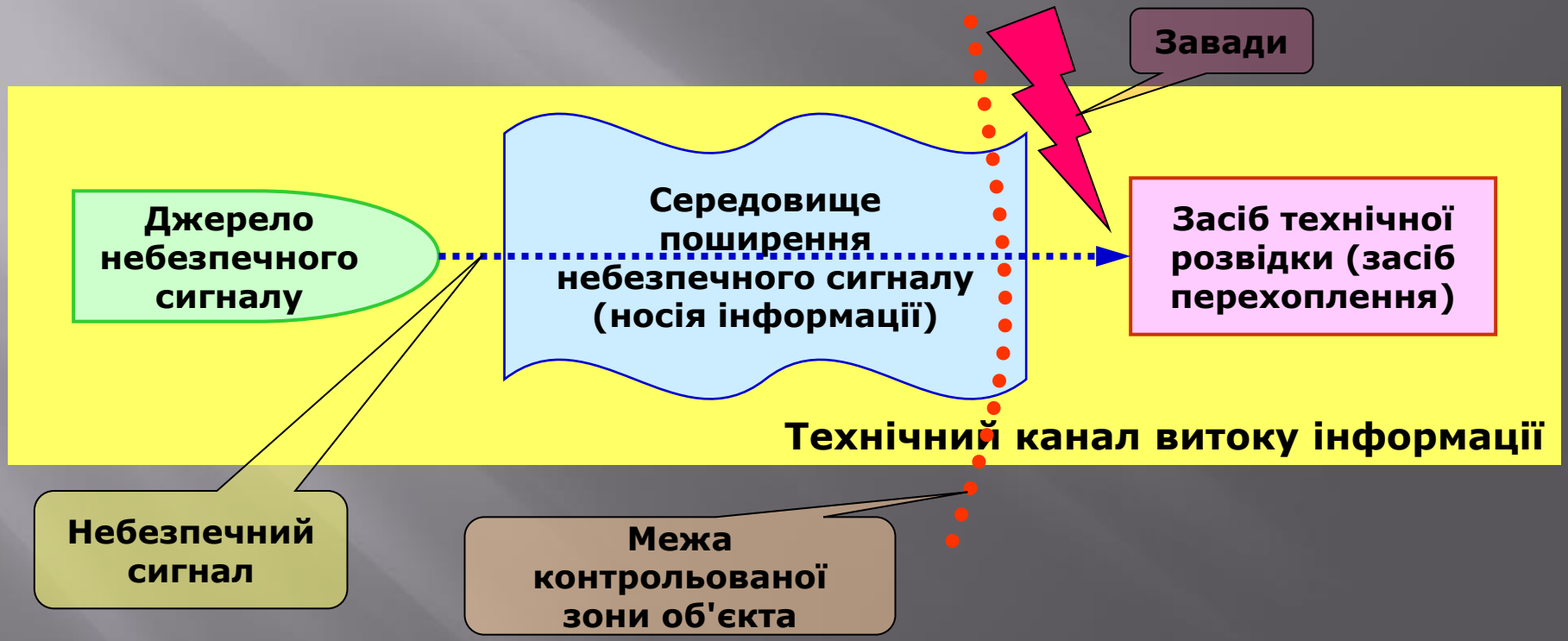
Технічні канали витоку інформації. Загальні поняття



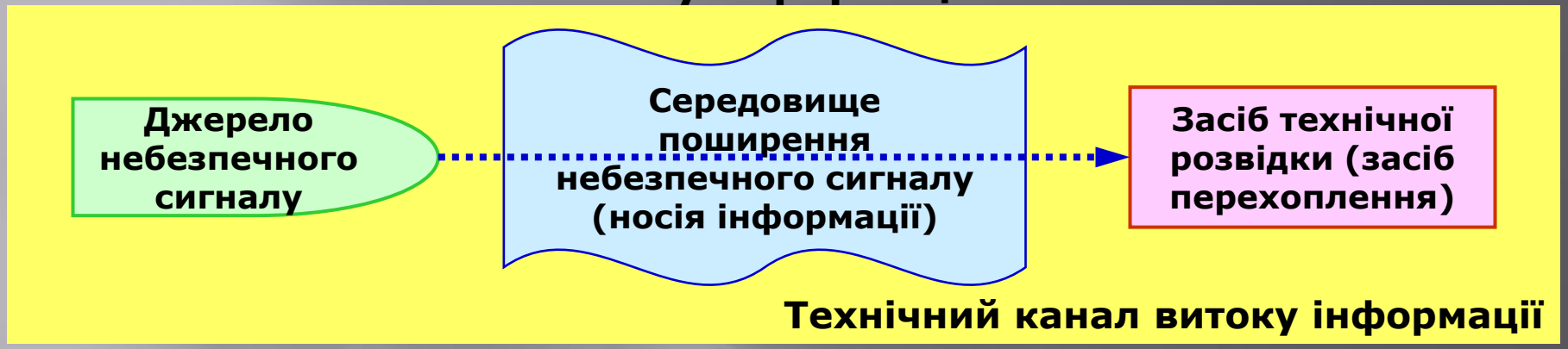
Технічні канали витоку інформації. Загальні поняття

технічний канал витоку інформації

сукупність трьох складових:
- **джерела небезпечного сигналу (носія інформації);**
- **середовища поширення небезпечного сигналу (носія інформації);**
- **засобу технічної розвідки (засобу перехоплення)**



Технічні канали витоку інформації. Загальні поняття



- **Носій інформації** - фізичне поле, сигнал чи хімічна речовина, які містять інформацію з обмеженим доступом
- **Середовище поширення носія інформації (інформативного сигналу, небезпечного сигналу)** – повітряне, водне та інші середовища; лінії електроживлення, заземлення, зв'язку, сигналізації, управління, спостереження та інші лінії; кінцеве та з'єднувальне обладнання; інженерні комунікації і спорудження, огороджувальні будівельні конструкції, світлопроникні елементи будинків і споруд (отвори); ґрунт, рослинність тощо, якими може поширюватися небезпечний сигнал
- **Засоби технічної розвідки (засоби знімання інформації)** – технічні засоби, які призначені для несанкціонованого знімання (здобування, перехоплення) інформації
- **Небезпечний сигнал** – сигнал (поле), у тому числі паразитний (побічний), або його компоненти (фрагменти) будь-якого фізичного походження, хімічна речовина, які містять інформацію, що підлягає захисту, і який може бути знятий (перехоплений) засобами технічної розвідки

Технічні канали витоку інформації. Загальні поняття

Наявність джерела небезпечного сигналу (носія інформації) та середовища поширення небезпечного сигналу (носія інформації)

обумовлює

потенційну загрозу конфіденційності інформації

За наявності і третьої складової - засобу технічної розвідки, за допомогою якого здійснюється несанкціоноване здобування інформації,

загроза реалізується

Технічні канали витоку інформації. Загальні поняття

Технічні канали витоку інформації

за природою створення поділяються на:

природні *(“ненавмисні”*) **технічні канали**

утворюються за рахунок фізичних або хімічних процесів, які супроводжують або становлять принцип оброблення інформації

штучні *(навмисні)* **технічні канали**

утворюються за рахунок формування інформативного сигналу засобами технічної розвідки (наприклад, ВЧ - нав’язування, лазерна акустика)

Технічні канали витоку інформації. Загальні поняття

Технічні канали витоку інформації. Загальні поняття

Побічне електромагнітне випромінювання і наведення (ПЕМВН) – електромагнітне випромінювання та наведення, що є побічним результатом функціонування технічного засобу і може бути носієм інформації, що підлягає захисту

канали ПЕМВН

поділяються на:

за видом середовища поширення небезпечного сигналу

- **канали побічних електромагнітних випромінювань (канали ПЕМВ);**
- **канали побічних електромагнітних наведень (канали ПЕМН).**

за причиною або фізичним явищем, завдяки яким небезпечний сигнал потрапляє в середовище поширення

- **канал побічних електромагнітних випромінювань ОТЗ;**
- **канал побічних електромагнітних випромінювань ДТЗС (випадкових антен) через наведення на них полів ПЕМВ ОТЗ;**
- **канал побічних електромагнітних наведень на лінії електроживлення ОТЗ;**
- **канал побічних електромагнітних наведень на лінії заземлення ОТЗ;**
- **канали побічних електромагнітних наведень на комунікацій (лінії електроживлення, заземлення, передачі даних тощо) ДТЗС;**
- **канали нерівномірного споживання струму при спрацюванні елементів ОТЗ.**

Технічні канали витоку інформації. Загальні поняття

Поняття та визначення:

Основні технічні засоби (ОТЗ) – розташовані на об’єкті інформаційної діяльності технічні засоби (та їх комунікації), які безпосередньо обробляють інформацію, що підлягає захисту.

Допоміжні технічні засоби та системи (ДТЗС) – розташовані на об’єкті інформаційної діяльності технічні засоби та системи (та їх комунікації), які безпосередньо не здійснюють обробку інформації, що підлягає захисту, але перебувають під впливом акустичних, електричних чи магнітних полів інформативного сигналу основних технічних засобів.

Сторонні комунікації – комунікації (телекомунікації), що проходять через ОІД (розташовані на ОІД), але не входять до складу ОТЗ та ДТЗС.

Випадкові антени - розташовані на ОІД ДТЗС та сторонні комунікації, які за рахунок ефекту електромагнітної індукції можуть виступати як перетворювачі енергії небезпечних сигналів та/або як середовища їх поширення за межі контрольованої зони.

Контрольована зона – територія (простір) навколо об’єкта інформаційної діяльності, на якій (у межах якого) виключено несанкціоноване розташування технічних і транспортних засобів та неконтрольоване перебування сторонніх осіб.

Питання 1. Предмет і завдання навчальної дисципліни

- **Предметом** вивчення навчальної дисципліни є теоретичні основи утворення каналів витоку інформації, способів несанкціонованого доступу до інформації технічними засобами і її руйнування, побудови пристроїв технічного захисту інформації та практична експлуатація технічних засобів захисту.

- **Метою навчальної дисципліни “Системи технічного захисту інформації ” є формування теоретичних знань та практичних навичок дослідження технологій передачі та обробки інформації в інформаційно-комунікаційних системах з метою виявлення можливих каналів несанкціонованого отримання інформації, вивчення причин і джерел виникнення технічних каналів просочування інформації, методів і способів несанкціонованого доступу до інформації і її руйнування, методів і технічних засобів захисту інформації, принципів побудови і експлуатації технічних засобів виявлення і захисту каналів передачі інформації.**

- *знати :*
- **класифікацію причин і джерел утворення технічних каналів просочування інформації;**
- **методи і засоби несанкціонованого отримання інформації по технічним каналам;**
- **методи і засоби руйнування інформації;**
- **технічні методи і засоби захисту інформації;**
- **технічні засоби пошуку та усунення каналів витоків інформації.**

- ***вміти :***
- **проводити аналіз можливих причин і джерел утворення технічних каналів просочування інформації;**
- **проводити аналіз технічних можливостей несанкціонованого отримання інформації в інформаційно – комунікаційних системах;**
- **застосовувати методики пошуку технічних каналів витоку інформації;**
- **застосовувати технічні засоби пошуку та заглушення каналів несанкціонованого витоку інформації**

- **На вивчення навчальної дисципліни відводиться 120 години / 4 кредитів ECTS.**
- **Із них 64 години за розкладом занять,**
  - **лекцій -32 години,**
  - **лабораторних занять 32 години.**

- **Завдання на самостійну роботу:**
- 1. Законспектувати основні положення Концепції технічного захисту інформації в Україні, затвердженої постановою Кабінету Міністрів України від 08.10.97 р., № 1126.
- 2. Законспектувати основні положення Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229.

Дякую за увагу!