**міністерство внутрішніх справ УКРАЇНИ**

**ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ**

**ВНУТРІШНІХ СПРАВ**

## ***Кафедра економічної та інформаційної безпеки***

### **ЛЕКЦІЯ**

## **з дисципліни**

**«Технічні засоби захисту об’єктів, інформації від несанкціонованого доступу»**

***Тема № 1****. Основні положення щодо організації системи захисту інформації*

**(2 години)**

для здобувачів вищої освіти ННІ ЗНПК, що навчаються на магістерському рівні вищої освіти

**Дніпро – 2019**

Лекцію підготував старший викладач кафедри економічної та інформаційної безпеки Махницький О. В.

Лекція обговорена та схвалена на засіданні кафедри

економічної та інформаційної безпеки

27.08.2019 р., протокол № 14

**ПЛАН ЛЕКЦІЇ**

Вступ

1. Умови безпеки інформації.

2. Державна політика і система ТЗІ в Україні.

3. Нормативно-правова база України у сфері ТЗІ.

Висновки

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

**Основні нормативні акти:**

1. Концепція технічного захисту інформації в Україні. Постанова КМУ №1126 8.10.97.

2. ДСТУ 3396.0-96.Захист інформації. Технічний захист інформації. Основні положення. Затверджено наказом Держстандарту України від 11.10.96 р. № 423.

3. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Затверджено наказом Держстандарту України від 19.12.96 р. № 511.

4. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р.

№200.

5. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.

6. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій систе мі.

**Підручники:**

1. Носов В.В., Манжай О.В. Організація та забезпечення інформаційної безпеки: Навч. посібник. – Харків: Вид-во Харк. нац. ун-ту внутр. справ, 2007.

**Інтернет-ресурси:**

1. Веб – портал Міністерства внутрішніх справ України [Електронний ресурс]. - Режим доступу: <http://www.mvs.gov.ua>
2. Веб – портал Національної поліції України [Електронний ресурс]. - Режим доступу: <http://www.npu.gov.ua>
3. Інформаційні ресурси Інтернет (за даними Державної науково – технічної бібліотеки України) [Електронний ресурс]. - Режими доступу: <http://www.gntb.gov.ua>/ua/e/temple.html?3.

**МЕТА ЛЕКЦІЇ**

Метою лекції є доведення основних положень щодо створення та забезпечення функціонування комплексної системи захисту інформації в підрозділах ОВС України.

**ВСТУП**

Основними завданнями вивчення дисципліни єзакладення знань та умінь із організації захисту інформації на об’єктах інформаційної діяльності як в підрозділах ОВС України, так і в інших установах; формування навичок аналізу зарубіжних систем забезпечення інформаційної безпеки з метою впровадження найкращих практик захисту інформації.

**І. ПИТАННЯ**

**Умови безпеки інформації**

Захист інформації є складовою частиною забезпечення національної безпеки України. Організація захисту інформації забезпечується правовими, організаційними і інженерно-технічними заходами. Організаційні і інженерно- технічні заходи складають суть *технічного захисту інформації*. Правові заходи захисту інформації є базисом, на який спираються організаційні і інженерно- технічні заходи щодо захисту інформації.

Що ж є об'єктом захисту? На сьогодні існує декілька сотень варіантів визначення суті терміну "інформація". Одне з визначень наступне, **інформація -** *це зафіксоване на носії уявлення про предмети, процеси, події, природні явища та інше*.

Під *фіксацією* (від лат. fixus – міцний, закріплений) розуміється закріплення чого-небудь в певному положенні або вигляді. Наприклад, письмово відомостей, думок. Інформація для свого існування завжди вимагає наявність носія.

При цьому, як носій інформації може виступати поле або речовина. В деяких випадках як носій інформації може розглядатися людина. В процесі інформаційних відносин носії можуть бути *носіями-джерелами (джерелами)* або носіями-одержувачами (одержувачами) залежно від напряму переміщення інформації. У законі України "Про інформацію" під *джерелами* інформації розуміються передбачені або встановлені Законом носії інформації: документи або інші носії інформації, які є матеріальними об'єктами, які зберігають інформацію. У загальному випадку *одержувачі сприймають* інформацію через сенсор (датчик, вимірювальний перетворювач). Процес *сприйняття* вельми складний, і складається з процесів прийому і перетворення інформації, що забезпечує віддзеркалення об'єктивної реальності і орієнтування в навколишньому світі. Сприйняття може включати:

* виявлення об'єкту в полі сприйняття;
* розрізнення окремих ознак в об'єкті;
* виділення в ньому інформативного змісту, адекватної меті дії;
* формування образу сприйняття.

У визначенні терміну "інформація" під *уявленням* розуміється образ або суть предмету, процесу, події, природного явища (і ін.), сприйняті датчиками приладів або безпосередньо органами чуття, а також створені продуктивною (що відтворює) і творчою *уявою* представників тваринного світу або елементами штучного інтелекту різних пристроїв, де *уява* це психічна діяльність, що полягає в створенні уявлень і уявних ситуацій, що ніколи в цілому не сприймалися людиною насправді. Розрізняють відтворюючу і творчу уяву.

Інформація зберігає свою сутність, якщо вона переміщається, тобто міняє свої просторові координати. Таке переміщення можна позначити двома основними операціями - читання (ознайомлення) та запис (зміна)

(рис. 1.1).





а) б)

Рис. 1.1

Якщо з ряду причин немає переміщення інформації, тобто немає можливості для одержувача усунути невизначеність відносно деякої частини довколишньої дійсності, то можна говорити, швидше за все, або про неможливість одержувачем адекватно (правильно) розпізнати сам факт наявності інформації в процесі пізнання (неможливість інтерпретації), або про відсутність фізичної можливості перенесення інформації у просторі.

У процесі своїй діяльності людина може наділити інформацію деякими властивостями, яких спочатку немає. Ці властивості користувач або власник інформації штучно створює з метою досягнення деяких бажаних умов використання інформації (носіїв інформації). Такими властивостями є:

* ***конфіденційність*** – властивість інформації бути захищеною від несанкціонованого ознайомлення (рис. 1.2);
* ***цілісність*** - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення (рис. 1.3);





Рис. 1.2 Рис. 1.3

* ***доступність*** - властивість інформації бути захищеною від
* несанкціонованого блокування доступу до неї (рис. 1.4.).

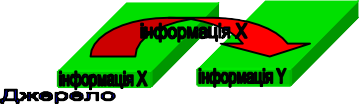


Рис. 1.4

Якщо звернути увагу на визначення створюваних властивостей інформації, то можна підкреслити, що поки не визначено власником інформації або уповноваженою їм особою

а) перелік осіб, які можуть ознайомлюватися з інформацією (для властивості конфіденційність) або змінювати інформацію (для властивості цілісність),

б) час і порядок доступу до інформації (для властивості доступність), в) порядок (спосіб) обмеження доступу до інформації інших осіб,

то зазначені властивості інформації ВІДСУТНІ.

Події, які потенційно можуть порушити одну з названих властивостей інформації відповідно, називають ***загрозами*** порушення **конфіденційності, цілісності** і **доступності інформації**.

Власне ***захист інформації*** - це визначення актуальних (бажаних) властивостей інформації (*конфіденційності*, *цілісності* і *доступності*) та протидія загрозам порушення визначених властивостей інформації.

Технічний захист інформації – це діяльність, спрямована на забезпечення організаційними і інженерно-технічними заходами конфіденційності, цілісності і доступності інформації, яка визначена власником або уповноваженою ним особою як об'єкт захисту.

Спираючись на вище приведене визначення інформації і суть технічного захисту інформації, можна сформулювати *парадигму1захисту інформації* - інформація вважається захищеною, якщо при переміщенні інформації дотримується режимна адекватність комунікабельних носіїв інформації.

**ВИСНОВКИ З ПЕРШОГО ПИТАННЯ:**

В першому питанні лекції ми розглянули базове поняття інформації та її захисту.

**ІІ. ПИТАННЯ**

**Державна політика і система ТЗІ в Україні**

Розвиток ТЗІ в Україні обумовлюється наступними основними чинниками:

* + стрімким розвитком суспільних і міждержавних відносин;
  + застосуванням технічних засобів обробки інформації і засобів зв'язку іноземного виробництва;
  + розповсюдженням засобів несанкціонованого доступу до інформації;
  + і т.д.

Нормативними документами у сфері ТЗІ визначені основні загрози безпеки інформації в Україні:

* + діяльність інших держав, що спрямована на отримання переваги в зовнішньополітичній, економічній, військовій і інших сферах;
  + недосконалість організації в Україні міжнародних виставок апаратури різного призначення (особливо пересувних) і заходів екологічного моніторингу, які можуть використовуватися для отримання інформації розвідувального характеру;
  + діяльність політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, що спрямована на отримання переваги в політичній боротьбі і конкуренції;
  + злочинна діяльність, що спрямована на протизаконне отримання інформації з метою досягнення матеріальної вигоди або нанесення шкоди юридичним або фізичним особам;
  + використання інформаційних технологій низького рівня, які приводять до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ і засобів ТЗІ;
  + недостатність документації на засоби забезпечення ТЗІ іноземного виробництва, а також низька кваліфікація технічного персоналу.

З метою протидії існуючим інформаційним загрозам в Україні йде процес створення системи ТЗІ.

Система ТЗІ визначається як сукупність:

* + суб'єктів, об'єднаних цілями і завданнями захисту інформації організаційними і інженерно-технічними заходами;
  + нормативно-правової бази;
  + матеріально-технічної бази.

Державна політика у сфері ТЗІ формується і реалізується з урахуванням наступних принципів:

* дотримання балансу інтересів особи, суспільства і держави, їх взаємної відповідальності;
* єдності підходів до забезпечення ТЗІ, які визначаються загрозами безпеки інформації і режимом доступу до неї;
* комплексності, повноти і безперервності заходів ТЗІ;
* відкритості нормативно-правових актів і нормативних документів з питань ТЗІ, які не містять відомості, що становлять державну таємницю;
* узгодженості нормативно-правових актів і нормативних документів з питань ТЗІ з відповідними міжнародними договорами України;
* обов'язковості захисту інженерно-технічними заходами:
  + інформації, яка складає державну і іншу передбачену законом таємницю;
  + конфіденційної інформації, яка є власністю держави;
  + відкритої інформації, важливої для держави, незалежно від того, де вказана інформація циркулює;
  + відкритої інформації, важливої для особи і суспільства, якщо ця інформація циркулює в державних органах, підприємствах, установах і організаціях;
* виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту:
  + конфіденційної інформації, яка не належить державі;
  + і відкритої інформації, важливої для особи і суспільства, якщо інформація циркулює поза межами державних органів, підприємств, установ і організацій;
* покладання відповідальності за формування і реалізацію державної політики у сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;
* ієрархічність побудови організаційної структури системи ТЗІ і керівництво її діяльністю у межах повноважень, визначених нормативно-правовими актами;
* методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;
* координація дій і розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації і системами забезпечення інформаційної і національної безпеки;
* фінансове забезпечення системи ТЗІ за рахунок державного бюджету України, бюджету Автономної Республіки Крим, місцевих бюджетів і інших джерел.

Спеціально уповноваженим центральним органом виконавчої влади, на який покладена відповідальність за формування і реалізацію державної політики у сфері ТЗІ згідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 [7] є Державна служба спеціального зв'язку та захисту інформації України (ДССЗ ЗІ).

Також згідно до Закону України «Про захист персональних даних» від 1.06.2010 створена Державна служба України з питань захисту персональних даних, яка має статус центрального органу виконавчої влади, і діяльність якої спрямовується і координується Кабінетом міністрів України.

Як суб'єкти в системі ТЗІ України виступають:

* ДССЗ ЗІ;
* органи, відносно яких здійснюється ТЗІ;
* державні наукові, науково-дослідні і науково-виробничі підприємства, установи і організації, які виконують завдання технічного захисту інформації;
* військові частини, підприємства, установи і організації всіх форм власності і громадяни-підприємці, які здійснюють діяльність щодо технічного захисту інформації по відповідних дозволах або ліцензіях;
* учбові заклади по підготовці, перепідготовці і підвищенню кваліфікації фахівців з технічного захисту інформації.

Всі заходи, пов'язані із захистом інформації, що є власністю держави, координуються і контролюються ДССЗ ЗІ. Основні завдання всіх суб'єктів системи ТЗІ України викладені в [4].

**ВИСНОВКИ З ДРУГОГО ПИТАННЯ:**

Під час розгляду другого питання лекції ми ознайомились з державною політика у сфері ТЗІ, з урахуванням яких принципів вона формується і реалізується.

**ІІІ. ПИТАННЯ**

**Нормативно-правова база України у сфері ТЗІ**

***Нормативно-правова база***

Рис. 1.6



**Загальнодержавні документи**

**Відомчі документи**

внутрівідомчі

міжвідомчі

Постанови уряду

Укази Президента

Стандарти

Закони, кодекси

Конституція

Відповідно до даного вище визначення нормативно-правова база є однією з базових складових частин системи технічного захисту інформації в Україні.

У загальному випадку нормативно-правову базу України можна умовно розділити на загальнодержавну і відомчу (рис. 1.6).

*Правову основу* технічного захисту інформації в Україні складають:

* Конституція України;
* Доктрина інформаційної безпеки України;
* Закони України:
  + "Про інформацію";
  + "Про державну таємницю";
  + "Про захист інформації в інформаційно-телекомунікаційних системах";
  + "Про захист персональних даних";
  + "Про Національну систему конфіденційного зв'язку";
  + "Про електронні документи і електронний документообіг";
  + "Про електронно-цифровий підпис";
* Положення "Про технічний захист інформації в Україні";
* "Концепція технічного захисту інформації в Україні";
* Державні стандарти України із захисту інформації;
* акти Президента України і Кабінету міністрів України;
* нормативно-правові акти Служби безпеки України та Державної служби спеціального зв'язку та захисту інформації України;
* ратифіковані міжнародні договори України з питань технічного захисту інформації.

На теперішній час нормативно-правову і методичну базу в сфері ТЗІ з урахуванням сфері застосування можна розділити на наступні види:

* законодавчі і концептуальні документи України в сфері ТЗІ;
* документи, що регламентують організацію ТЗІ в державних органах, організаціях, установах;
* документи, що регламентують технічний захист інформації в телекомунікаційних системах;
* документи, що регламентують захист інформації в комп'ютерних (інформаційно-телекомунікаційних ) системах від несанкціонованого доступу;
* документи, що регламентують криптографічний захист інформації;
* документи, що регламентують захист інформації від витоку по технічних каналах:
  + акустичним;
  + хімічним;
  + каналам побічних електромагнітних випромінювань і наведень (ПЕМВН);
* документи із протидії технічним розвідкам;
* документи, що регламентують господарську діяльність в сфері технічного захисту інформації;
* спеціальні нормативні документи колишнього СРСР, що включають:
  + норми ефективності захисту;
  + вимоги, вказівки, інструкції і рекомендації із захисту;
  + методики контролю і проведення спеціальних досліджень.

Стан нормативно-правової і методичної бази у сфері ТЗІ можна відстежувати на офіційному сайті ДССЗ ЗІ dsszzi.gov.ua.

**ВИСНОВКИ З ТРЕТЬОГО ПИТАННЯ:**

Під час розгляду третього питання лекції ми ознайомились з переліком документів що входять до нормативно правової бази.

**ВИСНОВКИ З ТЕМИ**

Сьогодні Ви отримали першу інформацію стосовно того, що захист інформації - це визначення актуальних (бажаних) властивостей інформації (конфіденційності, цілісності і доступності) та протидія загрозам порушення визначених властивостей інформації.

Технічний захист інформації – це діяльність, спрямована на забезпечення організаційними і інженерно-технічними заходами конфіденційності, цілісності і доступності інформації, яка визначена власником або уповноваженою ним особою як об'єкт захисту.

Спеціально уповноваженим центральним органом виконавчої влади, на який покладена відповідальність за формування і реалізацію державної політики у сфері ТЗІ згідно до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 є Державна служба спеціального зв'язку та захисту інформації України (ДССЗ ЗІ).

Стан нормативно-правової і методичної бази у сфері ТЗІ можна відстежувати на офіційному сайті ДССЗ ЗІ dsszzi.gov.ua.