**Лекція № 10:**

**Інформаційна безпека України**

1. Характеристика загроз інформаційній безпеці системи державного управління

2. Поняття інформаційної війни

3. Поняття та види загроз національним інтересам та національній безпеці в інформаційній сфері

4. Класифікація загроз

**Література**

1. Конституція України. URL:

<https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80>

1. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII. – Режим доступу: <http://zakon.rada.gov.ua/laws/show/2469-19>.
2. Ананьїн В. О. Національна безпека держави в сучасних умовах: монографія / В.О. Ананьїн, О. В. Ананьїн, В. В. Горлинський; за загальною редакцією В.О. Ананьїна. – К.: КПІ ім. Ігоря Сікорського, 2021. – 345 с.
3. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики: Вибр. наук. праці / О. С. Власюк. – К.: НІСД, 2016. – 528 с.
4. Глобальна та національна безпека: підручник / В. І. Абрамов, Г. П. Ситник, В. Ф. Смолянюк та ін. / за заг. ред. Г. П. Ситника. – К.: НАДУ, 2016. – 784 с.
5. Ліпкан В. А. Національна безпека України: навч. посібник для студ. вищих навч. закл. / В. А. Ліпкан; Національна академія внутрішніх справ. - К.: Кондор, 2008. – 552 с.
6. Ситник Г. П., Орел М. Г. Національна безпека в контексті європейської інтеграції України: підручник / Г. П. Ситник, М. Г. Орел; за ред. Г. П. Ситника. – К.: Міжрегіональна Академія управління персоналом, 2021. – 372 с.
7. Смолянюк В. Ф., Деменко О. Ф., Прибутько П. С. Основи національної безпеки України. Навчальний посібник.- К. Паливода А. В., 2017. –140 с.

***1. Характеристика загроз інформаційній безпеці системи державного управління***

Нині головним стратегічним національним ресурсом, основою економічної та оборонної могутності держави стає інформація та інформаційні технології;

1. загальна комп'ютеризація основних сфер діяльності призвела до появи широкого спектру внутрішніх і зовнішніх загроз, нетрадиційних каналів втрати інформації і несанкціонованого доступу до неї;
2. масове оснащення державних установ, підприємств, організацій і приватних осіб засобами обчислювальної техніки і включення їх до світових інформаційних просторів містить у собі реальну загрозу створення розгалужених систем регулярного несанкціонованого контролю за інформаційними процесами і ресурсами, навмисного втручання в них;
3. реальністю сьогодення стало застосування інформаційної зброї ї ведення інформаційних війн;
4. відставання вітчизняних інформаційних технологій змушує при створенні інформаційних систем закуповувати імпортну техніку і залучати іноземні фірми, через що підвищується імовірність несанкціонованого доступу до інформації, що обробляється, зростає залежність від іноземних виробників комп'ютерної і телекомунікаційної техніки, програмного забезпечення.

**Інформатизація** становить собою організаційний соціально-економічний і науково-технічний процес створення оптимальних умов для всебічного задоволення інформаційних потреб і реалізації прав громадян суспільства, органів державної влади й управління на основі формування і використання інформаційних ресурсів і використання інформаційних систем, мереж, ресурсів і інформаційних технологій із використанням обчислювальної і комунікаційної техніки.

*Основними завданнями інформатизації є:*

• всебічне інформаційне забезпечення потреб суб'єктів інформаційних відносин;

• створення єдиного безпечного інформаційного простору;

• створення, впровадження і використання інформаційних систем, інформаційних технологій і інформаційних продуктів загального значення;

• підготовка кадрів, підвищення їх кваліфікації у сфері інформатизації.

Таким чином можна говорити і про прояви інформаційної безпеки у самому процесі її забезпечення, таким чином можна виділити наступні рівні:

• нормативно-правовий — закони, нормативно-правові акти тощо;

• адміністративний — дії загального характеру, які вживаються органами державного управління;

• процедурний — конкретні процедури забезпечення інформаційної безпеки;

• програмно-технічний — конкретні технічні заходи забезпечення інформаційної безпеки.

**Інформаційна безпека**— складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України; вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України; неухильне дотримання конституційного права громадян на свободу слова доступу до інформації,

***2. Поняття інформаційної війни***

Вперше термін "інформаційна війна" з'явився наприкінці 80-х років ХХ століття. Вів став результатом плідної праці теоретиків збройних сил США і став уживаним після вдало проведеної роботи по знищенню СРСР. Активного застосування даний термін набув під час проведення воєнної компанії США в Іраку у 1991 році, де вперше були не лише застосовані інформаційні технології, а було відкрито наголошено на цьому, що спричинило ще більший резонанс.

**Інформаційна війна**: процес боротьби між суб'єктами із застосуванням інформаційної зброї.

**Інформаційна зброя**: засоби, які дозволяють вчинювати замислені дії із повідомленнями, що передаються, обробляються, створюються, знищуються і сприймаються.

**Інформаційна загроза**: вхідні дані, початково призначені для активізації в інформаційній системі алгоритмів, що відповідають за звичайний режим функціонування.

**Сугестія**: прихований інформаційний вплив на інформаційну систему, що самонавчається.

**Сугестивний вплив**: вплив з формування у інформаційної системи, що самонавчається, прихованих від неї самої цілей.

**Інформаційна війна** — дії, що вчинюються для досягнення інформаційної переваги у підтримці національної воєнної стратегії через вплив на інформацію та інформаційні системи противника при одночасному забезпеченні безпеки власної інформації і інформаційних систем.

Цілі інформаційної війни є дещо іншими, аніж війни у звичному розумінні: не фізичне знищення противника і ліквідація його збройних сил, а широкомасштабне порушення роботи фінансових, транспортних і комунікаційних мереж і систем, руйнування економічної інфраструктури і підкорення населення країни, що зазнала атаки, волі країни-переможця.

При цьому інформаційна війна включає наступні дії:

• здійснення впливу на інфраструктуру систем життєзабезпечення — телекомунікації, транспортні мережі, електростанції тощо;

• промислове шпигунство — порушення прав інтелектуальної власності, розкрадання патентованої інформації, викривлення або знищення важливих даних, проведення конкурентної розвідки;

• хакінг — злам і використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо.

Основним інструментом ведення інформаційної війни є інформаційна зброя. До «інформаційної зброї» відносять, по-перше, засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, не зважаючи на систему захисту, обмеження доступу до цієї інформації законних користувачів. По-друге, це безперечно інформаційно-психологічні засоби, які дезорганізують інформаційні системи шляхом дезінформації, формування помилкових логічних інформаційних концепцій, інтерпретацій та ін., впливаючи таким чином на суспільну думку, на життя суспільства, держави або групи держав в цілому.

Таким чином, **інформаційна зброя** — це пристрої та засоби, які призначені для нанесення протидіючій стороні максимальної шкоди в ході інформаційної боротьби (шляхом небезпечних інформаційних впливів).

Об'єктами впливу можуть бути: інформаційно-технічні системи, інформаційно-аналітичні системи, інформаційно-технічні системи, які включають людину, інформаційно-аналітичні системи, які включають людину, інформаційні ресурси, системи формування суспільної свідомості та думки, яка базується на засобах масової інформації та пропаганди, а також психіки людини.

 Інформаційна війна може бути спрямована проти трьох елементів: комп'ютер; програмне забезпечення; людина.

Однією з головних цілей інформаційної війни є придушення в людині морального творчого початку, зміна світогляду.

***3. Поняття та види загроз національним інтересам та національній безпеці в інформаційній сфері***

Відповідно до Закону України «Про основи національної безпеки України» до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні:

• прояви обмеження свободи слова та доступу громадян до інформації;

• поширення засобами масової інформації культу насильства, жорстокості, порнографії;

• комп'ютерна злочинність та комп'ютерний тероризм;

• розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що е власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

• намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

До загроз інформаційній безпеці системі управління національною безпекою належать: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання.

***4. Класифікація загроз***

Через їх чисельність відповідно до загальної класифікації загроз національній безпеці, виокремлюють загрози інформаційній безпеці.

**За джерелами походження:**

• природного походження — це небезпечні геологічні, метеорологічні, гідрологічні явища, деградацію ґрунтів чи надр, природні пожежі, масове руйнування (через природні катаклізми) каналів зв'язку, зміна стану водних ресурсів та біосфери тощо;

• техногенного походження — транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів системи управління національною безпекою тощо;

• антропогенного походження — вчинення людиною різноманітних дій з руйнування інформаційних систем, ресурсів, програмного забезпечення тощо.-До цієї групи за змістом дій належать: ненавмисні, викликані помилковими чи ненавмисними діями людини (наприклад, помилковий запуск програми, ненавмисне допущення через недотримання правил безпеки роботи в Інтернеті інсталяції закладок тощо); навмисні (інспіровані), результат навмисних дій людей (наприклад, навмисна інсталяція програм, які передають інформацію на інші комп'ютери, навмисне зараження вірусами, навмисна дезінформація тощо).

**За ступенем гіпотетичної шкоди:**

• загроза — явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів у інформаційній сфері і створюють небезпеку для системи управління національною безпекою, життєзабезпечення її системостворюючих елементів;

• небезпека — безпосередня дестабілізація функціонування системи управління національною безпекою.

**За повторюваністю вчинення:**

• повторювані — такі загрози, які мали місце раніше;

• продовжувані — неодноразове здійснення загроз, що складається з ряду тотожних загроз, які мають спільну мету.

За сферами походження:

• екзогенні — джерело дестабілізації системи лежить поза її межами;

• ендогенні — алгоритм дестабілізації системи перебуває у самій системі.

**За ймовірністю реалізації:**

• вірогідні — такі загрози, які за виконання певного комплексу умов обов'язково настануть. Прикладом може слугувати оголошення атаки інформаційних ресурсів системи управління НБ, яке передує власне атаці;

• неможливі — такі загрози, які за виконання певного комплексу умов ніколи не настануть. Такі загрози зазвичай мають більш декларативний характер, не підкріплений реальною і навіть потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякуючий характер;

• випадкові — такі загрози, які за виконання певного комплексу умов кожного разу протікають по-різному. Загрози даного рівня доцільно аналізувати за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах.

**За рівнем детермінізму:**

• закономірні — такі загрози, які носять стійкий, повторюваний характер, що зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки. Так, наприклад, будь-який суб'єкт системи забезпечення національної безпеки піддаватиметься інформаційним атакам, якщо в ньому не функціонує, або функціонує не на належному рівні система забезпечення інформаційної безпеки. Прикладом тому слугують численні атаки хакерів на офіційні сайти ФБР, ЦРУ, ДВБ США;

• випадкові — такі загрози, які можуть або трапитися або не трапитися. До таких загроз належать загрози хакерів дестабілізувати інформаційній системи органів державного управління.

**За значенням:**

• допустимі — такі загрози, які не можуть призвести до колапсу системи. Прикладом можуть слугувати віруси, які не пошкоджують програми шляхом їх знищення;

• неприпустимі — такі загрози, які:

1) можуть у разі їх реалізації призвести до колапсу і системної дестабілізації системи;

2) можуть призвести до змін, не сумісних із подальшим існуванням СНБ. Так, наприклад, вірус "і love you\*, спричинив пошкодження комп'ютерних систем у багатьох містах світу і завдав загального збитку майже 100 мільйонів доларів США.

За структурою впливу:

• системні — загрози, що впливають одразу на усі складові елементи системи управління національною безпекою;

• структурні — загрози, що впливають на окремі структури системи;

• елементні — загрози, що впливають на окремі елементи структури системи. Дані загрози мають постійний характер і можуть бути небезпечними лише за умови неефективності або непроведення їх моніторингу.

**За характером реалізації:**

* реальні — активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією;
* потенційні — активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління;
* здійснені — такі загрози, які втілені у життя;
* уявні — псевдоактивізація алгоритмів дестабілізації, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є.

**За ставленням до них:**

* об'єктивні — такі загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі через те, що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта. Відтак об'єктивні загрози, не відображені в офіційних документах, називають ненормативні загрози;
* суб'єктивні — така сукупність чинників об’єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою. За даного випадку визначальну роль у ідентифікації тих чи інших обставин і чинників відіграє воля суб'єкта управління, який і приймає безпосереднє рішення про надання статусу або ідентифікації тих чи інших подій в якості загроз безпеці.

За об'єктом впливу;

\* особа;

\* суспільство;

\* держава.