

ІНФОРМАТИКА



Урок 5

Види заходів протидії загрозам безпеки. Правові основи забезпечення безпеки інформаційних технологій

За навчальною програмою 2018 року



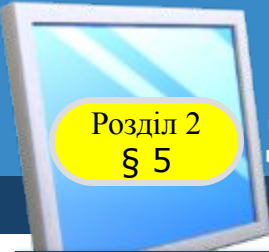
teach-inf.at.ua



Пропоную обговорити проблемне питання.

**Як
забезпечити
безпеку
інформаційних
технологій?**



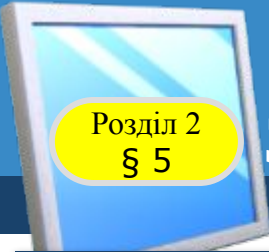


Основні об'єкти захисту інформації

Інформація з обмеженим доступом, тобто інформаційні ресурси, зокрема, ті, що містять відомості, які належать або до таємної, або до конфіденційної інформації

Технічні засоби приймання, обробки, зберігання та передання інформації: системи та засоби інформатизації; програмні засоби; автоматизовані системи керування тощо

Допоміжні технічні засоби і системи

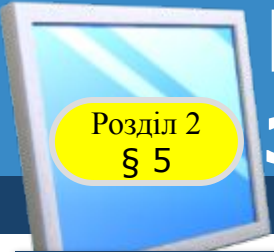


Важливими методами аналізу стану забезпечення інформаційної безпеки є методи описи і класифікації. Для здійснення ефективного захисту системи управління безпеки слід:

по-перше, описати

а лише потім класифікувати різні види загроз і небезпек, ризиків та викликів

і, відповідно, сформулювати систему заходів зі здійснення управління ними



Види заходів протидії загрозам безпеки



Як розповсюджені методи аналізу рівня забезпечення інформаційної безпеки використовуються методи дослідження причинних зв'язків.

За допомогою даних методів:

виявляються причинні зв'язки між загрозами та небезпеками;

здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки;

розробляються заходи щодо їх нейтралізації.



Серед методів причинних зв'язків можна назвати такі:

метод схожості,

метод розбіжності,

метод сполучення
схожості й розбіжності,

метод супроводжувальних
змін,

метод залишків.



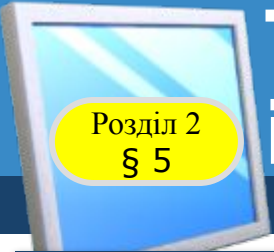


Виділяють декілька типів методів забезпечення інформаційної безпеки:

однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;

багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішенню власного завдання;





Продовження...

комплексні методи — багаторівневі технології, об'єднані у єдину систему координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

інтегровані високоінтелектуальні методи — багаторівневі, багатокомпонентні технології, побудовані на підставі могутніх автоматизованих інтелектуальних засобів з організаційним управлінням



Розробку концепції захисту рекомендується проводити в три етапи:

I етап – визначення цінності об'єкта захисту інформації.

II етап – аналіз потенційних дій зломисників

III етап – оцінка надійності встановлених засобів захисту інформації на об'єкті.

На основі концепції безпеки інформації розробляються стратегія безпеки інформації та архітектура системи захисту інформації, а далі – політика безпеки інформації



Види заходів протидії загрозам безпеки:

законодавчі (правові);

адміністративні;

організаційні (процедурні);

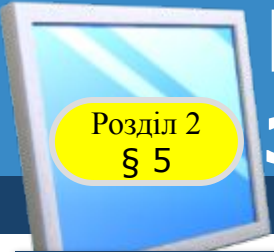
інженерно-технічні;

правові.



Правові заходи –
розробка норм, що
встановлюють
відповідальність за
комп'ютерні злочини,
захист авторських прав
програмістів,
удосконалювання
карного і цивільного
законодавства, а також
судочинства.





Інженерно-технічні засоби

**установка систем
захисту від збоїв в
електроживленні**

**програмні засоби
боротьби з вірусами**

**забезпечення захисту
від розкрадань і
диверсій**

**резервне копіювання та
архівування особливо
важливих документів**

**оснащення приміщень
системою охоронної
сигналізації**

**захист від несанкціонованого
доступу до комп'ютерної
системи**

**організація локальних
обчислювальних мереж з
можливістю перерозподілу
ресурсів, у разі виходу з ладу
окремих ланок**



Програмні засоби

спеціальні програми, програмні комплекси і системи захисту інформації в інформаційних системах різного призначення і засобах обробки даних (антивірусні програми, системи розмежування повноважень, програмні засоби контролю доступу)

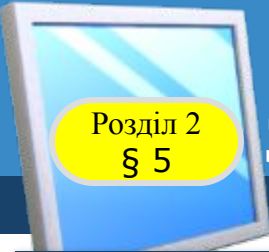
Криптографічні засоби

спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по мережах зв'язку, збереженої та обробленої на комп'ютерах з використанням методів шифрування.



Система захисту інформації – це організована сукупність спеціальних установ, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.





Види заходів протидії загрозам безпеки



Система захисту інформації повинна задовольняти такі умови:

бути надійною

**бути
нестандартною,
різноманітною**

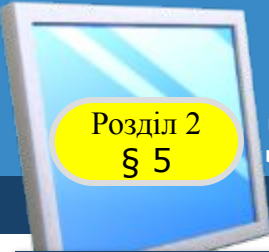
**бути комплексною,
мати цілісність**

**бути різноманітною за
використовуваними засобами,
багаторівневою з ієрархічною
послідовністю доступу**

**бути простою для технічного
обслуговування і зручною для
експлуатації користувачами**

**охоплювати весь технологічний
комплекс інформаційної
діяльності**

**бути відкритою для зміни і
доповнення заходів
забезпечення безпеки
інформації**



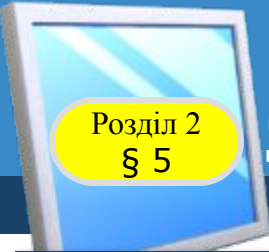
Принципи побудови системи безпеки інформації

безперервність захисту інформації;

активність, яка передбачає прогнозування дій злоумисника, розробку і реалізацію випереджаючих захисних заходів;

скритність, що виключає ознайомлення сторонніх осіб із засобами і технологією захисту інформації;

цілеспрямованість, яка передбачає зосередження зусиль щодо запобігання загроз найбільш цінної інформації;



Продовження...

комплексне використання;

мінімізація додаткових завдань і вимог до співробітників організації, викликаних заходами щодо захисту інформації;

надійність;

обмежений і контрольований доступ;

безперервність роботи системи;

адаптованість (пристосовність) системи до змін навколишнього середовища.



Розрізняють три шляхи захисту даних

Шляхи захисту даних

**Захист доступу до
комп'ютера**



**Захист даних на
дисках**



**Захист даних в
Інтернеті**

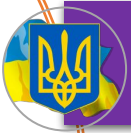




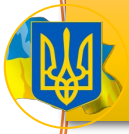
На законодавчому рівні в Україні прийнято декілька законів і видано постанови Кабінету Міністрів щодо забезпечення інформаційної безпеки. Серед них можна назвати:



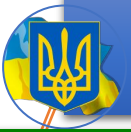
Закон України «Про інформацію»;



Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;



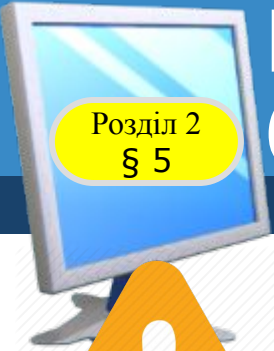
Закон України «Про державну таємницю»;



Закон України «Про захист персональних даних»,



Постанову Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».



Розділ 2
§ 5

Правові основи забезпечення безпеки інформаційних технологій



**Доктрина інформаційної безпеки України
затверджена у лютому 2017 року**

НОВИНИ

В Україні запрацювала
доктрина інформаційної
безпеки

ЗАБОРОНЕНО
ЗАБОРОНЯТИ



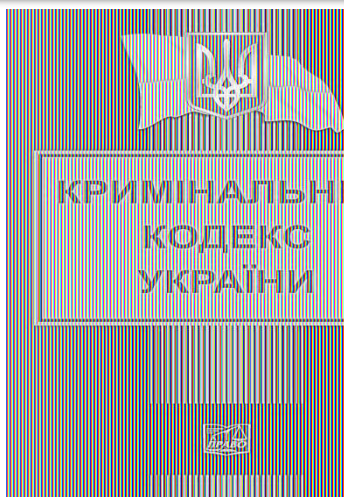
У прийнятих в Україні законодавчих нормах, вказується, зокрема, що захисту підлягає:

- і відкрита інформація, яка передається телекомунікаційними мережами;**
- і конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених Законом України «Про доступ до публічної інформації»;**
- і службова інформація;**
- і інформація, яка становить державну або іншу передбачену законом таємницю;**
- і інформація, вимога щодо захисту якої встановлена законом.**



Незаконне втручання в роботу комп'ютерів, комп'ютерних мереж та розповсюдження вірусів тягне за собою кримінальну відповідальність

**(Ст. 361
Кримінального
кодексу України).**



ІНФОРМАТИКА

Дякую за увагу!

10
(11)

За навчальною програмою 2018 року



Урок 5

teach-inf.at.ua