ІНФОРМАТИКА

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

За навчальною програмою 2018 року

Розділ 2
§ 5

Актуалізація опорних знань і життєвого досвіду

10
11

Пропоную обговорити проблемне питання.

Як забезпечити безпеку інформаційних технологій?

Розділ 2
§ 5

Види заходів протидії загрозам безпеки

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

Розділ 2
§ 5

Види заходів протидії загрозам безпеки

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

Розділ 2
§ 5

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.

Розділ 2
§ 5

Види заходів протидії загрозам безпеки

Серед методів причинних зв'язків можна назвати такі:

- метод схожості,
- метод розбіжності,
- метод сполучення схожості й розбіжності,
- метод супроводжувальних змін,
- метод залишків.

Розділ 2
§ 5

Типи методів забезпечення інформаційної безпеки.

Виділяють декілька типів методів забезпечення інформаційної безпеки:

***одноріvневі** 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;*

Розділ 2
§ 5

Типи методів забезпечення інформаційної безпеки.

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*

Розділ 2
§ 5

Концепція захисту інформації

Розробку концепції захисту рекомендується проводити в три етапи:

I етап – визначення цінності об'єкта захисту інформації.

II етап – аналіз потенційних дій зловмисників

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

Розділ 2
§ 5

Види заходів протидії загрозам безпеки

Види заходів протидії загрозам безпеки:

- *законодавчі (правові);*
- *адміністративні;*
- *організаційні (процедурні);*
- *інженерно-технічні;*
- *правові.*

Розділ 2
§ 5

Види заходів протидії загрозам безпеки

10
11

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

Розділ 2
§ 5

Види заходів протидії загрозам безпеки

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***

Розділ 2
§ 5

Види заходів протидії загрозам безпеки

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.

Розділ 2
§ 5

Види заходів протидії загрозам безпеки

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

Розділ 2
§ 5

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

Розділ 2
§ 5

Види заходів протидії загрозам безпеки

Принципи побудови системи безпеки інформації

***безперервність** захисту інформації;*

***активність**, яка передбачає прогнозування дій зловмисника, 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;*

Розділ 2
§ 5

Види заходів протидії загрозам безпеки

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.

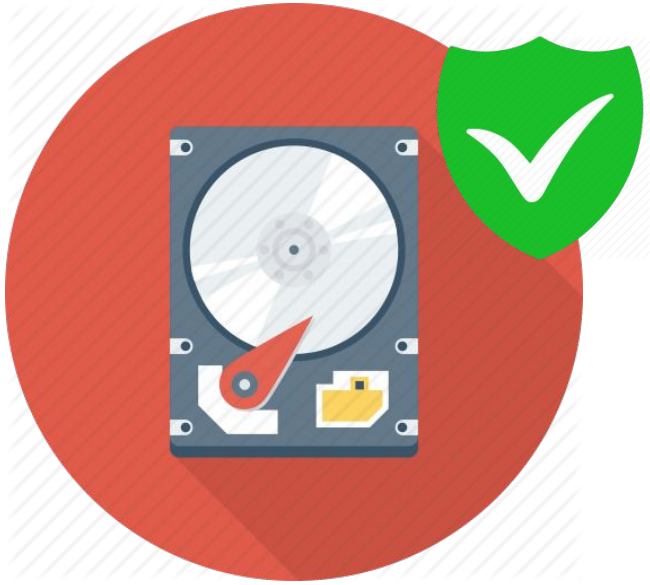
Розділ 2
§ 5

Види заходів протидії загрозам безпеки

Розрізняють три шляхи захисту даних

Шляхи захисту даних

- Захист доступу до комп'ютера
- Захист даних на дисках
- Захист даних в Інтернеті



Розділ 2
§ 5

Правові основи забезпечення безпеки інформаційних технологій

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

9

Доктрина інформаційної безпеки України затверджена у лютому 2017 року

Правові основи забезпечення безпеки інформаційних технологій

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

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

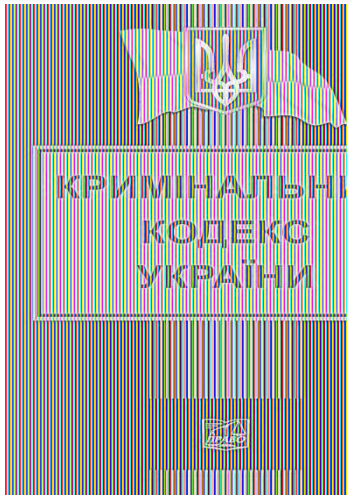
Розділ 2
§ 5

Правові основи забезпечення безпеки інформаційних технологій

10
11

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

(Ст. 361 Кримінального кодексу України).



Розділ 2
§ 5

Запитання для рефлексії

1. *Що на уроці мене більш за все вразило?*
2. *Як я оцінюю свою навчальну діяльність на уроці?*
3. *Чи є в мене бажання більше дізнаватися про види заходів протидії загрозам безпеки?*

Розділ 2
§ 5

Домашнє завдання

Зробити пост у соціальних мережах про правові основи забезпечення безпеки інформаційних технологій

Розділ 2
§ 5

Працюємо за комп’ютером

Створіть текстовий документ, що містить відомості про систему інформаційної безпеки.

Подайте знайдені відомості в текстовому документі у зручному вигляді (таблиці, схеми тощо). Розмісіть роботу на Google-диску, надайте доступ, для перегляду і редагування учителю і 2 однокласникам. Перегляньте проектну роботу своїх друзів.

ІНФОРМАТИКА

Дякую за увагу!

За навчальною програмою 2018 року