Урок № 5.

Тема уроку: Інструктаж з БЖД. Види заходів протидії загрозам безпеки. Правові основи забезпечення безпеки інформаційних технологій.

Сьогодні ти ознайомишся з різними видами заходів безпеки інформації, розглянемо їх переваги і недоліки, визначимо об'єкти захисту, принципи побудови системи інформаційної безпеки.

Правила поведінки за комп'ютером:

Пам'ятай:

- Робоче місце за комп'ютером потрібно тримати у порядку.
- Не клади зайвих речей на стіл біля комп'ютера.
- Прибирай пил з комп'ютера спеціальною ганчіркою, коли він вимкнений.

Виконуй:

- Слідкуй за осанкою (спина повинна бути прямою).
- Очі мають бути на відстані 50 – 60 см від екрану монітору.
- Кожні 30 хвилин роби перерву в своїй роботі.

В основі комплексу заходів щодо інформаційної безпеки повинна бути стратегія захисту інформації. У ній визначаються мета, критерії, принцип і процедури, необхідні для побудови надійної системи захисту. Найважливішою особливістю загальної стратегії інформаційного захисту є дослідження системи безпеки. Можна виділити два основних напрямки:

• аналіз засобів захисту;
• визначення факту вторгнення.

Види заходів протидії загрозам безпеки.

Всі заходи протидії комп'ютерним злочинам, що безпосередньо забезпечують безпеку інформації, можна поділити на:

• правові;
• організаційно-адміністративні;
• інженерно-технічні.

До ***правових заходів*** варто віднести розробку норм, що встановлюють відповідальність за комп'ютерні злочини, захист авторських прав програмістів, удосконалення карного і цивільного законодавства, а також судочинства.

До ***організаційно-адміністративних*** заходів відносяться: охорона комп'ютерних систем, підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною, наявність плану відновлення працездатності центру після виходу його з ладу, обслуговування обчислювального центру сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення роботи центру, універсальність засобів захисту від усіх користувачів (включаючи вище керівництво), покладання відповідальності на осіб, що повинні забезпечити безпеку центру, вибір місця розташування центру тощо.

До інженерно-технічних заходів можна віднести:

1) захист від несанкціонованого доступу до комп'ютерної системи,
2) резервування важливих комп'ютерних систем,
3) забезпечення захисту від розкрадань і диверсій,
4) резервне електроживлення, розробку і реалізацію спеціальних програмних і апаратних комплексів безпеки тощо.

Запам'ятай основні принципи побудови системи безпеки інформації :

Загальновідомо, що відділам безпеки, які займаються захистом інформації, протистоять різні організації і зловмисники, як правило, оснащені апаратними засобами доступу до інформації. Виходячи з цього, основу захисту інформації повинні складати принципи, аналогічні принципам отримання інформації, а саме:

− безперервність захисту інформації. Характеризується постійною готовністю системи захисту до відбиття загроз інформаційній безпеці в будь-який час;

− 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;

− комплексне використання різних способів і засобів захисту інформації, що дозволяє компенсувати недоліки одних перевагами інших.

При побудові системи захисту інформації потрібно враховувати також наступні принципи:

- мінімізація додаткових завдань і вимог до співробітників організації, викликаних заходами щодо захисту інформації;
- надійність в роботі технічних засобів системи, що виключає як нереагування на погрози (пропуски загроз) інформаційної безпеки, так і помилкові реакції при їх відсутності;
- обмежений і контрольований доступ до елементів системи забезпечення інформаційної безпеки;
- безперервність роботи системи в будь-яких умовах функціонування об'єкта захисту, в тому числі, короткочасному відключенні електроенергії;
- адаптованість (пристосованість) системи до змін навколишнього середовища.

До системи безпеки інформації висуваються також певні вимоги:

• чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;
• надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;
• зведення до мінімуму кількості спільних для декількох користувачів засобів захисту;
• облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;
• забезпечення оцінювання ступеня конфіденційної інформації;
• забезпечення контролю цілісності засобів захисту і негайне реагування на вихід їх з ладу.

Додаткове відео до уроку: "Правові основи забезпечення безпеки інформаційних технологій" http://surl.li/crtgn.
Матеріал з теми: https://www.youtube.com/watch?v=N-4y4Fw5HAk.