Лекція №

Тема. Інформаційні технології у навчанні. Основи інформаційної безпеки.

План

1. Використання електронних посібників.
2. Дистанційна форма навчання.
3. Програмні засоби навчання іноземних мов
4. Поняття інформаційної безпеки
5. Загрози, що надходять з Інтернету
   5.1. Хакери
   5.2. Віруси
   5.3. Спам

1. Використання електронних посібників

До сучасних інформаційних технологій, які використовують в навчальному процесі, відносять електронні та гібридні бібліотеки, електронні посібники, довідково-пошукові системи Інтернет, навчальні програми, мультимедійні курси з профільного предмету, електронні словники і програми-перекладачі.

Електронний посібник – це універсальний методичний посібник, який містить широке коло питань з різних навчальних дисциплін, викладених в стислій формі та призначених для використання в навчанні.

Електронний посібник має сполучати в собі функції підручника і вчителя, довідково-інформаційного посібника і консультанта, тренажера і програми, що контролює знання. В залежності від потреб і вже наявних знань, користувач сам вибирає матеріал для вивчення, його обсяг, технологію навчання. Контроль знань після вивчення кожного розділу може здійснюватися різними способами - за допомогою тестів, контрольних питань і т.п.

Таким чином, електронні підручники дають можливість збільшити кількість користувачів, підвищити наочність представлення матеріалу, використовувати електронний посібник тривалий час, звести до мінімуму витрати на пошук і підбір літератури, здійснювати контроль отриманих знань і ін.

2. Дистанційна форма навчання

Існує поняття очної форми навчання, коли учні безпосередньо спілкуються з викладачем, та ***дистанційної форми*** — навчання на відстані (дистанції). Як правило, освітні послуги в умовах дистанційного навчання надаються за допомогою комп'ютерних мереж. Учні реєструються на спеціальних навчальних порталах, отримують навчальні матеріали, індивідуальні завдання, за потреби скачують їх на свої комп'ютери. За запропонованим графіком навчання учні самостійно виконують завдання та одержані результати надсилають викладачеві на портал. Викладач перевіряє виконані завдання та виставляє кожному учневі оцінку або відповідну кількість балів, які заносяться до спеціального електронного журналу на навчальному порталі. Крім того, процес навчання може передбачати перевірку знань у вигляді тестування. Учні можуть консультуватися як із викладачем, так і між собою засобами, що знаходяться на навчальному порталі.

До переваг дистанційного навчання можна віднести:

- можливість вибору власних темпів навчання;
- можливість навчання на території, яка є більш комфортною для студента;
- різноманітність засобів і способів навчання;
- отримання знань в галузі новітніх технологій та вивчення предметів, недоступних у навчальних закладах.

3. Програмні засоби навчання іноземних мов

Інтернет-технології допомагають опанувати іноземну мову та сприяють її практичному застосуванню. Вони дають можливість:

- поглиблювати свої знання постійно, а не лише на уроках з іноземної мови;
- використовувати додаткові можливості, зокрема за допомогою дистанційних курсів;
- вивчати іноземні мови за допомогою мультимедійних курсів (на компакт-дисках або онлайн в Інтернеті);
- отримувати додаткові матеріали та тексти мовою оригіналу;
- виконувати вправи та відправляти їх електронною поштою на перевірку викладачеві;
- користуватися програмами-перекладачами, електронними словниками, зокрема в режимі онлайн;
- обговорювати різні питання через індивідуальне спілкування електронною поштою або на електронних форумах відповідною іноземною мовою.

Крім того, можна визначити власний рівень володіння певною іноземною мовою за допомогою електронного тестування чи співбесіди з викладачем.

Використовуючи комп'ютер, студент може оволодіти значно більшим обсягом інформації, ніж за такий самий час, працюючи з друкованим підручником. В електронних навчальних продуктах такої інформації міститься значно більше завдяки можливостям застосовувати аудіо-, відео- та інші форми її презентації.

4. Поняття інформаційної безпеки

Інформаційна безпека - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

- неповноту, невчасність та невірогідність інформації;
- негативні наслідки застосування інформаційних технологій;
- несанкціонований доступ до персональної інформації, що зберігається на комп’ютері, електронної пошти, сторінок в соціальних мережах та інше.

Спеціальне законодавство в області безпеки інформаційної діяльності представлено низкою законів. У їхньому складі особливе місце належить базовому Закону «Про інформацію, інформатизацію і захист інформації». Захист інформації - це комплекс заходів, направлених на забезпечення інформаційної безпеки.

Основою захисту більшості користувачів та їх ПК є антивірусні програми, які запобігають потраплянню шкідливого програмного забезпечення і відповідно захищають персональну інформацію від стороннього доступу. Для максимального захисту потрібно користуватися ліцензійними антивірусними програмами і постійно їх оновлювати. На даний час найбільш популярними антивірусними програмами є:

1) антивірус Касперського;

2) NOD 32;
3) Doctor Web.

Для захисту електронних поштових скриньок та персональних сторінок в соціальних мережах потрібно використовувати складні паролі, що містять не менше 8 символів і складаються із нелогічної послідовності символів, цифр та спецзнаків.

5. Загрози, що надходять з Інтернету

Кожен користувач Інтернету повинен мати чітке уявлення про основні джерела безпеки, що йому загрожують. Це насамперед діяльність хакерів, а також віруси та спам.

5.1. Хакери

Хакером називають людину, яка без дозволу проникає до чужої комп'ютерної системи з наміром викрасти або зруйнувати дані. Існує багато способів, за допомогою яких хакери проникають до чужих систем. Найбільш поширеними є такі:

- **Троянські коні**. Це шкідливі програми, які, потрапляючи на ПК, відкривають хакерам доступ до вашої системи, що дає можливість виконувати будь-які шкідливі дії: знищення даних, зараження програм, викрадення особистої інформації та ін..
- **Перевантаження сайту або мережі**. Генеруючи багато запитів довільного змісту до сайту або мережі, хакер збільшує їхнє робоче навантаження, внаслідок чого цей сайт або мережа не можуть нормально функціонувати.
- **Підміна адрес**. Хакер підмінює адреси сайтів у такий спосіб, що коли користувач вводить у браузері адресу якогось сайту, його спрямовують до зовсім іншого сайту.
- **Аналіз пакетів**. За допомогою спеціальних програм хакери можуть перехоплювати певну інформацію, що міститься у пакетах, які передаються мережею.
- **Соціотехніка**. Цей термін використовується для позначення шахрайських дій, спрямованих на отримання інформації, яка дає змогу проникнути до певної системи та даних, що в ній знаходяться. Соціотехніка зазвичай є грою хакера на довірі людини. Для цього використовуються сфальсифіковані сайти та фіктивні електронні повідомлення від імені реальних компаній з проханням надати особисту інформацію.

5.2. Віруси

Віруси – це невеликі програми, що можуть потрапляти на комп’ютер користувача без його відома і виконувати різноманітні шкідливі дії.

Шкідливі дії можуть виконуватись відразу, а можуть бути обумовлені настанням певної дати (наприклад, чорнобильський вірус, який активізується 26 квітня).

Існують десятки тисяч вірусів, але найбільш поширених нараховується 40-50. Всі комп’ютерні віруси поділяються на такі типи:

- завантажувальні віруси;
- файлові віруси;
- макровіруси;
- мережеві віруси.

5.3. Спам

Спамом називають небажану електронну пошту, тобто пошту, що надходить без вашої згоди. Найчастіше в якості спаму надходить різноманітна комерційна реклама. Привабливість такої реклами в її порівняно низькій вартості і досить великому охопленню потенційних клієнтів.

Люди отримують спам з різних причин. Проте часто вони самі є винуватцями того, що їхня електронна адреса потрапляє до спамерів. Для того, щоб зменшити ймовірність отримання спаму, необхідно знати перелік типових дій, які можуть призвести до того, що ваша адреса стане надбанням спамерів:

- запис до гостьової книги на якомусь з сайтів із зазначенням своєї електронної адреси;
- підписка на безкоштовне отримання електронною поштою прайс-листів, новин та іншої подібної інформації;
- відповідь на спам, що надійшов на вашу адресу;
- надання згоди на участь у групі новин;
- реєстрація свого доменного імені, яка вимагає надання персональної інформації;
- заповнення онлайнових форм при реєстраціях у форумах, інтернет-магазинах, опитуваннях та ін;
- участь у чаті.