



***Методичні рекомендації до заняття
з предмету «Інформатика» на тему:
«Програми обслуговування дисків.
Комп'ютерні віруси та антивірусні
програми»***

Конспект заняття

Тип уроку: урок введення нових знань з використанням інтерактивної технології– робота в групах та з використанням унаочнення, роздаткових матеріалів.

«Зібратися разом – це початок, триматися разом – це прогрес, працювати разом – це успіх»

(Генрі Форд, американський підприємець)

ХІД УРОКУ

I. Організаційна частина

Доброго дня ! Хто відсутній? Сьогодні у нас з вами не зовсім звичайний урок. Незвичайний тим, що в нас присутні гості. Але не хвилюйтеся. Нас об'єднує інтерес до інформатики.

Тож приязно подивимося один одному в очі, побажаємо натхнення в нашій

роботі. Які асоціації викликає у вас урок? Давайте розкладемо його по літерах. Учні називають, викладач записує на плакаті:

У – удача, успіх, Р – радість, раціональність, О – обдарованість, освіченість, К

– кмітливість, компетентність

- Сподіваюсь, що сьогодні на уроці на нас чекає і успіх, і радість, ви зможете

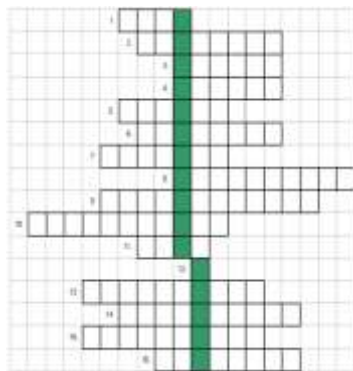
продемонструвати свою обдарованість і кмітливість.

II. Актуалізація опорних знань

- Для того, щоб пригадати матеріал попередніх уроків,

розгадаємо кросворд. Працюємо в групах. Яка група перша справиться з завданням отримає додатковий бал до загальної оцінки. Після

успішного виконання завдання в виділених клітинках ви зможете прочитати поняття, яке буде ключовим на сьогоднішньому уроці («комп'ютерний вірус»).



Питання до кросворда:

1. Буває локальний, фізичний, лазерний.
 2. Бувають системні, службові, прикладні...
 3. Як називається об'єднання комп'ютерів?
 4. Буває внутрішня і зовнішня.
 5. Як називається обчислювальна система, що складається з апаратної частини і програмного забезпечення?
 6. Як називається найбільш популярна глобальна мережа?
 7. Скажіть іншу назву гнучкого магнітного диска діаметром 3,5 дюйма, що має ємність 1,44 МБ
 8. Ім'я файлу складається з двох частин: назви файлу і ...
 9. Процес вмикання комп'ютера називають?
 10. Яка наука вивчає методи та засоби отримання, обробки, зберігання, передавання та подання інформації.
 11. Поіменованою ділянкою пам'яті комп'ютера, де зберігається інформація називають ...
 12. Як ще називають жорсткий магнітний диск?
 13. Програму, що здійснює діалог із користувачем, керує роботою комп'ютера, його ресурсами, запускає інші програми називають ... система?
 14. Відомості про явища навколишнього світу називають...
 15. Людина, що працює за комп'ютером і не є професіоналом називається (ко...)
 16. Як називається пристрій для читання дискет?
- Кросворд успішно розгадано. Звіримо відповіді.
Для багатьох користувачів комп'ютерів віруси – це щоденна головна біль і турбота. Чому?

ІІІ. Мотивація пізнавальної діяльності

Звернення до життєвого досвіду учнів

Ключове слово на сьогоднішньому уроці – «комп'ютерний вірус». Що це таке?

Можливо вам знайомі такі життєві ситуації:

1. Вчора комп'ютер працював, сьогодні раптом операційна система не завантажується, на екрані повідомлення: «Відсутній системний диск»...

2. Відкриваємо текстовий файл з рефератом, а він не відкривається, дані пошкоджені...
3. Вставляємо в комп'ютер флешку, хочемо записати на неї дані, а виникає повідомлення «Ви не маєте права доступу до даного пристрою»...
4. Комп'ютер раптово перезавантажується 10 разів за 2 години...
На всі ці складні ситуації ви отримаєте відповідь і знатимете після уроку як з ними боротися. Тому т ема заняття запишемо ;
Програми обслуговування дисків. Комп'ютерні віруси та антивірусні програми.

Епіграфом стане прислів'я **«Зібратися разом – це початок, триматися разом – це прогрес, працювати разом – це успіх»**
(Генрі Форд, американський підприємець)

Мета: вивчити основні програми обслуговування дисків, сформувати поняття комп'ютерного вірусу, ознайомити студентів з видами та типами вірусів, шляхами зараження персонального комп'ютера вірусами та основними методиками боротьби з ними.

Запишемо план:

Повідомлення плану:

1. Програми обслуговування дисків.
2. Історія комп'ютерної вірусології.
3. Класифікація вірусів.
4. Класифікація антивірусних програм.

Джерела та ознаки зараження комп'ютерними вірусами. Правила захисту інформації.

IV. Вивчення нового матеріалу.

Перегляд презентації

Викладач: На попередньому занятті Ви були об'єднані у групи і кожна група готувала завдання до сьогоднішнього уроку-консиліуму. *Консиліум з латинської – нарада, обговорення.*

Завдання: дослідити хвороби та виробити методи лікування «Комп'ютера».

Виступи представників груп.

-А тепер представник кожної групи доповість нам про результати своїх досліджень.

Першими виступають «Вірусологи-дослідники» - дають відомості про історію комп'ютерної вірусології **«Вікно в історію комп'ютерної вірусології»**

Все має свою історію, а чи мають її віруси?

Перші віруси з'явилися давно, ще на зорі епохи ЕОМ, і не завжди були шкідливими. Наприклад, в кінці 60-х в лабораторії Хегох була створена спеціальна програма, яка являлась прообразом сучасних вірусів, вона самостійно подорожувала по локальній обчислювальній мережі і перевіряла справність включених в мережу пристроїв. Проте згодом почали розробляти шкідливі програми-віруси. Одними з перших програм для нанесення шкоди комп'ютерним програмам були програми Virus 1, 2, 3 і Elk Cloner, розроблені для персональних комп'ютерів Apple II.

Перший прототип вірусу з'явився ще в 1971г.. Програміст Боб Томас, намагаючись вирішити завдання передачі інформації з одного комп'ютера на інший, створив програму Creeper, що мимоволі «перестрибувала» з однієї машини на іншу в мережі комп'ютерного центру. Правда ця програма не «саморазмножалась», не наносила збитку.

У 1989 р. 23-річний американський студент Роберт Морріс написав невеличку програму. За його задумом програма-жарт повинна була непомітно розповсюдитися з одного комп'ютера на інший, не заважаючи їхній роботі. Але допущена в програмі помилка змусила інформацію розповсюдитися з великою швидкістю, від чого всі канали зв'язку ЕОМ виявилися перевантаженими і наукова інформація, накопичена в обчислювальних центрах, у своїй більшості стала непридатною для використання. Всього за кілька годин найважливіші мережі східного і західного узбережжя США були виведені з ладу. Епідемія охопила шість тисяч комп'ютерів, об'єднаних у 70 систем, за допомогою яких відбувався обмін найважливішою

інформацією.

На сході були пошкоджені комп'ютерні центри таких великих закладів, як Масачусетський технологічний інститут, Гарвардський, Пітсбургський, Мерілендський і Вісконсинський університети. Науково-дослідна морська лабораторія. На заході — Каліфорнійський і Стенфордський університети, науково-дослідна лабораторія НАСА, Ліверпульська лабораторія ядерних досліджень. Усі вони були зв'язані супутниковою системою «АРПАНЕТ». А причиною всього стала маленька програма-жарт, запущена в систему.

Надалі такі програми почали називати комп'ютерними вірусами.

ТОП найнебезпечніших вірусів (таблиця)

Другими виступають «Вірусологи-теоретики» - повідомляють про класифікацію вірусів **Класифікація вірусів «Дерево знань»**

Прийом «Дерево знань»

За принципом поширення та функціонування:

- ✓ **завантажувальні віруси, або BOOT-віруси:** заражають boot-сектори дисків. Дуже небезпечні, можуть призвести до повної втрати всієї інформації, що зберігається на диску;
- ✓ **файлові віруси:** заражають файли.
- ✓ Поділяються на:
- ✓ а) віруси, що заражують програми (файли з розширенням .exe і .com);
- ✓ б) макровіруси: віруси, що заражають файли даних, наприклад документи Word або робочі книги Excel;
- ✓ **віруси-супутники:** використовують імена інших файлів;
- ✓ **віруси сімейства DIR:** спотворюють системну інформацію про файлові структури;
- ✓ **завантажувально-файлові віруси:** здатні заражати як код boot-секторів, так і код файлів;
- ✓ **віруси-невидимки, або Stealth-віруси:** фальсифікують інформацію, прочитану з диска так, що програма, якій призначена ця інформація, отримує неправильні дані. Ця технологія, яку іноді так і називають Stealth-технологією, може використовуватися як у BOOT-вірусах, так і у файлових вірусах;

- ✓ **ретровіруси:** заражають антивірусні програми, намагаючись знищити їх або зробити непрацездатними;
- ✓ **віруси-хробаки:** заражають невеликі повідомлення електронної пошти так званим заголовком, який по своїй суті є лише Web-адресою місцезнаходження самого вірусу. При спробі прочитати таке повідомлення вірус починає зчитувати через глобальну мережу Internet своє «тіло», яке після завантаження починає і свою деструктивну дію. Дуже небезпечні, оскільки виявити їх надзвичайно складно у зв'язку з тим, що заражений файл фактично не містить коду вірусу.

За деструктивними можливостями:

- ✓ **нешкідливі** (лише зменшують обсяг ОЗП);
- ✓ **шкідливі** (призводять до серйозних порушень у роботі ПК);
- ✓ **дуже шкідливі** (призводять до втрати даних та програм, знищення системної інформації та прискорюють зношення рухомих складових механізмів (головок вінчестера та ін.)).

Класифікація вірусів достатньо умовна, тому що постійно з'являються нові віруси, поведінка яких не вкладається в рамки одного класу.

За способом зараження:

- ✓ **резидентні:** при зараженні (інфікуванні) комп'ютера вірус залишає в оперативній пам'яті свою резидентну частину, що потім перехоплює звернення операційної системи до об'єктів зараження (файлів, завантажувальних секторів дисків і т. ін.) і вбудовується в них. Резидентні віруси містяться у пам'яті та є активними аж до вимикання чи перезавантаження ОС;
- ✓ **нерезидентні:** не заражають пам'ять комп'ютера і є активними обмежений час.

Треті беруть слово «Лікарі-практики» - повідомляють про поняття антивірусної програми, класифікацію антивірусних програм.

Зірка антивірусних програм

Отже, особливе місце в цьому списку займають програмні засоби захисту – антивірусні програми.

Антивіруси — це програми, які призначені для виявлення та знищення комп'ютерних вірусів.

До якого виду ПЗ вони відносяться? (Системного ПЗ)

Класифікація антивірусних програм:

- ✓ Програми-детектори.
- ✓ Лікарі (фаги).
- ✓ Програми-ревізори.
- ✓ Фільтри (сторожі).
- ✓ Вакцини (імунізатори).

Супровід.

Залежно від різних типів вірусів існують різні антивірусні програми:

✓ програми-детектори здійснюють пошук характерної для конкретного вірусу сигнатури в оперативній пам'яті й у файлах і при виявленні видають відповідне повідомлення. Недоліком таких антивірусних програм є те, що вони можуть знаходити тільки ті віруси, які відомі розроблювачам таких програм;

✓ лікарі (фаги), а також програми-вакцини не тільки знаходять заражені вірусами файли, а й «лікують» їх, тобто видаляють із файла тіло програми-вірусу, повертаючи файли у вихідний стан. На початку своєї роботи фаги шукають віруси в оперативній пам'яті, знищуючи їх, і тільки потім переходять до «лікування» файлів. Серед фагів виділяють поліфаги, тобто програми-лікарі, призначені для пошуку і знищення значної кількості вірусів. Найбільш відомі з них: Aidstest-, Scan, Norton Antivirus, Doctor Web;

✓ програми-ревізори належать до найнадійніших засобів захисту від вірусів. Ревізори запам'ятовують вихідний стан програм, каталогів і системних областей диска тоді, коли комп'ютер не заражений вірусом, а потім періодично або за бажанням користувача порівнюють поточний стан із вихідним. При порівнянні перевіряються довжина файла, код циклічного контролю (контрольна сума файла), дата і час модифікації, інші параметри. Програми ревізори мають досить розвинуті алгоритми, виявляють, Stealth- віруси і можуть навіть очистити

зміни версії програми, що перевіряється, від змін, спричинених вірусом. До програм ревізорів належить значно поширена в Україні програма Adinf;

✓ фільтри (сторожі) являють собою невеликі резиденти і програми, призначені для виявлення підозрілих дій при роботі комп'ютера, характерних для вірусів. Такими діями можуть бути:

- спроби корекції файлів із розширеннями .com, .exe;
- зміна атрибутів файла;
- прямий запис на диск за абсолютною адресою;
- запис у завантажувальні сектори диска;
- завантаження резидентної програми.

✓ Програми-фільтри дуже корисні, тому що здатні виявити вірус на початковій стадії його існування — до розмноження. Однак вони не «лікують» файли і диски. Для знищення вірусів потрібно застосовувати інші програми, наприклад фаги. Прикладом програми-фільтра є програма Vsafe, що входить до складу пакета утиліт MS DOS;

✓ вакцини (імунізатори) — це резидентні програми, що запобігають зараженню файлів. Вакцини застосовують у разі якщо відсутні програми-лікарі, які «лікують» цей вірус. Вакцинація є можливою тільки від відомих вірусів. Вакцина модифікує програму або диск таким чином, щоб це не відбивалося на їхній роботі, а вірус сприймав їх зараженими і припиняв спроби зараження. У наш час програми-вакцини практично не застосовуються.

Найвідоміші антивірусні програми: Doctor Web, Kasperskĭ Antivirus, Antivir XP тощо.

Вчитель:

Антивірусна програма AVP Є.Касперського AVP являється поліфагом і в процесі роботи перевіряє ОЗП, файли, в тому числі упаковані і архівні, а також системні сектори (Master Boot Record), завантажувальний сектор (Boot – сектор) і Partition Table. На відміну від DrWeb і Aidstest, AVP розпізнає біля 10000 вірусів, серед них поліморфні, stealth – і макровіруси, а також “Троянські програми”. Програма має евристичний сканер,

котрий, за затвердженням розробників антивіруса із KAMI, знаходить біля 80% всіх вірусів. Нові бази антивірусів до AVP з'являються приблизно один раз в тиждень.

Eset NOD32 Слайд 19

► Багато користувачів, звиклих до знаменитих пакетів ніби Dr.Web, AVP або Norton AntiVirus, напевно будуть здивовані тим, що маловідомий продукт NOD32 невеликої компанії Eset вже довгий час займає перше місце в тестуваннях, що проводяться журналом Virus Bulletin. Ця програма несе гордий значок VB100% (що означає, що NOD32 знаходить і винищує всі відомі «мікроби») аж з травня 1998 р., коли, власне, і почалася його розробка.

► Функціонально NOD32 складається із знайомих нам по інших антивірусах компонентів. Це AMON, резидентний монітор, перевіряючий пам'ять і відкриті файли, EMON — сканер електронної пошти, NOD32 — класичний «шукач», який запускається користувачем уручну або за розкладом, і IMON — аналізатор мережевого трафіку, перевіряючий http, ftp, smtp і інші winsock-протоколи. За великим рахунком, сам виконуваний файл NOD32 вам не буде навіть потрібно — три досконалі сканери покликані не допустити віруси і іншу «заразу» на ваш персональний комп'ютер.

Четвертими виступають «Лікарі-статисти» - повідомляють про джерела зараження і перші ознаки зараження.

Кошик ознак зараження

Комп'ютерний вірус — спеціально написана невелика за розміром програма, яка самостійно дописується до інших програм, змінюючи їх зміст, що приводить до порушень у роботі програм та приладів ПК.

Як відбувається зараження комп'ютерними вірусами?

Комп'ютерним вірусом — через зовнішні носії, через мережу Інтернет або локальну мережу.

Ознаки проявлення комп'ютерних вірусів:

- неправильна робота добре працюючих програм;
- повільна робота комп'ютера;

- неможливість завантажити ОС;
- зникнення файлів чи каталогів;
- несподіване збільшення кількості файлів на диску;
- зменшення розмірів вільної оперативної пам'яті;
- виведення на екран несподіваних повідомлень і зображень;
- часті зависання і збої в роботі комп'ютера.
- неспроможність зберігати документи Word в інших каталогах, крім Template;
- погана робота дисків;
- незрозумілі системні повідомлення, музикальні ефекти і т. ін.
- неспроможність завантажити файли;
- зникнення файлів користувача тощо.

Прийом «Кошик»

Крім вірусів руйнівними властивостями володіють **троянські програми** (на сьогодні вони є більш розповсюдженими).

В чому відмінність троянських програм від вірусів?

Якщо вірус проникає на комп'ютер непомітно, то троянську програму користувач сам записує на диск, вважаючи, що це корисна програма. Але за певних умов вона може почати свою руйнівну роботу.

Викладач: Приклад коду «Розіграй товариша»

Як результат всіх досліджень робимо висновок, що краще за лікування може бути профілактика.

Лікар який порівнює людський організм з комп'ютером та дає поради як не заразитися комп'ютерними вірусами.



Найкращий спосіб не хворіти – не заразитися!

Лікар: сформулювати головні профілактичні засоби.

Очікувані відповіді:

Перед використанням чужих носіїв інформації обов'язково перевіряйте їх на наявність вірусів. Не запускайте неперевірені файли, які отримані з мережі та електронною поштою.

Слід регулярно виконувати копіювання цінної інформації на зовнішні носії.

Завжди майте під рукою завантажувальний диск із антивірусною програмою.

Виконуйте періодичну перевірку пам'яті та всіх дисків вашого комп'ютера за допомогою свіжих версій антивірусних програм. Вчасно оновлюйте свої антивірусні програми. Тільки за постійного відновлення версій антивірусних програм можна встигнути за «творцями» нових вірусів і бути впевненими, що ваші дані й диски не будуть уражені.

Якщо, незважаючи на вжиті заходи, ваш комп'ютер заражений вірусами, скористайтеся будь-якою антивірусною програмою.

Правила захисту інформації

Ми, що підписалися нижче, згодні з приведеними правилами і зобов'язуємося неухильно їх виконувати з метою забезпечення безпеки особистої інформації і суспільної.

1. Кожен користувач ПК зобов'язаний встановити легальну антивірусну систему.
2. Антивірусна система повинна мати актуальні оновлення вірусних баз.
3. Кожен користувач зобов'язаний не рідше за один раз на місяць перевіряти ПК на наявність вірусних програм.
4. Кожен користувач перед відкриттям носія або файлу зобов'язаний перевіряти його на наявність вірусного файлу.
5. Кожен користувач зобов'язаний включити брандмауер і захистити підключення до мережі.
6. З метою недопущення зараження вірусними програмами ПК користувач зобов'язаний викачувати програми тільки з легальних, загальнодоступних сайтів. Не викачувати і не намагатися встановлювати програми-креки і зламані ліцензійні програми, оскільки вони є потенційними носіями вірусних файлів.
7. При виявленні вірусного файлу користувач зобов'язаний спробувати вилікувати даний файл, або, якщо лікування неможливе, видалити його.
8. Користувачеві рекомендується поширювати безкоштовні антивірусні програми і навчати основам захисту інформації

інших користувачів.

Стаття 361

Кримінального кодексу України

❖ Від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років, чи позбавленням волі на той самий термін.

❖ За повторне вчинення тих самих дій, передбачено покарання до п'яти років позбавлення волі з конфіскацією усіх програмних та технічних засобів, за допомогою яких було вчинено несанкціоноване втручання, які є власністю винної особи, а також позбавленням права обіймати певні посади чи займатися певною діяльністю.

Осмислення набутих знань, умінь і навичок

Інтерактивна вправа «Так-Ні» (Перегляд відео гостями)

Учні повинні відповісти на запитання тесту. Тест на екрані (картках). Діти залежно від відповіді піднімають угору руку з карткою «Так» або «Ні»

1. Чому комп'ютерний вірус є шкідливим?

- a) може завдати шкоди периферійним пристроям.
- b) може завдати шкоди комп'ютеру та інформації, що зберігається в ньому

2. Як можна виявити та знешкодити комп'ютерний вірус?

- a) установити та запустити антивірусну програму
- b) за допомогою помічника пошуку знайти та видалити з комп'ютера

3. Що є основним джерелом вірусів?

- a) Мережа Інтернет
- Б) нові документи

4. Чому деякі види вірусів називаються завантажувальними?

- a) через те, що вони проникають у завантажувальний сектор диска

b) через те, що вони завантажуються безперервно

5. **Роберт Морріс -**

a) Американський студент

b) Німецький дослідник

6. **Яким кольором на діаграмі де фрагментації відображаються файли, що не переміщаються?**

a) червоним

b) зеленим

7. **На що вказує мітка тому?**

a) На назву диску

b) На тип диску

8. **Які віруси називають невидимками?**

a) ті, які не завдають ніякої шкоди

b) ті, які маскуються, і їх важко виявити

9. **Яким чином файлові віруси інфікують файли?**

a) записують свій код

b) перейменовують

10. **Щоб програма антивірусу могла виявити нові віруси, потрібно:**

a) часто її перезапускати

b) оновлювати вірусну базу

Оцінювання учнів, аргументація оцінок.

VII. Домашнє завдання

Опрацювати опорний конспект та відповідний розділ підручника. Підготуватися до лабораторної роботи №4.

VIII. Рефлексія:

Чи сподобався вам урок? На ваших столах весь урок лежали і посміхалися до вас смайлики. Прошу вас висловити свій настрій на кінець уроку цими смайликами. Якщо вам урок сподобався і ви радо сприйняли нові знання – то залишіть смайлик з посмішкою, а якщо вам було некомфортно, чи можливо вам не сподобались якісь моменти уроку – то розверніть смайлик іншою стороною – там де він похмурий.

Дякую за співпрацю!

Презентація

