**Олена ГАРУС**

**Гриньківська ЗОШ І-ІІІ ст.**

**ім. М.В. Лисенка**

**Урок закріплення з теми «Комп’ютерні віруси» 9 клас**

**Мета уроку:**

• засвоїти і закріпити знання з теми «По­няття про віруси, антивірусні програми»;

• набути умінь та навичок в роботі з анти-вірусними програмами;

• формувати досконалі навички та знання у галузі комп'ютерних технологій;

• розвивати інтерес до комп'ютерних знань;

• сприяти розвитку уваги, пам'яті.

**Обладнання:**

• посвідчення, картки з номером палуби, медалі;

• завдання «Знайди відповідність» (2 екз.), текст для набору «Новини про ком­п'ютерні віруси» (1 екз.), словничок (10 екз.), кросворд (2 екз.);

• комп'ютери, принтер, програми Power Point, Microsoft Word, диск з програмним за­безпеченням «KasperskyAnti virus», програма-тест автоматизованої перевірки знань з теми «Комп'ютерні віруси», підручник з інформати­ки, фонограма пісні для розминки;

• кошик з яблуками, миска з водою, руш­ник, пілотка.

**ХІД УРОКУ**

**І. Вступна частина. Організаційний момент.**

*Учитель.* Наша команда подорожує океаном комп'ютерних знань. Ми побували на багатьох островах, дізналися багато нового, вдосконали­ли свої знання та навички і, звичайно ж, знай­шли собі цікавих друзів.

*Матрос.* Командо, капітане, земля! Я бачу землю! Це острів!

*Учитель.* Як чудово, це нові враження, знайомства. Я впевнена, ми чудово проведемо час. А ви?

*Діти.* Так! Причалюймо!

*Капітан.* Я як ваш капітан зійду на берег першим, для того, щоб дізнатися, що це за острів. Матросе, ходімо зі мною, поповнимо нашу провізію.

*Учитель.* Швидше повертайтеся... А ми з вами пограємо в нашу улюблену гру «Знайди зайве».

**ГРА «ЗНАЙДИ ЗАЙВЕ» *(3 хв)***

*Правила гри: потрібно знайти зайве слово з чотирьох поданих і пояснити, чого воно сто­сується. Правильні відповіді виділено жирним шрифтом.*

1. Вінчестер:

а) кластер;

б) гігабайт;

в) файлова система;

г) *бітрейт.*

2. Монітор:

а) частота оновлення екрана;

б) *швидкодія;*

в) роздільна здатність;

г)дюйм.

3. Процесор:

а) кеш 1-го та 2-го рівня;

б) частота;

в) *апертурна решітка;*

г) конвеєр.

4. Відеокарта:

а) графічний адаптер;

б) відеопам'ять;

в) частота роботи відеопроцесора;

*г) файлова фрагментація.*

*5.* Миша:

*а.) цифрова;*

б) оптична;

в) інфрачервона;

г) електромеханічна.

6. Клавіатура:

а) розкладка;

б) мала цифрова;

в) *планшетний;*

г) алфавітно-цифрова область.

7. Системний блок:

а) блок живлення;

б) *контрастність;*

в) електрична мережа;

г) кнопка перезавантаження.

8. Материнська плата:

*а) час доступу;*

б) чіпсет;

в)контролери;

г)адаптери.

9 Звукова карта:

*а) кут огляду;*

б) акустична система;

в) номінальна потужність;

г) пікова потужність.

10. Оперативна пам'ять:

а) пам'ять довільного доступу;

б) таймінги;

в) модуль;

**г)** ***яскравість.***

*Капітан (повертається).* Доброго дня! В мене для вас є сюрприз, пригощайтеся. *(Подає кошик з яблуками.)*

*Лікар.* Зачекайте, я повинна перевірити про­візію. *(Підходить і дивиться.)* Моя інтуїція мене не підвела, яблука заражені вірусом. Ка­пітане, а з вами все гаразд? Давайте я вас об­стежу. *(Обстежує капітана.)*

*Матрос.* Нарешті я повернувся, а капітан уже тут?

*Учитель.* Так.

*Лікар.* Друзі, у мене для вас погана новина. З нашим капітаном сталася біда. Він втратив пам'ять, але поки я не знаю, що стало причи­ною цього.

Матрос. А я здогадуюсь. Блукаючи остро­вом, я дізнався, що це «Острів Вірусів». *(Діти демонструють стурбованість.)*

*Учитель (визначення мети заняття)*

Ми впораємося. Наше завдання:

* дізнатися, які бувають типи вірусів;
* причини, способи і наслідки зараження вірусом;
* які існують антивірусні засоби;
* як уникнути зараження вірусом, а якщо вже пізно — як його позбутися.

А найперша та найважливіша наша з вами мета — врятувати каштана! До роботи!!!

**II. Основна частина**

*Учитель.* Зараз я розповім вам про комп'ю­терні віруси, їх типи, способи та ознаки зара­ження вірусом, про захист від них. *(Нижче наводиться текст. Розповідь буде здійснюва­тися з використанням мультимедійних мож­ливостей програми для створення презентацій PowerPoint, 13хв.)*

**Вступ**

Історія розвитку науки і техніки, як і істо­рія людства, має безліч прикладів драматично­го протистояння Добра і Зла. Не обійшлося без цього протистояння і в процесі комп'ютеризації суспільства.

Вважають, що ідею створення комп'ютер­них вірусів окреслив письменник-фантаст Т. Дж.Райн, який в одній із своїх книжок, на­писаній у СІЛА в 1977р., описав епідемію, що за короткий час охопила близько 7000 ком­п'ютерів. Причиною епідемії став комп'ютер­ний вірус, котрий передавався від одного ком­п'ютера до іншого, пробирався в їх операційні системи і виводив комп'ютери з-під контролю.

У 70-ті роки, коли вийшла книжка Т.Дж.Райна, описані в ній факти здавалися фантастикою, і мало хто міг передбачити, що вже наприкінці 80-х років XX ст. проблема комп'ютерних вірусів стане дійсністю, такою, що призведе до значних соціальних і матері­альних втрат.

Ситуація з вірусами загострилася кілька років тому. Якщо раніше кожний був зайня­тий безпекою свого комп'ютера і своїх даних, то зі збільшенням кількості комп'ютерів, з поя­вою корпоративних ліній, виходом в Internet проблема постала по-новому.

**Віруси для кожного...**

• Сворення Вірусу є бізнесом, причому не тільки для їх авторів, а й для тих, хто з цими вірусами бореться.

• Для декого — це хобі: хобі — збирання вірусних колекцій і хобі— написання вірусів.

• Іноді, створення вірусів — спосіб пока­зати свою зухвалість і незалежність, у деяких колах подібна діяльність просто необхідна для підняття свого престижу.

• Ще для когось віруси — це витвір ми­стецтва; бувають же лікарі за покликан­ням, це означає, що може бути і комп'ю­терний лікар за покли­канням.

• Для деяких віру­си є приводом для філо­софствування на теми створення і розвитку комп'ютерів.

• Але віруси — це також стаття криміналь­ного кодексу.

• Для багатьох користувачів комп'ютерів віруси — це щоденний головний біль, причина збоїв у роботі комп'ютера.

**Теоретичні відомості**

Вірус — це програма, яка виконує несанк­ціоновані дії, як правило, має руйнівну дію, а також здатна до саморозмноження з подаль­шим додаванням своїх копій до файлів, систем­них частин комп'ютера, і також на інші ком­п'ютери, об'єднані в мережу (причому дубліка­ти зберігають здатність до подальшого само-поширення).

**Ознаки зараження вірусом можуть бути такими:**

* Уповільнення роботи комп'ютера.
* Затримка при виконанні програм.
* Зміни в файлах.
* Зміна дати модифікації файлів без при­чини.
* Незрозумілі помилки Write-protection.
* Помилки при інсталяції та запуску WINDOWS.
* Неспроможність зберігати документи Word в інші каталоги, крім TEMPLATE.
* Погана робота дисків.
* Зникнення файлів.
* Неспроможність завантажити комп'ютер.
* Неспроможність завантажити файли.
* Незрозумілі системні повідомлення, му­зикальні ефекти і т.д.
* І, взагалі, неспроможність нормально працювати.

**Віруси можна поділити на класи за такими ознаками:**

**1) за середовищем перебування вірусу:**

• мережеві — поширюються по комп'ю­терній мережі;

• файлові — впроваджуються у виконувані файли;

• завантажувальні — проникають у заван­тажувальний сектор диска (Boot-сектор) або в

сектор, що містить системний завантажник вінчестера (Master Boot Record). Існують сполучення,наприклад:

• файлово-завантажувальні віруси — зара­жають як файли, так і завантажувальні сектори дисків. Такі віруси, як правило, мають досить складний алгоритм роботи й часто застосовують оригінальні методи проникнення в систему;

**2)** **за способом зараження середовища пе­ребування:**

• резидентний вірус — при інфікуванні комп'ютера залишає в оперативній пам'яті свою резидентну частину, що потім перехоплює звернення операційної системи до об'єктів за­раження й впроваджується в них (перебувають у пам'яті і є активними аж до вимикання або перезавантаження комп'ютера);

• нерезидентні віруси — не заражають па­м'ять комп'ютера і є активними обмежений час. Деякі віруси залишають в оперативній па­м'яті невеликі резидентні програми, які не по­ширюють вірус;

**3)** **за деструктивними можливостями:**

• нешкідливі — ті, які ніяк не впливають на роботу комп'ютера (крім зменшення вільної пам'яті на диску в результаті свого поширен­ня);

• безпечні — вплив яких обме­жується змен­шенням вільної пам'яті на диску й графічними, звуковими ефек­тами;

• небезпечні віруси — ті, які можуть призвес­ти до серйозних

збоїв у роботі, або до втрати чи пошкодження інформації;

• дуже небезпечні — ті, які можуть призве­сти до фізичного пошкодження обладнання (перезаписування ПЗП, виходу з ладу диско­вих пристроїв, пошкодження елементів мате­ринської плати тощо);

**4)** **за особливостями алгоритму вірусу:**

• «Компатайони-віруси» (companion) — це віруси, що не змінюють файли. Алгоритм ро­боти цих вірусів полягає в тому, що вони ство­рюють для ЕХЕ-файлів файли-супутники, що мають те саме ім'я, але з розширенням.СОМ, наприклад, для файла XCOPY.EXE створюєть­ся файл XCOPY.COM. Вірус записується в СОМ-файл і ніяк не змінює ЕХЕ-файл. При за­пуску такого файлу DOS першим виявить і ви­конає СОМ-файл, тобто вірус, що потім запус­тить й ЕХЕ-файл.

• «Віруси-хробаки» (worm) — віруси, які поширюються в комп'ютерній мережі й, так само як і компаньйони-віруси, не змінюють фай­ли або сектори на дисках. Вони проникають у пам'ять комп'ютера з комп'ютерної мережі, встановлюють мережеві адреси інших комп'ю­терів і розсилають по цих адресах свої копії;

• «Паразитичні» — всі віруси, які при поширенні своїх копій обов'язково змінюють вміст дискових секторів або файлів.

• «Студентські»—украй примітивні віру­си, часто нерезидентні й ті, які містять велику кількість помилок.

• «Стелс-віруси» (віруси-невидимки, stealth), що являють собою програми, які «підставляють» замість себе незаражені ділян­ки інформації. Крім цього, такі віруси при звер­танні до файлів використовують досить оригі­нальні алгоритми, що дозволяють приховува­ти їх діяльність від резидентних антивірусних моніторів.

• «Поліморфік-віруси» (віруси-примари, або ті, які самі шифруються, polymorphic) — їх досить важко виявити, бо вони не мають сиг­натур, тобто не утримують жодної постійної ділянки коду. У більшості випадків два зразки того самого поліморфік-вірусу не будуть мати жодного збігу. Це досягається шифруванням основного тіла вірусу й модифікаціями програми-розшифровувача.

• «Макро-віруси» — віруси цього сімейства використовують можливості макромов, вбудо­ваних у системи обробки даних (текстові редак­тори, електронні таблиці й т.д.). У цей час най­поширеніші макро-віруси текстові документи, що заражають редактори Microsoft Word.

• «Ретровіруси» — звичайні файлові віру­си, що заражають антивірусні програми, зни­щують їх або роблять їх непрацездатними.

• «Multipartition-віруси» можуть вражати одночасно EXE, COM, boot-сектор, MBR, FAT і директорії. Якщо вони володіють поліморфни­ми властивостями і елементами невидимості, стає зрозуміло, що такі віруси — одні з найбільш небезпечних.

• «Троянські програми» (Trojans) — ви­конують шкідливі дії замість оголошених ле­гальних функцій або разом з ними. Вони не спроможні до самовідтворення і передаються тільки при копіюванні користувачем. Після запуску вони зазвичай знищують себе разом з іншими файлами на диску.

• «Поштова бомба» — велика кількість електронних повідомлень (від 10 тис.), які відсилаються на електронну адресу користу­вача з метою виведення з ладу системи або перешкод для отримання корисних повідом­лень.

**Засоби захисту від вірусів:**

• Детектори (сканери) — їх метою є поста­новка діагнозу, лікуванням буде займатися інша антивірусна програма або професійний програміст— «вірусолог»;

• Фаги (поліфаги) — програми, спроможні найти і знищити вірус (фаги) або кілька вірусів (поліфаги);

• Ревізори — цей тип антивірусів контро­лює всі можливі способи зараження комп'ю­терів;

• Охоронці — резидентні програми, пос­тійно знаходяться у пам'яті комп'ютера і кон­тролюють усі операції;

• Вакцини — використовуються для об­робки файлів і завантажувальних секторів з метою запобігання зараженню відомими віру­сами.

**Приклади антивірусних програм**

|  |  |
| --- | --- |
| **Назва антивірусу** | **Коротка характеристика** |
| Aditest | Aidstest є поліфагом, він може знаходити і знищувати відомі йому віруси. Програма розпізнає приблизно 2тисячі вірусів. Він не може впоратися з поліморфними вірусами, не може також перевіряти упаковані файли, не має евристичного аналізу |
| DrWeb | DrWeb є поліфагом, однак може «читати» упаковані файли і архіви, файли даних в форматах Word і Excel, роззброює поліморфні віруси. При завантаженні програми спершу DrWeb перевіряє самого себе на цілісність, після чого тестує ОЗП — залежно від налагоджень. Епідемію дуже небезпечного вірусу JneHalf зупинив саме DrWeb |
| ADinf | ADinf Cure Module - ревізор диска (Advanced Diskinfoscope) дозволяє знайти звичайні, stealth - ֊ поліморфні віруси. Антивірус має в своєму розпорядженні лікуючий блок ревізора Adinf — Adinf Cure Module — може знешкодити до 97 % всіх вірусів |
| NAV | Антивірусні продукти Пітера Нортона користуються популярністю вже понад 10 років. До переваг NAV можна віднести: продуманий інтерфейс, легкість інсталяції, оптимальну ціну та можливість знищувати віруси в за архівованих файлах |

**Висновок**

Отже, проблема захи­сту комп'ютерів від вірусів має велике зна­чення у наш час. Ця си­туація була зумовлена певними причинами. Раніше віруси просочу­валися на робочі місця з піратського диска, а за­раз — з ліцензійним ПЗ, через Інтернет. Усі нама­гаються виправити ситу­ацію, ігри на робочому місці частково заборо­нені, але...

Звичайно, Word і Excel де-факто є міжна­родними стандартними редакторами, а макро-віруси не пишуть тільки ледачі. При достатньо активному документообігу, як із західними партнерами, так і всередині держави, макро-віруси можуть повністю паралізувати роботу компанії, на заході вже таке практикувалось.

Друга проблема — Інтернет. Немає гарантії, що на файлових серверах вам не дадуть пару-трійку вірусів. Вихід один — захист. А тут, зви­чайно, постає проблема вибору — який анти­вірус кращий.

*Учитель.* Як Ви гадаєте, чи буде нам корис­ною ця інформація?

*Діти.* Так, вона нам дуже допоможе!

*Учитель.* А тепер спробуйте дізнатися щось корисне про віруси. Як відомо, ще з давніх часів скарбницею знань вважалася книга. Але я ду­маю, що в наш час інформаційних технологій вам також знадобиться комп'ютер. Для того, щоб з ним працювати, треба вміти підключати всі його складові.

Зараз я поділю вас на дві групи, використо­вуючи маленьку гру «Пілотка». Отже, в мене є пілотка, в якій є стільки папірців, скільки і вас. На них написано номер палуби на якій ви по­винні виконувати завдання. Зараз усі по черзі будуть витягати папірці з пілотки і озвучувати те, що там написано. І залежно від того, що кожний витяг—він займає місце в певній групі.

*Учні діляться на дві групи: ті, які будуть працювати з книгами (група № 1* — *палуба № 1) та ті, які працюватимуть за комп'юте­ром (група № 2 — палуба № 2). Після вико­нання завдання перша група перевіряє другу і в разі успішного виконання завдання дає дозвіл на роботу за комп'ютером.*

ЗАВДАННЯ «ЗНАЙДИ ВІДПОВІДНІСТЬ» АБО «ПІД'ЄДНАЙ ПРАВИЛЬНО» *(5хв) Учням дається перелік складових ПК в одній колонці та способи їх підключення в іншій. Необхідно знайти відповідність написів у таблиці.*

**Правильні відповіді**

|  |  |
| --- | --- |
| Пристрій | Спосіб підключення |
| 1 . Монітор | Вихід на відеокарті + роз'єм на системному блоці |
| 2. Системний блок | Мережа електроживлення |
| 3. Миша, клавіатура | СОМ, PS/2, USB, спеціальні порти для відповідних пристроїв |
| 4. Колонки | Вихід на звуковій карті |
| 5. Принтер | LPT, USB + Мережа електроживлення |
| 6. Модем | СОМ + Мережа електроживлення |
| 7. Сканер | COM, USB + Мережа електроживлення |

|  |  |
| --- | --- |
| Пристрій | Спосіб підключення |
| 1 . Монітор | СОМ, PS/2, USB |
| 2. Системний блок | Вихід на звуковій карті |
| 3. Миша, клавіатура | Мережа електроживлення |
| 4. Колонки | COM, USB + Мережа електроживлення |
| 5. Принтер | СОМ + Мережа електроживлення |
| 6. Модем | Вихід на відеокарті + роз'єм на системному блоці |
| 7. Сканер | LPT, USB + Мережа електроживлення |

***Учитель.***Так, ви добре володієте інформа­цією про підключення пристроїв до ПК. Тому — до роботи за комп'ютерами. Ваше завдання — набрати текст про відомі в історії комп'ютерні віруси та новинки у сфері комп'ютерних вірусів з використанням можливостей тексто­вого редактора Word та роздрукувати його, а потім ознайомити всіх присутніх з цією інфор­мацією. До роботи!

**

*(Група № 2 починає працювати за комп'ю­тером. Завдання* — *вибрати основні відомості та надрукувати.)*

**ВІРУСИ, ВІДОМІ В ІСТОРІЇ *(7хв)***

Під час досліджень, проведених однією з американських асоціацій з боротьби з комп'ю­терними вірусами, за сім місяців 1988 р. ком­п'ютери, які належали фірмам-членам асоці­ації, піддавались дії 300 масових вірусних атак, які знищили близько 300 тис. комп'ютерних систем, на відтворення яких було витрачено ба­гато часу і коштів.

У кінці 1989 р. в пресі з'явилося повідомлен­ня про знаходження в Японії нового, надзви­чайно підступного і руйнівного вірусу (його на­звали «хробаком»). За короткий час він знищив велику кількість машин. Переповзаючи від комп'ютера до комп'ютера, по комунікаціях, «хробак» спроможний знищувати вміст пам'­яті, не залишаючи надій на відновлення даних.

Розроблений у Пакистані в 1986 p., вірус отримав назву «Pakistanibrain». Він повністю замінює вміст стартового сектора і використо­вує 6 доповнюючих секторів, які помічені в FAT-диску як дефектні. Заражені дискети от­римують нове ім'я COPYRIGHT@BRAIN. На­слідками зараження цим вірусом можуть бути: уповільнене завантаження ОС, часткова втра­та даних.

Близько 5 % виявлених заражень припадає на « Alameda Virus», який також належить до цієї групи. Цей вірус заміщує вміст завантажу­вального сектора, переписуючи і зберігаючи в ньому оригінал у першому вільному секторі на диску. Механізм і наслідки зараження цим віру­сом такі самі, як і в «Pakistani brain».

«Israeli Virus» заражає програми типу СОМ, ЕХЕ. Вірус збільшує їх розмір на 1813 байти.

Збитки, яких завдають комп'ютерні віруси, зростають, а їх небезпечність для таких важливих систем, як оборона, транспорт, зв'язок, поставила проблему комп'ютерних вірусів в ряд тих, які, як правило, знаходяться під пиль­ним наглядом органів державної безпеки.

*Учитель, (звертається до групи № 1)* А ті, що працюватимуть з книгою, повинні дізнати­ся про профілактичні засоби щодо зараження комп'ютерним вірусом. *(Робота з підручни­ком.)*

Молодці, я вами дуже задоволена. Ви всі добре попрацювали і я також не гаяла часу. Я роздобула чарівний словничок, який містить усю необхідну інформацію про віруси. І в мене є він для кожного, тримайте... *(Роздає словни­чок кожному.)*

*Учитель.* Мені здається, що всі ми трішки втомилися, я вам пропоную розім'ятися. *(Діти покидають свої робочі місця та, співаючи пісню, виконують розминку, 5 хв.)*

*Учитель.* Моряки, я сподіваюся, що ви не забули про нашого каштана. І я впевнена, для того, щоб дізнатися, яким вірусом він зараже­ний, необхідно вдосконалювати свої знання про віруси. І саме тому я вам пропоную наступне завдання — кросворд англійською та українсь­кою мовою. Тому давайте я дам вам загадку англійською мовою. А ви знаєте, хто це такі? *(Діти відповідають.)*

Отже, слухайте мою загадку:

*One little apple on a tree*

*Two apples for you and me*

*Three apples by the door*

*And four apples on the floor*

*The apples are good and sweet*

*Can you count them all, Pete?*

***(10.)***

*(З якого ряду перша людина відгадає загад­ку* — *той і розгадуватиме кросворд англійсь­кою мовою.)*

Ще я хочу нагадати вам про чарівні слов­нички, вони вам знадобляться для виконання поставленого завдання. Бажаю успіху! *(Учні приступають до розв'язання кросворду.)*

**Кросворд**

*(запитання однакові для англійського та українського варіанта, 7 хв)*

**По горизонталі:**

1. Різновид атак вірусів, тобто велика кількість повідомлень на поштову скриньку користувачів, а також поштові сервери з метою виведення їх із ладу. Вони можуть швидко пе­реповнити окрему поштову скриньку і це стає бар'єром для отримання нових листів.

4. Спеціальна частина меню всіх програм, при виклику якої з'являється вікно, де у зро­зумілій формі пояснюється, як використовувати програму або її окрему функцію. Викли­кається натисненням клавіші F1.

6. Програмне забезпечення, яке знаходить та видаляє вірус з пам'яті дисків комп'ютера. Більшість з них можуть перевіряти ПК кожен раз при його вмиканні і контролювати на віру­си всі файли, які потрапляють із зовні в систе­му, наприклад по електронній пошті.

8. Пристрій для зберігання даних, який ще називають гнучким диском. Диск, покритий магнітним шаром та вміщений в пластиковий корпус. Найпопулярніші розміром 3,5 дюйма та ємністю 1,44 Мб. Є простим та перевіреним засобом для обміну невеликими файлами між ПК.

12. Помилка, яка призводить, у кращому випадку, до аварійного завершення роботи про­грами, а в гіршому — до зависання комп'ютера з втратою всіх даних, які не зберігалися. До появи таких помилок призводять комп'ютерні віруси, помилки в програмному забезпеченні, перебої в енергоживленні, механічні несправ­ності комп'ютерних пристроїв і т.д.

13. Збій у роботі програми, внаслідок чого користувач не може виконати певні дії чи опе­рації, які передбачені програмою. Як правило, в роботі програми вони з'являються через певні недоліки та неточності, які були допущені при створенні програми, а також через невірні дії користувача. Інколи джерелом їх виникнення можуть бути комп'ютерні віруси.

14. Утиліта для перевірки правильності ро­боти програмного та апаратного забезпечення (наприклад, перевірка диска).

**По вертикалі:**

2. Повідомлення, яке виводить операційна система у випадку виникнення апаратної або програмної помилки, наприклад «Програма виконала недопустиму по­милку».

3. Зависання комп'ютера, коли він виконує неприпус­тиму операцію. До цієї ситу­ації призводять збої в облад­нанні або помилки в програм­ному забезпеченні. Для вихо­ду з положення необхідно натиснути кнопку Reset на системному блоці або комбі­націю клавіш Alt + Ctrl + Del на клавіатурі.

5. Повідомлення, яке ви­никає внаслідок того, що комп'ютерна програма не може виконати ту чи іншу операцію. Вони з'являються при виникненні несправностей під час роботи програми або збоїв в опе­раційній системі. Повідомлення інформує ко­ристувача про те, що виникли проблеми, та пропонує шляхи їх вирішення.

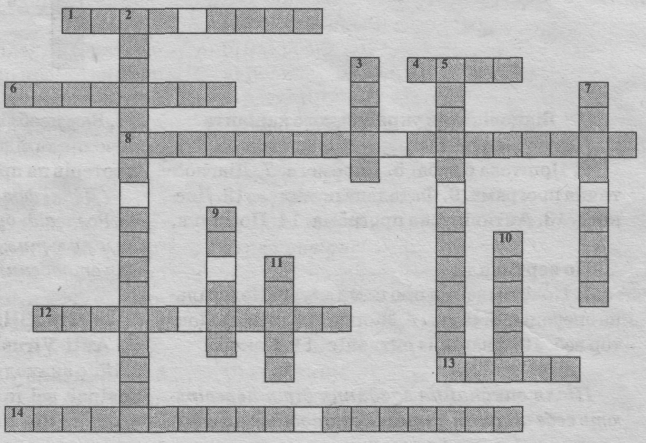
7. Пристрій для постійного зберігання інфор­мації. Дані на ньому зберігаються на одній або кількох пластинах, які вміщені в герметично закритий корпус. Обмін даними з ПК здійсню­ють головки читання/запису і спеціальний набір мікросхем. Обсяг цього пристрою від 40 до 120 Гб, але вже трапляються моделі, ємність яких вимірюється терабайтами.

9. Одна з найпопулярніших антивірусних програм, до складу якої входять засоби пере­вірки пам'яті та дисків, засоби оновлення че­рез Інтернет, а також «планувальник» їх робо­ти. Вона проста у використанні і не потребує багато ресурсів ПК.

10. Комп'ютерні ентузіасти, які насолод­жуються вивченням всього, що пов'язано з комп'ютерними системами та можуть само­стійно розширювати їх функціональність шляхом написання спеціальних програм. Цей термін почав застосовуватися щодо будь-яко­го користувача ПК, який проникає в захищені комп'ютерні системи з метою зламу або краді­жки конфіденціальної інформації, а також займається написанням комп'ютерних вірусів.

11. Програма, яка, як правило, має руйнів­ну дію, а також здана до саморозмноження з наступним додаванням своїх копій до файлів, системних областей комп'ютера, і також на інші комп'ютерів, які об'єднані в мережу (при­чому дублікати зберігають здатність до подаль­шого самопоширення).

**Кросворд англійською мовою**



**Відповіді для англійського варіанта**

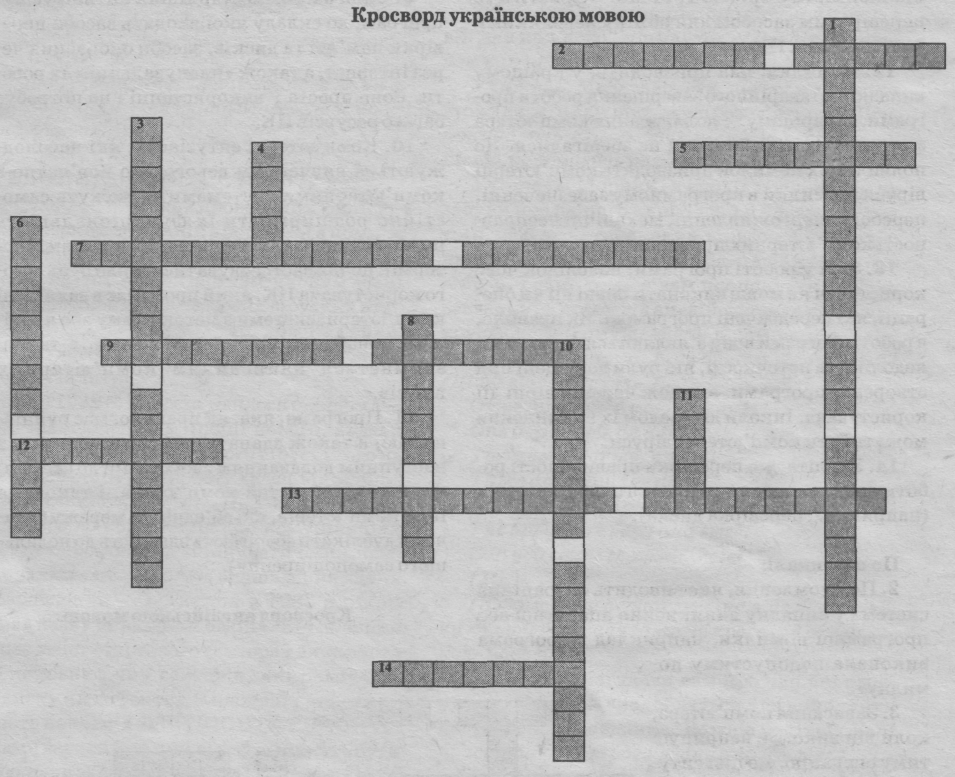
**По горизонталі:**

1. Mail bomb. 4. Help. 6. Diskette. 8. Antivirus software. 12. Fatal error. 13. Error. 14. Diagnostic program.

**По вертикалі:**

2. Illegal operation. 3. Crash. 5. Error message. 7. Hard disk. 9. Dr. Web. 10. Hacker. 11. Virus.

**Кросворд українською мовою**

**

**Відповіді для українського варіанта**

**По горизонталі:**

2. Поштова бомба. 5. Допомога. 7. Діагнос­тична програма. 9. Фатальна помилка. 12. Дис­кета. 13. Антивірусна програма. 14. Помилка.

**По вертикалі:**

1. Повідомлення про помилку. 3. Нелегаль­на операція. 4. Вірус. 6. Жорсткий диск. 8. Док­тор веб. 10. Аварійна ситуація. 11. Хакер.

*Після виконання завдання діти перевіря­ють себе шляхом, читання відповідей по черзі спочатку по горизонталі, а потім по верти­калі.*

*Учитель.* Ну якщо ви так добре впоралися з кросвордом, то давайте перейдемо до практич­ного. Моя розповідь буде про найпопулярнішу антивірусну програму Kaspersky Antivirus. Я розповім про можливості програми, її основні елементи та їх призначення та про те, як її на­лагодити.

Після цього, ті, хто ще не працював з ком­п'ютером, будуть мати таку можливість, а ті хто, вже працював, будуть за цим спостерігати. Вам необхідно налагодити програмне забез­печення та відсканувати вінчестер одного з ком­п'ютерів на предмет зараження вірусами.

*(Деякі фрагменти розповіді наведено ниж­че. Розповідь буде здійснюватися з використан­ням мультимедійних можливостей програми для створення презентацій PowerPoint.)*

ОСНОВНІ КОМПОНЕНТИ KAV *(3 хв)* Anti-Virus Monitor — компонент, який по­стійно знаходиться в пам'яті ПК і на льоту пе­ревіряє всі програми, які запускаються, і ті файли, що використовують ці програми.

Монітор дозволяє запобігти проникненню ззовні і розмноження комп'ютерних вірусів.

Anti-Virus Scanner — перевіряє файли на диску на предмет їх зараження вірусом. Модуль призначений для знаходження та лікування вже заражених файлів.

Anti- Virus Updater — оновлення антивірусних баз. Нові бази містять найбільш повні спис­ки вірусів, що дозволяє виявляти та лікувати навіть найновіші їх різновиди.

**Основні характеристики AVP**

• області сканування (диски, дискети);

• об'єкти сканування (файли, сектори, па­м'ять);

• дії (лікування, звіт, видалення);

• оновлення бази (через Інтернет);

• перевірка (наприклад, щоденно). Практичне завдання: встановити антивірусну програму на один із комп'ютерів та відсканувати вінчестер на предмет зараження вірусами.

*Діти сідають за комп'ютери та виконують завдання (3 хв)*

*Учитель.* Отже через деякий час ми отри­маємо детальний звіт про стан зараження віру­сами нашого комп'ютера. А вам сподобалось працювати з програмою?

*(Діти відповідають.)*

*Лікар.* Так, ми дізналися багато нового та цікавого і вдосконалили свої вміння. Це допо­могло мені дізнатися про вірус, який атакував капітана. Не хвилюйтеся, з ним все гаразд, він уже прийшов до тями. Розумієте, його вірус був нешкідливим. Але пам'ятайте, не всі віруси такі, багато з них небезпечні — тому будьте дуже обережні.

*Учитель.* Це стосується не тільки комп'ю­терних вірусів, а й таких, які небезпечні для людини. Наприклад, вірус грипу дуже актуаль­ний для цієї пори року. Тому вдягайтеся теп­ліше.

*Лікар.* Стривайте, в мене є ідея, як врятува­ти сюрприз капітана. Потрібно просто вимити яблука і після цього їх можна їсти. Завжди па­м'ятайте, що перед тим як з'їсти якийсь овоч чи фрукт, його потрібно помити. Матросе, допо­можіть мені!

*(Лікар та матрос миють яблука.)*

*Учитель.* Ось і все, ми виконали найголов­ніше завдання і можемо вирушати далі в подо­рож. Але слідкуючи, як ви дружно та старанно виконували всі вправи сьогодні, я хочу вас зао­хотити, а саме надати вам ступінь магістра за знання з теми «Комп'ютерні віруси». Для цьо­го вам необхідно виконати автоматизований тест перевірки знань. Прошу сідати за комп'ю­тери. Бажаю успіху!

*Діти виконують автоматизований тест перевірки знань з теми «Комп'ютерні віруси».*

**ЗАПИТАННЯ ТЕСТУ *(7хв)***

1. Програма, яка має властивості до само-розмноження, додає свої копії до файлів та має руйнівну дію:

*а) вірус;*

б)архіватор;

в) операційна система;

г) графічний редактор.

2. Як ти не можеш заразити свій комп'ютер вірусом:

а) через дискету;

б) через Інтернет;

**в)** ***створивши документ;***

г) в локальній мережі.

3. Що не є ознакою зараження вірусом:

а) уповільнення роботи комп'ютера та про­грам;

б) *відсутність звуку на комп'ютері;*

в) зникнення файлів;

г) неспроможність завантажити комп'ютер.

4. Віруси, які заражають завантажувальні сектори HHD та FDD:

а) ретровіруси;

б) *завантажувальні;*

в)хробаки;

г) макровіруси.

5. Віруси, які заражають файли Word, Excel:

а) завантажувальні;

б) хробаки;

**в)** ***макровіруси;***

г) стелс-віруси.

6. Віруси, які фальсифікують інформацію так, що програма отримує невірні дані:

**а)** ***стелс-віруси;***

б) макровіруси;

в) поштова бомба;

г) ретровіруси.

7. Віруси, які заражають антивірусні програми:

а) макровіруси;

б) поштова бомба;

в) стелс-віруси;

г) *ретровіруси.*

8. Нескінченна кількість повідомлень з ме­тою виведення з ладу комп'ютера:

а) *поштова бомба;*

б)хробаки;

в) стелс-віруси;

г) ретровіруси.

9. Шкідливі програми, здатні розмножуватися, але не заражають інші файли:

а)ретровіруси;

б) поштова бомба;

в) хробаки;

г) стелс-віруси.

**10.** Яка з програм не є анти-вірусною:

a) Kaspersky;

б)DrWeb;

***в) Prompt;***

г)Aidtest.

**11.** Програми, які спро­можні знайти і знищити вірус:

а) ревізори;

б) охоронці;

в) сканери;

г) *фаги.*

**12.** Програми, метою яких є лише постановка діагнозу:

а) ***сканери;***

б) фаги;

в) ревізори;

г) охоронці.

**13.** Програми, які контро­люють усі можливі способи за­раження вірусом:

а) фаги;

***б)ревізори;***

в) охоронці;

г) сканери.

**14.** Резентні програми, які постійно знаходяться в пам'яті комп'ютера і контролюють усі oперації:

а) ревізори;

***б)******охоронці;***

в) сканери;

г)фаги.

**15.** Чи потрібно оновлювати анти-вірусні бази?

***а) так, обов'язково.***

б) ні, необов'язково.

в) не знаю;

г) інший варіант.

*(За результатами тесту проходить вру­чення медалей, 3 хв.)*

**III. Висновок.**

***Учитель.*** Вітаю вас з отри­манням такого почесного зван­ня, як ступінь магістра, і хочу поздоровити вас із тим, що ви бездоганно впоралися з усіма труднощами, які приготував вам «Острів Вірусів».

Ви довели всім, що ви, кур­санти Клубу юних моряків, — не тільки знаєте елементи ПК, а й умієте їх підключати, відмінно працюєте з анти-вірусними базами та перевіряєте жорсткий диск комп'ютера на віруси.

А те, що всі так чудово впоралися з автоматизованим тестом, дає мені змогу спра­ведливо зазначити, що ви — фахівці з теми «Комп'ютерні віруси».

Командо, ви такі дружні, згуртовані й чудово виконуєте завдання разом. І саме завдя­ки вашим зусиллям ми вряту­вали нашого капітана.

Я дуже задоволена, що ми з такими результатами покину­ли «Острів Вірусів» і продов­жуємо свою подорож по без­крайому океану комп'ютерних знань.

Здоров'я, наснаги та успіхів у вивченні комп'ютер­них наук і не тільки. До на­ступного уроку! До побачення!