**Тема. Поняття комп’ютерного вірусу.**

**Мета.** Ввести поняття комп’ютерного вірусу; ознайомити з історією та класифікацією вірусів, шляхами зараження та методиками боротьби з вірусами.

**Тип уроку:** комбінований урок.

**Обладнання:** комп’ютер, презентація, підручник

**Хід уроку**

І. Організація класу до уроку.

ІІ. Мотивація навчальної діяльності.

*Бесіда з учнями*

* Що ви знаєте про людські віруси?
* Як можна заразитися вірусом?
* Що робити, коли людина заразилася вірусом?
* До чого призводить діяльність вірусів в організмі?
* Як ви вважаєте, чи може комп’ютер захворіти?
* Чи чули ви про комп’ютерні віруси?

*Розповідь учителя.*

З часом до Інтернету під’єднується дедалі більше користувачів. Проте жлдних засобів захисту від несанкціонованих дій Інтернет не має. Загальнодоступність та поширення Інтернету призвели до появи певної категорії людей, яких називають хакерами. Хакери без дозволу власника комп’ютера використовують або знищують дані чи програми. Мотиви їхніх дій можуть бути різними: помста, винагорода, самовираження (дехто робить це задля розваги, інші – щоб показати свою кваліфікацію). Тому виникла актуальна проблема захисту під’єднаних до Інтернету комп’ютерних систем.

ІІІ. Вивчення нового матеріалу.

1. Поняття вірусу.

Для населення школи іншим користувачам застосовуються найрізноманітніші засоби. Основну загрозу становлять комп’ютерні віруси, хробаки та програми типу троянський кінь.

Комп’ютерні віруси – це спеціальні програми в машинних кодах або фрагменти програм, здатні без відома та згоди користувача розмножуватися та розповсюджуватися на інші програми шляхом копіювання свого коду у файли, що зберігаються в системі. Вони, як і біологічні віруси, досить малі порівняно з іншими програмами.

Програми-віруси називаються так через те, що за способом поведінки вони нагадують біологічні віруси, які постійно розмножуються і заражають живий організм.

При запуску заражених програм можуть виконуватися різні небажані дії: псування файлів та каталогів, спотворення результатів обчислень, засмічення або вилучення даних із пам’яті, створення перешкод у роботі комп’ютера і ін..

Об’єктами зараження є виконувані файли програм або файли операційної системи, а також документи, що містять програмний код. Коли вірус потрапляє до комп’ютера, його власник може про це навіть не здогадуватися. Часто вірус може себе деякий час не викривати, і лише після настання певної дати чи події активізуватися та завдати шкоди комп’ютерній системі. Зараження комп’ютера вірусом відбувається лише тоді, коли на ньому виконується заражений програмний файл або відкривається заражений документ. Виконання заражених програм автоматично викликає активізацію вірусу, що призводить до зараження нових програм. Процес поширюється дуже швидко.

1. Історія комп’ютерних вірусів і троянських програм.

Історія вірусів почалася в 1950-х роках. Ще в 1951 р. один із «батьків» обчислювальної техніки Дж. фон Нейман запропонував метод створення механізмів, що самовідновлюються. Його розробки підтримали інші вчені і в результаті з’явилися ігрові програми, що базуються на вірусній технології. Використавши наукові і практичні результати, деякі програмувальними почали розробляти такі програми з метою завдання шкоди. Автори вірусів спрямували свої зусилля на персональні комп’ютери через їх масовість та відсутність засобів захисту на апаратному рівні та на рівні операційної системи. У 1961 р. В.Висотський, Х.Макілрой та Р.Моріс винайшли незвичайну гру «Дарвін», в якій кілька виконуваних програм, названих «організмами», завантажувались до пам’яті комп’ютера. Організми, які створювались одним гравцем, мали знищити представників іншого виду та захопити життєвий простір. Переможцем вважався той гравець, чиї організми захоплювали всю пам’ять або набирали найбільшу кількість балів.

Перші випадки масового зараження комп’ютерів вірусами зафіксовано в 1987 р. Тоді з’явився Пакистанський вірус братів Алві. Так вони вирішили покарати американців за придбання незаконних копій програмного забезпечення. У результаті було заражено понад 18 тис. персональних комп’ютерів США, а звідти вони надійшли і в СРСР. Другий вірус – Ліхайський – поширився з одноіменного університету США. В лютому 1989р. цим вірусом були знищені дані на 4 тис. комп’ютерів США. Після цього кількість вірусів стрімко зросла, а відтак почали розробляти засоби захисту від них.

У 1988 р. Роберт Морріс молодший створив перший масовий мережний хробак. 60000-байтна програма розроблялась із розрахунку на знищення операційних систем UNIX. Хробак Морріса вразив понад 6200 комп’ютерів, завдавши збитки на 96 мільйонів доларів. У травні 1990 р. суд присяжних визнав Морріса винним. Його було засуджено до умовного ув’язнення терміном на 2 роки, 400 годин громадських робіт і 10 тис. доларів штрафу.

У 1989 р. з’явився перший «троянський кінь» - AIDS. Вірус робив недоступними всі дані на жорсткому диску та відображав на екрані лише один напис: «Надішліть чек на 189$ на таку адресу». Автора програми було заарештовано під час отримання готівки. Перші антивірусні програми появилися у 1984р.

1. Види вірусних програм.

Робота в групах і з підручником та додатковим матеріалом. Учні класу діляться на 4 групи. Завдання кожної групи вивчити особливості вірусів певного виду: 1) за середовищем перебування вірусу; 2) за способом зараження середовища перебування; 3) за деструктивними можливостями; 4) за особливостями алгоритму вірусу. Завдання кожної групи з’ясувати особливості вірусів і заповнити таблицю.

|  |  |  |
| --- | --- | --- |
| **Класи вірусів** | **Види вірусів із класу** | **Особливості вірусів** |
| за середовищем перебування вірусу | Мережеві |  |
| Файлові |  |
| Завантажувальні |  |
| Файлово-завантажувальні |  |
| за способом зараження середовища перебування | Резидентні |  |
| Нерезидентні |  |
| за деструктивними можливостями | Нешкідливі |  |
| Безпечні |  |
| Небезпені |  |
| Дуже небезпечні |  |
| за особливостями алгоритму вірусу | «Віруси-хробаки» |  |
| «Паразитичні» |  |
| «Студентські» |  |
| «Макро-віруси» |  |
| «Ретровіруси» |  |
| «Троянські програми» |  |

Кожна група розповідає про свої види вірусів і заповнюють спільно таблицю на дошці і кожен учень у зошиті.

1. Антивірусні програми.

Для боротьби з комп’ютерними вірусами можна придбати спеціальні програми, які називають антивірусами. Антивіруси призначені для виявлення і знешкодження вірусів. Вони працюють на комп’ютері й перевіряють на наявність вірусів усі файли, які завантажуються з Інтернету, отримуються електронною поштою, переписуються на жорсткий диск або запускаються на виконання з ком пакт-диска чи дискети.

Антивірусні програми поділяють на сканери, монітори, ревізори чи вакцини залежно від принципу їх дії. (при поясненні використовується презентація)





*Бесіда з учнями*

* Чи є у вас на комп’ютері антивірусна програма?
* Яка саме?
* Чи ви її оновлюєте?
* Чому потрібно оновлювати постійно антивірусну програму?
* Чому є багато видів антивірусних програм, чому немає єдиної?
* Яку антивірусну програму варто використовувати?

*(На запитання «Яку антивірусну програму варто використовувати?» в учнів розбігаються думки, тому вчитель радить учням дослідити антивірусні програми. Учні класу діляться на групи. Кожна група учнів досліджує одну із антивірусних програм. Учні готують проект про антивірусні програми)*

IV. Закріплення вивченого матеріалу.

1. Розгадати кросворд.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | |  | | --- | |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 2 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 3 |  |  |  |  |  |  |  |  |  |  |
|  |  | 4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 5 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 6 |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 7 |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 8 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 9 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 10 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 11 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1. Вірус, який є активний у визначені моменти часу. | | | | | | | | | | | |  |  |  |
|  | 2. Вірус, який перехоплює звертання ОС до уражених файлів і | | | | | | | | | | | | | | |
|  | секторів диска і підставляють незаражені. | | | | | | | | | |  |  |  |  |  |
|  | 3. Програми, які модифікують файли і диски таким чином, що | | | | | | | | | | | | | | |
|  | вірус аналізуючи вакциновану програму чи диск, вважає, що | | | | | | | | | | | | | | |
|  | вона вже заражена. | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | 4. Вірус зменшує обсяг пам'яті і запроваджує графічні і | | | | | | | | | | | | |  |  |
|  | звукові ефекти. | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 5. Програми, які дозволяють виявити програми, які заражені | | | | | | | | | | | | | | |
|  | одним із відомих їм вірусів. | | | | | |  |  |  |  |  |  |  |  |  |
|  | 6. Вірус, який має зашифроване тіло, завдяки чому дві копії | | | | | | | | | | | | | | |
|  | одного вірусу не маютьоднакових ділянок коду. | | | | | | | | | | | |  |  |  |
|  | 7. Вірус, який поширюється в комп'ютерній мережі. | | | | | | | | | | | |  |  |  |
|  | 8. Вірус, який файл не змінює, а виконується раніше вихідної | | | | | | | | | | | | | | |
|  | програми. |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 9. Вірус, який приєднується до файлів. | | | | | | | | |  |  |  |  |  |  |
|  | 10. Програми, що знешкоджують віруси в заражених файлах | | | | | | | | | | | | | | |
|  | та відновлюють файли. | | | | |  |  |  |  |  |  |  |  |  |  |
|  | 11. Вірус, який зменшує обсяг пам'яті на диску. | | | | | | | | | | |  |  |  |  |
|  | 12. Вірус, який є активний під час роботи комп'ютера. | | | | | | | | | | | | |  |  |

1. Перевірити програму, що є доповненням до клавіатурного тренажера на наявність вірусів за допомогою он-лайн програми:
2. Відкрити браузер і на панелі адрес ввести <http://www.kaspersky.ru>.
3. Запустити сканер для перевірки файлів, клацнувши на кнопці Kaspersky File Scaner.
4. За допомогою кнопки Огляд вказати файл, який необхідно перевірити: Patch\_UA.exe.
5. Якщо сканер знайде вірус, то можна обрати одну з наступних дій, клацаючи на відповідній кнопці: Вилікувати файл (якщо ця операція можлива, то кнопка буде червоною), Змінити назву (до назви файла допишеться розширення VIR), Видалити файл (інфікований файл видаляється разом з вірусом), Продовжити (вірус залишається, а процес сканування продовжиться), Припинити сканування (припиниться робота сканера). У випадку відсутності вірусів у файлі буде відображено повідомлення про це. На завершення роботи на екрані відображатимуться відомості про результати сканування.

V. Підсумки уроку і домашнє завдання.

Вивчити §24

Підготуватись до проекту.