Полтавська академія неперервної освіти ім. М.В. Остроградського

Відділ розвитку природничих та математичних дисциплін

Розробка уроку інформатики для 9-го класу:

Захист даних. Шкідливі програми, їх типи, принципи дії і боротьба з ними.

Виконав: Злидар Артур Анатолійович учитель Балясненської загальноосвітньої школи І-ІІІ ступенів Диканської селищної ради Полтавського району Полтавської області, інформатика

ПОЛТАВА – 2023

**СТРУКТУРА УРОКУ**

**І. ОРГАНІЗАЦІЙНИЙ ЕТАП……………………………………………………………3**

**ІІ. АКТУАЛІЗАЦІЯ ОПОРНИХ ЗНАНЬ……………………………………………….3**

**ІІІ. ОГОЛОШЕННЯ ТЕМИ ТА МЕТИ УРОКУ. МОТИВАЦІЯ НАВЧАЛЬНОЇ ДІЯЛЬНОСТІ………………………………………………………………………………4**

**IV. ВИВЧЕННЯ НОВОГО МАТЕРІАЛУ………………………………………………5**

**V.  ЗАКРІПЛЕННЯ ВИВЧЕНОГО МАТЕРІАЛУ…………………………………….12**

**VI. ЗАСВОЄННЯ НОВИХ ЗНАНЬ, ФОРМУВАННЯ ВМІНЬ………………………12**

**VІІ. ПІДСУМКИ УРОКУ.ОЦІНЮВАННЯ РОБОТИ УЧНІВ………………………12**

**VІІI. ДОМАШНЄ ЗАВДАННЯ…………………………………………………………..12**

**Захист даних. Шкідливі програми, їх типи, принципи дії і боротьба з ними.**

**Очікувані результати:**

* Учні познайомляться з видами шкідливих програм та їх принципами дії; ознайомляться із шляхами захисту даних;
* розвиватимуть логічне мислення; формуватимуть вміння діяти за інструкцією, плануватимуть свою діяльність, аналізуватимуть i робитимуть висновки;
* виховуватимуть інформаційну культуру, уважність, акуратність, дисциплінованість.

**Тип уроку**: засвоєння нових знань;

**Хід уроку**

**І. Організаційний етап**

* привітання
* перевірка присутніх
* перевірка готовності учнів до уроку

**ІІ. Актуалізація опорних знань** *(повторення вивченого матеріалу, кросворд)*

1. Нормативно-правовий акт вищої юридичної сили, що регулює найважливіші суспільні відносини шляхом встановлення загальнообов'язкових правил, прийнятий в особливому порядку (законодавчим органом влади), або безпосередньо народом.

2. Кваліфікований ІТ-фахівець, який знається на комп’ютерних системах і втручається в роботу комп’ютера, щоб без відома власника дізнатися деякі особисті відомості або пошкодити дані, що зберігаються в комп’ютері.

3. Один з найпопулярніших і прибуткових (для тих, хто його реалізує) видів атак. Зловмисник створює сайт, який у точності копіює дизайн і можливості сайта будь-якого банку, інтернет-магазину або платіжної системи. Мета – збір конфіденційної інформації – паролі, коди тощо.

4. Шкідлива програма, що сповільнює роботу ПК.

5. Уникнення тимчасового або постійного приховування даних від користувачів, котрі мають права доступу.

6. Розділ інформатики, що вивчає закономірності забезпечення захисту інформаційних ресурсів фізичних осіб, підприємств, організацій, державних установ тощо від втрати, порушення функціонування, пошкодження, спотворення, несанкціонованого копіювання та використання це інформаційна?

7. Небажані рекламні електронні листи, повідомлення на форумах, телефонні дзвінки чи текстові повідомлення, що надходять без згоди користувача.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | **1.** | **З** | **А** | **К** | **О** | **Н** |  | | | | |
|  | | | | **2.** | **Х** | **А** | **К** | **Е** | **Р** |  | | | | | |
| **3.** | **Ф** | **І** | **Ш** | **И** | **Н** | **Г** |  | | | | | | | | |
|  | | | **4.** | **В** | **І** | **Р** | **У** | **С** |  | | | | | | |
|  | | | | **5.** | **Д** | **О** | **С** | **Т** | **У** | **П** | **Н** | **І** | **С** | **Т** | **Ь** |
|  | | | **6.** | **Б** | **Е** | **З** | **П** | **Е** | **К** | **А** |  | | | | |
|  | | | **7.** | **С** | **П** | **А** | **М** |  | | | | | | | |

**ІІІ. Оголошення теми та мети уроку . Мотивація навчальної діяльності**

На сьогоднішньому уроці ви дізнаєтесь: які є види шкідливих програм, як класифікують шкідливі програми та які існують шляхи захисту даних.

**IV. Вивчення нового матеріалу**

**Захист даних**

Захист даних базується на правових та організаційних принципах. Правові принципи відображено у законодавчих та інших нормативних актах. Організаційні принципи реалізуються системою заходів, поданих у таблиці.

|  |  |
| --- | --- |
| **Цілі захисту даних** | **Заходи** |
| Захист від втрати даних унаслідок стихійних явищ, збоїв у роботі електричних мереж, некомпетентності працівників тощо | Використання додаткових пристроїв автономного електроживлення, створення копій особливо важливих даних і зберігання їх  у захищених місцях |
| Захист від умисного пошкодження  комп’ютерного та мережевого обладнання, викрадення даних безпосередньо з пристроїв | Створення системи охорони з розмежуванням доступу до особливо важливого обладнання |
| Захист від викрадення даних працівниками | Уведення різних рівнів доступу до даних, використання персональних захищених паролів, контроль за діяльністю працівників |
| Захист від викрадення, спотворення чи знищення даних з використанням спеціальних комп’ютерних програм | Використання спеціального антишпигунського та антивірусного програмного забезпечення, шифрування даних, що передаються мережами, використання паролів доступу та обов’язкового дублювання даних |

**Шкідлива програма** — комп’ютерна програма або переносний код, призначений для реалізації загроз даним, що зберігаються в інформаційній системі, або для прихованого нецільового використання ресурсів системи, або іншої дії, що перешкоджає нормальному функціонуванню інформаційної системи.

**Для  шкідливих  комп’ютерних програм характерно:**

1. Швидке розмноження шляхом приєднання своїх копій до інших програм, копіювання на інші носії даних, пересилання копій комп’ютерними мережами.

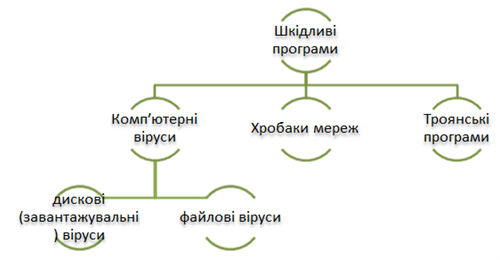
2. Автоматичне виконання деструктивних дій, які вносять дезорганізацію в роботу комп’ютера:

* знищення даних  шляхом  видалення  файлів  певних  типів  або форматування дисків;
* внесення змін  у  файли,  зміна  структури  розміщення  файлів  на диску;
* зміна або повне видалення даних із постійної пам’яті;
* зниження  швидкодії  комп’ютера,  наприклад  за  рахунок  заповнення оперативної пам’яті своїми копіями;
* постійне (резидентне) розміщення в оперативній пам’яті від моменту  звернення  до  ураженого  об’єкта  до  моменту  вимкнення комп’ютера, і ураження все нових і нових об’єктів;
* примусове перезавантаження операційної системи;
* блокування запуску певних програм;
* збирання і пересилання копії даних комп’ютерними мережами, наприклад пересилання кодів доступу до секретних даних;
* використання  ресурсів  уражених  комп’ютерів  для  організації колективних атак на інші комп’ютери в мережах;
* виведення звукових або текстових повідомлень, спотворення зображення на екрані монітора тощо.

**За рівнем небезпечності дій шкідливі програми розподіляють на:**

* *безпечні —* проявляються  відео  та  звуковими  ефектами,  не  змінюють файлову систему, не ушкоджують файли і не виконують шпигунські дії;
* *небезпечні—* призводять до перебоїв у роботі комп’ютерної системи: зменшують  розмір  доступної  оперативної  пам’яті,  перезавантажують комп’ютер тощо;
* *дуже небезпечні—* знищують дані з постійної та зовнішньої пам’яті, виконують шпигунські дії тощо.

**Класифікація шкідливих програм за принципами розповсюдження та функціонування**



**Комп’ютерні віруси** — це програми, здатні записувати свій код у код інших програм, створювати свої дублікати та виконувати несанкціоновані дії на комп’ютері.

**За середовищем існування  віруси розподіляють на:**

* дискові (завантажувальні) віруси – віруси, які заражають спеціальні частини носія даних. озмножуються копіюванням себе в службові ділянки дисків та інших змінних носіїв, яке відбувається під час спроби користувача зчитати дані з ураженого носія; Вони заражають системні частини дисків, які містять програму початкового завантаження комп’ютера.
* файлові віруси – віруси, які знаходяться у файлах і папках операційної системи комп’ютера. Файлові віруси — це блоки програмного коду, які додають себе до програмного коду інших програм і таким чином змінюють зміст файлів. При запуску зараженої програми на виконання починає працювати й код вірусу.
* макровіруси — це різновид комп’ютерних вірусів, створених засобами макросів, вбудованих у додатку Microsoft Office, CorelDRAW тощо. Зараження виникає, коли заражений документ відкривається у вікні прикладної програми, якщо підтримується можливість виконання макрокоманд. До макровірусів належать також віруси, які розповсюджуються за допомогою вкладених документів, що надсилаються електронною поштою.

Хробаки (черв’яки) комп’ютерних мереж — пересилають свої копії комп’ютерними мережами з метою проникнення на віддалені комп’ютери.

Більшість черв’яків поширюються, прикріпившись до файлів електронної пошти, електронних документів тощо. З ураженого комп’ютера хробаки намагаються проникнути на інші комп’ютери, використовуючи список електронних поштових адрес або іншими способами.

Троянські програми — програми, що проникають на комп’ютери користувачів разом з іншими програмами, які користувач «отримує» комп’ютерними мережами.

Як і інші шкідливі програми, троянські програми можуть виконувати зазначені вище деструктивні дії, але в основному їх використовують для виконання шпигунських дій.

Значна частина шкідливих програм у початкові періоди зараження не виконують деструктивних дій, а лише розмножуються. Це так звана пасивна фаза їхнього існування. Через певний час, у визначений день або по команді з комп’ютера в мережі шкідливі програми починають виконувати деструктивні дії – переходять в активну фазу свого існування.

Серед вірусів виділяють ті, що використовують спеціальні способи приховування своїх дій і знаходження в операційній системі комп’ютера:

* поліморфні  (мутанти) *—* віруси,  які  при  копіюванні  змінюють  свій вміст так, що кожна копія має різний розмір; їх важче визначити, використовуючи пошук за відомою довжиною коду вірусу;
* стелс (*англ. stealth – хитрість, викрут, stealth virus – вірус (невидимка*) –  віруси,  що  намагаються  різними  засобами  приховати  факт  свого існування в операційній системі. Наприклад, замість дійсного об’єкта, ураженого  вірусом,  антивірусній  програмі  надається  для  перевірки його неуражена копія.

З прикладами вірусних програм ти можеш ознайомитися на сайті Української антівірусної лабораторії, на сторінці Вірусна енциклопедія за адресою https://zillya.ua/virus/all.

**«Симптоми» зараження комп’ютера вірусом:**

* часті зависання і збої в роботі комп’ютера;
* повільна робота комп’ютера при запуску програм;
* неможливість завантаження операційної системи; зникнення файлів і папок або спотворення їхнього вмісту;
* часте звернення до жорсткого диска (часто блимає лампочка на системному блоці);
* браузер зависає або поводиться несподіваним чином (наприклад, вікно програми неможливо закрити).

**Методи боротьби з комп’ютерними вірусами**

Антивірусні програми – спеціальне програмне забезпечення для захисту даних і комп'ютерних систем від шкідливих програм.

Антивірусні програми до складу операційної системи не входять, їх треба встановлювати окремо. Програми розрізняють за їхнім призначенням.

Детектори – виявляють файли, заражені вірусами.  
Лікарі (фаги) – «лікують» заражені програми або документи, видаляючи із заражених файлів віруси.  
Ревізори – запам’ятовують стан програм і дисків та порівнюють їх поточний стан із попереднім і повідомляють про виявлені невідповідності.  
Фільтри – перехоплюють звернення до системи, які використовуються вірусами для розмноження і заподіяння шкоди.

Блокувальники – перехоплюють вірусонебезпечні дії (відкриття файла для запису, запис у завантажувальний сектор диску тощо) і повідомляють про це користувача.  
Сканери – сканують (перевіряють) файли на жорсткому диску і в оперативній пам’яті.  
Імунізатори – повідомляють користувача та/або перешкоджають зараженню вірусами.

**Звичайно антивірусні програмні пакети мають у своєму складі:**

* програму-сканер, яка переглядає всі файли, системні сектори, пам’ять з метою пошуку вірусів, тобто унікального програмного коду;
* антивірусний монітор, який автоматично завантажується в оперативну пам’ять після вмикання комп’ютера та виконує перевірку на віруси всіх файлів, з якими ведеться робота; також ця програма звичайно відстежує всі звернення до жорсткого диска;
* ревізор змін, який запам’ятовує певні дані кожного файлу та системних секторів. Ці дані зберігаються, і при кожному їх завантаженні та зміненні ревізор порівнює й повідомляє про зміни;
* засоби оновлення антивірусних баз через Інтернет, які дозволять своєчасно виявити та знищити нові комп’ютерні віруси.

Приклад:

Одними з найпопулярніших комерційних антивірусних програм є ESET NOD 32, BitDefender, Kaspersky Internet Security тощо. Майже не поступаються їм за ефективністю безкоштовні програми: 360 Total Security, Panda Free Antivirus, Avast Free Antivirus, Avira Free Antivirus та інші. Українська антівірусна лабораторія пропонує кілька версій свого продукту Zillya!

**Методи профілактики зараження комп’ютерними вірусами**

Усі існуючі заходи боротьби з комп’ютерними вірусами можна поділити на дві  
категорії:

* профілактичні заходи, спрямовані на резервне збереження даних та недопущення  
  зараження вірусами через піратське програмне забезпечення;
* заходи щодо знищення комп’ютерних вірусів та лікування заражених програм і даних.

**Для профілактики зараження комп’ютера вірусами слід дотримуватись певних правил:**

* регулярно оновлювати програми антивірусного захисту;
* систематично перевіряти комп’ютер на наявність вірусів;
* користуватися лише ліцензійним програмним забезпеченням;
* не використовувати для роботи підозрілі й чужі файли, зовнішні носії тощо  
  без попередньої перевірки антивірусними програмами;
* не відкривати приєднані до електронної пошти файли без попередньої їхньої  
  перевірки на наявність вірусів;
* систематично здійснювати резервне копіювання даних на незалежні носії;
* не завантажувати з Інтернету файли з розширенням exe з неперевірених сайтів;
* обмежити коло користувачів вашого комп’ютера, вимагати неухильного дотримання правил антивірусного захисту;
* при використанні ОС Windows працювати під обліковим записом без прав адміністратора.

**V.  Закріплення вивченого матеріалу.** *«Вправа продовжіть речення» *

**VI. Засвоєння нових знань, формування вмінь.**

*Використовуючи мережу «Інтернет» та підручник виконайте вправу 1.*

Вправа 1. Охарактеризуйте одну з антивірусних програм за такими вимогами:

* країна «виробник»;
* коли була створена перша версія;
* чи потребує «ліцензії»;
* характерні особливості програми.

**VІІ. Підсумки уроку. Оцінювання роботи учнів.**

*Враховуючи відповіді учнів на уроці та виконане завдання вчитель виставляє оцінки учням.*

**VІІI. Домашнє завдання.**

Опрацювати п. 1.4, ст. 43 виконати вправу 7 письмово.