Список використаних джерел

1. Дизайнерська діяльність: екологічне проектування. Науково-методичне видання / В. О. Свірко, О. В. Бойчук, В. М. Голобородько, А. Л. Рубцов, О. В. Кардаш, О. В. Чемакіна. Київ : УкрНДІ ДЕ, 2016. 196 с.

2. Мінаєв А.В. Поняття «субкультура» та «контркультура» в аспекті молодіжного проекту другої половини 60-х років XX ст. у країніх Західної Європи та США. Зб. наук. статей ЧНУ ім. Ю. Федьковича. Чернівці : Рута, 2007. Вип. 3. URL: http://ukrreal.info/ua/svit/104780-v-monako-predstavili-pervyy-ukrainskiy-elektromobil-synchronous-foto

КОМП'ЮТЕРНІ ВІРУСИ ТА АНТИВІРУСНИЙ ЗАХИСТ: ОСНОВНІ АСПЕКТИ

Паржин А. Ю.

Полтавський національний педагогічний університет імені В. Г. Короленка

Анотація. *У статті описується загрозу, яку становлять комп'ютерні віруси для безпеки і конфіденційності даних на персональних комп'ютерах та мережах. У роботі детально описується, як комп'ютерні віруси можуть проникнути в систему та які наслідки це може мати для користувача. Описується також, як працюють антивірусні програми та як вони можуть захистити комп'ютер від шкідливих програм. Стаття містить корисні поради для користувачів, які допоможуть зменшити ризик інфікування комп'ютера вірусами.*

Ключові слова: *комп'ютерні віруси, антивірусний захист.*

У сучасному світі комп'ютери та інші пристрої з підключенням до Інтернету стали невід'ємною частиною нашого життя. Ми використовуємо їх для навчання, спілкування, розваг та багатьох інших цілей. Однак, залежність від технологій відкриває шлях для розвитку комп'ютерних вірусів. Ці віруси є

шкідливими програмами, які можуть завдати шкоди вашому комп'ютеру та викрасти ваші особисті дані. Щоб захистити себе від цих загроз, потрібно мати антивірусний захист. У цій статті ми розглянемо, що таке комп'ютерні віруси та як вони працюють, а також розглянемо різні методи захисту від них. Для початку визначимось із самим поняттям комп'ютерного вірусу.

Комп'ютерний вірус – це вид шкідливого програмного забезпечення, який може самостійно розмножуватися та поширюватися через комп'ютерну мережу або зберігатися на диску під час використання інших програм. Вірус може приховано проникати в комп'ютерну систему через заражені файли, підозрілі сайти, електронну пошту, застарілі програми або через інтернет-мережу [1].

Перший відомий комп'ютерний вірус називався «Creeper» і з'явився він в 1971 році на мейнфреймах під управлінням операційної системи TENEX. Цей вірус розробили програмісти компанії BBN Technologies для тестування можливостей мережевих протоколів.

«Creeper»" був програмою, яка копіювалася сама з себе з одного комп'ютера на інший через мережу і відображалася на екрані з повідомленням «I'm the creeper, catch me if you can!» («Я - creeper, піймай мене, якщо зможете!»). Після цього він видаляв себе з комп'ютера, на якому він розмножився.

У відповідь на «Creeper» був розроблений програмний продукт «Reaper»", який простежував появу «Creeper» на мережі, вилучав його з комп'ютерів і встановлював барикади, щоб надалі захиститися від подібних вірусів.

Хоча «Creeper» був безпечним і не завдавав жодної значної шкоди, він вважається першим комп'ютерним вірусом у світі. З тих пір, віруси стали значно складнішими і більш небезпечними, їх з'явилося надзвичайно багато. Нині, віруси та інші види зловмисного програмного забезпечення є серйозною загрозою для безпеки інформації в Інтернеті, і вони щодня нападають на мільйони комп'ютерів по всьому світу [2].

На сьогоднішній день найбільш поширеними серед шкідливих програм є троянські програми та черв'яки. Розглянемо основні типи вірусів:

1. *Хробак (Worm).* Хробак – тип вірусу, який створює копії самого себе і розповсюджується через комп'ютерну мережу без дозволу користувача. Його шкода полягає в засмічуванні комп'ютеру, через що він починає працювати повільніше.

2. *Вірус-маскувальник (Rootkit).* Це вірус, який приховує свою присутність на комп'ютері шляхом зміни функціонування операційної системи, щоб приховати свою власну присутність і дії, які робить зловмисник на зараженому комп'ютері. Він маскує шкідливі програми, щоб уникнути їх виявлення антивірусними програмами.

3. *Вірус-шпигун (Spyware).* Вірус-шпигун збирає конфіденційну інформацію про користувача, тобто, інформацію про адреси, паролі, дані кредитних карт.

4. *Зомбі (Zombie).* Вірус-зомбі дозволяє зловмисникові керувати комп'ютером користувача здалеку. Він може здійснювати атаки на інші комп'ютери, які були заражені вірусом. Користувач може навіть не здогадуватися, що його комп'ютер зомбований і використовується зловмисником.

5. *Рекламний вірус (Adware).* Програма-реклама, яка відображає рекламу на комп'ютері користувача без його згоди. Цей тип вірусу може встановлюватися разом з іншими програмами, які користувач завантажує з Інтернету, або може бути встановлений безпосередньо через вразливість в операційній системі. Реклама розташовується в робочому інтерфейсі.

6. *Вірус-блокувальник (Winlock).* Шкідлива програма, яка заблоковує доступ до комп'ютера, вимагаючи від користувача внести певну суму грошей або виконати певні дії, щоб отримати пароль або ключ для розблокування. Звісно, що після переказу грошей на рахунок зловмисника банер нікуди не зникає.

7. *Троянські віруси (Trojan).* Троянська програма є найнебезпечнішим типом вірусів, тому що вона приховується під корисною програмою або файлом, щоб отримати доступ до комп'ютера та виконувати різні шкідливі дії

без відома користувача. Він збирає конфіденційну інформацію користувача, встановлює додаткові програми та навіть видаляє важливі файли. І до того моменту, поки користувач не запустить цю саму нешкідливу програму, троян не несе ніякої небезпеки і виявити його нелегко [3].

Як захиститись від комп'ютерних вірусів? Забезпечення захисту персонального комп'ютера стало реальною проблемою сьогоднішнього дня. Основними ознаками наявності комп'ютерних вірусів є уповільнення роботи деяких програм і комп'ютера в цілому, збільшення розмірів файлів, поява нових дивних файлів, виникнення несподіваних звукових і відео ефектів, нестійка робота, самостійні перевантаження та інше. Джерелом появи вірусів і інших шкідливих програм є заражені флешки, дискети, компакт-диски, вкладені файли електронної пошти, підозрілі Інтернет сайти, локальна мережа, креки, зламані хакерами програми та ігри і т.п. Щоб захистити комп'ютер від проникнення вірусів, злому хакерами для початку необхідно виконати наступні дії.

Основні рекомендації щодо захисту від шкідливих ПЗ, які допоможуть уникнути зараження:

- Інсталюйте антивірусну програму, постійно оновлюйте її та регулярно скануйте свій пристрій.
- Встановіть програму захисту від шкідливих програм, щоб запобігти інсталяції програмного забезпечення без вашого відома.
- Ніколи не встановлюйте програмне забезпечення, яке ви завантажуєте з Інтернету, якщо ви не впевнені, що воно походить із надійного джерела.
- Не відкривайте вкладення електронної пошти, якщо їх не було відскановано. Навіть фото може містити вірус.
- Не використовуйте зламане програмне забезпечення, так як воно часто містить шкідливі програми і троянських коней [4]

Список використаних джерел

1. Вікіпедія. «Комп'ютерний вірус». URL: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E

%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81

2. Вікіпедія. Комп'ютерний вірус «Creeper». URL: https://ru.wikipedia.org/wiki/Creeper

3. Види комп'ютерних вірусів. URL: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81

4. Правила безпеки від зараження вірусами. URL: https://bitdefender.ua/blog/kak-zashhitit-komp-yuter-ot-virusov-10-pravil/

ФОРМУВАННЯ ІНФОМЕДІЙНОЇ ГРАМОТНОСТІ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ НА ЗАНЯТТЯХ З «КУЛЬТУРИ СУЧАСНОЇ ДІЛОВОЇ КОМУНІКАЦІЇ»

Педченко С. О.

Полтавський національний педагогічний університет імені В. Г. Короленка

Анотація. *Йдеться про проблему формування інфомедійної грамотності в здобувачів другого (магістерського) рівня вищої освіти під час опанування дисципліни «Культура сучасної ділової комунікації». Основну увагу звернено на вправи з вироблення мовно-комунікативної компетентності, набуття якої дає змогу майбутнім фахівцям почуватися безпечно в умовах інформаційної війни.*

Ключові слова: *Інфомедійна грамотність, культура сучасної української мови, ділова комунікація, комунікативна компетентність.*

Мова як семіотично-інформаційна система є важливим професійним інструментом для фахівця будь-якої спеціальності. У цьому зв'язку вибіркова компонента для здобувачів другого (магістерського) рівня освіти «Культура сучасної ділової комунікації» відіграє виняткову роль, адже орієнтована