**НПУ імені М.П.Драгоманова**

**Факультет інформатики**

**Кафедра комп’ютерної інженерії та освітніх вимірювань**

**САМОСТІЙНА РОБОТА № 2**

**з курсу**

**«Комп'ютерні мережі та хмарні обчислення»**

**ТЕМА:**

**«Комп’ютерні віруси та антивірусні програми»**

Студент: Логвиненко В.В.

Група: 11 КНм

Факультет інформатики

Викладач: професор Франчук В.М.

**Зміст**

[**Зміст** 2](#_Toc28193717)

[**Комп’ютерні віруси та антивірусні програми** 3](#_Toc28193718)

[**1. Історія виникнення** 3](#_Toc28193719)

[**2. Класифікація комп’ютерних вірусів** 4](#_Toc28193720)

[**3. Загальні властивості та поведінка вірусів** 5](#_Toc28193721)

[**4. Антивірусні програми** 6](#_Toc28193722)

**Комп’ютерні віруси та антивірусні програми**

**1. Історія виникнення**

Перші дослідження штучних структур, що мають властивість самовідтворення, проводились в середині двадцятого століття вченими-кібернетиками Джоном фон Нейманом, Норбертом Вінером та академіком АН УРСР Віктором Михайловичем Глушковим.

Перші експерименти із самовідтворюваними програмами розпочались у 1962 році, коли було створено комп’ютерну гру Darwin (автори Висотський В.А., Макилрой Г.Д., Моррис Р.).

Розповсюдження комп’ютерних вірусів розпочалось наприкінці 70-х років, коли з’являються перші персональні комп’ютери Apple та починається їх масовий продаж, а також починають інтенсивно розвиватись мережі на базі телефонних ліній.

Вирішальним етапом в історії комп’ютерних вірусів став 1984 рік, коли італійські програмісти Черуті Р. та Морокуті М. підготували та розповсюдили серед широкої громадськості теоретичні матеріали з практичної реалізації вірусних програм.

В той же час з’являється термін «комп’ютерний вірус». Офіційно вважається, що його вперше вжив працівник Лехайського університету (США) Фред Коен у 1984 році на 7-й конференції з безпеки інформації, що проходила у США.

Перші спроби організовано протидіяти вірусним програмам були розпочаті у 1985 році Томом Нельфом. Він створив список небезпечних програм, який отримав назву «грязна дюжина» (The Dirty Dozen). В наш час вірусний бюлетень можна отримати в мережі Internet на сайті www.virusbtn.com.

На території бувшого СРСР ринок персональних комп’ютерів і комп’ютерні віруси з’являються у 1988 році. Першу спробу у створенні вітчизняної вірусної програми зробив Чижов А.А. у тому ж році.

На сьогоднішній день у світі відомо до 20 тисяч вірусів.

Наведемо лише декілька прикладів, які стали найбільш відомими.

**Приклад 1.** Студент Корнелського університету (США) Роберт Моррис у 1989 році створив вірус, внаслідок дії якого було заражено більш як 6 тисяч комп’ютерів та 70 інформаційних систем. Потерпілими виявились, зокрема, комп’ютерні центри НАСА, Ливерморської лабораторії ядерних досліджень, Гарвардського, Питсбургського, Мерилендського, Висконсинського, Каліфорнійського та Стенфордського університетів. Автор віруса був засуджений до трьох місяців ув’язнення та штрафу у 270 тисяч доларів. Вирок міг би бути і більш жорстким, але суд врахував, що вірус не псував дані, а тільки розмножувався. Пікантність ситуації полягала в тому, що батьком Морриса був відповідальний працівник відділу безпеки комп’ютерів Агентства національної безпеки США.

**Приклад 2.** Пакистанський вірус було створено братами Амджатом та Базитом Алві. Так вони вирішили покарати американців, що купували дешеві, але незаконні копії програмного забезпечення в Пакистані. Такі копії брати стали продавати, попередньо заражуючи їх спеціально розробленим вірусом. Таким шляхом тільки в США було заражено більш як 18 тисяч комп’ютерів.

**Приклад 3.** Лехайський вірус був розповсюджений зловмисником в одноіменному університеті США. За декілька днів вірус знищив інформацію декількох сотень дискет з бібліотеки обчислювального центру університету та особистих дискет студентів. Тільки в США цім вірусом було заражено близько 4 тисяч комп’ютерів.

**2. Класифікація комп’ютерних вірусів**

**Комп’ютерним вірусом** називають спеціально створену, невелику за розмірами програму, здатну самовідтворюватись та приєднувати свої точні або дещо видозмінені копії до інших програм та документів або вкорінювати їх в системні області диску та оперативної пам’яті з метою порушення нормальної роботи комп’ютера.

Найбільш поширеною є класифікація вірусів за середовищем їх перебування. За цією ознакою віруси розподіляють на:

* файлові;
* завантажувальні (бутові);
* мережеві;
* макровіруси.

**Файлові віруси.** Це найбільш розповсюджена група вірусів, що заражують програмні файли. Файлові віруси можуть укорінюватись у виконуваних файлах та в драйверах пристроїв. Найчастіше файлові віруси заражують виконувані файли з розширеннями COM і EXE. Файлові віруси розподіляються на резидентні та нерезидентні.

**Завантажувальні (бутові) віруси.** Ці віруси відрізняються від файлових резидентних тільки тим, що переносяться через завантажувальний сектор диска. Зараження комп’ютера таким вірусом відбувається при завантаженні із зараженої дискети, при цьому вірус стає резидентним. Самі дискети можуть бути заражені при використанні їх на зараженому комп’ютері.

**Мережеві віруси.** Такі віруси розповсюджуються мережею, не заражуючи програми. Найпоширенішим типом мережевих вірусів є комп’ютерні «черв’яки». Вони здатні самовідтворюватися з великою швидкістю на всіх ділянках комп’ютерної мережі. Негативний ефект дії таких вірусів полягає у зниженні пропускної здатності мережі та у помітному уповільненні роботи найбільш завантажених серверів.

**Макровіруси.** На даний момент віруси цього типу є найбільш розповсюдженими. На відміну від файлових вірусів вони перебувають не у програмних файлах, а в документах офісних застосувань (Microsoft Word, Microsoft Excel тощо). Створюють макровіруси відповідними засобами макромови. Для зараження макровірусом достатньо, наприклад, відкрити заражений документ Word, і макровірус, що знаходиться в ньому, перепише себе у головний шаблон NORMAL.DOT. Внаслідок цього кожний документ, що відкривається, буде зараженим. Негативний ефект дії макровірусів полягає у блокування команд відкриття та збереження документів, установки шрифтів тощо.

**3. Загальні властивості та поведінка вірусів**

Основними шляхами зараження комп’ютерів вірусами є зйомні диски (дискети, компакт-диски), спільно використовувані документи, що містять макроси, а також комп’ютерні мережі.

**До ознак появи вірусів** можна віднести такі:

* уповільнення роботи комп’ютера;
* зменшення обсягу вільної оперативної пам’яті комп’ютера;
* неможливість завантаження або непередбачені перезавантаження операційної системи;
* часті «зависання» та збої в роботі комп’ютера;
* неможливість запуску, відмова або неправильна робота програм, що раніше функціонували успішно;
* пошкодження файлів (зміна вмісту, розмірів, розширення, атрибутів, дати та часу створення);
* руйнування файлової структури (зникнення або поява нових файлів, спотворення каталогів, поява збійних секторів на диску, руйнування нульової доріжки диску, непередбачене переформатування диску тощо);
* періодична поява на екрані монітора недоречних повідомлень;
* звукові ефекти (звучання мелодій, писки, свисти);
* відеоефекти (поява різноманітних малюнків, яскравої нерухомої крапки, мигання або стирання екрану, зміна символів та кольорів, перевертання екрану тощо);
* перекручування роботи клавіатури (блокування вводу, поява зайвих символів, заміна символів, перемикання стану клавіш тощо);
* непередбачені спалахування сигнальної лампочки дисковода.

**Головна властивість віруса** – здатність до самовідтворення. Це – єдиний критерій, що дозволяє відрізнити вірус від будь-якої іншої шкідливої програми.

Але у загальному випадку віруси мають також і **інші властивості**:

* наявність інкубаційного періоду;
* спосіб активізації;
* самозахист від виявлення.

На протязі інкубаційного періоду вірусом ніякі дії не виконуються або, можливо, він тільки самовідтворюється. Такий період дозволяє приховати джерело віруса і канал його проникнення, а також заразити якнайбільшу кількість об’єктів. Тривалість інкубаційного періоду може залежати від дати та часу, від настання певної події, від наявності потрібної конфігурації апаратних або програмних засобів тощо.

Файловий вірус, в залежності від того, є він резидентним чи нерезидентним, по-різному активізує свою діяльність.

Нерезидентний вірус міститься безпосередньо у складі зараженої програми. Коли заражена програма розпочинає роботу, то спочатку управління отримує вірус. Вірус знаходить і заражує інші програми, після чого виконує свої шкідливі дії. Далі вірус повертає управління тій програмі, в якій перебуває, а та продовжує свою роботу як звичайно.

Резидентний вірус складається з інсталяційної та резидентної частин. При запуску зараженої програми управління спочатку отримує інсталяційна частина, який розміщує резидентну частину в ОЗП та вносить певні зміни в обробку переривань. Періодично отримуючи управління за перериваннями, резидентна частина вірусу заражує інші програми та виконує свої шкідливі дії до перезавантаження операційної системи.

Щоб запобігти своєму виявленню, віруси можуть застосовувати досить складні **способи маскування**. Найпоширеніші з них такі:

* спосіб, що робить вірус «невидимим»;
* самомодифікація.

**«Невидимі» віруси.** Деякі резидентні віруси (файлові, завантажувальні) захищаються від виявлення тим, що перехоплюють звернення операційної системи до заражених областей пам’яті і підставляють замість них «чисту» інформацію. Таким способом вірус може маскувати як збільшення обсягу зараженої інформації, так і своє тіло в ній (Stealth-технологія маскування, названа за аналогією з проектом STEALTH створення літаків-невидимок).

**Самомодифікуючі віруси.** Ці віруси, які називають також поліморфними, захищаються від виявлення зміною свого тіла при кожному самовідтворенні. Для цього вони містять (або можуть генерувати) спеціальну підпрограму для шифрування та дешифрування свого тіла (дескріптор). Ключ шифрування може залежати від часу, від характеристик програми, яку вірус заражує, тощо. Дешифрування виконується тільки безпосередньо перед початком роботи вірусу. Таким чином, тіло віруса не містить якогось сталого ланцюжка байтів, за допомогою якого його можна було б розпізнати.

**4. Антивірусні програми**

Масове розповсюдження комп’ютерних вірусів викликало розробку антивірусних програм. Їх **основні різновиди** такі:

* програми-сканери (поліфаги), здатні виявляти файли, заражені відомими вірусами, а також лікувати їх шляхом «викусування» тіла вірусу;
* програми-ревізори, здатні запам’ятовувати початковий стан файлів та системних областей диску, а потім регулярно порівнювати його з поточним і виявляти невідповідності;
* програми-фільтри (сторожа), резидентні програми, здатні перехоплювати всі запити до операційної системи на виконання «підозрілих» дій і повідомляти про них користувачеві.

Існують також апаратно-програмні засоби блокування можливості проникнення в комп’ютер вірусів.

Розглянемо **основні антивірусні пакети**.

**Пакет AVP** розроблений провідною російською фірмою «Лаборатория Касперского». Він складається із трьох програм: програми-сканера AVP Scanner, програми-фільтра AVP Monitor та програми-ревізора AVP Inspector.

**Пакет антивірусних програм Norton AntiVirus** (NAV) вважається одним з найкращих за рівнем автоматизації та функціональними можливостями. Пакет NAV містить утиліту антивірусного захисту, планувальник завдань, а також програму створення резервних копій. Основні можливості пакета: вибір об’єктів перевірки, автоперевірка при будь-яких операціях з файлами (запуск, відкриття, копіювання, створення тощо), перевірка при запуску операційної системи, планування проведення антивірусних перевірок тощо.

Розглянемо основні положення методики захисту від комп’ютерних вірусів.

Існує три **рубежі захисту від комп’ютерних вірусів**:

* запобігання появі вірусів;
* запобігання вірусній атаці, якщо вірус все ж таки з’явився на комп’ютері;
* запобігання руйнівним наслідкам, якщо атака все ж таки відбулась.

Систему безпеки інформації треба створювати «з кінця», тобто із запобігання руйнівним наслідкам будь-якого характеру.

Основним методом захисту від руйнівних наслідків вірусної атаки є щоденне резервне копіювання. За таких умов у випадку пошкодження або втрати інформації жорсткий диск може бути переформатований. На «чистий» диск встановлюють операційну систему та все необхідне програмне забезпечення з дистрибутивних носіїв. Потім відновлюють дані, які беруть з резервних носіїв.

В особливо відповідальних випадках передбачають створення не менше як двох резервних копій, що зберігаються на зовнішніх носіях в різних місцях. Між цими копіями здійснюють ротацію: на протязі тижня щоденно копіюють дані на носії резервного комплекту А, потім їх замінюють комплектом Б, і т.д.

Якщо під час роботи користувач помітив ознаки появи вірусів, то необхідно негайно припинити роботу, вимкнути комп’ютер, перезавантажити комп’ютер з «чистої» системної дискети і вжити заходів до виявлення та знешкодження вірусів, а також до відновлення пошкодженої інформації. При знешкодженні вірусів та відновленні пошкодженої інформації може виникнути потреба у переформатуванні жорсткого диску, відновленні завантажувального сектору та файлів операційної системи для системного диску, перевірці правильності установки параметрів конфігурації комп’ютера, знищенні заражених файлів та заміні їх архівними копіями, перевірці цілісності файлової системи та поверхні диску.

**Рекомендації, що стосуються запобігання появі вірусів**:

* Для антивірусних програм-сканерів та програм-ревізорів слід застосовувати автозапуск з метою регулярного антивірусного контролю при кожному вмиканні комп’ютера. На комп’ютері слід установити також і антивірусні резидентні програми-фільтри, які в процесі поточної роботи контролюватимуть «підозрілі» звернення до диску (форматування, запис у завантажувальний сектор, прямий запис за фізичною адресою) та файлової системи (створення та модифікація виконуваних файлів, зміна атрибутів файлів), а також постановки в резидент. При роботі у Windows можна скласти розклад антивірусного контролю за допомогою утиліти ‘Мастер обслуживания’.
* Слід відмовитись від використання неліцензованого програмного забезпечення, а також отриманого із ненадійних джерел. Особливо небезпечними тут є ігрові програми. Ніколи не треба запускати невідомі виконувані файли.
* Будь-яка інформація, що надходить у комп’ютер на зовнішніх носіях або із мережі, повинна контролюватись за допомогою антивірусних програм-сканерів. Винятком є випадок звичайного копіювання (навіть і заражених зовнішніх носіїв або файлів), оскільки при цьому комп’ютер заражений бути не може. Будь-яка інформація, отримана з мережі без запиту або від незнайомого адресата, має знищуватись без розгляду.
* Безконтрольний доступ до вашого комп’ютера сторонніх осіб, особливо тих, що мають власні диски, має бути виключеним.
* Не слід користуватись чужими дисками, а також своїми дисками на сторонньому комп’ютері. Не треба передавати свої диски іншим особам для використання.
* Необхідно періодично оновлювати антивірусні програми та бази вірусних сигнатур. Бажана періодичність оновлення – один раз у два тижні, допустима – один раз на три місяці. Сучасні антивірусні програми дозволяють створювати графіки оновлення сигнатурних баз, завантажуваних із Internet.
* Необхідно обов’язково створити «ремонтний набір» із дисків, серед яких один має бути системним з використовуваною операційною системою, а решта повинна містити антивірусні програми, програми-архіватори, а також утиліти обслуговування диску та файлової системи.