6. Типи комп'ютерних хакерів [Електронний ресурс]. – Режим доступу: https://glennbouchard.com/uk/361-tipe-tipe-hacker-komputer.html – Назва з екрану.

Шаповал А. І.,
студентка ІІ курсу спеціальності 029 «Інформаційна, бібліотечна та архівна справа»,
Науковий керівник: Шуляк С. О., кандидат педагогічних наук, доцент, декан факультету менеджменту і бізнесу ВП «Миколаївська філія Київського національного університету культури і мистецтв»,
м. Миколаїв

КОМПЮ’ТЕРНІ ВІРУСИ ЯК ВИД ЗАГРОЗ В КІБЕРПРОСТОРІ

Сучасний світ характеризується інтенсивним розвитком інформаційних технологій. Але побічною стороною розвитку цих технологій є розвиток різного виду шкідливого програмного забезпечення, одним з найбільш розповсюджених якого є комп’ютерні віруси.

Комп'ютерний вірус (англ. computer virus) – комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера.

Назва програми «комп'ютерний вірус» походить від однойменного терміну з біології за її здатність до саморозмноження. [2].

Не існує єдиної системи класифікації та іменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO в 1991 році). Серед них: віруси – супутники (використовують імена інших файлі), файлові віруси, завантажувальні віруси (здатні вражати як код boot-секторів, так і код файлів), віруси DIR (спотворюють системну інформацію про файлові структури), макровіруси (віруси, що заражують файли даних, наприклад, документи Word або робочі книги Excel [3].

Кожного року комп'ютерні віруси причиняють шкоди розміром в декілька мільярдів доларів, викликаючи системні критичні помилки, зупиняючи великі сайти та вебдодатки, знищуючи або модифікуючи файли, підвищуючи час відклику

Основні типи вірусів:

Хробаки – Worm. Хробак – програма, яка робить копії самої себе. Її шкода полягає в засмічуванні комп'ютеру, через що він починає працювати повільніше. Відмінною особливістю хробака є те, що він не може стати частиною іншої нешкідливою програми [3].

Виділяють наступні типи хробаків:

- поштові хробаки(Email-worm);
- хробаки, використовують інттернет-пейджери(IM-worm);
- хробаки у irc-каналах (IRC-worm);
- хробаки для файлообмінних мереж (P2P-worm);
- інші мережні хробаки (Net-worm) [1].

Віруси-маскувальники – Rootkit. Ці віруси використовуються для приховування шкідливої активності. Вони маскують шкідливі програми, щоб уникнути їх виявлення антивірусними програмами. Rootkit'и також можуть модифікувати операційну систему на комп'ютері і замінювати основні її функції, щоб приховати своє власне присутність і дії, які робить зловмисник на зараженому комп'ютері [3].

Віруси-шпигуни – Spyware. Шпигуни збирають інформацію про поведінку і дії користувача. Здебільшого їх цікавить інформація – адреси, паролі, дані кредитних карт.

Зомбі – Zombie. Віруси зомбі дозволяють зловмисникові керувати комп'ютером користувача. Комп'ютери – зомбі можуть бути об'єднані в мережу (бот-нет) і використовуватися для масової атаки на сайти або розсилання спаму. Користувач може навіть не здогадуватися, що його комп'ютер зомбований і використовується зловмисником [3].

Рекламні віруси – Adware. Програми-реклами, без відома користувачів вбудовуються в різне програмне забезпечення з метою демонстрації рекламних оголошень. Як правило, програми-реклами вбудовані в програмне забезпечення, що поширюється безкоштовно. Реклама розташовується в робочому інтерфейсі. Найчастіше такі- програми також збирають і переправляють своєму розробникові персональну інформацію про користувача [3].

Віруси-блокувальники – Winlock. Такі програми блокують користувачеві доступ до операційної системи. При завантаженні комп'ютеру з'являється вікно, в якому користувача звинувачують у скачуванні неліцензійного контенту або порушенні авторських прав. І під загрозою повного видалення всіх даних з комп'ютера вимагають відіслати смс на номер телефону або поповнити його рахунок. Звісно що після переказу грошей на рахунок зловмисника, банер нікуди не пропадає [3].

Троянські програми – це шкідливі програми, які зовні виглядають як легальний програмний продукт, але при запуску здійснюють несанкціоновані користувачем дії, спрямовані на знищення, блокування, модифікацію або копіювання інформації, порушення роботи комп'ютерів або комп'ютерних мереж. На відміну від вірусів і черв'яків, представники даної категорії не мають здатності створювати свої копії, що володіють можливістю подальшого самовідтворення [4].

До даної категорії програм відносяться:

Backdoor (бекдор) – шкідлива програма, призначена для прихованого віддаленого управління зловмисником ураженого комп'ютера. За своєю функціональністю бекдори багато в чому нагадують різні системи адміністрування, що розробляються та розповсюджуються фірмами- виробниками програмних продуктів. Ці шкідливі програми дозволяють робити з комп'ютером все, що в них заклав автор: приймати чи відсилати файли, запускати і знищувати їх, виводити повідомлення, стирати інформацію, перезавантажувати комп'ютер і т.д. [4].

Exploit (експлойт) – програми, в яких містяться дані або виконуваний код, що дозволяють використовувати одну або декілька вразливостей в програмному забезпеченні на локальному або віддаленому комп'ютері зі свідомо шкідливої метою [4].

Rootkit – програма, призначена для приховування в системі певних об'єктів або активності. Приховування, як правило, піддаються ключі реєстру (наприклад, що відповідають за автозапуск шкідливих об'єктів), файли, процеси в пам'яті зараженого комп'ютера, шкідлива мережева активність. Сам по собі Rootkit нічого шкідливого не робить, але даний тип програм в переважній більшості випадків використовується шкідливими програмами для збільшення власного часу життя в уражених системах в силу утрудненого виявлення [4].

Trojan – шкідлива програма, призначена для здійснення несанкціонованих користувачем дій, що тягнуть за собою знищення, блокування, модифікацію або копіювання інформації, порушення роботи комп'ютерів або комп'ютерних мереж, і при цьому не потрапляє ні під одну з інших троянських поводжень [4].

Отже, комп’ютерний вірус – це невелика за розміром програма, яка може приєднуватися до інших програм і виконувати різні небажані дії на комп’ютері. Програма, всередині якої міститься вірус, називається зараженою. Коли така програма починає працювати, то комп’ютерний вірус знаходить і заражає інші програми, а також чинить будь-які шкідливі дії. Кожного року комп'ютерні віруси причиняють шкоди розміром в декілька мільярдів доларів, викликаючи системні критичні помилки, зупиняючи великі сайти та веб-додатки, знищуючи або модифікуючи файли.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Безпека інформаційно-комунікаційних систем [Електронний ресурс]. – Режим доступу: http://virt.ldubgd.edu.ua/pluginfile.php/39805/mod_resource/content/3/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%201.4.pdf– Назва з екрану.
2. Комп'ютерний вірус [Електронний ресурс]. – Режим доступу: 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 – Назва з екрану.
3. Основні види вірусних програм [Електронний ресурс]. – Режим доступу: https://zillya.ua/osnovni-vidi-virusnikh-program – Назва з екрану.

4. Шкідливі програми [Електронний ресурс]. – Режим доступу: https://msn.khnu.km.ua/pluginfile.php/397142/mod_resource/content/1/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F%207%D0%B2%D1%96%D1%80%D1%83%D1%81%D0%B8.pdf – Назва з екрану.

Смирнова Д. М.,
студентка І курсу спеціальності 029 «Інформаційна, бібліотечна та архівна справа»,
Науковий керівник: Єрмолаєва Г. А., кандидат педагогічних наук, доцент кафедри інформаційної, бібліотечної та архівної справи
ВП «Миколаївська філія Київського національного університету культури і мистецтв», м. Миколаїв

БЛОГІНГ ЯК ІНСТРУМЕНТ СПІЛКУВАННЯ У СОЦІАЛЬНИХ МЕРЕЖАХ

Поява і розвиток соціальних мереж сприяє розвитку нової культури і усього суспільства. Такий спосіб комунікації виконує велику кількість функцій, дозволяє людині самореалізуватися, отримувати нову корисну інформацію. Але головною метою використання соціальних мереж є соціалізація і інтеграція, прагнення до встановлення стосунків з іншими користувачами. Будь-яка функція соціальної мережі переплітається з комунікаційною і, зрештою, трансформується в комунікацію[1].

Блог – це вебсайт, головний зміст якого – регулярно додавані записи, зображення чи мультимедіа. Для блогів характерні короткі записи тимчасової значущості[2].

За версією газети «Вашингтон профайл» (англ. WashingtonProfile), першим блогом вважають сторінку Тіма Бернса-Лі, де він, починаючи з 1992 року, публікував новини. Широке використання блогів розпочалося з 1996року. У серпні 1999 року комп'ютерна компанія «PyraLabs» із Сан-Франциско відкрила сайт Blogger. Це була перша безкоштовна блогова служба. Згодом Bloggerбув викуплений компанією Google[3].

Надзвичайна популярність блогів зумовлена двома головними обставинами: по-перше, публікувати інформацію в Інтернеті за допомогою блогів досить легко – фактично, створення нового посту зводиться до набирання його тексту у відповідному полі та відправки його на сервер шляхом натисканням кнопки «Публікувати» або подібної. Після цього пост зберігається на сервері, який автоматично формує веб-сторінки, різні посилання, додає стиль форматування