УДК 004.4

Рудь О. С., здобувачка,
Ніколюк П. К., професор
кафедри інформаційних технологій

КОМП'ЮТЕРНІ ВІРУСИ ТА ЗАХИСТ ВІД НИХ

Донецький національний університет імені Василя Стуса, м. Вінниця

Сьогодні, живучи в світі інформаційних технологій, використання комп'ютерів стало невід'ємною частиною нашого життя. Широке застосування ПК, на жаль, має й сторону, яка пов'язана з появою вірусних програм, що робить неможливим їх належне функціонування. В результаті вірусних атак руйнується файлова структура дисків, пошкоджується персональна база даних користувача. Загалом, створення та розповсюдження комп'ютерних вірусів є дуже шкідливою діяльністю, яка завдає багато збитків для користувачів. Через це в деяких країнах це є злочином та карається законом, проте злочинців визначити дуже непросто.

Для початку визначимось із самим поняттям комп'ютерного вірусу. Комп'ютерний вірус - це такий вид шкідливого програмного забезпечення, що поширює свої копії задля зараження та пошкодження даних на пристрої жертви атаки. Віруси можуть потрапити на ПК з інших вже інфікованих пристроїв, через носії інформації (CD, DVD і т.д) або через інтернет-мережу[1].

Перший комп'ютерний вірус

Перші комп'ютерні віруси народилися в академічних колах і були створені для зовсім інших цілей, ніж зараження систем і створення хаосу серед користувачів комп'ютерів. Наприклад, в кінці 50-х років британський математик Л. Пенроуз опублікував доповідь під назвою «Самовідтворювальні машини», огляд простої двовимірної моделі, здатної до самовідтворення, мутації і атаки комп'ютерних систем. У цей момент вчені і дослідники були стурбовані виключно штучним інтелектом і процвітаючою сферою робототехніки. Через кілька років троє дослідників з Bell Telephone Laboratories почали експериментувати з програмною грою під назвою «Дарвін». У пам'ять комп'ютера завантажується декілька асемблерних програм, котрі називають «організмами». Організми створені одним гравцем належать до одного виду. Основною метою було вивчити розташування пам'яті, припинити дію протилежної програми, що запускається в цьому місці, а потім заповнити вільний простір копіями себе. Переможцем вважається той гравець чий організм захопив усю оперативну пам'ять.

Сама гра була просто нешкідливою розвагою, але її можна розглядати як народження небезпечного програмного забезпечення, яке в подальшому буде використовуватися зовсім по-іншому[2].

Види комп'ютерних вірусів

На сьогодні найбільш розповсюдженими серед шкідливих програм є троянські програми та черв'яки (рис 1).

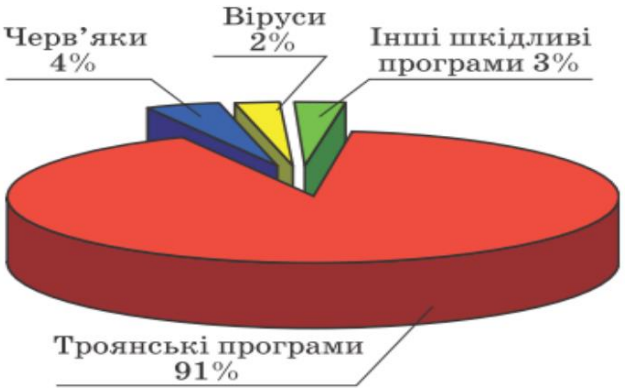

Рис. 1- Діаграма розповсюдженості шкідливих програм

Розглянемо 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.
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 свою власну присутність і дії, які робить зловмисник на зараженому комп'ютері.
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.
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.

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.
Троянські віруси (Trojan)	Троянська програма є найнебезпечнішим типом вірусів, так як вона маскується в інших нешкідливих програмах. І до того моменту, поки користувач не запустить цю саму нешкідливу програму, троян не несе ніякої небезпеки і виявити його нелегко. В основному трояни використовуються для крадіжки, зміни або видалення особистих даних користувача. Відмінною особливістю вірусу-трояна є те, що він не може самостійно розмножуватися.

Як захиститись комп'ютерних від вірусів?

Чим інтенсивніше розвиваються комп'ютерні технології, тим більше активізуються хакери, «запускаючи» в мережі масу шкідливих програм. Ще зовсім недавно їх діяльність була порівняно нешкідливою, і підлаштовані користувачам каверзи завдавали всього лише тимчасовий дискомфорт. Але тепер, коли практично у кожної людини в комп'ютері зберігається безліч конфіденційної інформації, «гуляючі» в інтернеті віруси придбали іншу спрямованість. Деякі кіберзлочинці, які не бажають заробляти чесним шляхом, створюють і запускають в мережу програми, які дозволяють збагачуватися за чужий рахунок. І якщо не запобігти зараженню свого комп'ютера вірусом, то можна опинитися в числі їх жертв.

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 [3].

Список використаних джерел

1. *Шкідливий код, який може пошкодити або видалити файли та програми на вашому комп'ютері.*
2. *URL: Комп'ютерний вірус - що таке вірусні програми, основні види | ESET*

3. *Вікіпедія - Комп'ютерна гра «Дарвін».*
4. *URL: Дарвін (комп'ютерна гра) — Вікіпедія (wikipedia.org)*
5. *3.Правила безпеки від зараження вірусами*
6. *URL: Рекомендації, як захистити комп'ютер від вірусів: 10 правил безпеки від зараження інтернет-вірусами | Bitdefender.ua*

УДК 004:351.862.2

Семен О.Д. здобувач
Зелінська О.В. доцент
кафедри інформаційних технологій

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ЗАХИСТ НАСЕЛЕННЯ ПІД ЧАС ВІЙНИ

Донецький національний університет імені Василя Стуса м. Вінниця

У сучасному світі інформаційні технології відіграють неоціненну роль у багатьох сферах життя. Наука значно спростила людям життя, створивши інтернет. Але, на жаль, блага цивілізації дуже часто використовуються людьми проти людей. Окрім війни на полі бою, є війна в інформаційному просторі. Як інформаційні технології впливають на захист населення під час війни?

У стані стресу суспільство дуже чутливе до будь-якого впливу, тому вороги не нехтують цим скористатися, проводячи інформаційно-психологічні операції, з метою поширення паніки. Існує багато способів інформаційного впливу [2]:

1. поширення фейків
2. маніпулювання
3. поширення дезінформації

Про кожен з цих способі поговоримо окремо. Фейк – це спотворений, або вигаданий факт, для подання неправдивої інформації. Поширюючи фейки ворог керує настроями населення, залякуючи його чи навпаки заспокоюючи, щоб використати їх вигідним для себе чином. Наприклад, під час війни росія активно поширювала фейки про успішний прорив української лінії оборони та про те, що деякі міста на сході вже під контролем російських військ, таким чином сіючи паніку серед населення.

Маніпулювання – це заклики до певних дій, підкріплені мотивуючими фактами. Такими діями вороги могли створювати дефіцит продовольчих товарів або виманювати дані про населення чи положення військ ЗСУ. Наприклад, після поширення інформації в інтернеті про наступ на місто в Херсонській області та спонукання до створення запасів, в решті міст України почалась масова закупівля солі, бо мав статися її дефіцит. Виявилося, що це був фейк, дефіциту солі не сталося, але населення створило штучний дефіцит, викупивши всю сіль. Цей приклад добре пояснює принцип маніпулювання [3].