Список використаних джерел

1. Хакерська етика. Матеріал з Вікіпедії — вільної енциклопедії. [Електронний ресурс] // Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Хакерська_етика.

2. Кто такие Хакеры и Кракеры? Категория: Компьютерная безопасность. [Електронний ресурс] // Режим доступу до ресурсу: https://www.infoconnector.ru/kto-takie-khakery-i-krakery.

3. Трофимов, В. В. Інформатика: підручник для бакалаврів / Трофимов В. В.; під ред. В. В. Трофімова - 2-е вид., Випр. і доп. - М.: Видавнитство Юрайт, 2015. - 917 с. - (Серія: Бакалавр. Академічний курс)

4. Безпека в інтернеті [Електронний ресурс] // Режим доступу до ресурсу: http://www.rl.kiev.ua/ua/poleznaya-informatsiya/bezopasnost-v-internete/.

УДК 004.056.53:351.746:007](477)

КІБЕРАТАКИ В УКРАЇНІ 2014-2019 РР.

Марченко В.С., студ. гр. КБ-161,
Ткач Ю.М., завідувач кафедри кібербезпеки та математичного моделювання, д.пед.н., доц.
Чернігівський національний технологічний університет

Кожен день у світі з'являються нові віруси та виникають загрози як безпеці окремого громадянина так і країні в цілому. Одні зловмисники використовують старі алгоритми, коди та схеми, інші створюють нові, однак у них завжди є дещо спільне (наприклад, шляхи проникнення на чужий комп'ютер, принципи роботи тощо). Таким чином, потрібно вивчати особливості функціонування шкідливого програмного забезпечення, для того, щоб в майбутньому мати можливість уникнути загрози.

Атака на систему «Вибори» ЦИК (травень-листопад 2014 р.). Угруповання хакерів "КіберБеркут" опублікувала в Інтернеті структуру інформаційних систем Центральної виборчої комісії. Також злочинці запевняли, що у їх розпорядженні є закрите поштове листування членів ЦВК України, технічна документація системних адміністраторів ЦВК і окружних виборчих комісії. До сьогодні достеменно не відомо чи був це злом або вірус. Але фактом залишається те, що схеми, які з'явились в інтернеті є справжніми.

Атака на енергетичний сектор BlackEnergy (грудень 2015 р.-січень 2016 р.).Про дану атаку повідомила компанія «Прикарпаттяобленерго» Авторство даного віруса приписують російській хакерської групи Sandworm. Через цю атаку залишилась велика частина західної України (Івано-Франківська область) без електрики. Даний вірус мав змогу відключати ряд процесів і пошкоджувати файли запуску.

Атаки Red Petya, Green Petya і GoldenEye (жовтень-грудень 2016). Перші віруси-шифрувальники сімейства Petya. Ці віруси шифровали дані зараженого комп'ютера і вимагали 0,9 біткоїна для розшифрування a GoldenEye навіть 1,3 біткоїна. Було заражено тисячі компютерів і нанесені мільоні збитки. Хакери заробили 3,99 біткоїна.

Атака GreyEnergy на транспортну компанію (жовтень- грудень 2016). Зараження відбувалось через взлом сервера або по електронній пошті (зараженим файлом). Даний вірус збирав інформацію (логіни і паролі) він був націлений на промислові мережі критичної важливості

Атака WannaCry (травень- червень 2017). Вірус-шифрувальник, який передавався через протоколи обміну файлами. Його ціль була - інфікувати великі компанії і державні установи (через локальні мережі). Злочинці вимагали від 300- до 600 доларів за ключ, який повинен був дешифрувати файли. Майже всі випадки зараження припадають на комп'ютери під управлінням Windows 7. Його головна особливість в том, що заразитися можна було нічого не робивши через вразливість Microsoft. Збитки понесли більше 100 компаній по всій України.

Атака банківського сектору TeleBots (січень-березень 2017). Вірус розповсюджувався завдяки програмі M.E.Doc. Разом із підробленим оновленням щахраї розіслали так званий бекдор, а потім по всій локальній мережі. Користувачами програми є близько півмільйона компаній та фізичних осіб-підприємців, вона встановлена на близько мільйон комп'ютерів по всій країні. Отже можна зробити висновок, що збитки були великі.

Атака Globelnposter Ransomware (вересень- жовтень 2017) Вірус-шифрувальник. Злочинці вимагали 2500 грн, для дешифрування. Особливістю його була націленість на Україну тому, що повідомлення про дешифрування було українською мовою, але у файлах була також і англійська мова. При цьому шахраї вимагали заплатити через айбокс (він знаходиться лише на території України). Даний вірус зупинив роботу багатьох великих компаній.

Атака бізнес сектора DanaBot (жовтень-грудень 2018). Це банківський троян, який навчений розсилати себе для подальшого зараження. Зараження комп'ютерів відбувалось після того, коли людина відкривала файли, що був прикріплений до електронного листа. А сам вірус викрадав логіни і паролі до всіх програм (почта, банківські рахунки і т.д.). Було дві особливості даного ПЗ: перший збирає поштові адреси з існуючих ящиків жертв, а другий, якщо поштовий сервіс працює на базі Open-Xchange, троян впроваджує скрипт, який таємно розсилав спам від імені жертви.

Атака Filecoder.Shade (січень 2019). Це вірус-шифрувальник, атака якого завжди починалась з отримання жертвою листа російською мовою з ZIP-архівом info.zip або inf.zip. У вкладенні, в середині архіву, знаходився завантажувач, який і загружав шифрувальника. Після зараження жертва отримувала інструкції з оплати російською та англійською мовами в TXT-файлі.

Наразі активно розповсюджується шкідливе програмне забезпечення, яке використовує WinRAR exploit (#CVE-2018-20250) (лютий- березень 2019). Дана прогармка надає можливість розпакувати файли з архіву в потрібну зловмисникам папку, а не призначену користувачем. Таким чином вони можуть помістити шкідливий код в папку автозавантаження Windows, який буде автоматично виконуватися при кожному завантаженні системи.

Сьогодні, під час підготовки до виборів, активно іде фішингова розсилка (28.03.2019) від імені Центру соціальних та маркетингових досліджень (SOCIS). Тому треба бути пильними.

Висновок. Для того щоб себе захистити від вірусів потрібно: мати антивірусні програми, правильно їх налаштувати; знати через які порти відбувається зараження і закрити їх; не переходити на підозрілі сторінки та не скачувати невідомі файли; під час встановлення програм не вимикати антивірусну програму; не водити свої дані на підозрілих сайтах. Значна частина атак відбувались через халатне ставлення людини до безпеки, отже потрібно проводити роз'яснювальну роботу серед користувачів щодо можливих шляхів зараження та навчати людей основним принципах захисту своїх комп'ютерів.

Список використаних джерел

1. Громадське [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://hromadske.ua/posts/naslidki-kiberataki
2. Cert [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://cert.gov.ua/news/56

УДК 004.056.5:004.75

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ ТЕХНОЛОГІЯХ

Полевод О.М., Трощилов М.О. студ гр. КБ-171
Базилевич В.М., доцент
Чернігівський Національний Технологічний Університет

Вступ. На сьогоднішній день хмарні сервіси стали настільки поширеними і тісно інтегрованими з обладнанням провідних виробників комп'ютерів і різних гаджетів, що багато хто навіть не замислюються про те, де саме зберігаються їхні дані і що з ними може статися. Хмарні обчислення — це модель забезпечення зручного доступу на вимогу через мережу до обчислювальних ресурсів, які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера.

Основні поняття та визначення. Хмарні системи забезпечують просту й уніфіковану взаємодію між постачальником і користувачем включають програмне забезпечення, тобто сервісну підсистему, та базу даних із багаторазовим доступом. Хмарний сервіс є особливою клієнт-серверною технологією, яка передбачає використання клієнтом ресурсів (процесорного часу, оперативної пам'яті, дискового простору, мережевих каналів, спеціалізованих контролерів, програмного забезпечення тощо) групи серверів у мережі, які взаємодіють наступним чином:

- для клієнта вся група виглядає як єдиний віртуальний сервер;
- клієнт може прозоро та гнучко змінювати обсяги споживання ресурсів у разі зміни своїх потреб.

За допомогою провайдерів хмарних рішень можна орендувати через мережу Інтернет обчислювальні потужності та дисковий простір. Переваги такого підходу – доступність і можливість гнучкого масштабування. Під час використання хмарних технологій програмне та технічне забезпечення надається користувачеві як Інтернет-сервіс. NIST США запропонував модель хмари, яка складається з п'яти основних характеристик, трьох моделей обслуговування і чотирьох моделей розгортання. Основні характеристики хмари:

- самообслуговування на вимогу;
- універсальний доступ по мережі;
- об'єднання ресурсів;
- облік споживання.
- Існують такі моделі обслуговування у хмарних технологіях:
- програмне забезпечення як послуга (SaaS); - користувач не купує SaaS-додаток, а
- орендує його
- платить за його використання деяку суму в місяць. SaaS провайдер піклується про

працездатність додатків, здійснює технічну підтримку користувачів, самостійно встановлює оновлення. Таким чином, користувач менше думає про технічну сторону питання, а зосереджується на своїх бізнес-цілях.

- платформа як послуга (PaaS) - модель надання хмарних обчислень, при якій споживач отримує