ІНФОРМАТИКА

Загрози безпеці інформації в автоматизованих системах

За навчальною програмою 2018 року

Урок 2

teach-inf.at.ua

Розділ 1
§ 2

Актуалізація опорних знань і життєвого досвіду

Пропоную визначити свої асоціації до слів:

Комп'ютерний вірус

Спам

Інтернет-шахрайство

Розділ 1
§ 2

Загрози безпеці інформації в автоматизованих системах

Автоматизована система (АС) – це організаційно-технічна система, що реалізує інформаційну технологію і поєднує:

- *обчислювальну систему (ОС);*
- *фізичне середовище;*
- *персонал;*
- *інформацію, що обробляється*

Розділ 1
§ 2

Загрози безпеці інформації в автоматизованих системах

***Загроза** — це потенційна можливість певним чином порушити інформаційну безпеку.*

Спроба реалізації загрози називається атакою

А той, хто вчиняє таку спробу, — зловмисником

Потенційні зловмисники називаються джерелами загроз

Розділ 1
§ 2

Загрози безпеці інформації в автоматизованих системах

Найчастіше загроза є наслідком наявності вразливих місць у захисті інформаційних систем (таких, наприклад, як):

Можливість доступу сторонніх осіб до критично важливого устаткування

або помилки в програмному забезпеченні

Розділ 1
§ 2

Загрози безпеці інформації в автоматизованих системах

Проміжок часу:

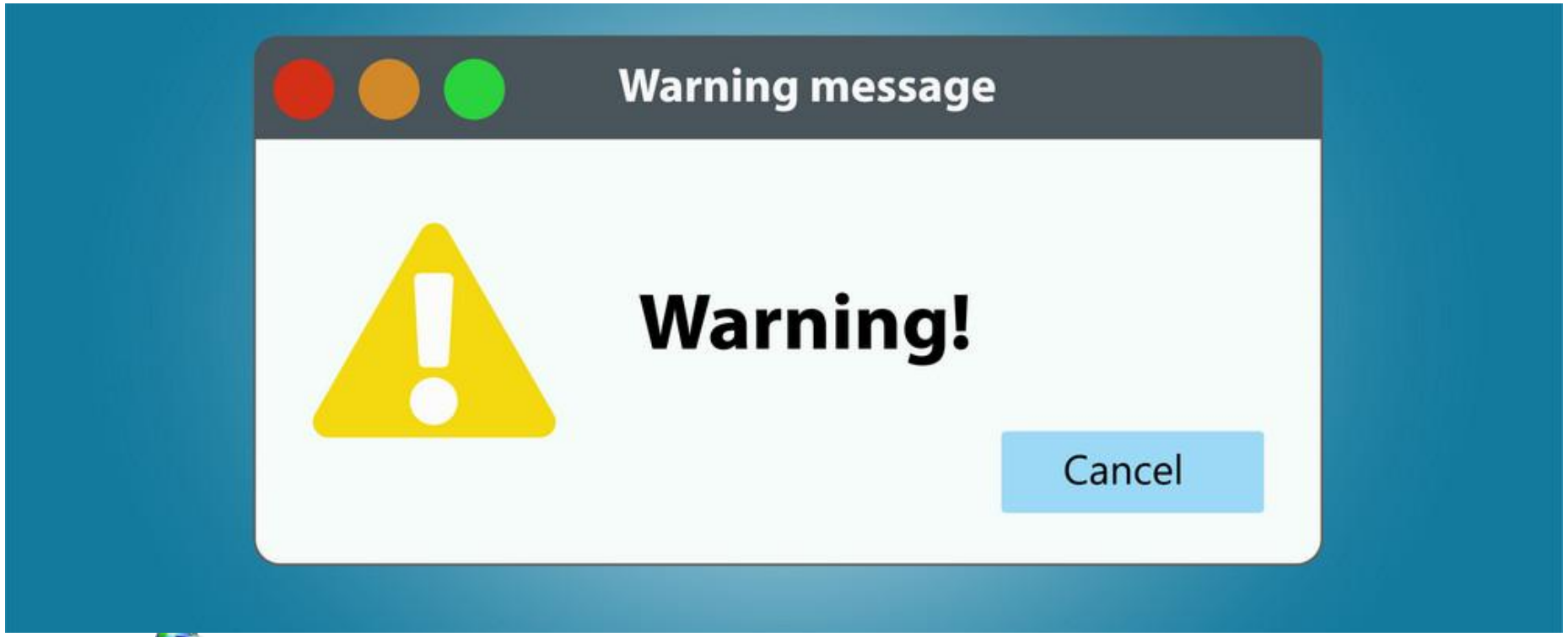
від моменту, коли з'являється можливість використати слабке місце	***називається вікном небезпеки асоційованим з даним уразливим місцем***	***і до моменту, коли прогалина ліквідується***

Поки існує вікно небезпеки, можливі успішні атаки на інформаційну систему.

Розділ 1
§ 2

Загрози безпеці інформації в автоматизованих системах

Якщо мова йде про помилки у ПЗ, то вікно небезпеки «відкривається» з появою засобів використання помилки й ліквідується після накладанні «латок», що її виправляють.



Розділ 1
§ 2

Загрози безпеці інформації в автоматизованих системах

Основні загрози інформаційній безпеці користувача Інтернету, які йдуть від авторизованих користувачів та електронних методів впливу.

Загрози користувачам Інтернету

Від авторизованих користувачів

- *Зумисне пошкодження чи викрадення даних хакерами*
- *Пошкодження даних внаслідок необережних дій*

Електронні методи впливу

- *Комп'ютерні віруси*
- *Спам*
- *Фішинг*

Розділ 1
§ 2

Загрози інформаційній безпеці

Значна частина загроз інформаційній безпеці виникає внаслідок користування ресурсами Інтернету. Серед них основними загрозами є такі:

- ***потрапляння в інформаційну систему шкідливого програмного забезпечення:***

вірусів	***мережевих хробаків***	***троянських програм***	***клавіатурних шпигунів***	***рекламних систем та ін.***

Загрози інформаційній безпеці

Продовження...

- ***інтернет-шахрайство, наприклад фішинг — вид шахрайства, метою якого є виманювання персональних даних у клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо;***

Розділ 1
§ 2

Загрози інформаційній безпеці

Продовження...

- ***несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем,***

наприклад у результаті цілеспрямованої хакерської атаки — дій, що спрямовані на порушення штатного режиму функціонування системи, порушення доступності її сервісів, отримання несанкціонованого доступу до конфіденційних відомостей, порушення цілісності даних тощо;

Загрози інформаційній безпеці

Продовження...

- ***потрапляння комп'ютера до ботнет-мережі (англ. botnet від robot і network — робот і мережа) через приховане встановлення програмного забезпечення, яке використовується зловмисником для виконання певних, найчастіше протиправних, дій з використанням ресурсів інфікованих комп'ютерів.***

Розділ 1
§ 2

Загрози інформаційній безпеці

Продовження...

Такими діями можуть бути розсилання спаму, добір паролів перебором усіх можливих варіантів, отримання персональних даних про користувачів, крадіжка номерів кредитних карток, паролів доступу, атаки з метою відмови в обслуговуванні — так звані

DDoS-атаки (англ. Distributed Denial of Service — розподілена відмова в обслуговуванні), щоб порушити доступ до деякого інтернет-сервісу шляхом перевантаження його обчислювальних ресурсів та ін.;

Загрози інформаційній безпеці

Продовження...

«крадіжка особистості» (англ. Identity Theft — крадіжка персональних даних) — несанкціоноване заволодіння персональними даними особи, що дає можливість зловмиснику здійснювати діяльність від її імені:

- ***підписувати документи***
- ***отримувати доступ до ресурсів***
- ***користуватися послугами***
- ***знімати кошти з банківських рахунків тощо***

Розділ 1
§ 2

Загрози для мобільних пристроїв

Ви знаєте, що смартфони — це мобільні телефони, доповнені функціями персонального комп'ютера, зі своєю операційною системою та іншим програмним забезпеченням.

Тому для смартфонів характерні ті самі загрози, що і для стаціонарних комп'ютерів:

віруси	***троянські програми***	***мережеві хробаки***	***рекламні модулі та ін.***

Як і стаціонарні комп'ютери, смартфони можуть потрапити до ботнет-мережі.

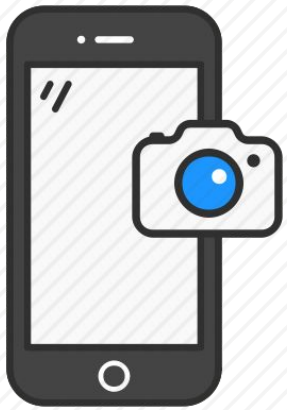
Розділ 1
§ 2

Загрози для мобільних пристроїв

Найчастіше смартфон постійно увімкнений, має підключення до мережі Інтернет, завжди розташований поруч із власником, містить різноманітні пристрої введення/виведення:

мікрофон

відео-камеру



GPS-навігатор та ін.

Зі смартфоном нерідко зв'язані грошові рахунки — в оператора мобільного зв'язку або банківські рахунки. Усе це підсилює небезпеку.

Розділ 1
§ 2

Загрози для мобільних пристроїв

Існують шпигунські програми, які зловмисники використовують для шпигування за користувачем смартфона. Використовуючи їх, можна:

перехоплювати повідомлення про всі здійснені дзвінки	***показувати вміст СМС-листування***	***показувати дані про відвідані сайти***
знімати камерою телефона оточення користувача	***визначати його місце розташування***	***включати мікрофон і записувати всі розмови***

Розділ 1
§ 2

Загрози для мобільних пристроїв

Ще один аспект загроз для користувачів мобільних телефонів полягає в роботі з платними послугами.

Підписка з використанням СМС на онлайн-гру, певний сайт, будь-який сервіс, який вимагає регулярну оплату, можуть призводити до списування з рахунку значних коштів. Іноді такі СМС можуть надсилатися троянськими програмами.

Розділ 1
§ 2

Загрози для мобільних пристроїв

Однак не всі користувачі дбають про безпеку та встановлюють антивірусне програмне забезпечення на свої смартфони.

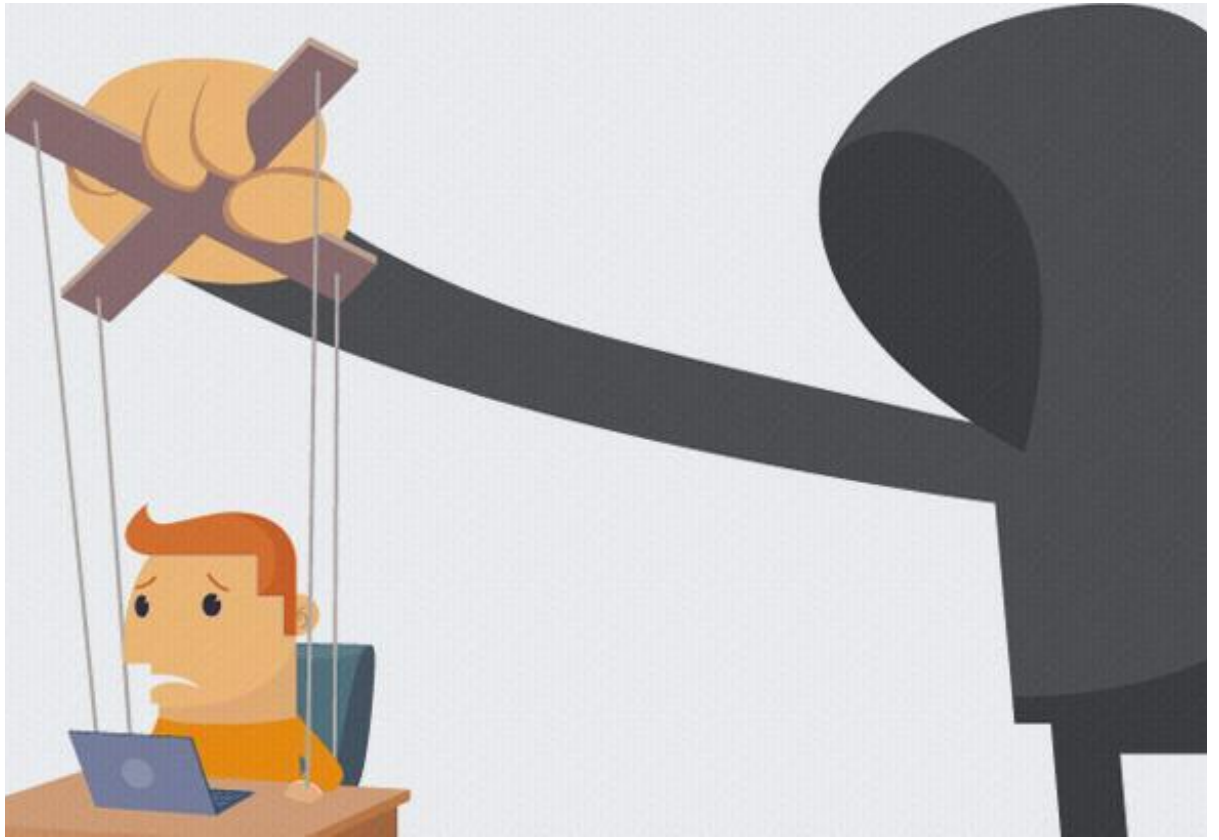
Avast Mobile Security	Eset Mobile Security & Antivirus	Anti-virus Dr.Web тощо

Розділ 1
§ 2

Соціальна інженерія

Соціальна інженерія *— це наука, що вивчає людську поведінку та фактори, які на неї впливають.*

У наш час результати досліджень із соціальної інженерії часто використовують зловмисники для маніпуляції, щоб спонукати людину виконати певні дії чи розголосити конфіденційну інформацію.



Розділ 1
§ 2

Соціальна інженерія

За даними антивірусної лабораторії Zillya! Антивірус (zillya.ua), наразі більшість заражень шкідливими програмами комп'ютерів і мереж відбувається шляхом обману користувачів з використанням методів соціальної інженерії.

Соціальна інженерія

Найбільш поширені прийоми, які використовують зловмисники:

надсилання електронних листів, зміст яких спонукає користувача відкрити прикріплений до листа файл. Як наслідок, може бути активована троянська програма. Зловмисники розраховують на емоційну реакцію користувача на повідомлення в листі або на звичайну цікавість;

Розділ 1
§ 2

Соціальна інженерія

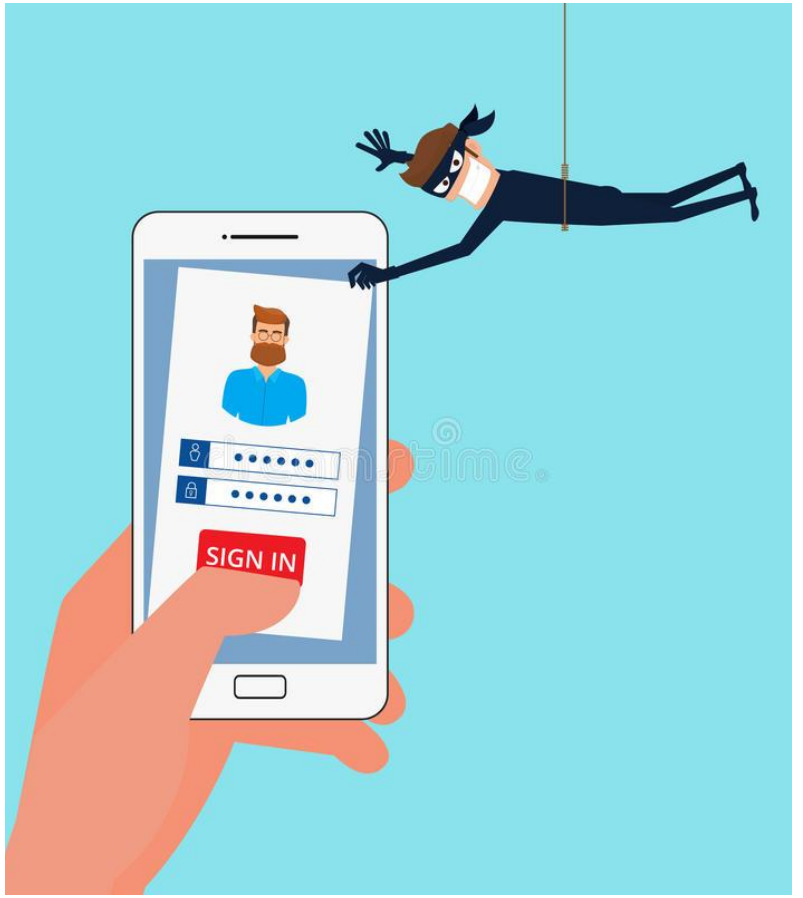
(Продовження...) Прийоми, які використовують зловмисники:

створення сайтів, які дуже схожі на справжні, для отримання логінів і паролів користувачів. Це один з прийомів фішингу. Шахрайство базується на некоректно введених у браузері адресах сайтів, на підміні пошукових запитів;

Соціальна інженерія

(Продовження...) Прийоми, які використовують зловмисники:

комбінація двох попередніх методів — надсилання електронного листа з пропозицією перейти на фішинговий сайт.



Запитання для рефлексії

1. *Які труднощі я зміг подолати на уроці?*
2. *Чи маю я задоволення від роботи на уроці?*
3. *Наскільки старанно я працював на уроці?*
4. *Чи досяг я особистої мети на цьому уроці?*

Розділ 1
§ 2

Домашнє завдання

Зробити пост у соціальних мережах про загрози безпеці інформації. Зробити записи у «Щоденнику особистих вражень у вивченні інформатики»

Розділ 1
§ 2

Працюємо за комп’ютером

ІНФОРМАТИКА

Дякую за увагу!

За навчальною програмою 2018 року

Урок 2

teach-inf.at.ua