Інформатика, 10 клас

БАЗОВИЙ МОДУЛЬ

ТЕМА 1 «**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СУСПІЛЬСТВІ**», УРОК 2

Узагальнююче повторення

1. Фронтальна бесіда по основним поняттям теми попереднього уроку

2. Творча робота у групах

Завдання: Складіть схему основних інформаційних процесів у таких інформаційних системах:

1 група: бібліотека школи;

2 група: телефонний довідник смартфона;

3 група: система прогнозування погоди;

4 група: довідникова система вакантних місць на ринку праці в місті).

Урок 3. ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УРОК 3, ТЕМИ 1 «**ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В СУСПІЛЬСТВІ**»

ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У зв’язку зі зростаючою роллю інформаційно-комунікаційних технологій у сучасному суспільстві проблема захисту даних від втрати, викрадення, спотворення або пошкодження даних потребує посиленої уваги. Вирішення цієї проблеми сприяє забезпеченню інформаційної безпеки як окремої особистості, організації, так і всієї держави.

Інформаційна безпека — це стан захищеності систем передавання, опрацювання та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність даних.

Також під інформаційною безпекою розуміють комплекс заходів, спрямованих на забезпечення захищеності даних від несанкціонованого доступу, використання, оприлюднення, внесення змін чи знищення.

Конфіденційність

- Під конфіденційністю розуміють забезпечення доступу до даних на основі розподілу прав доступу, захист від несанкціонованого ознайомлення. До деяких даних право доступу мають усі користувачі, до інших — певні групи людей, а є особисті дані, доступ до яких може мати тільки одна людина.

Доступність

- Доступність означає забезпечення доступу до загальнодоступних даних усім користувачам і захист цих даних від блокування зловмисниками.

Цілісність

- Цілісність передбачає захист даних від їх зловмисного або випадкового знищення чи спотворення.

Питання інформаційної безпеки

Останнім часом до питань інформаційної безпеки включено питання інформаційного впливу на особистість і суспільство. У лютому 2017 року указом Президента України була затверджена Доктрина інформаційної безпеки України, яка визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Життєво важливими інтересами суспільства та держави визнано такі:

- захист українського суспільства від агресивного впливу деструктивної пропаганди;
- захист українського суспільства від агресивного інформаційного впливу, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;
- всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірних та об'єктивних відомостей та ін.

Кримінальним кодексом України передбачено кримінальну відповідальність за порушення інформаційної безпеки.

Довідничок

Деструкція — порушення або руйнування нормальної структури чого-небудь.

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

З технічної точки зору, залежно від результату шкідливих дій, можна виділити такі види загроз інформаційній безпеці:

- отримання несанкціонованого доступу до секретних або конфіденційних даних;
- порушення або повне припинення роботи комп'ютерної інформаційної системи;
- отримання несанкціонованого доступу до керування роботою комп'ютерної інформаційної системи;
- знищення та спотворення даних.

Значна частина загроз інформаційній безпеці виникає внаслідок користування ресурсами Інтернету.

Серед них основними загрозами є такі:

потрапляння в інформаційну систему шкідливого програмного забезпечення: вірусів, троянських програм, мережевих хробаків, клавіатурних шпигунів, рекламних систем та ін.;

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;

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;

потрапляння комп'ютера до ботнетмережі (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. 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.;

«крадіжка особистості» (англ. Identity Theft — крадіжка персональних даних) — несанкціоноване заволодіння персональними даними особи, що дає можливість зловмиснику здійснювати діяльність (підписувати документи, отримувати доступ до ресурсів, користуватися послугами, знімати кошти з банківських рахунків тощо) від її імені.

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., орієнтовані на різні типи мобільних пристроїв. Як і стаціонарні комп'ютери, смартфони можуть потрапити до ботнет-мережі.

Найчастіше смартфон постійно увімкнений, має підключення до мережі Інтернет, завжди розташований поруч із власником, містить різноманітні пристрої введення/виведення: мікрофон, відеокамеру, GPS-навігатор та ін. Зі смартфоном нерідко зв'язані грошові рахунки — в оператора мобільного зв'язку або банківські рахунки. Усе це підсилює небезпеку.

Існують шпигунські програми, які зловмисники використовують для шпигування за користувачем смартфона. Використовуючи їх, можна перехоплювати повідомлення про всі здійснені дзвінки, показувати вміст СМС-листування та дані про відвідані сайти, знімати камерою телефона оточення користувача, визначати його місце розташування, включати мікрофон і записувати всі розмови.

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.

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

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.

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.

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

Людські слабкості — жадібність, нечесність, честолюбство та інші — також часто використовують для досягнення зловмисної мети. Троянські програми найчастіше потрапляють на комп'ютер під час спроби користувача використати неліцензійне, «зламане», програмне забезпечення, у якому міститься прихований троянський модуль. Також троянські програми містяться в генераторах кодів і так званих «кряках» — програмах для «зламування» платних програмних засобів

ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В ІНТЕРНЕТІ

Для того щоб максимально уникнути загроз під час роботи в Інтернеті, варто дотримуватися певних правил. Наведемо поради, що надані CERTUA (англ. Computer Emergency Response Team of Ukraine — команда України з реагування на комп'ютерні надзвичайні події) — спеціалізованим структурним підрозділом Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України (cert.gov.ua):

1. Використовуйте тільки ліцензійне програмне забезпечення. Установлюйте програми тільки з офіційних джерел. Перед установленням читайте відгуки інших користувачів, якщо вони доступні.

2. Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп'ютери. Бажано, щоб оновлення антивірусних баз здійснювалося регулярно та автоматично.

3. Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.


Не відкривай невідомі тобі файли
Не повідомляй пароль
Запитуй у дорослих
Не розповідай про себе
Будь обережним з незнайомцями
Не відповідай на листи незнайомцю
sms
Не поспішай надсилати SMS
Не зустрічайся з незнайомцями

ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В ІНТЕРНЕТІ

4. Використовуйте надійні паролі. Не використовуйте на різних інтернет-ресурсах один і той самий пароль, змінюйте його регулярно.

5. Приєднуйтеся тільки до перевірених Wi-Fi-мереж. Не відправляйте важливі дані (дані кредитних карток, онлайн-банкінгу тощо) через публічні та незахищені Wi-Fi-мережі.

6. Установіть фільтр спливаючих вікон у браузері.

7. Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузера (мал. 1.4) та URL-адреси веб-сайтів, щоб визначити, чи не підроблений сайт ви відвідуєте.

Будьте обережні, якщо в адресному рядку браузера відображаються інші позначки:

ⓘ — інформація або не захищено. З'єднання із сайтом не конфіденційне;

⚠ — не захищено або небезпечно. Уникайте перегляду таких сайтів.

ПРАВИЛА БЕЗПЕЧНОЇ РОБОТИ В ІНТЕРНЕТІ

8. Не відкривайте повідомлення електронної пошти від невідомих вам осіб і прикріплені до них файли, яких ви не очікуєте.

9. Подумайте про можливі ризики для вас перед тим, як викласти щось у мережу Інтернет. Дуже легко розмістити дані в мережі Інтернет, але дуже складно їх видалити з неї.

10. Створюйте резервні копії важливих для вас даних, зберігайте їх на носіях даних, відключених від мережі Інтернет.

Корисним є створення в операційній системі Windows облікового запису користувача, який не має прав адміністратора. Якщо під час роботи в Інтернеті з таким обліковим записом на комп'ютер потрапить троянська програма, вона не буде запущена на виконання.

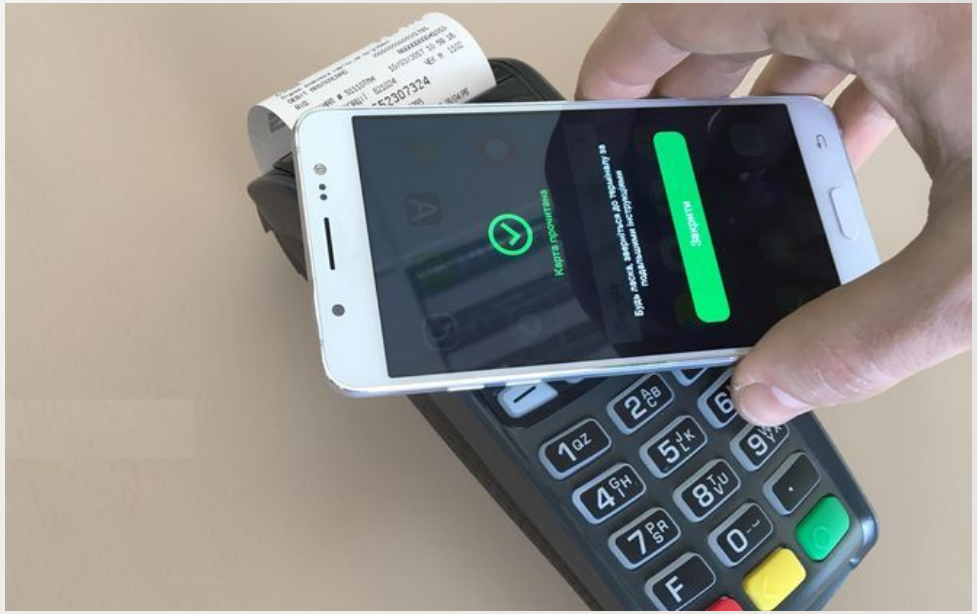
Для користувачів електронної пошти та соціальних мереж рекомендується використовувати додаткові заходи безпеки. Один з них — двохетапна перевірка.

Двохетапна перевірка (також кажуть двофакторна авторизація) — це спосіб входу до облікового запису, при якому потрібно, крім уведення логіна та пароля, виконати певну додаткову дію, наприклад увести код, отриманий в СМС, на електронну пошту або в голосовому повідомленні.

Також для дуже важливих акаунтів використовуються унікальні зовнішні накопичувачі та зчитувачі біометричних даних.

Для користувачів смартфонів є окремі рекомендації:

- не телефонуйте на незнайомі номери;
- уважно контролюйте послуги, на які ви підписуєтеся;
- установлюйте мобільні додатки лише з офіційних магазинів: PlayMarket (Android), AppStore (iOS), Marketplace (WindowsPhone);
- уважно стежте за тим, які дозволи вимагає програма під час установлення та оновлення програмного забезпечення на мобільних пристроях.



Робота за комп'ютером

Увага! Під час роботи з комп'ютером дотримуйтеся вимог безпеки життєдіяльності та санітарно-гігієнічних норм.

Завдання

Налаштуйте двохетапну перевірку для вашого облікового запису Google.

Для цього:

1. Відкрийте браузер, увійдіть до свого облікового запису.
2. Виберіть кнопку *Додатки Google* і додаток Мій обліковий запис . Виконайте Вхід і безпека ⇒ Вхід в обліковий запис Google ⇒ Двохетапна перевірка.
3. Виберіть кнопку Розпочати.
4. Уведіть повторно пароль від облікового запису.
5. Погодьтеся або змініть номер телефона на сторінці Налаштуйте свій телефон, виберіть гіперпосилання *Далі*.
6. Уведіть код, що надійде на мобільний телефон, та виберіть гіперпосилання *Далі*.
7. Виберіть гіперпосилання Увімкнути.
8. Виберіть у групі Резервні коди гіперпосилання Згенерувати.
9. Виберіть гіперпосилання Завантаження та збережіть згенеровані коди у вашій папці. Ними можна скористатися *для* входу в обліковий запис, якщо телефона немає поруч.
10. Закрийте вікно Збережіть резервні коди.
11. Вийдіть з вашого облікового запису.
12. Увійдіть повторно до облікового запису. *Для цього:*
    1. Уведіть логін і пароль.
    2. На сторінці Двохетапна перевірка введіть код, що надійде на телефон, або виконайте Більше варіантів ⇒ Ввести один з восьмицифрових резервних кодів і введіть один з кодів, що містяться у збереженому файлі. Виберіть кнопку *Далі*.
13. Ознайомтеся з порадами *для* безпеки в Інтернеті від сервісу Google. *Для цього:*
    1. Виконайте *Додатки Google* ⇒ Мій обліковий запис ⇒ Вхід і безпека ⇒ Вхід в обліковий запис Google.
    2. Виберіть у нижній частині сторінки Вхід і безпека гіперпосилання. Ваша безпека понад усе в усіх наших починаннях.
    3. Ознайомтеся на сторінці Конфіденційність з порадами в рубриці Найкращі поради *для* безпеки в Інтернеті.
15. Закрийте вікно браузера.

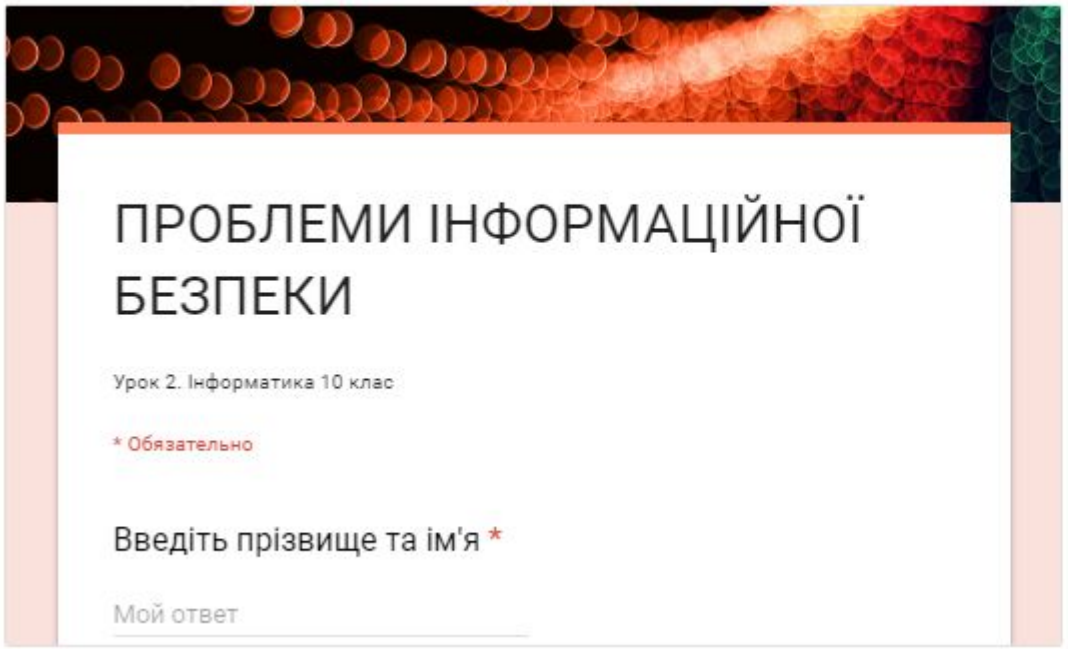
Самозанурення

Повторення вивченого на уроці.

Завдання:

Опрацюйте опорний конспект з теми уроку

Виконання тестових завдань



Виконати тестові завдання

Перейти до тесту

Тренувальні вправи

1. Ознайомтеся з повним текстом порад для безпеки в мережі Інтернет від команди CERT-UA (cert.gov.ua/?p=848) та порівняйте їх з правилами інтернет-безпеки від Профспілки працівників освіти і науки України (pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html). Зверніть увагу, які рекомендації збігаються. З якими загрозами вони пов’язані?

2. Знайдіть на сервісі YouTube в ідео з теми Основи інформаційної безпеки. Перегляньте відео. Запишіть у зошит рекомендації з інформаційної безпеки, які раніше ви не знали.

3. Знайдіть в Інтернеті Абетку інформаційної безпеки від A до Z. Ознайомтеся з термінами з питань інформаційної безпеки. Запропонуйте свої терміни для доповнення абетки.

Завдання додому

1. Опрацювати матеріал теми в електронному посібнику, або підручник з інформатики п.1.2.

2. При потребі виконайте тест повторно

3. Практичне завдання:

Зареєструйтеся на курс Основи інформаційної безпеки від антивірусної лабораторії Zillya! Антивірус (zillya.ua/prometheus). Ознайомтеся з матеріалами курсу.

Дізнайтеся про можливість налаштування двохетапної перевірки облікового запису в соціальних мережах. Налаштуйте двохетапну перевірку для вашого облікового запису в одній із соціальних мереж.