Тема 7. Основи інформаційної безпеки

Вступ

Інтернет — це феноменальний за своїми можливостями засіб. Зараз мова піде про небезпеки пов'язані з його використанням. Інтернет охоплює майже весь світ, а отже ця мережа доступна і для тих людей, які мають далеко не найкращі наміри, тому захист від зловмисників став одною з основних проблем користувачів Інтернету.

Хакери

Багато хто знає, що хакер – це злочинець, який зламує чужі комп’ютери, в основному за допомогою Інтернету, краде паролі, секретну і особисту інформацію, наживається на цьому. Але чи так це насправді?

Зараз є багато різних видів хакерів. Є хакери, що вламуються в систему з метою розширення свого професійного кругозору; інші – заради забави, не спричиняючи відчутної шкоди електронним мережам і комп'ютерам.

Хáкер — особливий тип комп'ютерних спеціалістів, які без дозволу проникають до чужої комп'ютерної системи з наміром викрасти або зруйнувати дані.

Відомі хакери

Роберт Морріс — автор хробака Морріса

Адріан Ламо — відомий зламом Yahoo

Джонатан Джеймс — американський хакер, став першим неповнолітнім, засудженим за хакерство

Джон Дрейпер — один з перших хакерів в історії комп'ютерного світу

Кевін Поулсен — зламав базу даних ФБР і отримав доступ до засекреченої інформації

Загрози під час роботи в Інтернеті

Серед основних загроз використання комп'ютерних мереж для користувачів, виділяють:

1. Комунікаційні ризики
2. Контенті ризики
3. Споживчі ризики
4. Технічні ризики

Комунікаційні ризики

- ризики, що пов’язані зі спілкуванням у мережі та використанням онлайн-ігор:

БУЛІНГ - залякування, приниження, цькування, переслідування, компрометація людей з використанням особистих або підробних матеріалів, розміщених в Інтернеті, надсилання повідомлень з використанням різних сервісів;

КОМПРОМЕТУВАТИ - виставляти в негарному вигляді, шкодити добрій славі;

КІБЕР – ГРУМІНГ - входження в довіру людини для використання її в сексуальних цілях;

ОНЛАЙН – ІГРИ - надмірне захоплення може призвести до втрати реальності, нерозуміння та несприйняття норм і правил людського співіснування, комп’ютерної залежності.

Контенті ризики

- ризики, що пов'язані з доступом до матеріалів, розміщених у мережі, матеріалів шкідливого характеру або таких, що не відповідають віковим особливостям розвитку дитячої психіки.

Такі матеріали як правило містять:

- сцени насилля, жорсткої поведінки з людьми та тваринами;
- пропаганду расової або національної ненависті;
- рекламу або пропаганду використання тютюну, алкоголю та наркотиків, азартних ігор;
- пропаганду релігійних вірувань, заборонених законодавством, або спільнот, що не мають офіційних дозволів на свою діяльність;
- пропаганду шкідливих лікарських засобів і методів боротьби з хворобами, відмови від лікування;
- нецензурну лексику;
- матеріали для дорослих.

Споживчі ризики

- ризики, що пов’язані з порушенням прав споживачів:

- реклама та продаж через мережу інтернет-магазинів низькоякісної продукції;
- купівля підроблених товарів відомих виробників;
- втрата коштів через невиконання обіцянок надіслати товар, невідповідність товару за якістю або за виробником (шахрайство);
- викрадання персональних даних для зняття коштів без відома користувача з його рахунків.

Технічні ризики

- ризики, що пов’язані з роботою шкідливих програм:

- Віруси
- Хробаки (черв’яки)
- Трояни
- Скрипт-віруси
- Дропери
- Боти
- Руткіти
- Експлойти
- Бекдори
- Шпигунські програми
- Рекламні модулі або Adware

Загрозу також становить **фішинг** та **спам** як різновид інтернет-шахрайства.

Підміна адреси

Хакер підмінює адреси сайтів у такий спосіб, що коли користувач зводить у браузері адресу якогось сайту, його спрямовують до зовсім іншого сайту.

Іноді на такому альтернативному сайті міститься негативна інформація про власника того сайту, який збирався відвідати користувач.

Перевантаження сайту або мережі

Генеруючи багато запитів довільного змісту до сайту або мережі, хакер збільшує їхнє робоче навантаження внаслідок чого цей сайт або мережа не можуть нормально функціонувати.

Троянські коні

Троянські коні - це шкідливі програми, які розповсюджуються шляхом обману.

Троянські коні відкривають хакерам доступ до системи, можуть спричинити руйнування інших та виконання інших програм.

Віруси та хробаки

Існують програми, що мандрують Інтернетом та, потрапивши на комп'ютер чи до локальної мережі, завдають тієї чи іншої шкоди. Особливо небезпечними є два види таких програм — віруси та хробаки.

Що таке мережевий черв'як?

– це програма зі шкідливим кодом, яка атакує комп'ютери в мережі та поширюється через неї. Активний мережевий черв'як може знижувати продуктивність пристрою жертви, видаляти файли або навіть вимикати певні програми.

Якщо на комп'ютері було виявлено загрозу такого типу, інфіковані файли рекомендується негайно видалити, оскільки вони можуть містити шкідливий код.

Віруси

Комп'ютерний вірус - це спеціально створена програма для виконання несанкціонованих дій на комп'ютері.

Найбільш масштабною загрозою вважається, комп’ютерний вірус «Меліса», розроблений у 1999 році американцем Девідом Л. Смітом. Протягом декількох годин загроза інфікувала десятки тисяч комп’ютерів у всьому світі, в тому числі і пристрої державних установ. Варто зазначити, що загроза поширювалася електронною поштою із вкладеним документом Word, після чого інфікований лист автоматично надсилався ще на 50 адрес жертви.

За даними дослідників, шкідлива програма «Меліса» завдала збитків у розмірі 80 мільйонів доларів США.

Хробаки

Хробак комп'ютерний - це само розповсюджувана програма, яка може подолати всі три етапи розповсюдження самостійно(звичайний хробак), або використовує агента-користувача тільки на 2-му етапі (поштовий черв'як).

Хробак – це програма, яка дуже схожа на вірус. Він здатний до самовідтворення і може призвести до негативних наслідків для системи. Головною особливістю комп’ютерного хробака є те, що він поширюється не тільки по всьому комп’ютеру, але й автоматично розсилає свої копії електронною поштою.

Спам

Спам - це небажані повідомлення у будь-якій формі, які надсилаються у великій кількості. Найчастіше спам надсилається у формі комерційних електронних листів, надісланих на велику кількість адрес, а також через миттєві та текстові повідомлення (SMS), соціальні медіа або навіть голосову пошту.

Боротися зі спамом дуже складно навіть корпорації, яка щорічно витрачає мільйони доларів на антивірусне програмне забезпечення

Шляхи захисту даних

Серед заходів безпеки, яких повинен дотримуватися кожен користувач, перше місце займає його особиста організованість і відповідальне ставлення до зберігання важливих даних.

Розрізняють три шляхи захисту даних

- Захист доступу до комп'ютера
- Захист даних на дисках
- Захист даних в Інтернеті

Захист доступу до комп'ютера

Для запобігання несанкціонованому доступу до даних, що зберігаються на комп'ютері, використовують **облікові записи**.

Пуск - Панель управління – Облікові записи користувачів – Керування іншим обліковим записом – Створення облікового запису

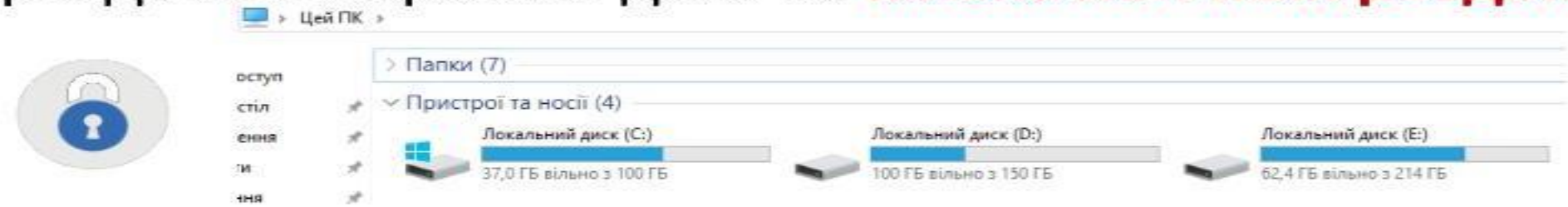
При щоденній роботі за комп'ютером використовуйте обліковий запис Windows без прав адміністратора.

Це простий, безкоштовний і доступний кожному спосіб захисту від більшості шкідливих програм.

Захистити конфіденційну інформацію можна також шляхом архівування та встановлення пароля на архів. Такий спосіб захисту доцільно використовувати й під час листування.

Захист даних на дисках

Для зберігання даних та їх захисту від пошкодження варто розділити жорсткий диск на **кілька логічних розділів**.



На кожний диск, папку та файли локального комп'ютера, а також комп'ютера, підключеного до локальної мережі, встановлюються певні **права доступу** **(повний, тільки читання, доступ за паролем)**.

Встановіть антивірус одразу після встановлення операційної системи і постійно його оновлюйте.

Користуйтеся ліцензійними або з вільною ліцензією програмним забезпеченням, вчасно їх оновлюйте.

Безпечне видалення даних

Пам’ятайте, що у разі випадкового видалення інформації є можливість її відновити.

Для видалення файлів і папок із можливістю їх відновлення використовують, як вам відомо, папку **Кошик**.

Не копіюйте нову інформацію на жорсткий диск. Вимкніть комп’ютер, зверніться у сервісний центр.

Зберігайте робочі файли не на системному диску.

Для повного стирання даних доцільно використовувати спеціальні програми, наприклад, Eraser, CCleaner, які на місце видалених даних записують нові.

Захист даних в Інтернеті

Безпечний Інтернет

Для забезпечення інформаційної безпеки в Інтернеті недостатньо захистити дані на комп'ютері-клієнті або комп'ютері-сервері. Зловмисник може перехопити дані під час обміну ними через канали зв'язку. Захист даних забезпечується спеціальним криптографічним протоколом шифрування даних під час їхнього передавання.

Захищений сайт - це сайт, який використовує для обміну даними протоколи захищеного зв'язку.

Щоб визначити, що сайти захищені, слід звернути увагу на їхню URL-адресу - вона починається з https://. Це - протокол зашифрованого підключення, що забезпечує більш ефективний захист даних. У деяких браузерах поруч із назвою протоколу відображається значок замка — це означає, що з'єднання захищене й більш безпечне.

Захист даних в Інтернеті

Для захисту даних під час роботи в Інтернеті доцільно також використовувати підключення, захищене шифруванням.

Наприклад, за замовчуванням Google шифрує з'єднання з Gmail, а також при виборі інших сервісів Google, наприклад Google Диск, активується **протокол шифрування SSL**, який використовується до завершення сеансу роботи.

ВАЖЛИВА ІНФОРМАЦІЯ

Пам'ятай:

спілкування в Інтернеті не є твоїм обов'язком, тому якщо тобі це більше не подобається або тебе лякають твої Інтернет-друзі, то лише вимкни комп'ютер і не повертайся більше до спілкування онлайн!

Увага! Неможна розкривати і ділитися в соціальних мережах (та і загалом, зустрічаючи незнайомців) особистими даними:

- місцем прогулянок;
- номером телефону;
- часом коли вдома відсутні батьки;
- адресою;
- номерами банківських карток;
- повним ім'ям та іменами членів своєї родини

Брандмауери

Для запобігання інтернет-загрозам між комп'ютером і мережею встановлюють перешкоди - між мережеві екрани (нім. Brandmauer, англ. Firewall - вогнестійка стіна»).

Брандмауери захищають комп'ютер від зловмисного проникнення або потрапляння шкідливих програм. Але не запобігають витоку конфіденційної інформації користувача та завантаженню вірусів.

ОС Windows має вбудований персональний брандмауер.

Брандмауер - це технічний пристрій (маршрутизатор, роутер тощо) або програмний засіб для контролю даних, що надходять до комп'ютера через мережу.

Щоб увімкнути і налаштувати його, слід виконати команди:

Пуск → Панель керування → брандмауер Windows.

Засоби браузера, призначені для гарантування безпеки

Браузери Mozilla Firefox, Safari, Opera, Google Chrome мають багато вбудованих засобів захисту.

Одним із найпопулярніших браузерів для комп'ютерів, телефонів і планшетів є Google Chrome, який:

- попереджає про відкриття сайту із загрозою фішингу або шкідливих програм;
- ізольовано відкриває веб-сторінки, що в разі загрози приводить до закриття лише однієї шкідливої веб-сторінки;
- дозволяє вимкнути збереження конфіденційних даних;
- надає можливість налаштувати показ спливних вікон.

Корисні поради:

Для уникнення ризиків, пов'язаних з роботою в Інтернеті, варто дотримуватися таких порад:

Не наддавайте незнайомим людям та не надсилайте через відкриті мережі персональні дані, дані про паролі доступу до поштових скриньок, акаунтів у соціальних мережах;

Нікому і ніколи не повідомляйте особисту фінансову інформацію.

Суворо конфіденційні дані:

- **Термін дії картки**
- **CVV-2 код**
- **PIN-код**

Для переказу коштів достатньо:

- **Імені власника картки**
- **Номеру картки**

Корисні поради:

Уважно поводьтеся з паролями

Для створення паролів використовуйте:

- **Складне слово чи вислів**
- **Великі і маленькі літери**
- **цифри**

Змінюйте паролі:

- **Для нових акаунтів**
- **Періодично (раз на 3-6 міс.)**
- **У разі підозрілих ситуацій**

Прив’яжіть номер мобільного телефону до важливих акаунтів (двохфакторна авторизація)

Не відкривайте вкладень до листів від незнайомих осіб.

Уважно ставтесь до посилань в повідомленнях у соц. мережах та інших месенджерах

Корисні поради:

Не надсилайте СМС-повідомлення для отримання будь-яких послуг в Інтернеті

Використовуйте **окрему картку** для інтернет оплати

Користуйтеся лише знайомими банкоматами, огляньте банкомат перед використанням

Уважність – практично єдиний спосіб захисту від скімінгу.

Корисні поради:

Всі вищезгадані поради стосуються і мобільних пристроїв (смартфонів, планшетів).

Встановлюйте мобільні додатки лише з офіційних магазинів

Google Play

App Store

Windows phone

Періодично перевіряйте ваші мобільні пристрої на предмет незнайомих додатків на головному екрані та в меню

При встановленні та оновленні додатків уважно стежте за тим, які **дозволи вони вимагають**

ВИСНОВОК

Нові віруси та інші методи вторгнення до вашої комп’ютерної системи виникають майже щодня. Тому регулярно перевіряйте наявність оновлень на сайті своєї антивірусної програми. Повідомлення про нові віруси та інші небезпеки з’являються в Інтернеті постійно.