

Захист даних. Шкідливі програми та їх типи, боротьба з ними



Захист даних



об'єкту інформаційної системи
Захист від умисного пошкодження ПК та

Створення системи охорони



працівниками
Захист від викрадення даних власними

Уведення різних рівнів доступу до даних



Захист від викрадення, створення чи пошкодження
даних з використанням ПК

Антишпигунські та антивірусні програми, шифрування
даних

Види шкідливих програм (за рівнем небезпечності дії)



[Empty box for description of safe malware]

[Empty box for description of unsafe malware]

[Empty box for description of very unsafe malware]

Категорія шкідливих програм

За принципом розповсюдження та функціонування шкідливі програми поділяються на:

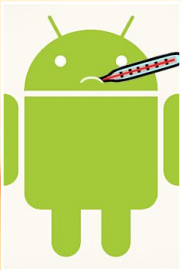


Комп'ютерні віруси

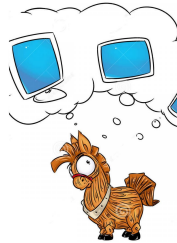
- дискові
- файлові



Хробаки (черв'яки) комп'ютерних мереж



Рекламні модулі, або ADWARE

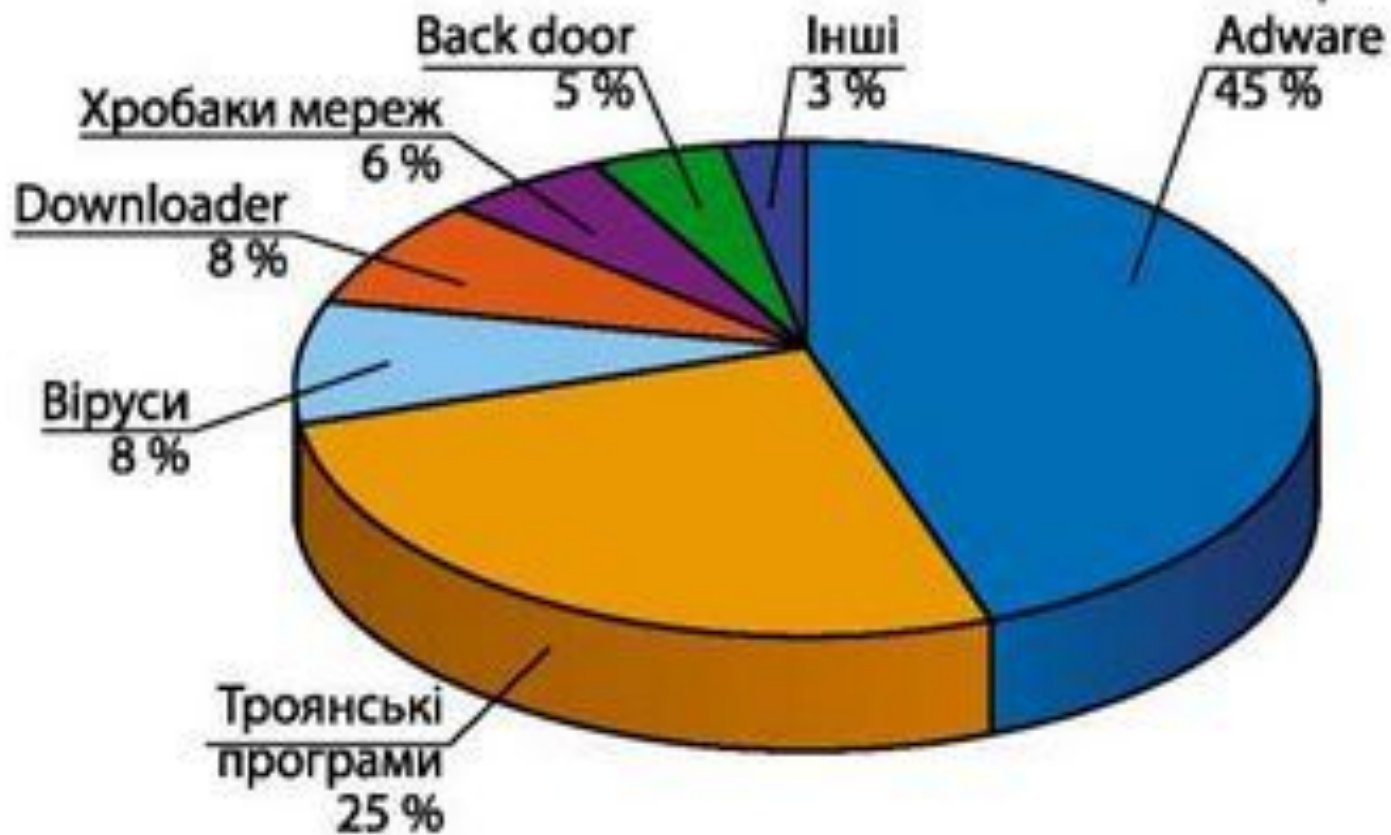


Троянські програми



Руткіти, експлойти, бекдори, завантажувачі

Діаграма розповсюдження шкідливих програм



Шкідливі програми

- **Рекламне програмне забезпечення, Adware** — [програмне забезпечення](#), яке в процесі свого використання показує користувачеві [рекламу](#). Розробник додає покази реклами у ПЗ для отримання відрахувань від рекламодавця.
- **Руткіт** — [програма](#) або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі. Це такий спеціальний модуль ядра, який зламувач встановлює на зламаний ним комп'ютерній системі відразу після отримання прав [с](#)



Троянські програми, трояни, троянці

Різновид шкідницького ПЗ, яке не здатне поширюватися самостійно, тому розповсюджується людьми.

Шкідливі дії: заважати роботі користувача, шпигувати за користувачем, використовувати ресурси комп'ютера для якої-небудь незаконної діяльності.

Клас загроз, які намагаються видати себе за корисні програми й таким чином змушують користувача запустити їх.



Комп'ютерні віруси



- **Завантажувальні (дискові) віруси** - комп'ютерний вірус, що записується в завантажувальний сектор диска чи флеш-накопичувача й активізується при завантаженні комп'ютера.
- **Файлові віруси** — тип комп'ютерних вірусів, що розмножуються використовуючи файлову систему шляхом запису свого коду в код виконуваного файлу конкретної операційної системи.
- **Хробак комп'ютерний** — це програма, яка може подолати всі три етапи розповсюдження самостійно (звичайний хробак), або використовує агента-користувача тільки на 2-му етапі (поштовий черв'як). Хробаки майже завжди шкодять мережі

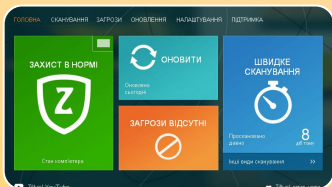
Засоби боротьби з шкідливими програмами



Антивірусні програми - спеціальне ПЗ, що використовують для захист даних



Антивірусні бази – сукупність даних про відомі на даний момент часу шкідливі програми



Сучасні антивірусні програми це комплекс програм, що мають набір модулів для захисту від різних загроз



Приклади антивірусних програм: AVAST, Avira, NOD32, Panda, Zillya!

Модулі, що можуть входити до складу антивірусної програми

Файловий монітор

- Перевіряє файли і диски, відомості про які потрапляють в ОП

Поштовий фільтр

- Перевіряє пошту користувача на наявність шкідливих програм

Антифішинг

- Блокує сайти призначені для викрадення персональних даних

Антиспам

- Блокує проникнення рекламних повідомлень

Батьківський контроль

- Надає батькам можливість слідкувати за роботою дитини в мережі

Поведінковий аналізатор

- Аналізує стан системи та порівнює їх із станом що був на початку роботи ПК

Профілактика ураження шкідливими програмами

Установіть

антивірусну програму

Регулярно здійснюйте

перевірку ПК на віруси

Постійно оновлюйте

антивірусні бази

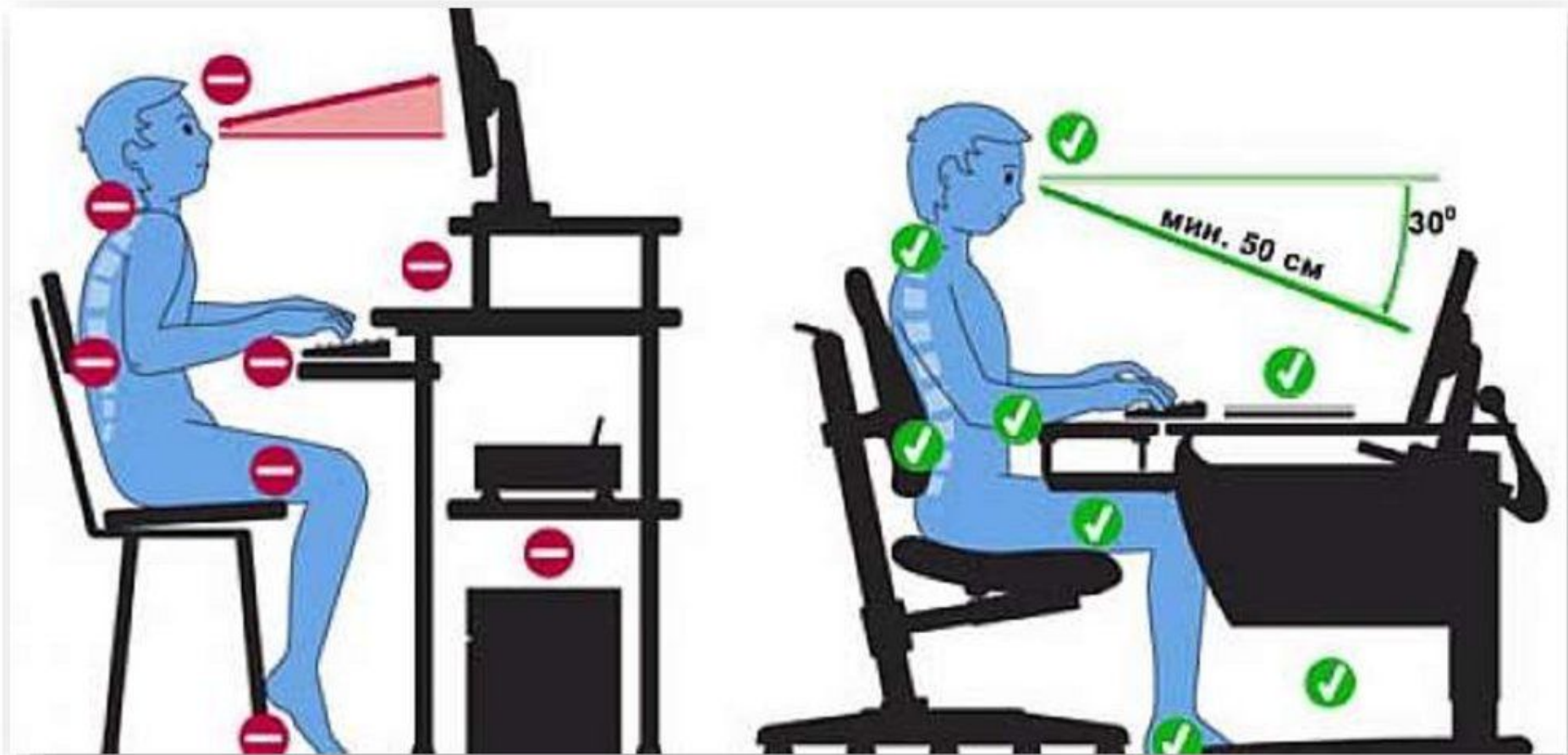
Проводьте резервне

копіювання цінних файлів

Не відкривайте

листи від невідомих
адресатів

Працюємо за ПК



Виконання практичного завдання

Охарактеризуйте одну з антивірусних програм за такими вимогами:

- країна «виробник»;
- коли була створена перша версія;
- чи потребує «ліцензії»;
- характерні особливості програми.



