



# ТЕМА: Безпека роботи з інформацією.

# Чим регулюються відносини в інформаційній сфері?

Конституція, Закони, нормативні акти



# Чим регулюються відносини в інформаційній сфері?

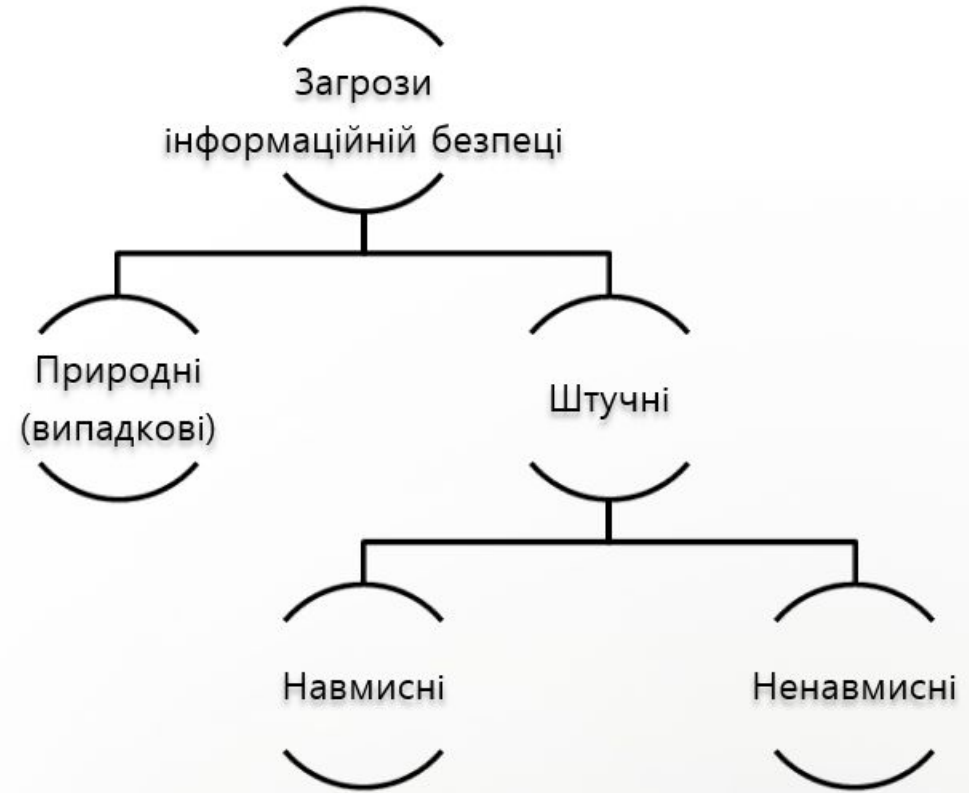
Звернути  
увагу

Доручення МВС України від 19.03.2015 № 13155/Ав «Про заходи із протидії витоку службової інформації»

Доручення МВС України від 24.04.2015 № 19130/Ав «Про недопущення витоку інформації, що утворюється в службовій діяльності»

Наказ Національної поліції України від 07.12.2015 № 176 «Про запобігання негативним наслідкам використання інтернет-ресурсів російських провайдерів»

# Класифікація методів впливу на інформацію



# Класифікація методів впливу на інформацію (ПРИРОДНІ)



Природні  
(випадкові)

Природні:

стихійні лиха

пожежи

повіні

техногенні катастрофи

**інші явища, що не залежать від людини**



# Класифікація методів впливу на інформацію (ПРИРОДНІ)



Природні  
(випадкові)

**Інші явища, що не залежать від людини:**

збої та відмови технічних засобів

алгоритмічні та програмні помилки

вихід з ладу пристроїв для збереження інформації під впливом зовнішніх факторів



# Класифікація методів впливу на інформацію (ШТУЧНІ)

## Навмисні



- Кража (копіювання) документів
- Несанкціонований доступ до інформації
- Перехоплення інформації
- Підробка інформації
- Хакерськ атака

## Ненавмисні



- Помилки користувачів
- Необережність користувача
- Неуважність користувача



# Класифікація методів впливу на інформацію (мінімізація загроз)





# Алгоритм захисту при роботі з переносними комп'ютерами та/або з'ємними носіями



# Алгоритм захисту при роботі з переносними комп'ютерами та/або з'ємними носіями



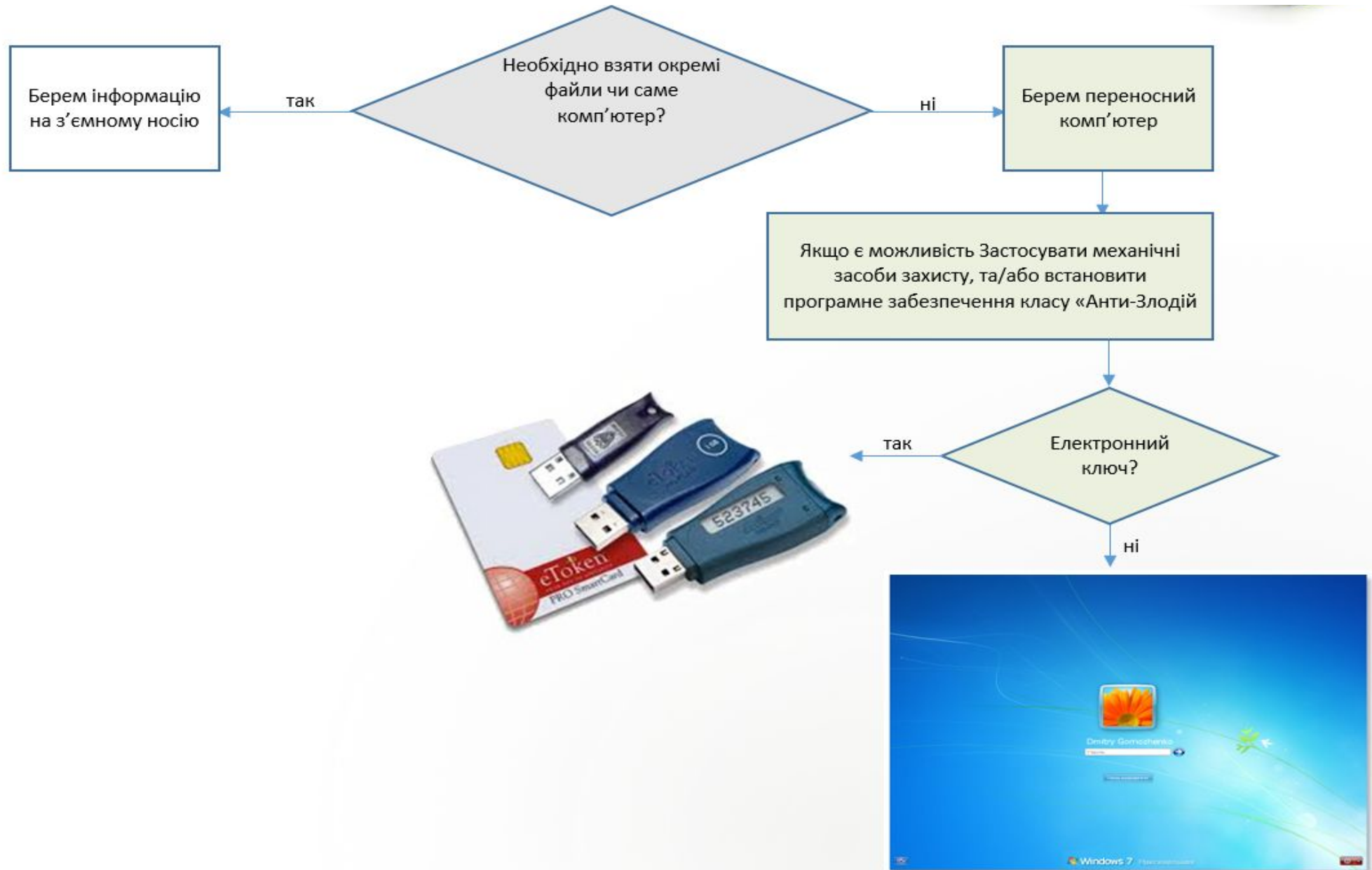
# Алгоритм захисту при роботі з переносними комп'ютерами та/або з'ємними носіями



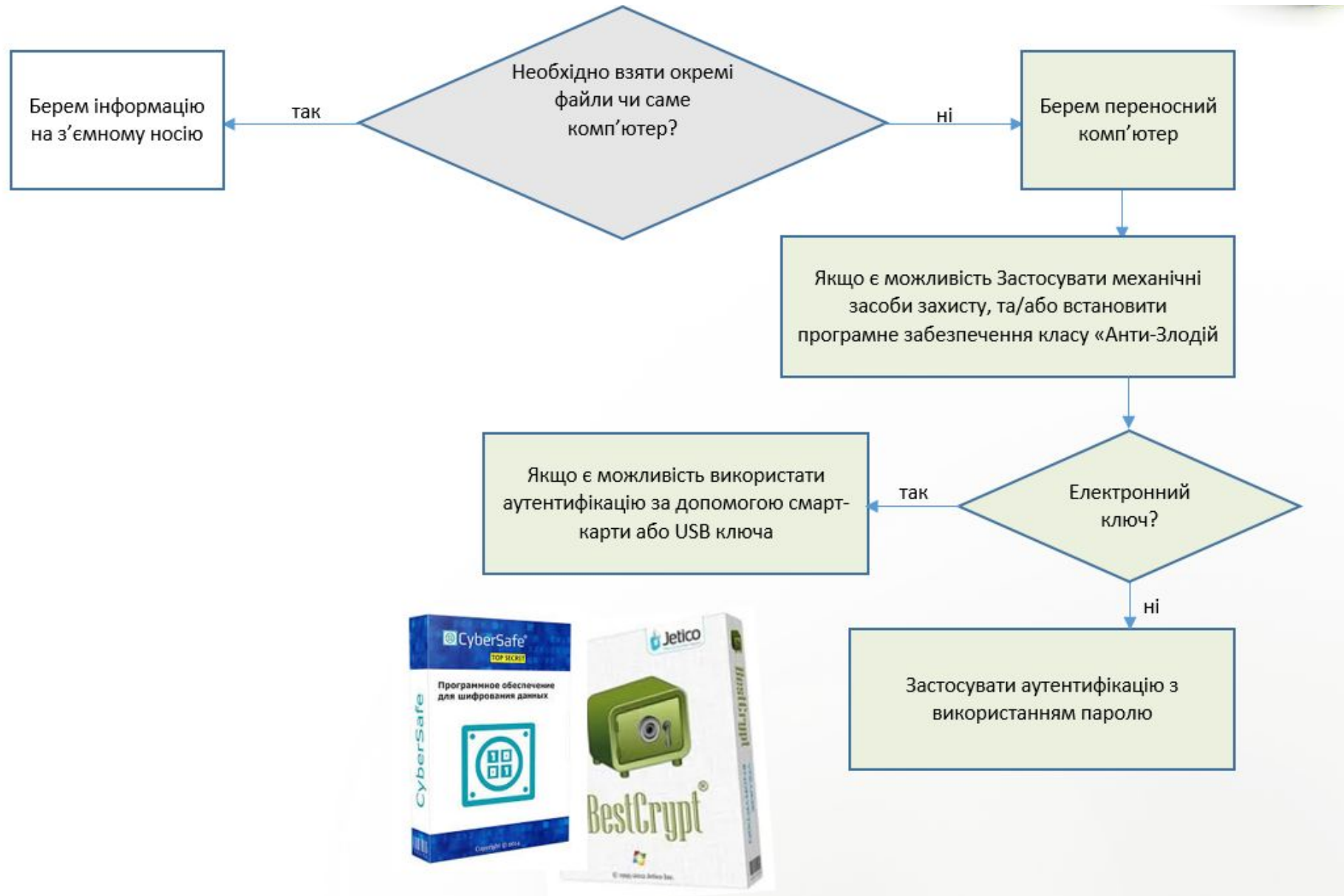
# Алгоритм захисту при роботі з переносними комп'ютерами та/або з'ємними носіями



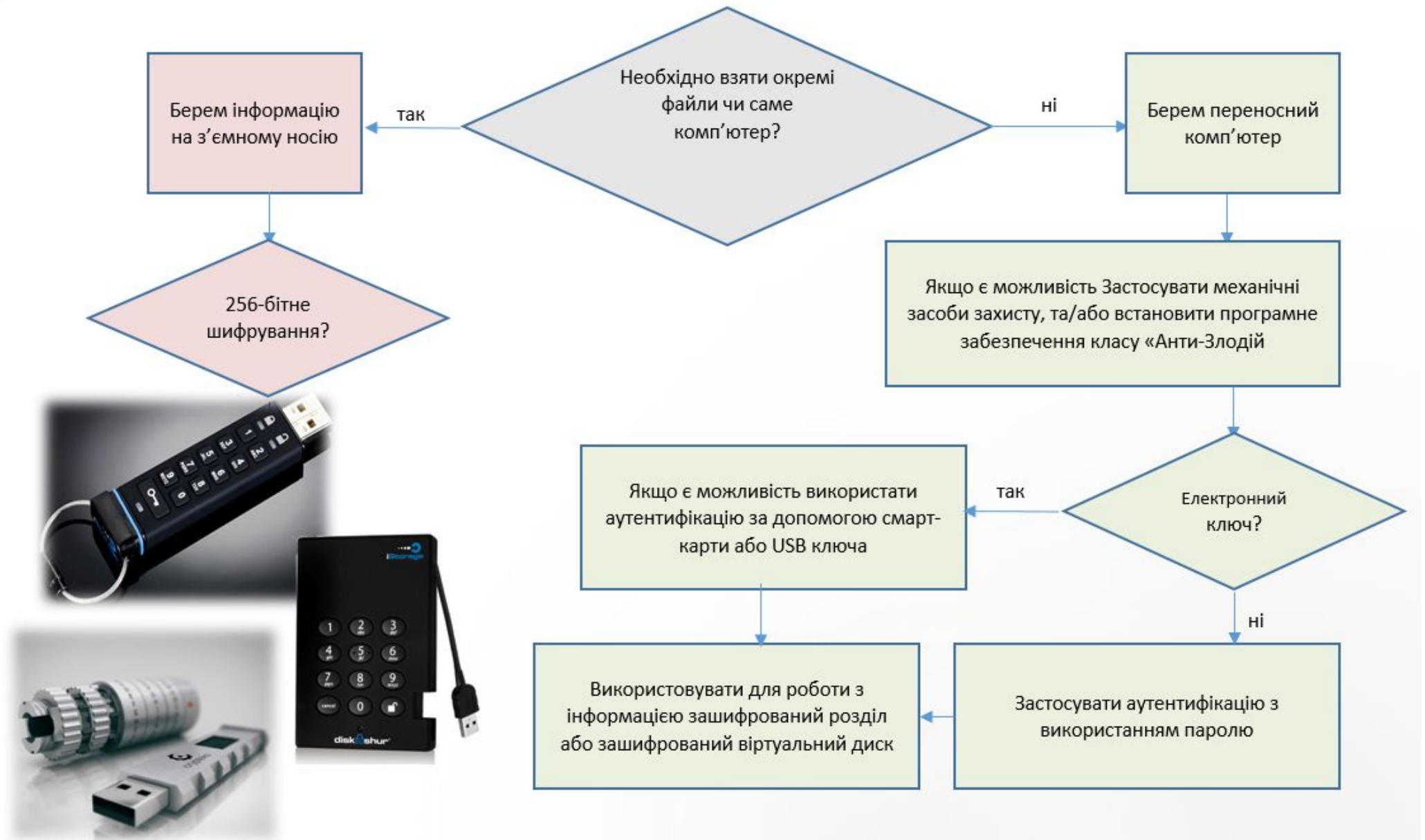
# Алгоритм захисту при роботі з переносними комп'ютерами та/або з'ємними носіями



# Алгоритм захисту при роботі з переносними комп'ютерами та/або з'ємними носіями



# Алгоритм захисту при роботі з переносними комп'ютерами та/або з'ємними носіями



# Захист при повсякденній роботі. Комп'ютер залишаємо на короткий термін.





# Захист при повсякденній роботі. Комп'ютер залишаємо на довго.

---

Відключити у BIOSі комп'ютера можливість завантаження з зовнішніх пристроїв

Встановити пароль на вхід до BIOSа комп'ютера.

Використати шифрування

# Мінімізація вірусної небезпеки.



Використовувати в роботі операційну систему Linux, або дотримуватися наступних правил для комп'ютерів сімейства Windows:



На комп'ютері повинен бути встановлений антивірусний пакт

- Встановити його необхідно до процедури підключення до мережі Інтернет
- Багато встановити антивірус до підключення до локальної мережі
- Антивірусний пакет повинен включати в себе програму-монітор



Антивірусний пакет треба використовувати

- Проведення періодичної перевірки всієї системи
- Перевірка носіїв що підключаються до комп'ютера
- Перевірка файлів отриманих з зовнішніх джерел



Дотримання безпеки при роботі в мережі Інтернет

- Використання нових версій інтернет браузерів
- Встановлення драйверів для пристроїв лише з офіційних джерел
- Обережне ставлення до контенту у мережі Інтернет



Дотримання безпеки при роботі з електронною поштою

- Не відкривати пошту від незнайомих адресатів та "відповіді" від адресатів яким не писали
- Не відкривати листів рекламного характеру або з незрозумілим заголовком
- Не відкривати вкладення від сторонніх адресатів, особливо якщо вказується, що всі пояснення та інструкції саме в файлі-додатку. Інші вкладення перед відкриттям перевіряти антивірусом



Дотримання безпеки при роботі з офісними програмами

- Запуск макросів у офісних програмах здійснювати лише у разі необхідності, а не за замовченням
- Відкривати файли офісних програм, що отримано зовні лише після перевірки антивірусною програмою

# Соціальні мережи як джерело небезпеки.

