**НПУ імені М.П.Драгоманова**

**Факультет інформатики**

***Кафедра комп’ютерної інженерії***

**ЛАБОРАТОРНА РОБОТА № 5**

з курсу

***«Безпека програм та даних»***

**ТЕМА: Захист даних від шкідливих програм.**

**Студент : Трембіцький Нікіта**

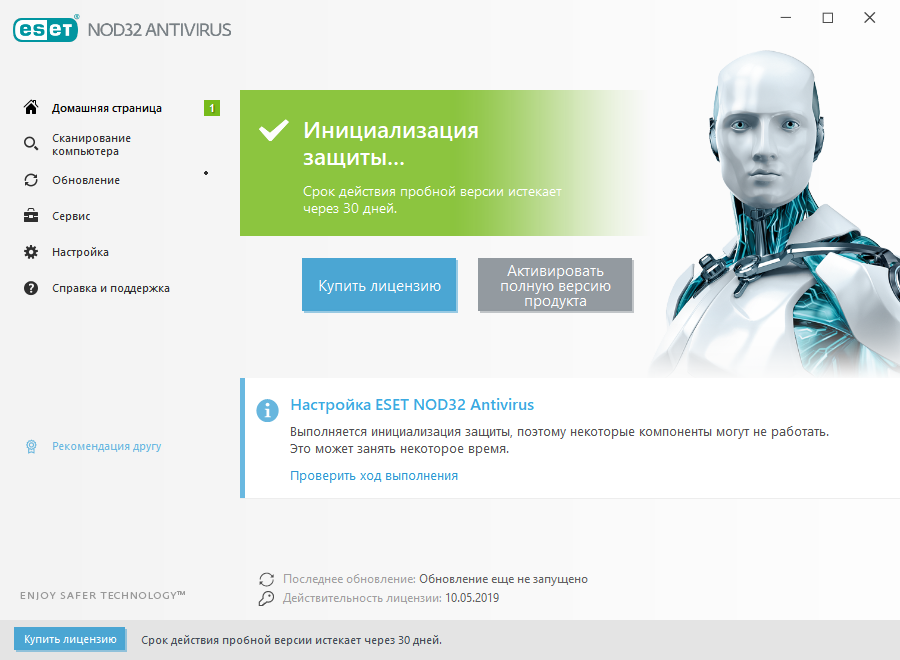
**Група : 31ІПЗ**

**Факультет : Інформатики**

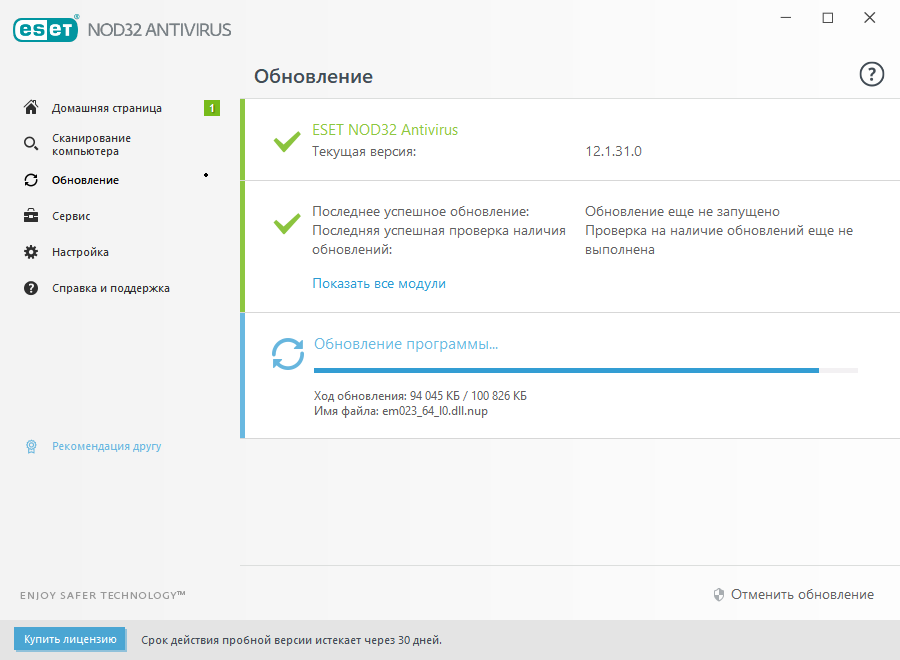
**Викладач : Галицький О.В.**

Київ 2019

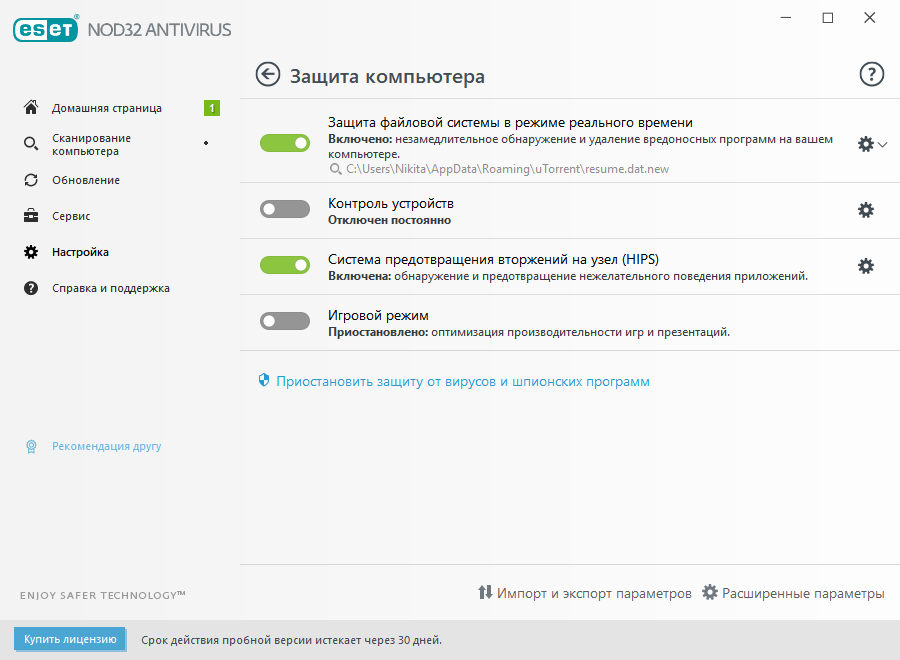
**1.** Завантажити антивірусну програму:



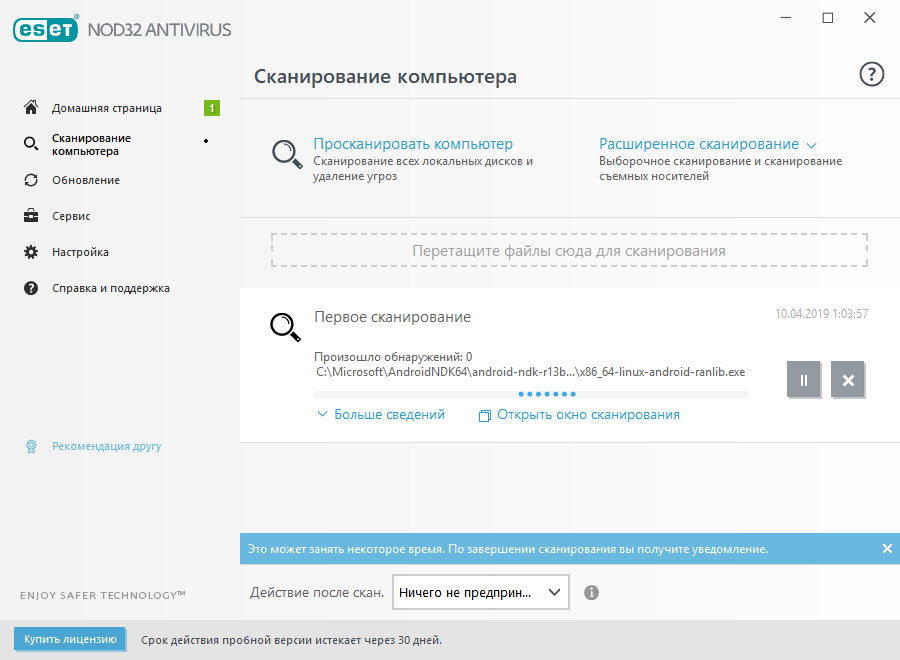
**2.** Оновити антивірусну базу використовуючи глобальну мережу Internet або локальну папку:



**3.** Ознайомитися із засобами налаштування параметрів програми: область перевірки, список об’єктів, порядок дій:



**4.** Перевірити комп’ютер на наявність вірусів. Прокоментувати повідомлення що з’являються на екрані:



**5.** Самостійно ознайомитися з додатковими можливостями антивірусної програми:

**Антивірус та Антишпигун**  
Забезпечує проактивний захист від усіх видів цифрових загроз, включаючи віруси, руткіти, черв’яки та шпигунські програми.

**Антифішинг**  
Перешкоджає відвідуванню підроблених веб-сайтів, які використовують шахраї для виманювання конфіденційної інформації, зокрема імен користувача, паролів чи банківських даних.

**Сканування під час завантаження файлів**   
Зменшує час сканування шляхом перевірки лише певних типів файлів, наприклад, архівів, під час процесу завантаження.

**Розширений сканер пам'яті**   
Забезпечує покращене виявлення стійкого шкідливого програмного забезпечення, яке використовує декілька рівнів шифрування для приховування своєї діяльності.

**Захист атак на основі скриптів**   
Виявляє атаки шкідливих скриптів із використанням Windows PowerShell, а також шкідливих JavaScripts, які можуть здійснювати атаки через браузер. Існує підтримка браузерів Mozilla Firefox, Google Chrome, Microsoft Internet Explorer та Microsoft Edge.

**Захист від програм-вимагачів**   
Знешкоджує шкідливе програмне забезпечення, яке блокує доступ до особистих даних та вимагає викуп за доступ до них.

**Сканер UEFI**  
Захищає від загроз, які атакують комп’ютер на найглибшому рівні, навіть перед запуском Windows – в системах з інтерфейсом UEFI.

**Сканування на основі хмарних технологій**   
Прискорює швидкість сканування за допомогою занесення до «білого» списку безпечних файлів на основі репутаційної бази даних ESET Live Grid® та проактивно виявляє невідомі загрози на основі репутації.

**Захист від експлойтів**  
Потужний захист від шкідливих програм, прихованих від традиційних методів виявлення. Виявляє та запобігає спробам використання уразливостей популярних додатків, таких як веб-браузери, PDF редактори, поштові клієнти, програми MS Office та Java.

**Контроль пристроїв**   
Дозволяє запобігти неавторизованому копіюванню особистих даних на зовнішні пристрої. Надає можливість блокувати змінні носії — компакт-диски, DVD-диски, USB-накопичувачі та дисководи, а також пристрої, які підключаються через Bluetooth, FireWire та послідовні/паралельні порти.

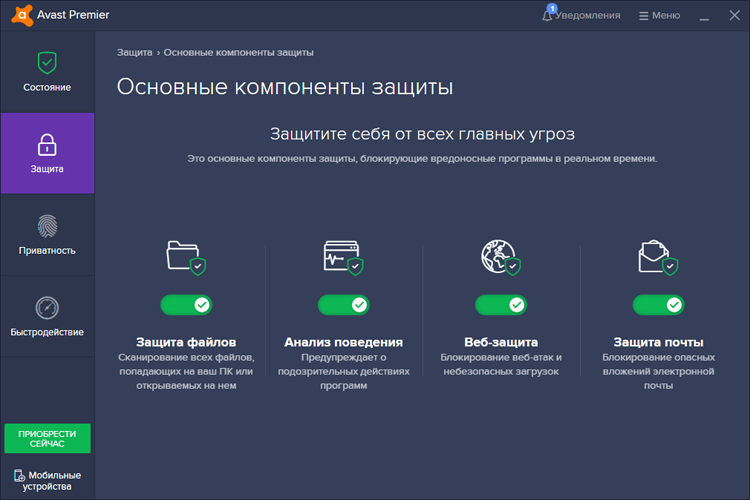
**Сканування у режимі очікування**   
Покращує продуктивність здійснюючи поглиблене сканування, коли комп'ютер не використовується. Допомагає виявити потенційні загрози, перш ніж вони заподіють шкоду.

**Cистема запобігання вторгненням (HIPS)**   
Дозволяє більш точно налаштувати поведінку системи та надає можливість встановити правила для системного реєстру, активних процесів та програм.

**6.** За допомогою пошукової системи глобальної мережі Інтернет знайти та дослідити програмні засоби для виявлення вірусів (антивірусні програми, програми для виявлення і лікування окремих вірусів), які не потрібно встановлювати (інсталювати) на комп’ютер. Описати 3 програмних засоби за наступною схемою:

* + **Назва** - AVAST, **версія** - 12.3.2280, **автори** - AVAST Software.
  + **Ліцензія** (спосіб розповсюдження) – 30 днів/ ліцензія.
  + **Технічні характеристики програмного засобу** та мінімальні вимоги до програмноапаратних засобів - Windows XP—10 (32/64-bit), Linux, Macintosh, Palm OS, Windows Server Edition, Android
  + **Режим роботи** виконання на боці клієнта.
  + **Наявність Інтернет-підтримки** – оновлення.
  + **Мова інтерфейсу** - Багатомовний (45 мовних пакетів).
  + **Особливості управління об’єктами інтерфейсу програми** - управління відбувається за допомогою миші та клавіатури, присутні гарячі клавіши, легкий у використанні.
  + **Позитивні особливості програми**:
  1. Відалення шпігунського програмного забезпечення (англ. Spyware) з комп'ютера.
  2. Можлівість встановлення пароля на зміну настройок програми.
  3. Багатомовній інтерфейс, підтримка 45 мов.
  4. Голосові ПОВІДОМЛЕННЯ при віявленні шкідлівої програми и при успішному оновленні вірусної бази даних. До п'ятої Версії вікорістовувався чоловічий голос. Починаючі з п'ятої - жіночий.
  + Можливі застосування програмного засобу.

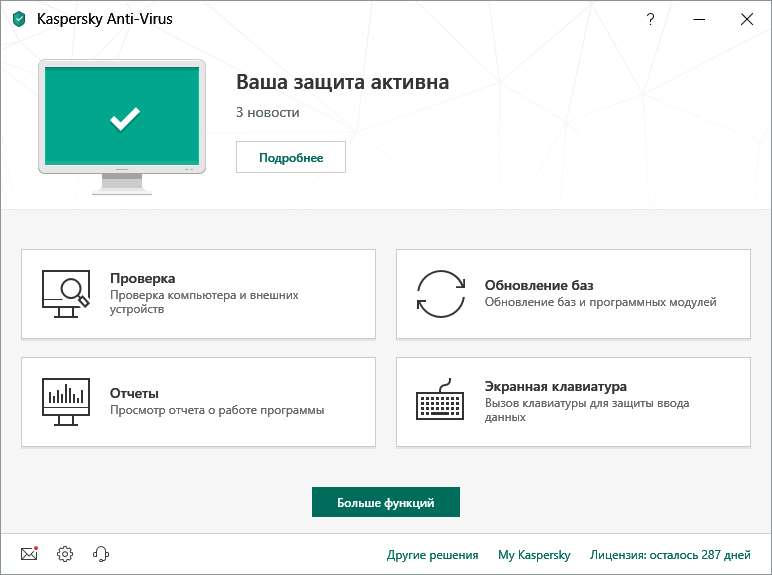
Екран файлової системи — основний компонент сканера в реальному часі. Відстежує всі локальні операцій з файлами та папками на комп'ютері. Екран пошти — відстежує весь трафік програм для роботи з електронною поштою і сканує всі листи до того, як вони потраплять на комп'ютер, таким чином запобігаючи можливій шкоді. Здійснює перевірку трафіку по протоколах POP, SMTP, IMAP і NNTP.



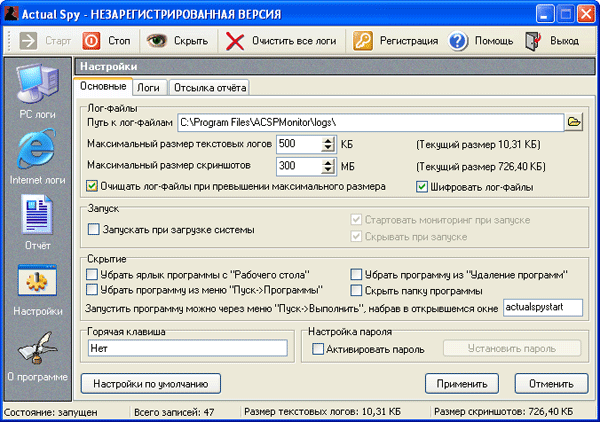
* + **Назва** - Kaspersky Anti-Virus, **версія** - 16.0.0.614, **автори** - Лабораторія Касперського.
  + **Ліцензія** (спосіб розповсюдження) - Власницьке програмне забезпечення.
  + **Технічні характеристики програмного засобу** та мінімальні вимоги до програмноапаратних засобів - Microsoft Windows, Linux.
  + **Режим роботи виконанн**я на базі клієнта.
  + **Наявність Інтернет-підтримки** – оновлення через інтернет.
  + **Мова інтерфейсу** - багатомовна.
  + **Особливості управління об’єктами інтерфейсу програми** - управління відбувається за допомогою миші та клавіатури, присутні гарячі клавіши, легкий у використанні.
  + **Позитивні особливості програми**.

1. Захист від вірусів, троянських програм і черв'яків є
2. Захист від шпигунських та рекламних програм
3. Перевірка файлів в автоматичному режимі і на вимогу
4. Перевірка поштових повідомлень (для будь-яких поштових клієнтів)
5. Перевірка інтернет-трафіку (для будь-яких інтернет-браузерів)
6. Захист інтернет-пейджерів (ICQ, MSN)
7. Проактивний захист від нових шкідливих програм
   * **Можливі застосування програмного засобу.**

Автоматичне налаштування програми в процесі установки. Готові рішення (для типових проблем). Наочне відображення результатів роботи програми



**7.** За допомогою пошукової системи глобальної мережі Інтернет знайти, за можливості продемонструвати та описати (опис в довільній формі) одну шпигунську програму наступного типу:



**Actual Spy**

<http://www.actualspy.ru/>

Статус: share

Мова: rus

Розмір: 1,6 Мб

Програма шпіон - призначена для прихованого спостереження за комп'ютером.

Можливості:

1. Реєструє всі натискання клавіш, розрізняє регістр і російську розкладку. Можна зареєструвати тільки символи і цифри, без запам'ятовування системних клавіш (таких як Ctrl, Shift і т.д.).

2. Робить знімки екрану (скріншоти) через заданий проміжок часу.

3. запам'ятовує запуск і закриття програм.

4. Стежить за вмістом буфера обміну.

5. Вся інформація зберігається в зашифрованому лог-файлі.

6. Зручний інтерфейс перегляду логів, а також перегляд скріншотів.

7. Формує звіт в текстовому і html-форматі.

8. Відсилає звіт на вказаний e-mail.

9. Може працювати в звичайному і прихованому режимі.

10. У прихованому режимі невидима у всіх операційних системах (навіть у процесах Windows NT / 2000 / XP) .

11. Можливість встановити пароль на доступ до Actual Spy, щоб ніхто крім вас не міг переглянути логи.

12. Не визначається антивірусами.

13. Швидка установка, зручний і зрозумілий інтерфейс, широкий набір функцій, гнучка система налаштувань.