Практична робота № 2

Тема: Оцінка ефективності сучасних антивірусних засобів

Теоретичні відомості

Комп'ютерний вірус - це, як правило, дуже невелика програма (модуль) мовою Асемблера, яка написана програмістом високої кваліфікації.

Комп'ютерний вірус - це самовідтворююча програма, яка може ввести свої клони в файл, завантажувальний сектор диска, драйвер пристрою, оперативну пам'ять, прикладні програми тощо. Він пошкоджує дані, зменшуючи об'єм вільного дискового простору, блокує роботу системи, не санкціновано перезавантажує комп'ютер тощо. Щоденно появляються 6-8 нових різновидностей вірусів. Не дивлячись на те, що не раз робилася спроба створення єдиної системи класифікації комп'ютерних вірусів, її до сих пір не існує. Один і той же вірус може мати різні коди і назви.

Вірусу може присвоюватись код, який складається з буквеного префікса, кількісної характеристики і буквеного суфікса. Наприклад, файлові віруси мають суфікси C (від. com) і E (від. exe), завантажувальні - B, D або M, пакетні - J. Префікс характеризує місце розміщення вірусного ядра. Суфікс використовується у випадку, якщо два віруси мають однакові префікси і характеристику. Крім того, віруси можуть характеризуватися місцем першого виявлення чи створення, способом проявлення.

Комп'ютерні віруси класифікуються за признаками:

- місце розміщення програмного ядра вірусної програми;
- спосіб пошкодження обчислювальної системи;
- деструктивні результати;
- спосіб проявлення вірусів.

Основні типи вірусів:

1) файлові віруси - пошкоджують програмні файли (з розширенням com і exe);

2) завантажувальні віруси - переносяться із системи в систему через завантажувальний сектор і пошкоджують тільки BOOT-сектори дискет і жорстких дисків;

3) пакетні віруси - пошкоджують файли з розширенням bat;

4) мережеві віруси - поширюються через локальні або глобальну мережі і пошкоджує її програми;

5) мікровіруси - (становлять 80 процентів усіх існуючих) пошкоджують документи Word і Excel;

6) віруси-невидимки - заражають комп'ютер, залишаються непоміченими системою контролю;

Евристичні алгоритми - це одна з антивірусних технологій, яка полягає у тому, що система шукає не самі віруси, а результати їх дії або сліди.

Вірусні програми можуть маскувати свою присутність за допомогою часової затримки.

Спочатку вірус записується його розробником на одну дискету. Далі при тиражуванні цієї дискети він потрапляє на інші дискети. Цей процес звичайно проходить лавиноподібно.

Модуль вірусу спочатку приєднується до файлу або проникає середину його (частіше до програм). Потрапивши разом з файлом у комп'ютер, вірус починає діяти самостійно. Він може розмножуватись, тобто створювати свої копії, які проникають в інші програми.

Дія вірусу на файли виявляється по різному. Одні типи файлів він тільки псує. Це звичайно файли, які містять текстову інформацію та деякі інші типі даних (таблиці, бази даних тощо) В інші типи файлів він проникає, заражаючи їх. Таки файли називають

зараженими. До них зокрема відносяться файли операційної системи, файли, які виконуються, та деякі інші.

Спочатку дія вірусу ніяк не проявляється. Він поступово руйнує файли і проникає у програми, розміщені на жорсткому диску. Коли вірус проник у багато програм, тоді раптом виявляється, що одна програма зовсім не працює, друга працює неправильно, а третя видає на екран не зрозумілі повідомлення тощо.

Фініш дії вірусу може бути дуже сумним: зіпсована програма, над якою ви працювали не один рік, загублено великий обсяг даних, які збирались десятками людей тощо.

Первинне джерело вірусу вже було названо. Інші джерела такі:

- дискета з якої ви копіюєте заражену програму;
- комп'ютерна мережа, за якою разом з файлами передаються і віруси;
- вінчестер, на який попав вірус у результаті роботи з зараженими програмами;
- вірус, який залишився у внутрішній пам'яті комп'ютера від попереднього користувача;

Як уникнути вірусів? Для цього потрібно дотримуватись таких рекомендацій:

- не користуватись випадковими програмами. Прагніть користуватись тільки ліцензійними програмами, знайте, що найчастіше заражені ігрові комп'ютерні програми;
- завжди майте архівні копії файлів, в абсолютній чистоті яких ви впевнені;
- не передавайте своїх дискет у користування іншим особам;
- якщо до вас хтось працював на комп'ютері обов'язково ввімкніть комп'ютер чи перезавантажте його клавішею Reset (але не клавішами Ctrl+Alt+Del)
- якщо ви розробили свою програму зразу ж створіть її архівну копію;
- закривайте дискету на запис. На жорсткому диску доцільно мати логічні диски захищені від запису;
- не довіряйте стороннім особам комп'ютер з жорстким диском.

Допускаючи їх до роботи не дозволяйте їм користуватись дискетами, які не були перевірені антивірусними програмами.

Але навіть в тому випадку коли виконуються всі ці рекомендації не можна бути абсолютно впевненим, що вірус не проникне у ваш комп'ютер.

Для виявлення та ліквідації вірусу розроблено багато антивірусних програм. Однак ні одна антивірусна програма не може гарантувати 100% виявлення і усунення вірусу. До того ж самі антивірусні програми іноді є самі джерелами вірусу. Один вірус вони можуть знищити, а інший новіший - ввести.

Знайте, що як ліки буває не рятують людину від хвороби, так і антивірус не завжди рятує від комп'ютерного вірусу. Як засоби нападу попереджують засоби захисту, так і віруси попереджують антивірусні програми. Спочатку з'являється конкретний тип вірусу, а вже потім розробляється під неї відповідна антивірусна програма.

Антивірусні програми поділяють на спеціалізовані та універсальні.

Спеціалізовані антивірусні програми здатні знаходити та ліквідувати тільки певні типи уже відомих вірусів. З невідомими вірусами ці програми боротись не можуть.

Щодо надійності виявлення вірусу спеціалізованими програми значно перевищують універсальні.

Універсальні антивіруси, орієнтовані на цілі класи вірусів, в свою чергу поділяються на резидентні та ревізори. Резидентні постійно присутні у пам'яті комп'ютера і періодично здійснюють перевірку на наявність вірусів. Антивіруси - ревізори здатні лише установити чи піддавався файл будь-яким змінам (у тому числі і вірусним) після останнього його використання.

Захист від комп'ютерних вірусів. Основна тактика захисту

від інфікованих програм комп'ютерними вірусами полягає у використанні програмного забезпечення із надійних джерел, у регулярному контролі стану найбільш важливої інформації в комп'ютерній системі. Всі поступаючі в роботу нові документи повинні піддаватись перевірці антивірусними програмами.

Щоб уникнути тяжких наслідків, які викликаються дією вірусних програм, користувач повинен дотримуватись ряд правил:

- завершувати робочий день перевіркою комп'ютера антивірусною програмою;
- найбільш цінна інформація повинна зберігатися в архівах на перемінних носіях;
- при виявленні ознак пошкодженні слід негайно закінчити роботу, перезавантаживши з системної дискети комп'ютер та перевіривши диски антивірусною програмою.

В антивірусній програмі закладенні потужні засоби боротьби з мікровірусами. Програма містить евристичний аналіз, який дозволяє виявити вірусоподібні коди, які можуть належати невідомим, а також іншим складним вірусам. Успіх такого аналізу-82 проценти.

Найпопулярнішими серед користувачів є антивірусні програми Aidtest, Doctor Web, ADinf, MSAV, (входить до складу MS-DOS 6. **), Norton Anti Virus.

Програма Aidtest забезпечує знаходження та знищення із заражених програм певних типів вірусів, відомих на момент модернізації антивірусної програми. В міру появи нових вірусів ця програма постійно удосконалюється. Перелік виявлених вірусів додається до програми.

Працює Aidtest в DOS і запускається з командного рядка.

Приклади запуску: Aidtest- перевіряються всі файли TXT,

COM, SYS на всіх логічних дисках вінчестера. Aidtest a: - перевіряють такі самі

файлі тільки на дискеті установленій у дисководі A. Aidtest d: /Dos/g - перевірка всіх типів файлів (ключ / g) каталогу Dos диску D: Aidtest c: /g/f - перевірка та лікування усіх типів файлів диска c: Програма Aidtest є є спеціалізованою антивірусною програмою.

Програму Doktor Web потрібно віднести до універсальних антивірусних програм. Вона дозволяє знаходити і знищувати відомі та невідомі віруси з пам'яті та з дисків комп'ютера. Невідомі віруси знаходять завдяки наявності спеціального евристичного аналізатора. Програма може працювати у діалоговому режимі, має дуже зручний інтерфейс, який можна настроювати.

Для запуску програми необхідно ввести у командний рядок DOS команду DRWEB. Після натискання клавіші Enter на екрані з'явиться головне вікно. У верхній частині вікна зображується меню: "Dr. Web", "Тест", "Настройки", "Дополнения" і "Помощь".

Призначення меню:

Dr. Web - використовується для отримання інформації про програму, тимчасового виходу в DOS та завершення роботи програми;

Тест - дозволяє запустити програму в режимі перевірки та лікування файлів;

Настройки - використовується для налагодження інтерфейсу програми та зміни режимів її роботи;

"Дополнения" - забезпечує підмикання зовнішніх файлів-без даних, які мають інформацію про нові віруси;

"Помощь" - призначена для отримання довідкової інформації.

Режим пошуку вірусів вмикається вибором команди тестування

в меню Тест, або натискуванням клавіші F5. При цьому на екрані над головним вікном з'являється діалогова панель "Путь для тестирования". У рядку введення цієї панелі потрібно указати диск, каталог (каталоги) або групи файлів, де потрібно шукати віруси.

Тестування починається після натискування кнопки OK діалогової панелі. Для тестування з лікуванням потрібно натиснути Ctrl+F5.

Результати роботи програми у її головному вікні. Програми ADinf і MSAV - це антивірусні програми-ревізори. ADinf є однією з найкращих сучасних програм свого класу, яка за правильного використання виявляє практично всі існуючі віруси. Вона слідкує за цілісністю інформації на жорсткому диску, а також за всіма її змінами. Завдяки цьому, програма дозволяє своєчасно виявити не тільки відомі, але й нові віруси. За такого самого принципу побудована антивірусна програма MSAV.

Хоча антивіруси повністю і не гарантують виявлення вірусів та лікування від них магнітних дисків, потрібно привчити себе систематично користуватися цими програмами. В практичній потрібно використовувати різні антивірусні програми. Методика їх використання може бути різною. Для початківця рекомендуємо перед копіюванням файлів з чужої дискети перш за все перевірити її різними антивірусними програмами.

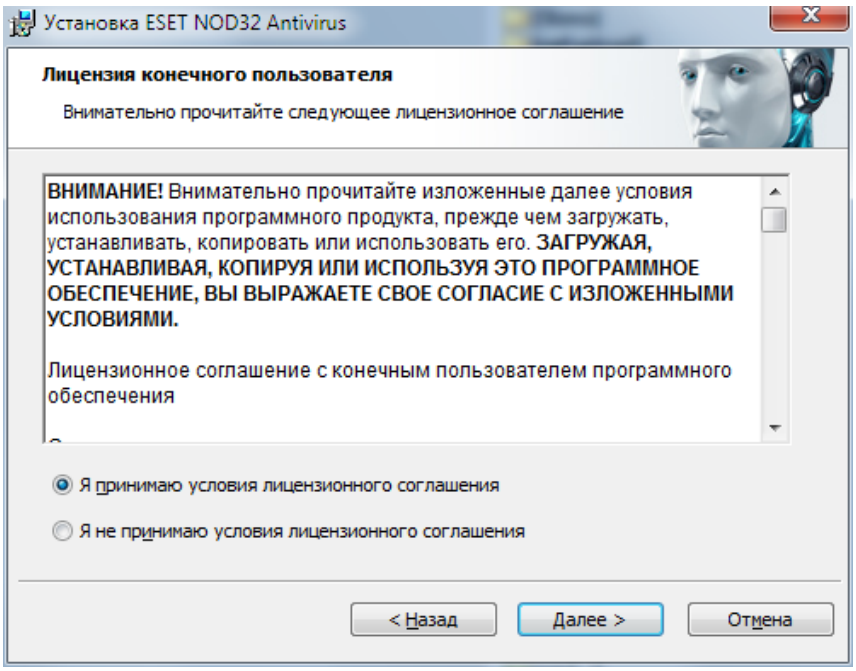
Практичне завдання

Завдання 1

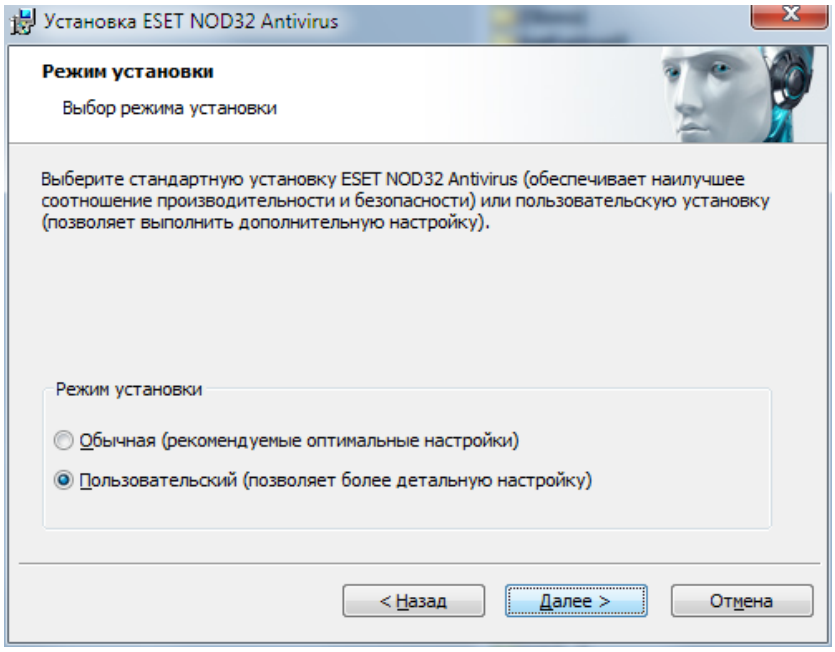
Інсталяція антивірусного засобу

Скачуємо NOD32 з офіційного сайту та запускаємо файл. При відкритті Мастера установок натискаємо Далее:

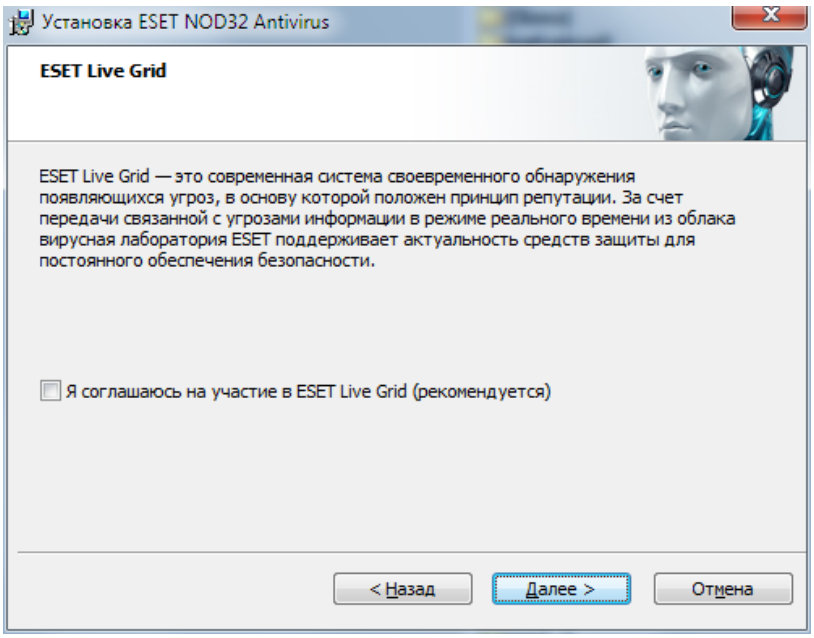
Приймаємо умови ліцензованої згоди:



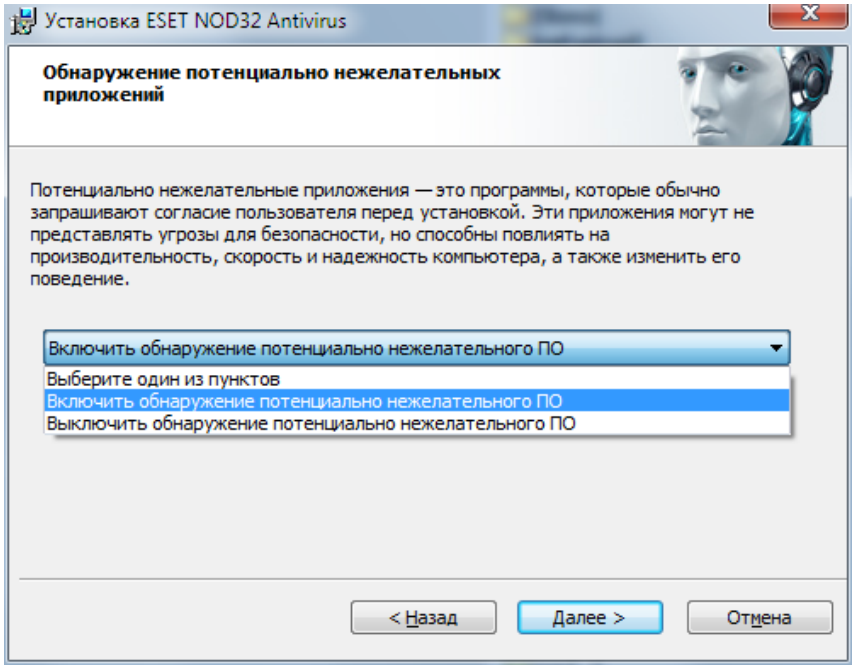
Обираємо режим роботи *Пользовательский,* для того щоб не упустити важливі елементи установки:



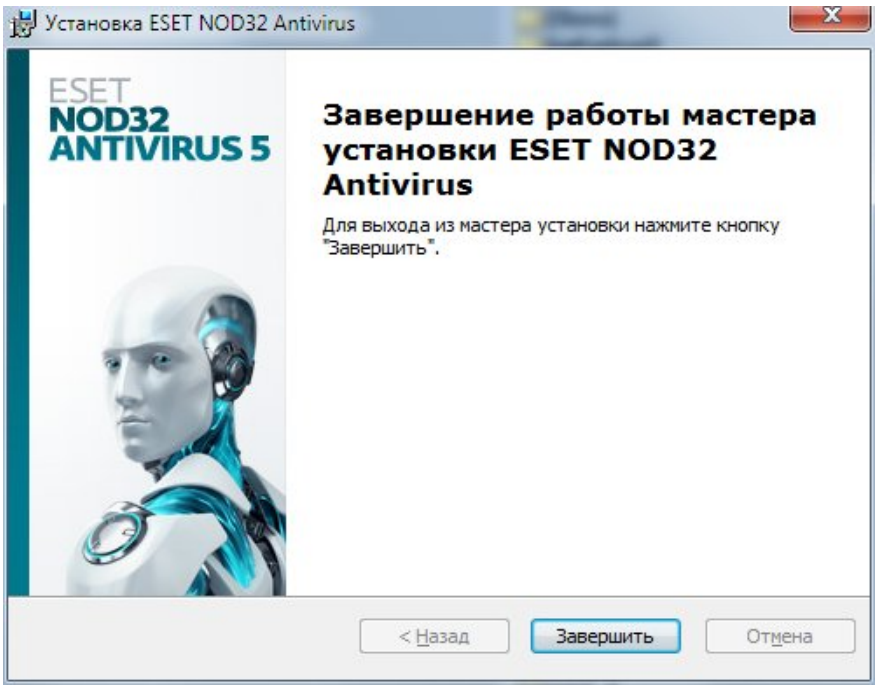
Дійшовши до кроку ESET Live Grid знімаємо прапорець. Навіщо нам зайвий шпигун в системі?



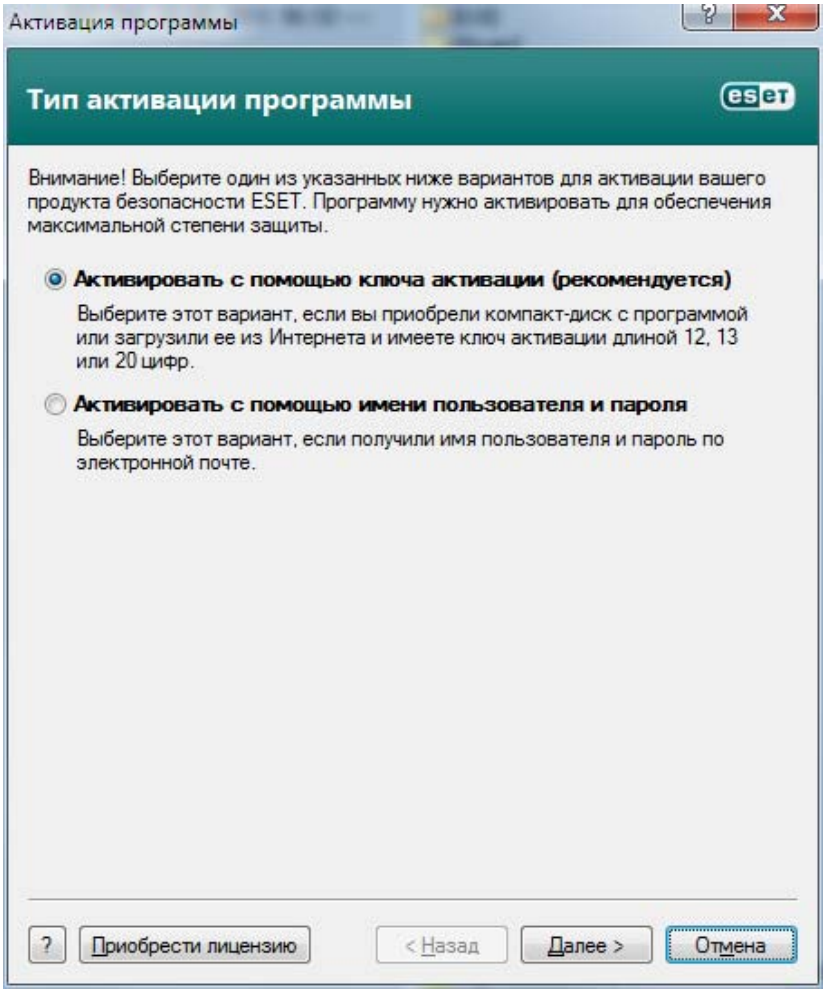
Вмикаємо виявлення потенційно небезпечного програмного забезпечення:



У випадку вдалої установки з’явиться наступне вікно:



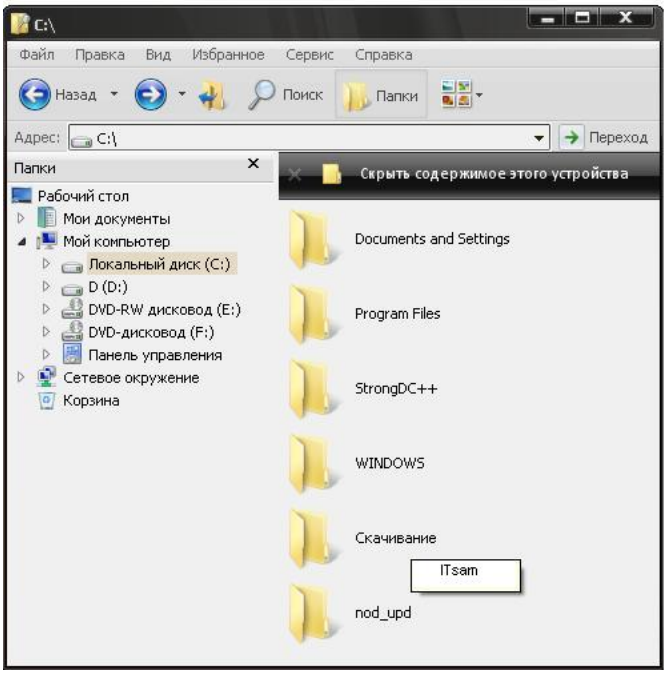
Активуємо демо версію програми за допомогою пароля, котрий висилається на електронну пошту:



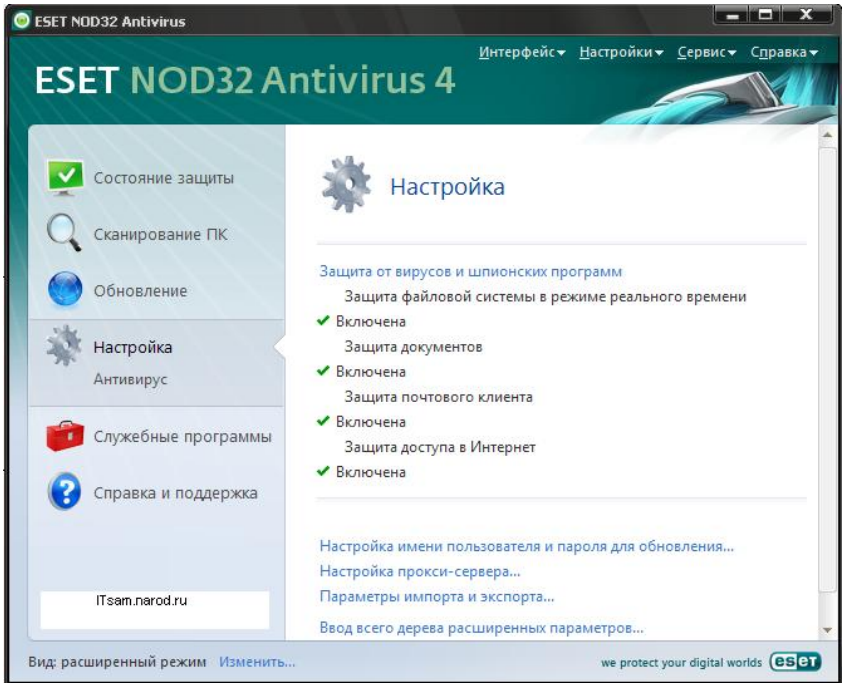
Завдання 2

Оновлення бази даних антивірусу offline

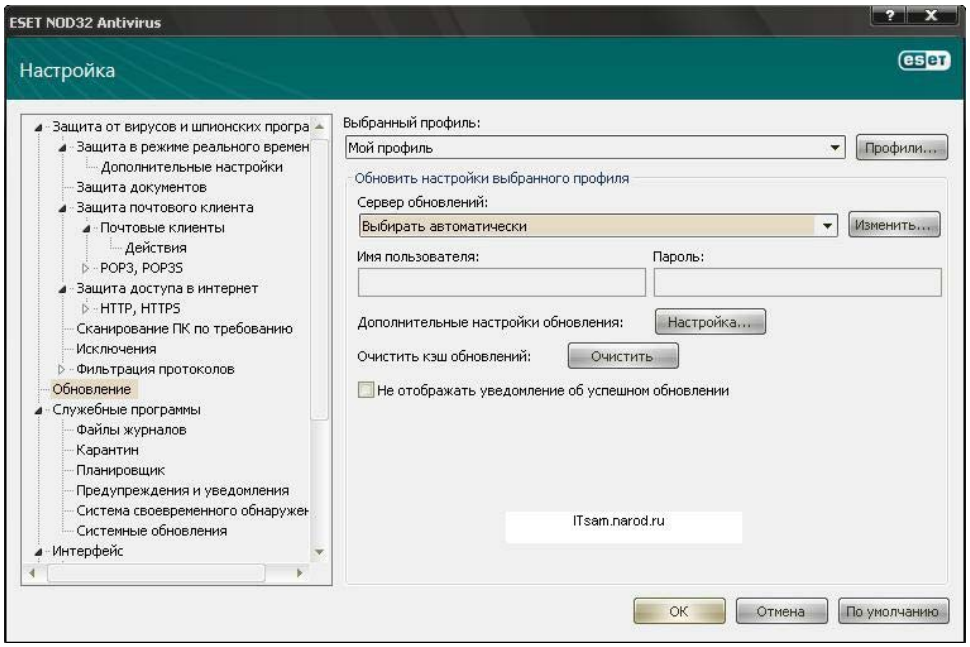
Для оновлення бази даних антивірусу NOD 32 offline необхідно скачати архів з оновленням для Вашої версії з офіційного сайту. Оскільки оновлення зазвичай завантажується у вигляді архіву, тому необхідно спочатку розархівувати папку та назвати її nod_upd (це не обов'язково, але краще дотримуватися даних вимог). Потім помістити папку з оновленнями в кореневу директорію диску С (C:\nod_upd), в папці не повинні міститись інші вкладені папки, лише файли оновлення.



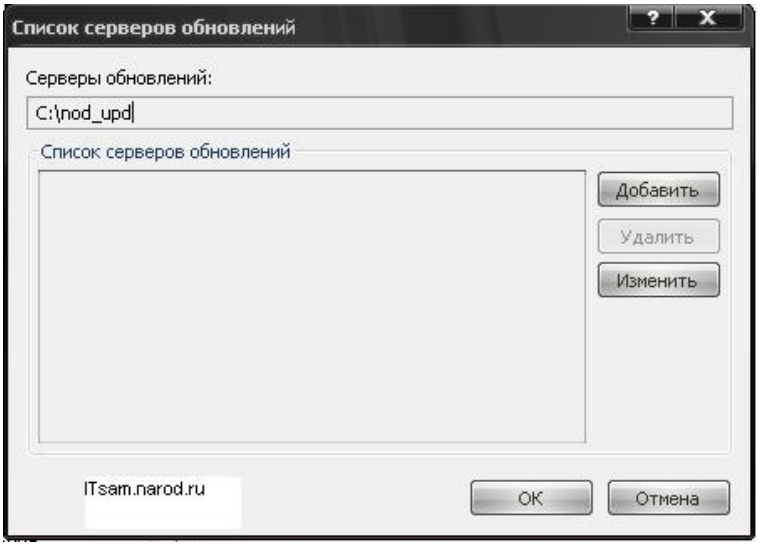
Потім на вкладці «Настройка» антивірусу NOD32 обираємо «Ввод всего дерева расширенных параметров...»», а деяких версіях необхідно обирати пункт «Перейти к расширенным параметрам…».



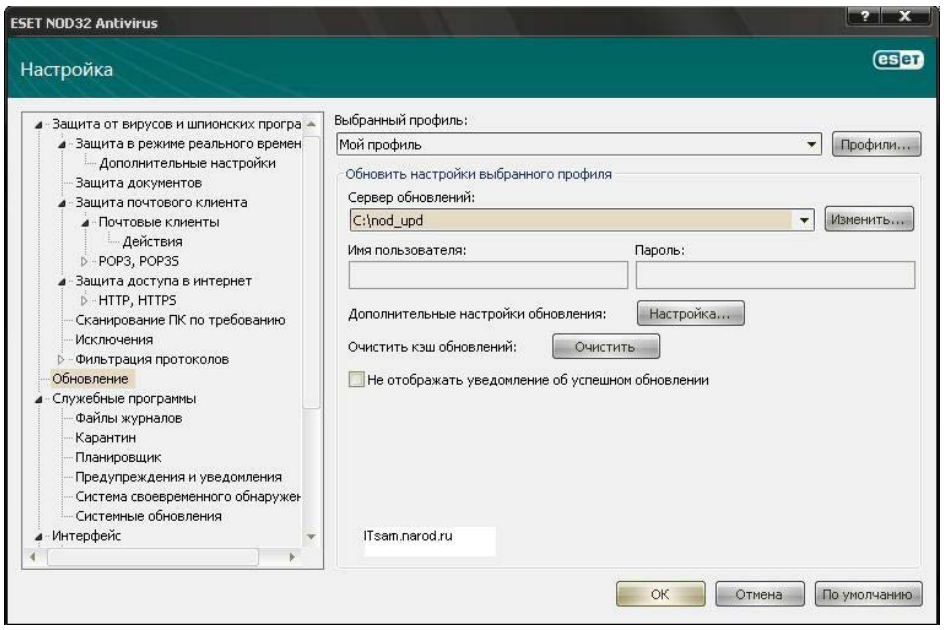
На вкладці «Ввод всего дерева расширенных параметров...» обираємо «Обновление» і навпроти вкладки «Сервер обновлений» натискаємо кнопку «Изменить».



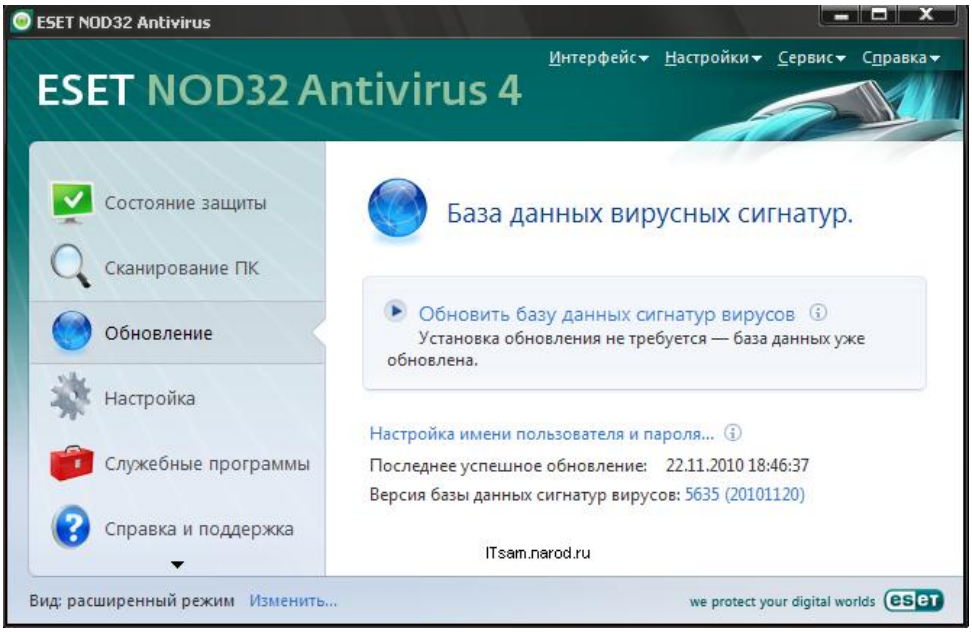
В полі «Серверы обновлений» прописуємо **C:\nod_upd** потім натискаємо «Добавить» і «ОК»:



Потім на вкладці «Сервер обновлений» обираємо **C:\nod_upd** і натискаємо «ОК»:



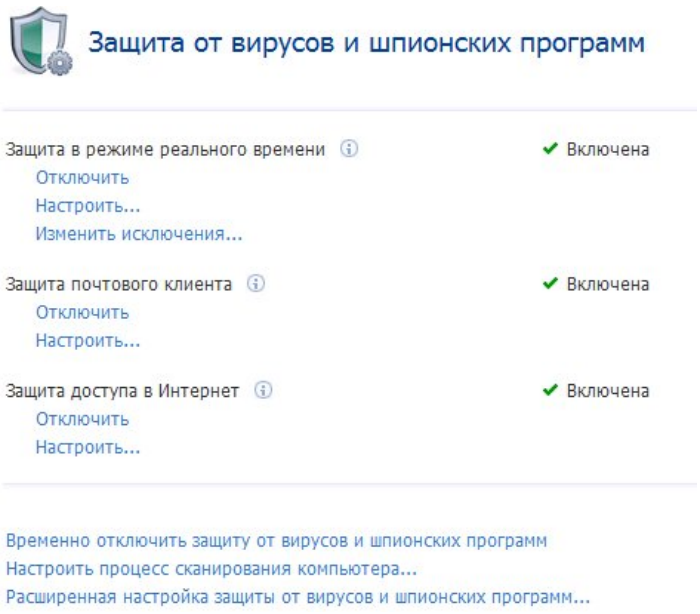
Потім переходимо на вкладку «Обновление» і натискаємо «Обновить базу иру с сигнатур иру сов» і антивірус NOD32 оновлюється offline із папки C:\nod_upd. Рекомендується завантажувати оновлення приміром раз в місяць і просто замінювати папку C:\nod_upd на більш нову версію.



Завдання 3

Налаштування антивірусного засобу

Налаштувань у NOD 32 досить багато, розглянемо найбільш важливі з них. І перше в чому необхідно переконатися, чи ввімкнений захист всіх можливих видів: в режимі реального часу, поштового клієнта, доступу в Інтернет. Керувати цим захистом можна з секції головного меню вікна «Настройка»:

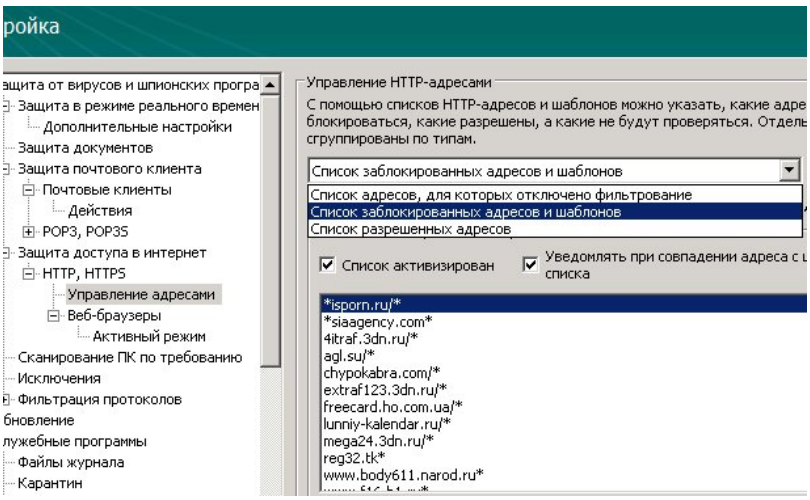


Інші параметри не менш важливі, вони містяться в додаткових налаштування, котрі можна викликати кнопкою F5.

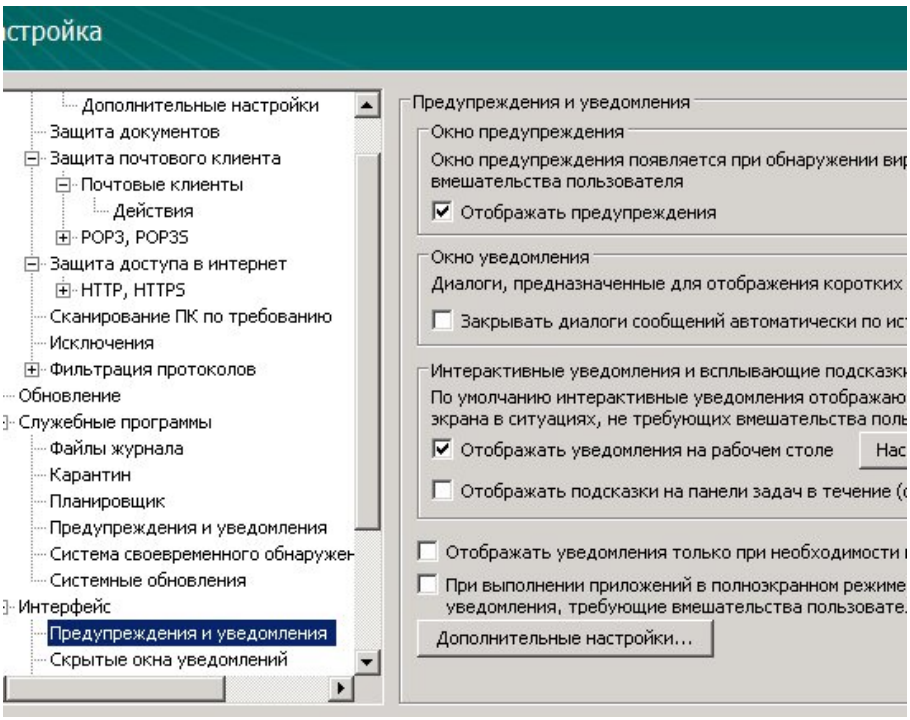
На вкладці **Защита от вирусов и шпионских программ** повинні бути відміченні всі прапорці: а саме, противірусна технологія *Anti-Stealth,* котра дозволяє знаходити приховані загрози, і *Self-defense*. Остання попереджає відключення антивірусу іншими програмами, тобто дотримується постійого функціонування, якщо тільки сам користувач не вимкне NOD 32.

На вкладці **Защита почтового клиента** можна встановити параметри, за якими буде перевірятися пошта. Щоб виконувалася така перевірка обов'язково необхідно відмінити опцію «Включить проверку писем» на підвкладці POP3.

Далі на вкладці **Защита доступа в Интернет** обов'язково повинен бути ввімкнен захист, оскільки в більшості випадків саме із мережі і трапляється зараження. На підвкадці *http,HTTPS* обов'язково необхідно ввімкнути перевірку трафіка, який проходить по цих протоколах. На підвкладці *Управление адресами* можна керувати списками неперевіряємих та заблокованих web-адрес.



Одне з не менш важливих налаштувань, на котре хотілося б звернути увагу – *показ уведомлений.* Ввімкнути чи вимкнути їх можна на підвкладці «Предупреждения и уведомления». При активній опції будуть показуватися спливаючі попередження, у випадку коли виявлятиметься вірус чи пройшло оновлення бази даних чи самої програми. В протилежному випадку віруси будуть видалятися без повідомлення.

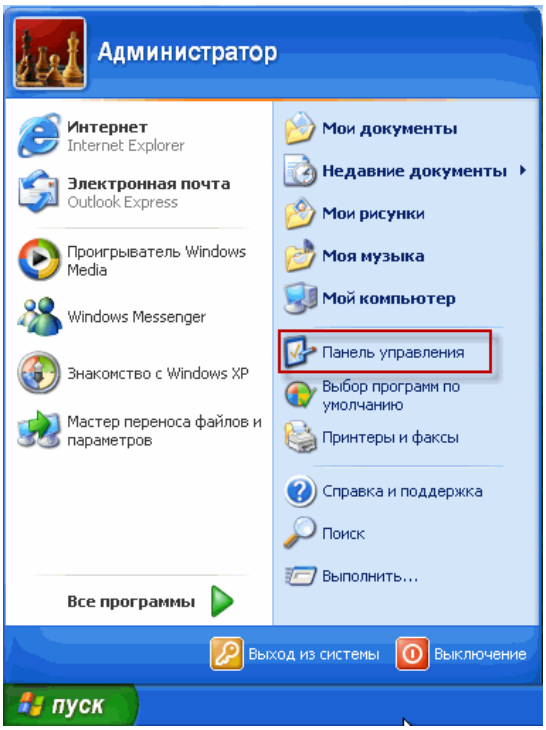


Завдання 4

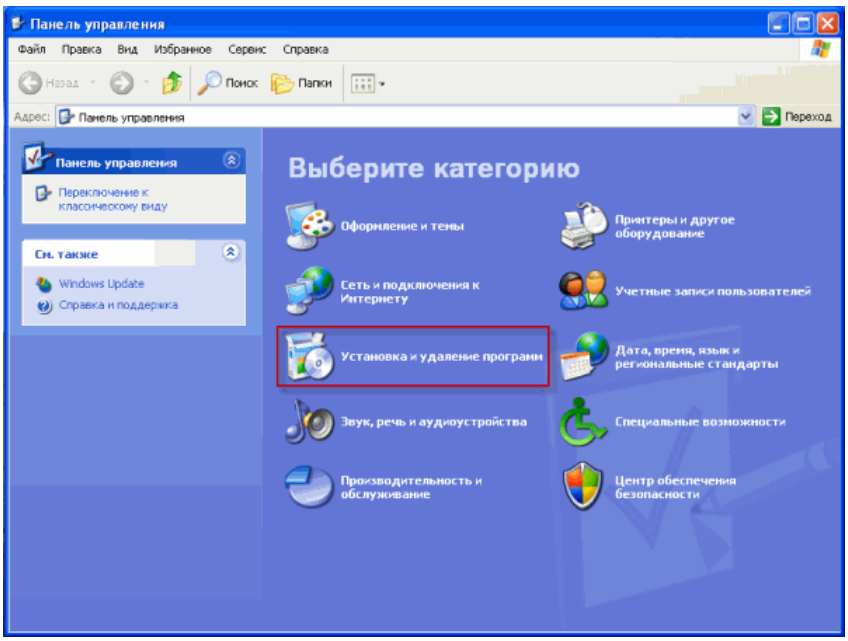
Видалення програмного засобу

Для видалення антивірусу NOD 32 натискаємо в кутку екрану кнопку Пуск та виконуємо наступні дії:

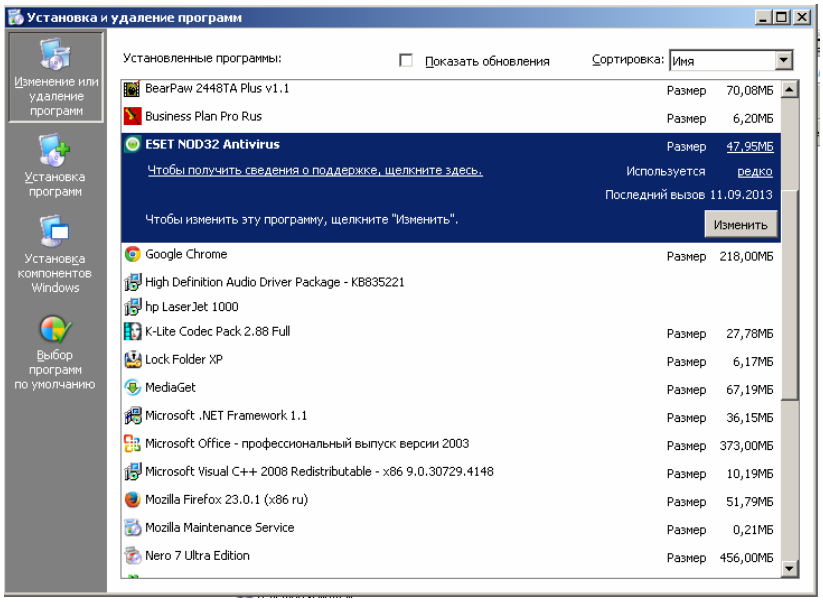
1. Обираємо пункт меню **Панель управления:**



2. У вікні **Панель управления** обираємо роділ **Установка и удаление программ:**



3. В списку програм обираємо антивірус **ESET Nod32** та натискаємо кнопку **Удалить/Изменить** :



4. Почнеться видалення **ESET Nod32** з вашого комп’ютера. Після чого необхідно перезавантажити комп’ютер.

Оформити звіт з практичної роботи аналогічно до звіту з Практичної роботи №1

Контрольні запитання

1. Що представляє собою комп'ютерний вірус?
2. Які групи вірусів існують і які із них найбільш небезпечні?
3. Яким чином проявляється дія вірусу на файли?
4. Які існують джерела вірусів?
5. Яких рекомендацій потрібно дотримуватися для уникнення вірусів?
6. Які програми використовуються для боротьби з вірусами?

7. На яких положеннях будується тактика захисту від вірусу?

8. Що таке вірусоподібні дії? Що слід зробити користувачу, коли такі дії мають місце?

9. У чому зміст евристичного пошуку вірусів?