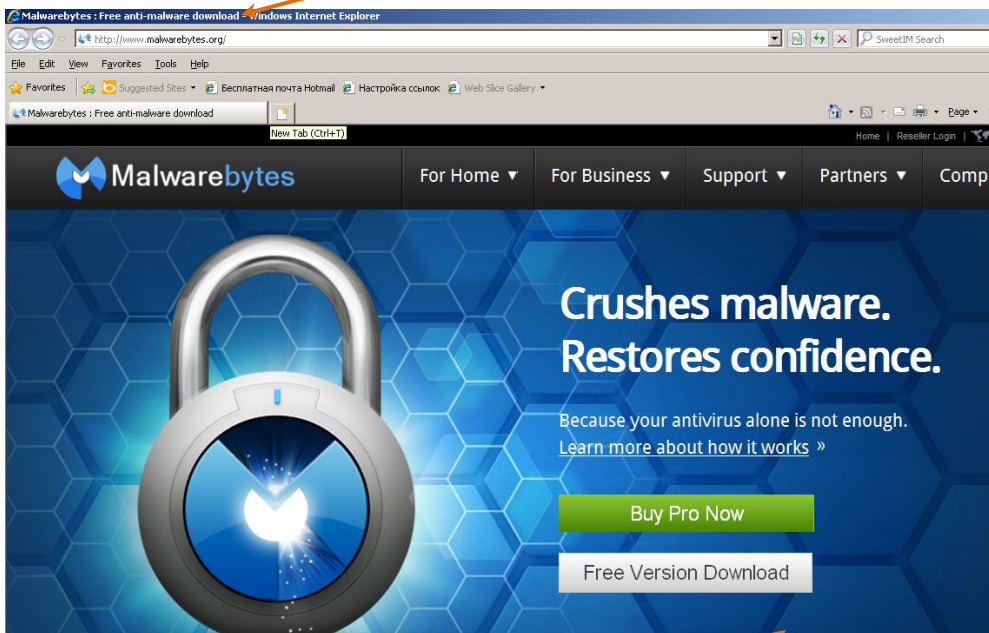


Рекомендації по перевірці робочих станцій клієнтів банку, які працюють з системами дистанційного обслуговування рахунків, на вміст вірусного коду

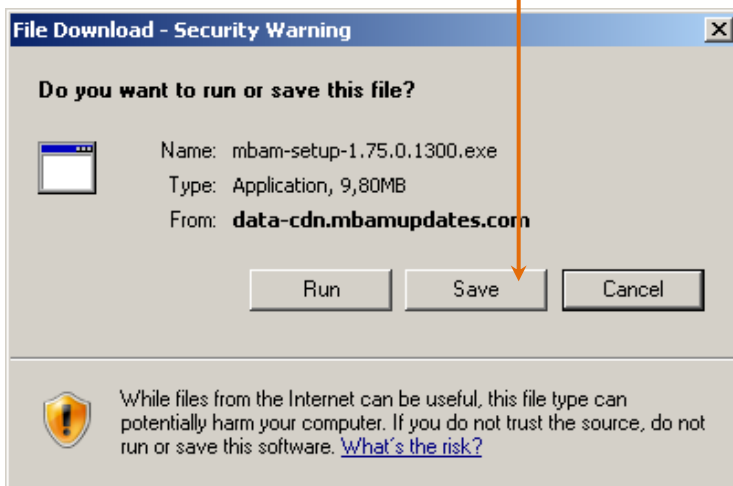
Для завантаження антивірусного програмного забезпечення запустіть Internet Explorer: (якщо Ви використовуєте інший WEB браузер, зображення, наведені в документі, можуть відрізнятись від того, що Ви бачите на своєму екрані)



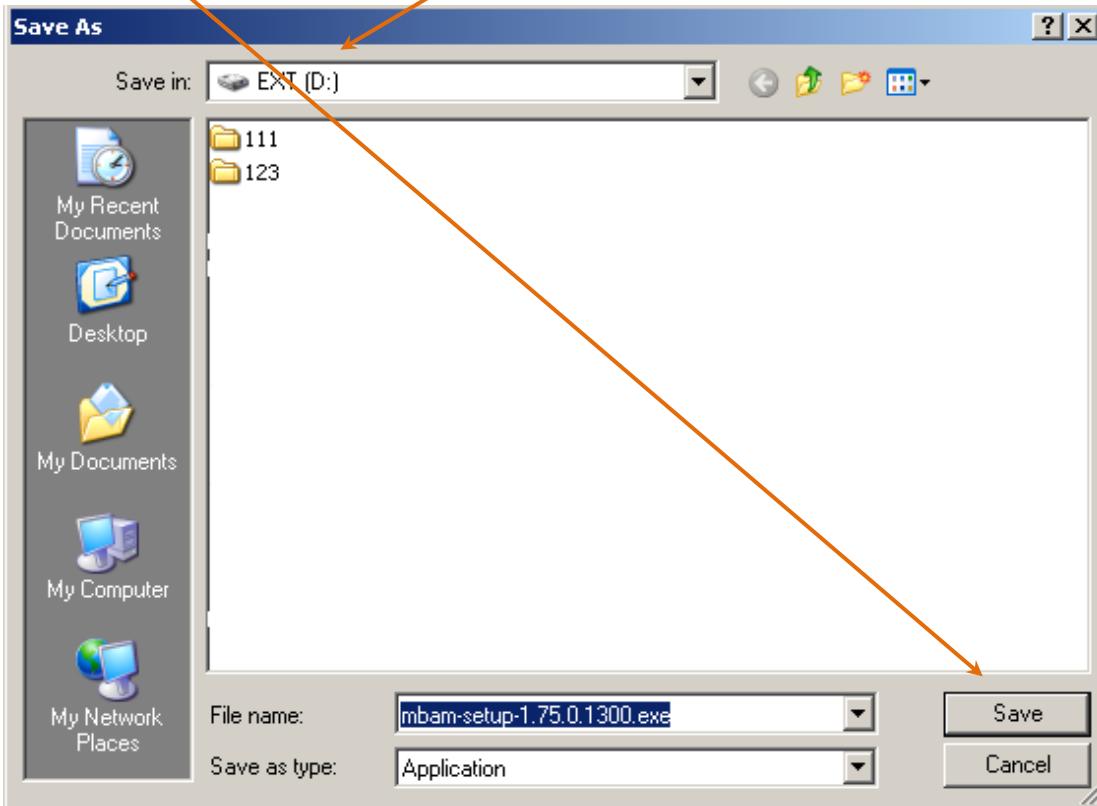
У панелі адреси пропишіть <http://www.malwarebytes.org/> і натисніть клавішу **Enter**. Після цього відкриється сторінка :



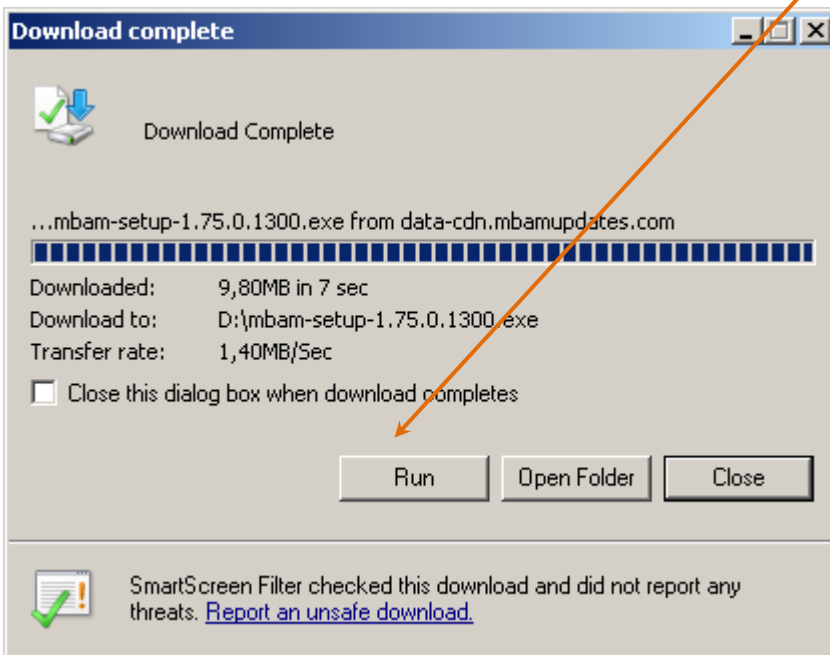
На сторінці, яка відкрилася, необхідно натиснути **Free Version Download**, після чого у вікні завантаження файлу необхідно натиснути **Save** та вказати шлях, куди зберегти файл.



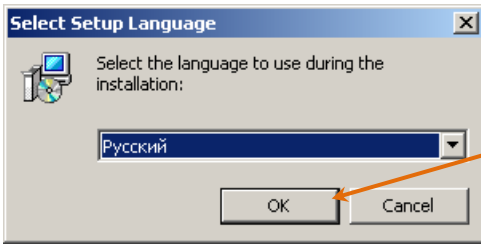
Рекомендовано завантажити файл на диск **D:**, після вибору місця, куди буде збережено файл, натиснути **Save**:



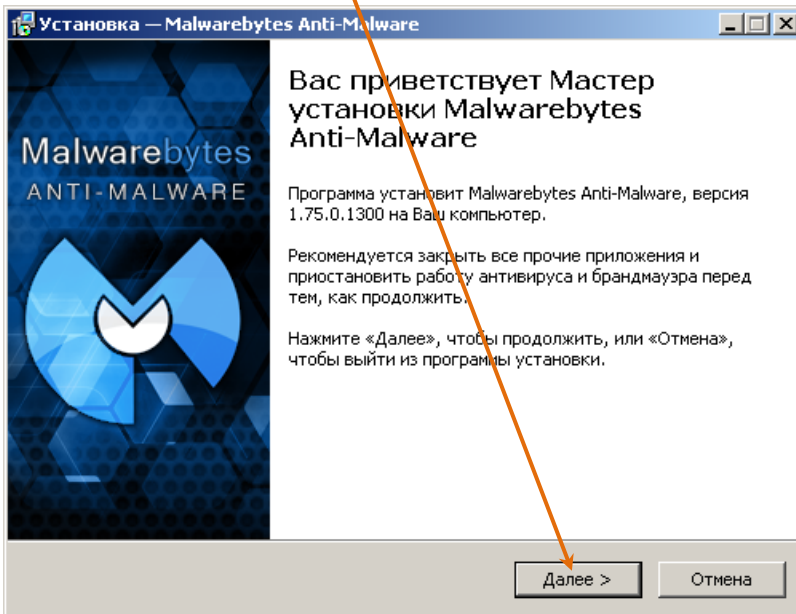
По завершенню етапу завантаження файлу у наступному вікні натиснути **Run** для запуску сканеру для проведення інсталяції на робочій станції.



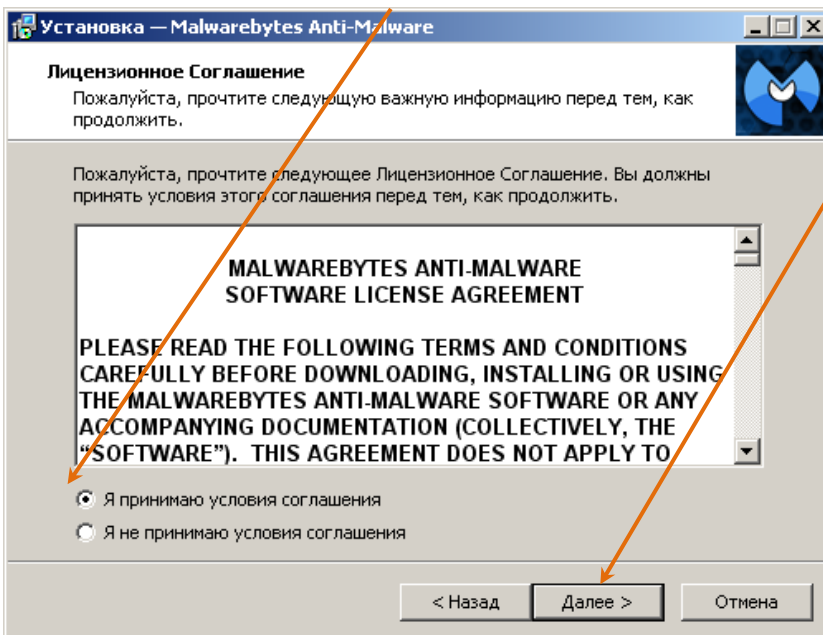
У наступному вікні вибрати мову інтерфейсу програмного забезпечення та натиснути **OK**



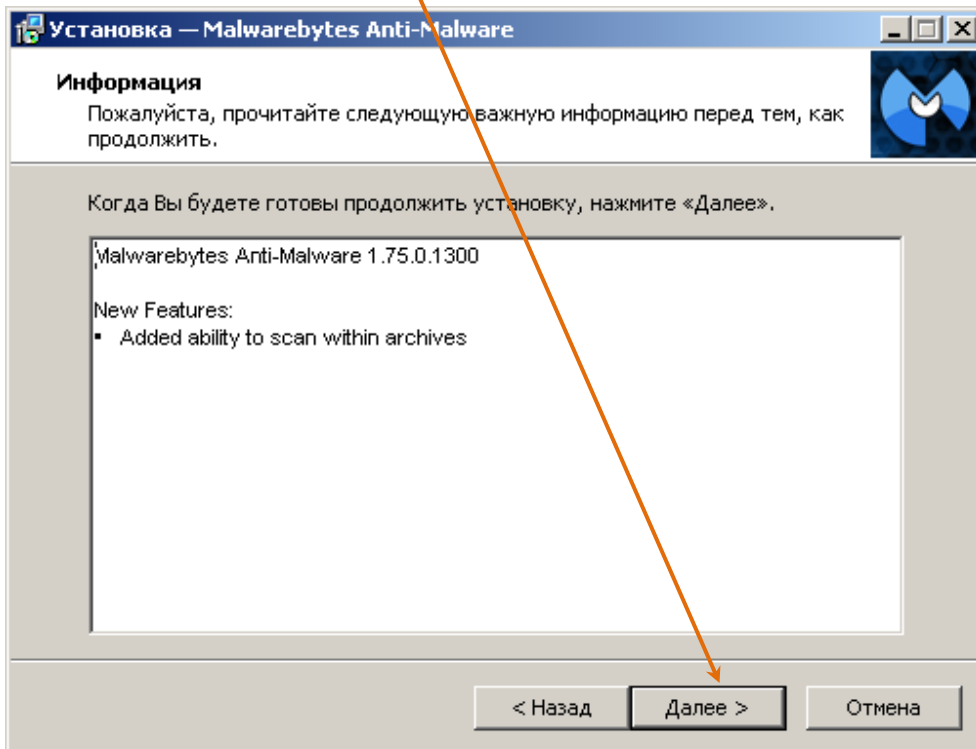
У новому вікні натиснути **Далее**



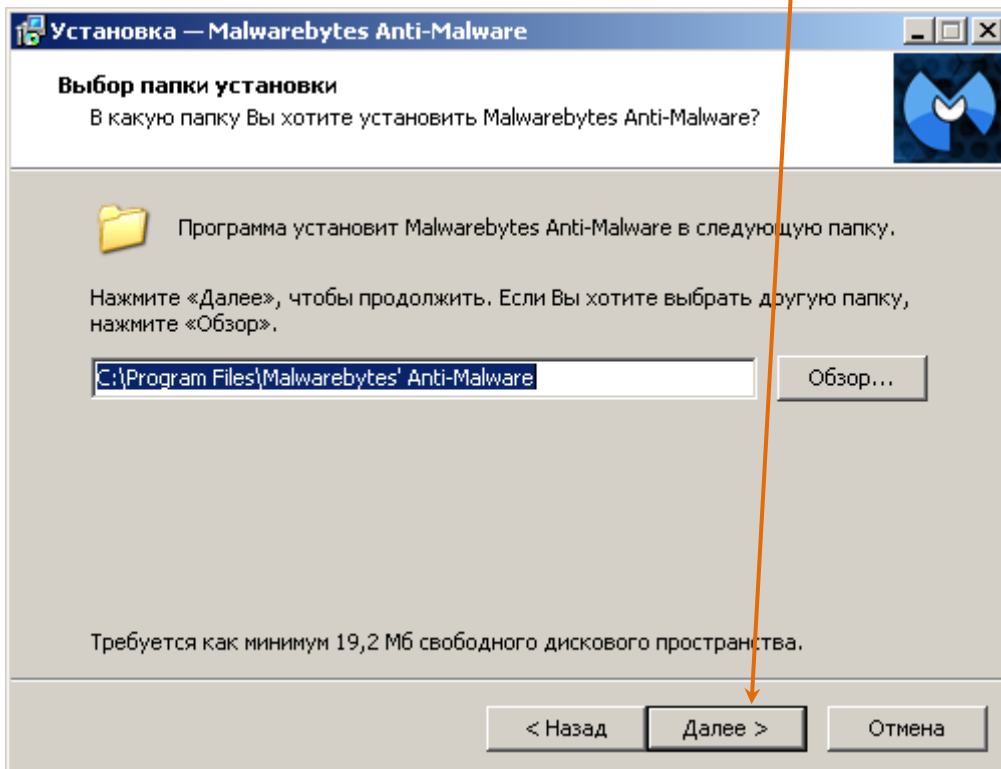
У наступному вікні обрати «**Я принимаю условия соглашения**» і натиснути **Далее**



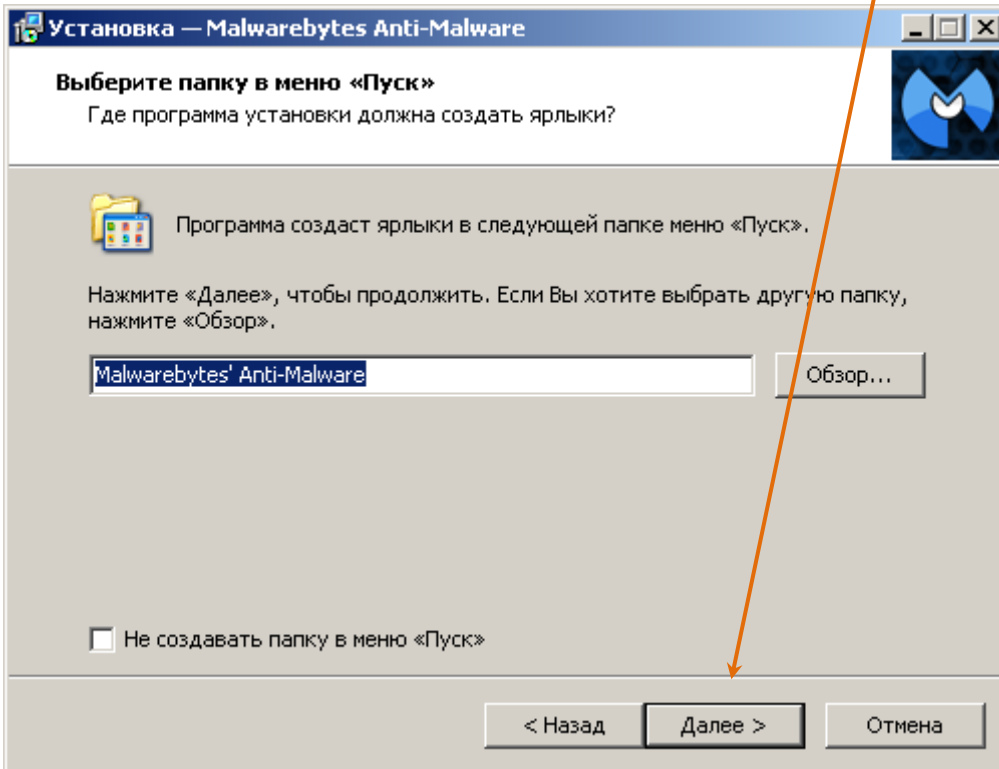
У наступному вікні натиснути **Далее**



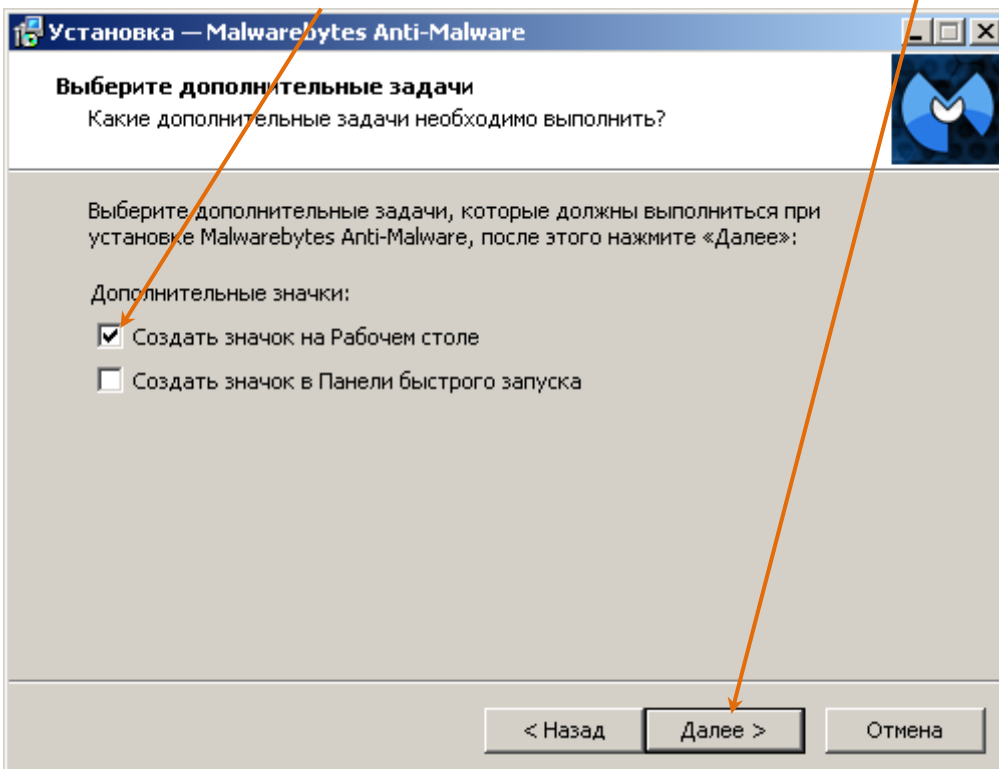
У новому вікні зміни не вносяться. Необхідно натиснути **Далее**



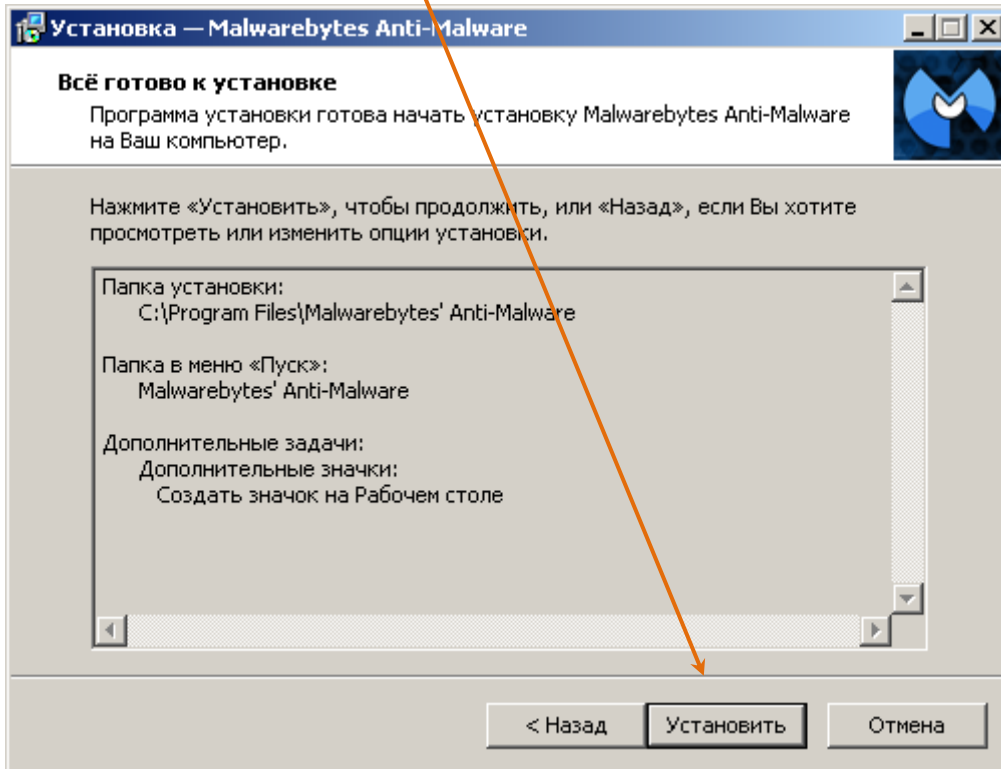
У наступному вікні зміни не проводяться. Необхідно натиснути **Далее**



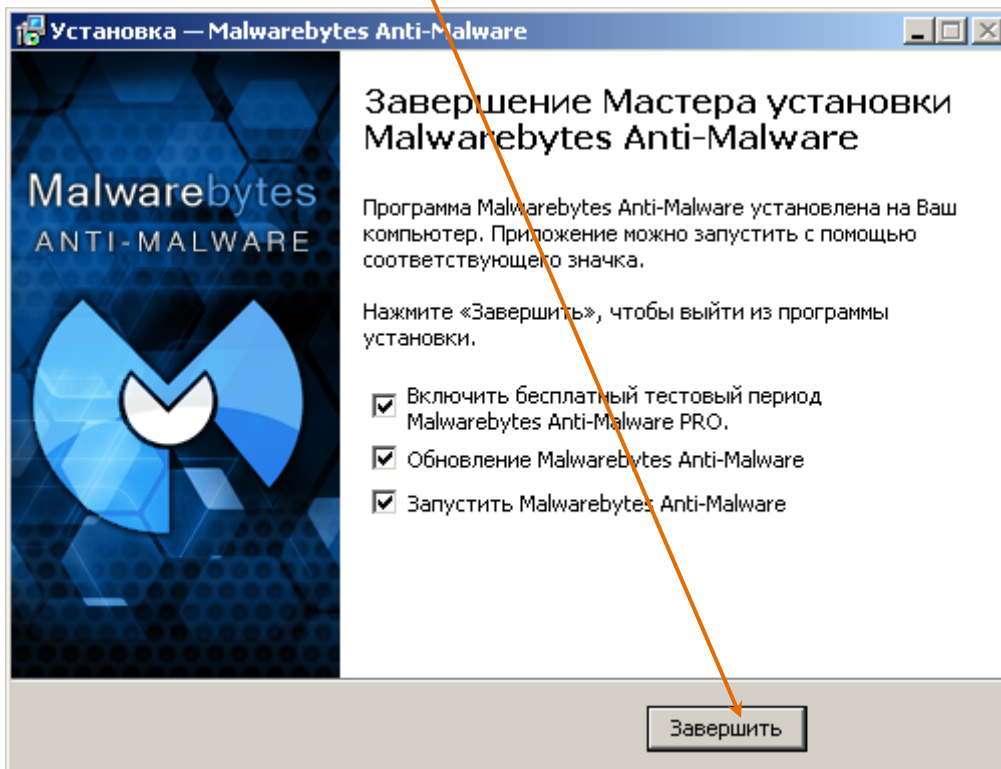
Для того, щоб ярлик для запуску програмного забезпечення розмістити на робочому столі, необхідно відмітити «Создать значок на Рабочем столе» та натиснути **Далее**



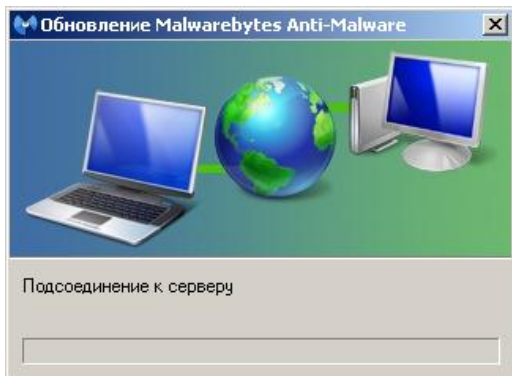
У наступному вікні треба натиснути **Установить**



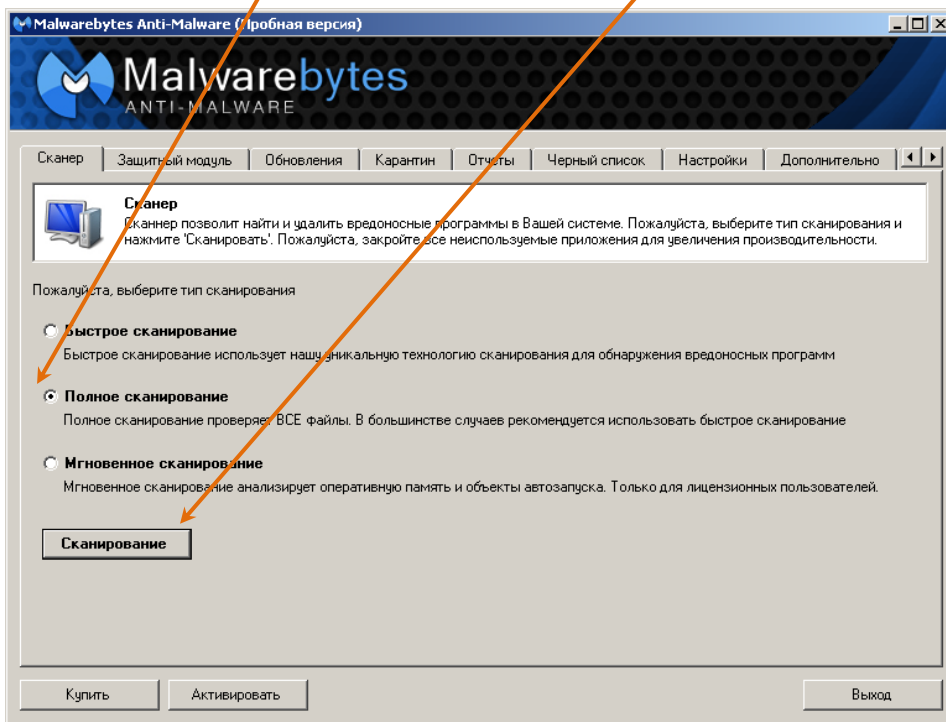
В наступному вікні натиснути **Завершить**



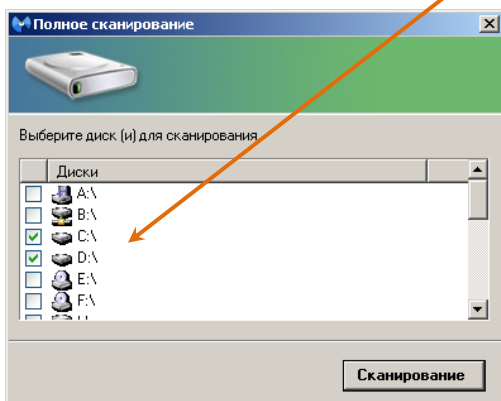
Антивірусна програма оновить антивірусні бази



Після чого запуститься сканер для перевірки робочої станції на вміст вірусного коду. Необхідно вибрати **Полное сканирование** і натиснути **Сканирование**

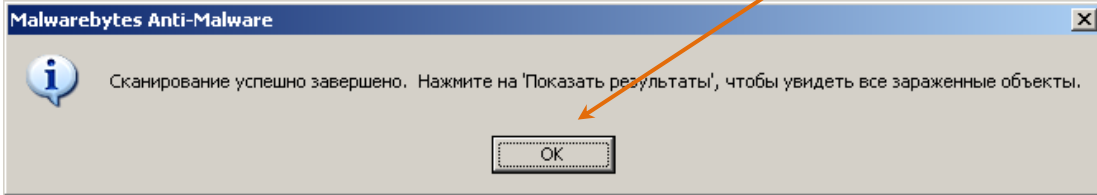


У наступному вікні вибрати **локальні диски** робочої станції та натиснути **Сканирование**

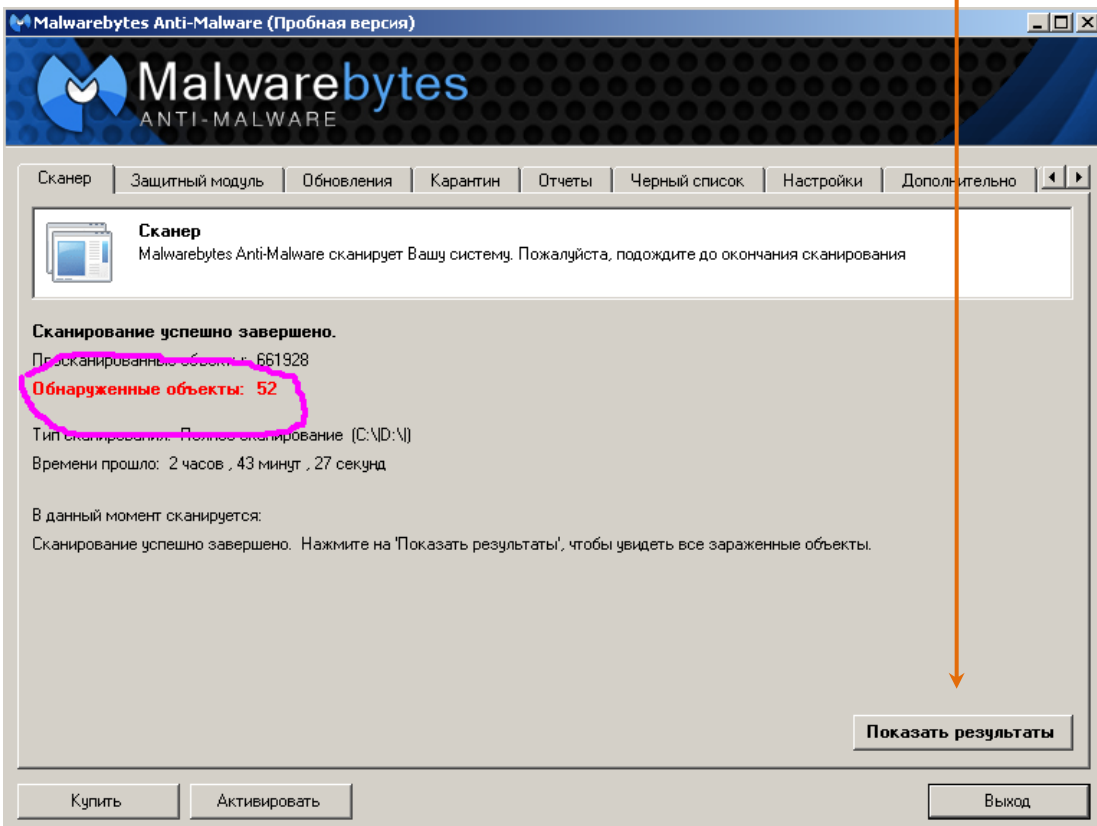


Сканування робочої станції розпочато, необхідно дочекатися закінчення сканування.

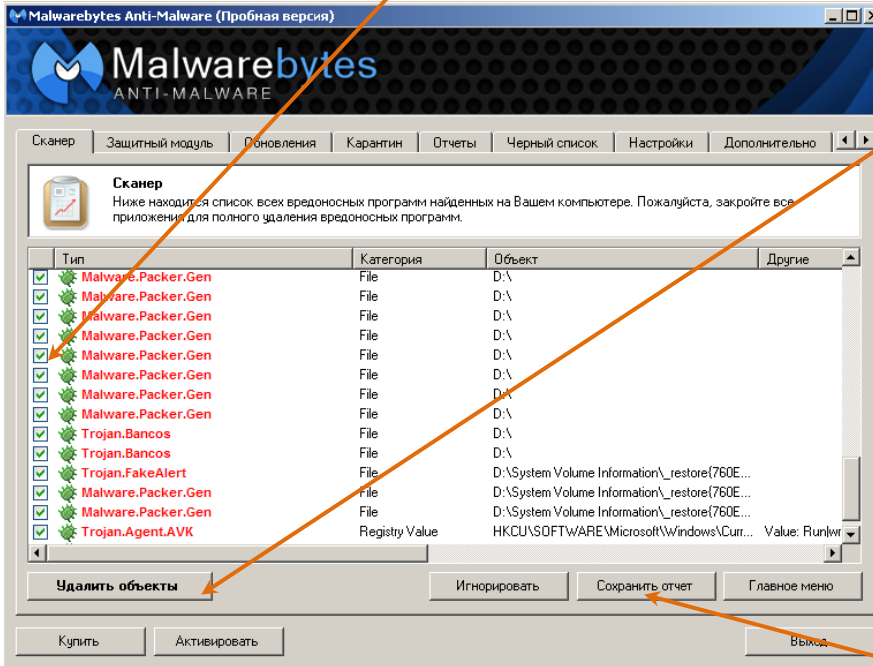
По завершенню сканування з'явиться повідомлення, треба натиснути **OK**



Для просмотра результатов сканування в вікні сканера необхідно натиснути **Показать результаты**

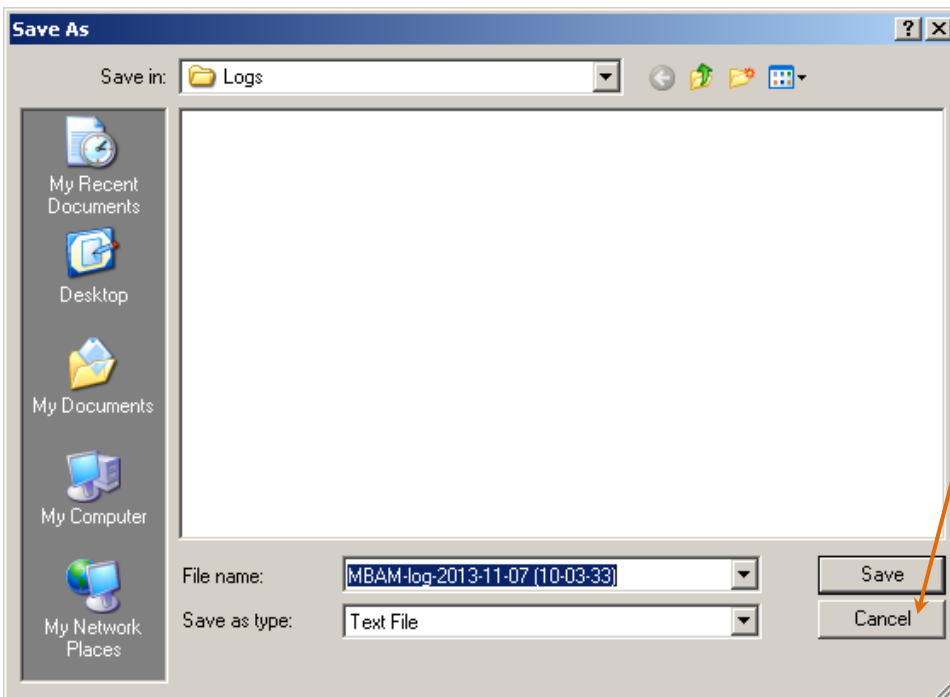


У наступному вікні відкриється список потенційно небезпечних об'єктів (**УВАГА!!! перелік знайдених об'єктів також може містити неліцензійне програмне забезпечення, яке використовується на робочій станції**), тому необхідно провести аналіз та встановити вірусний код для подальшого знищення шляхом виділення вірусних програм та натисканням «Удалить объекты» (у разі необхідності для визначення вірусних програм необхідно звернутися по допомогу до кваліфікованого спеціаліста з інформаційних технологій)

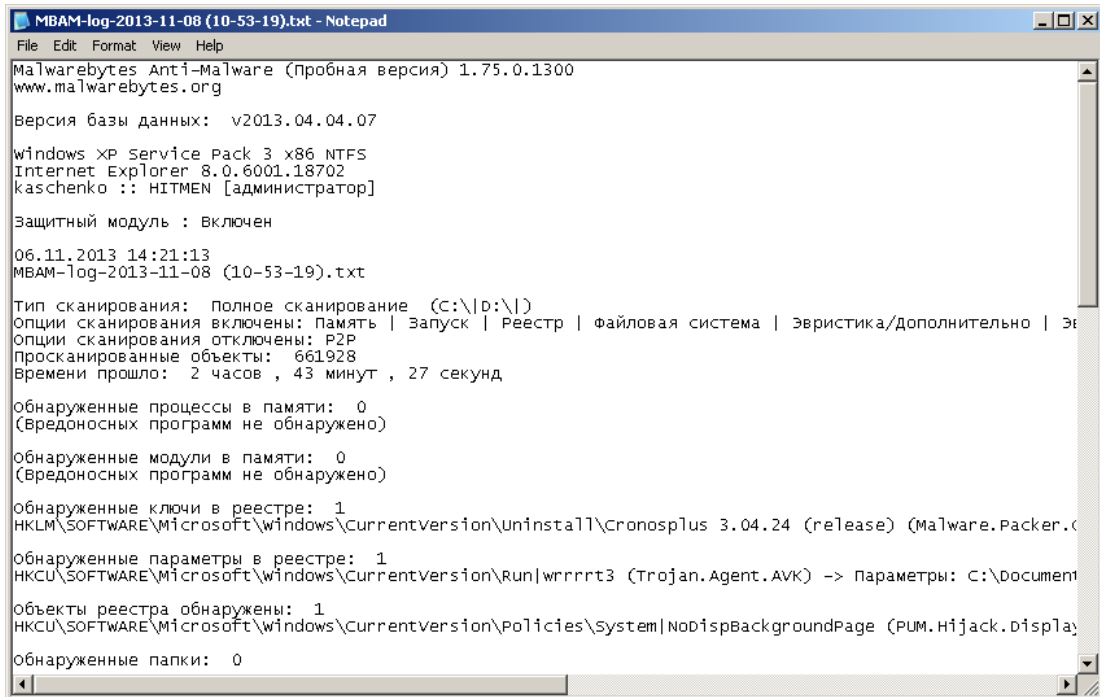


Після проведення процедури видалення вірусів необхідно натиснути **Сохранить отчет**.

Необхідно вибрати місце, куди буде збережено звіт про результати сканування та натиснути **Save**



З'явиться вікно зі звітом по результатах сканування



```
MBAM-log-2013-11-08 (10-53-19).txt - Notepad
File Edit Format View Help
Malwarebytes Anti-Malware (Пробная версия) 1.75.0.1300
www.malwarebytes.org

Версия базы данных: v2013.04.04.07

Windows XP Service Pack 3 x86 NTFS
Internet Explorer 8.0.6001.18702
kaschenko :: HITMEN [администратор]

Защитный модуль : Включен

06.11.2013 14:21:13
MBAM-log-2013-11-08 (10-53-19).txt

Тип сканирования: полное сканирование (C:\|D:\|)
Опции сканирования включены: Память | Запуск | Реестр | файловая система | Эвристика/дополнительно | Э
Опции сканирования отключены: P2P
Просканированные объекты: 661928
Времени прошло: 2 часов , 43 минут , 27 секунд

обнаруженные процессы в памяти: 0
(Вредоносных программ не обнаружено)

обнаруженные модули в памяти: 0
(Вредоносных программ не обнаружено)

обнаруженные ключи в реестре: 1
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Cronosplus 3.04.24 (release) (Malware.Packer.C
обнаруженные параметры в реестре: 1
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\wrrrrt3 (Trojan.Agent.AVK) -> Параметры: C:\Document
Объекты реестра обнаружены: 1
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\NoDispBackgroundPage (PUM.Hijack.Display
обнаруженные папки: 0
```

Після збереження звіт необхідно направити на електронну адресу info@piraeusbank.ua, після чого обліковий запис у системі дистанційного обслуговування рахунків буде розблокований.