

# Інструкція користувача

**Zillya!**<sup>™</sup> Антивірус  
для бізнесу

# Зміст

1. Ліцензійна угода .....	5
2. Складові Zillya! Антивірус для Бізнесу.....	7
2.1. Панель адміністратора.....	7
2.2. Серверна частина .....	7
2.3. Клієнтські частини .....	8
3. Установка Zillya! Антивірус для Бізнесу.....	8
3.1. Установка Серверу з Панеллю адміністратора .....	8
3.1.1. Вимоги до комп'ютера-адміністратора .....	8
3.1.2. Установка Серверної частини з Панеллю адміністратора .....	9
3.1.3. Активація Ліцензії .....	13
3.2. Установка Клієнтських частин .....	15
3.2.1. Підготовка до встановлення Клієнтських частин .....	15
3.2.2. Централізована віддалена установка клієнтів .....	18
3.2.3. Установка клієнтів «вручну» .....	25
4. Використання Zillya! Антивірус для Бізнесу .....	27
4.1. Сканування .....	27
4.1.1. Види сканування .....	27
4.1.2. Запуск сканування з Панелі адміністратора .....	27
4.1.3. Запуск сканування з Клієнтської частини.....	28
4.2. Дії над загрозами: .....	29
4.2.1. Характеристика дій, що застосовуються до загроз.....	29
4.2.2. Застосування дій над загрозами з Панелі адміністратора .....	29
4.2.3. Застосування дій над загрозами з Клієнтської частини .....	31
5. Оновлення продукту Zillya! Антивірус для Бізнесу .....	33
5.1. Вірусні бази .....	33
5.1.1. Оновлення Вірусних баз з Панелі адміністратора .....	33
5.1.2. Оновлення Вірусних баз з Клієнтської частини.....	34

5.1.3. Оновлення Вірусних баз без підключення до Інтернет .....	37
5.2. Оновлення програмних модулів.....	38
5.2.1. Оновлення програмних модулів з Панелі адміністратора .....	38
5.2.2. Оновлення програмних модулів з Клієнтської частини.....	38
6. Управління Ліцензією.....	39
6.1. Активація комерційної Ліцензії.....	39
6.2. Призначення Ліцензій на Клієнтських комп'ютерах.....	39
7. Захист паролем Панелі адміністратора та Клієнтських частин .....	42
7.1. Встановлення та зміна паролю для Панелі адміністратора .....	42
7.2. Встановлення та зміна паролю для Клієнтських частин .....	43
8. Компоненти захисту Zillya! Антивірус для Бізнесу: .....	43
8.1. Файловий монітор «Вартовий».....	43
8.1.1. Опис файлового монітору «Вартовий» .....	43
8.1.2. Налаштування «Вартового» з Панелі адміністратора.....	43
8.1.3. Налаштування «Вартового» з Клієнтської частини .....	44
8.2. Брандмауер.....	45
8.2.1. Опис Брандмауеру .....	45
8.2.2. Налаштування Брандмауеру з Панелі адміністратора .....	46
8.2.3. Налаштування Брандмауеру з Клієнтської частини.....	47
8.3. WEB-фільтр:.....	48
8.3.1. Опис WEB-фільтру .....	48
8.3.2. Налаштування WEB-фільтру з Панелі адміністратора .....	48
8.3.3. Налаштування WEB-фільтру з Клієнтської частини.....	49
8.4. USB-захист .....	50
8.4.1. Опис USB-захисту .....	50
8.4.2. Налаштування USB-захисту з Панелі адміністратора.....	50
8.4.3. Налаштування USB-захисту з Клієнтської частини .....	51
9. Загальні налаштування продукту Zillya! Антивірус для Бізнесу .....	51

9.1. Сканування поштових повідомлень.....	51
9.2. Зміна налаштувань з Панелі адміністратора .....	51
9.3. Зміна налаштувань з Клієнтської частини .....	52
10. Додаткові можливості Панелі адміністратора:.....	53
10.1. Управління групами комп'ютерів .....	53
10.2. Статистика та історія.....	54
10.3. Вікно «Про програму».....	55
11. Додаткові можливості Клієнтських частини: .....	56
11.1. Евристичний аналізатор.....	56
11.2. Диспетчер задач та Диспетчер автозавантаження .....	56
11.3. Планувальник.....	56
12. Зворотній зв'язок.....	57

# 1. Ліцензійна угода кінцевого користувача програмного продукту Zillya! Антивірус для Бізнесу ТОВ «Олайті Сервіс»

## 1. Ліцензійна Угода

Ця ліцензійна угода (далі Угода) укладається між користувачем (далі Користувач) і ТОВ «Олайті Сервіс» (далі Розробник), що є правовласником виключних прав на програмний продукт Zillya! Антивірус для Бізнесу (далі Програмний Продукт), який є власною розробкою ТОВ «Олайті Сервіс».

Встановлення і використання Програмного Продукту означає прийняття Користувачем умов даної Угоди. Якщо Користувач не згоден з деякими положеннями Угоди або з Угодою в цілому, Користувач не може встановлювати, використовувати та копіювати цей Програмний Продукт.

Користувачу надається право використовувати Програмний Продукт на вказаний у реєстраційному ключі термін, згідно придбаної ліцензії. Користувач має право на використання Програмного Продукту на тій кількості комп'ютерів, що оговорено ліцензією, і лише для захисту цих комп'ютерів та інформації на них. Використання Програмного Продукту для інших цілей можливе лише на підставі окремої угоди з Розробником та за ціною, що встановлюється Розробником.

## 2. Авторське Право

Виключні майнові авторські права на Програмний Продукт належать Розробнику. Програмний Продукт містить комерційну таємницю та іншу конфіденційну інформацію, що належить Розробнику. Програмний Продукт захищений законодавством України та Міжнародним законодавством. Ви можете використовувати Програмний Продукт тільки у відповідності з правами Користувача, що приведені в цій Угоді.

## 3. Права Користувача

Розробник надає Користувачеві невиняткове обмежене право використовувати Програмний Продукт у такий спосіб:

- Застосовувати Програмний Продукт відповідно до прямого функціонального призначення.
- Користувач не має право передавати дистрибутив Програмного Продукту іншим особам. Дозволяється мати одну інсталювану копію програмного продукту на кожен придбаний ліцензію.
- Користувач не має права змінювати, декомпілювати, дешифрувати і проводити інші дії з кодом Програмного Продукту з метою отримання інформації про реалізовані технології та алгоритми.

#### **4. Обмежена відповідальність**

Програмний Продукт надається на умовах «як є», відповідно до принципу “as is”, який загальноприйнятий у міжнародній комп’ютерній практиці. Це означає, що за проблеми, що виникають у процесі експлуатації Програмного Продукту, Розробник відповідальності не несе.

Розробник прикладає усі зусилля для того, щоб зменшити ризик виникнення проблем технічного або іншого характеру. Розробник надає Користувачеві послуги з технічної підтримки Програмного Продукту на умовах чинних правил надання технічної підтримки Розробника.

Розробник не відповідає за фінансові та інші збитки, отриманні Користувачем при використанні Програмного Продукту.

#### **5. Умови використання окремих функцій Програмного Продукту**

Користувача повідомлено і він погоджується, що Програмний Продукт містить функціональний компонент для передачі інформації Розробнику щодо помилок та збоїв Програмного Продукту. Ці дані не містять жодної особистої інформації та ніяких відомостей про дані на комп’ютері, інстальовані програмні продукти, налаштування користувача. Інформація, що передається Розробнику, використовується виключно з метою усунення недоліків Програмного Продукту та не використовуватиметься з іншою метою.

Користувача повідомлено і він погоджується, що Програмний Продукт може встановлювати додаткові модулі під час оновлення продукту. Такі додатки використовуються виключно з метою розширення функціоналу Програмного Продукту.

#### **6. Припинення дії Угоди**

Ця Угода буде керуватись у відповідності з Українським та Міжнародним законодавством. Розробник може припинити дію цієї Угоди, якщо Користувач не дотримується умов і положень цієї Угоди. В такому випадку Користувач повинен знищити всі копії Програмного Продукту та його складові частини.

Користувач може припинити дію Угоди, знищивши всі копії Програмного Продукту і супровідної документації.

## 2. Складові Zillya! Антивірус для Бізнесу

### 2.1. Панель адміністратора

Продукт Zillya! Антивірус для Бізнесу передбачає централізоване керування усім антивірусним захистом в локальній мережі з одного комп'ютера. Таке керування здійснюється через складову програми, що має назву Панель адміністратора. Вона є центром керування, який дозволяє конфігурувати налаштування клієнтських комп'ютерів, запускати та планувати сервісні завдання.

**Панель адміністратора** – це графічна оболонка централізованого керування комп'ютерами-клієнтами. Дозволяє переглядати стан захисту кожного з комп'ютерів та локальної мережі загалом, змінювати налаштування та запускати завдання. Доступ до Клієнтських частин здійснюється посередньо через Сервер.

Тобто, Панель адміністратора приймає команди для комп'ютерів-клієнтів від адміністратора мережі, після чого передає їх Серверній частині. Також вона приймає та відображає дані, передані комп'ютерами-клієнтами через Серверну частину адміністратору (наприклад, інформацію щодо подій та статистику).

Зручність Панелі адміністратора полягає в можливості віддаленого централізованого управління захистом клієнтських комп'ютерів з будь-якого місця лише за IP-адресою.

### 2.2. Серверна частина

Серверна частина встановлюється на комп'ютер одночасно з Панеллю адміністратора та залишається на даному ПК навіть у випадку, якщо Панель адміністратора перенесено на інший комп'ютер.

Серверна частина забезпечує виконання завдань, призначених з Панелі адміністратора для комп'ютерів-клієнтів та зворотню взаємодію цих складових. Тобто, Серверна частина забезпечує зв'язок між Панеллю адміністратора та комп'ютерами-клієнтами.

**З цих причин ми рекомендуємо не вимикати комп'ютер з встановленою на ньому Серверною частиною без нагальної потреби та не залишати даний ПК вимкненим на тривалий час!**

**Сервер** – це службова програма, встановлена на комп'ютері з доступом до мережі Інтернет, яка об'єднує собою всі клієнтські частини, завантажує та поширює оновлення, передає команди з Панелі адміністратора на Клієнтські частини.

Серверна частина не має графічної оболонки.

## 2.3. Клієнтські частини

На кожен комп'ютер, який планується захистити антивірусом, необхідно встановити Клієнтську частину. Навіть якщо необхідно захистити комп'ютер з Панеллю адміністратора та Серверною частиною.

**Клієнтська частина** – це складова продукту Zillya! Антивірус для Бізнесу, яка забезпечує захист комп'ютера, на якому вона встановлена. Клієнтська частина приймає через Сервер та виконує команди від Панелі адміністратора, звітує Серверу про події безпеки та інше.

## 3. Установка Zillya! Антивірус для Бізнесу

### 3.1. Установка Серверу з Панеллю адміністратора

#### 3.1.1. Вимоги до комп'ютера-адміністратора

Мінімальні технічні вимоги до комп'ютера, на який встановлюється Серверна частина з Панеллю адміністратора:

**Операційна система:** Windows XP SP2/SP3, Windows Vista x86/x64, Windows 7 x86/x64, Windows 8 x86/x64, Windows 2003 Server x86/x64, Windows 2008 Server x86/x64.

**Частота процесора:** 1,5 ГГц або вище

**Оперативна пам'ять:** 1 Гб або більше

**Місце на жорсткому диску:** 120 Мб або більше

**Зверніть увагу:** даний комп'ютер має знаходитись у вимкненому стані якомога менше!

Панель адміністратора у майбутньому може бути перенесена на менш потужний комп'ютер, але Серверна частина має залишатися на даному ПК.

Мінімальні технічні вимоги до комп'ютера з Панеллю адміністратора:

**Операційна система:** Windows XP SP2/SP3, Windows Vista x86/x64, Windows 7 x86/x64, Windows 8 x86/x64, Windows 2003 Server x86/x64, Windows 2008 Server x86/x64.

**Частота процесора:** 800 МГц

**Оперативна пам'ять:** 256 Мб



### 3.1.2. Установка Серверної частини з Панеллю адміністратора

Інсталятор продукту Zillya! Антивірус для Бізнесу передбачає можливість установки як всіх компонентів відразу, так і вибірково установку.

**Для успішної установки Серверної частини з Панеллю адміністратора рекомендуємо дотримуватись наступної послідовності дій:**

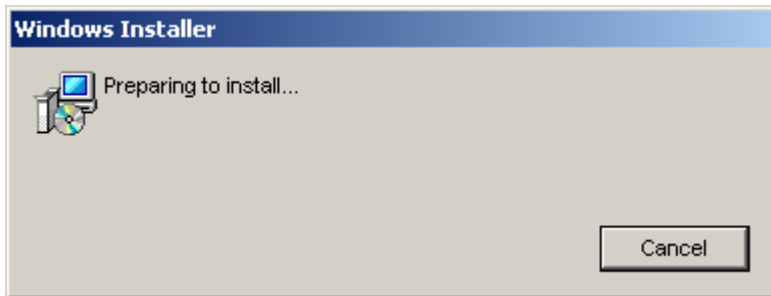
1. Оберіть комп'ютер, який слугуватиме комп'ютером-адміністратором та використовуватиметься для управління захистом на інших комп'ютерах в локальній мережі. Впевніться, що даний ПК відповідає мінімальним технічним вимогам, описаним в пункті **3.1.1**.
2. Запустіть на обраному комп'ютері установочний пакет Zillya! Антивірус для Бізнесу, що має назву ZillyaEnterpriseSecurity\_ua.msi:



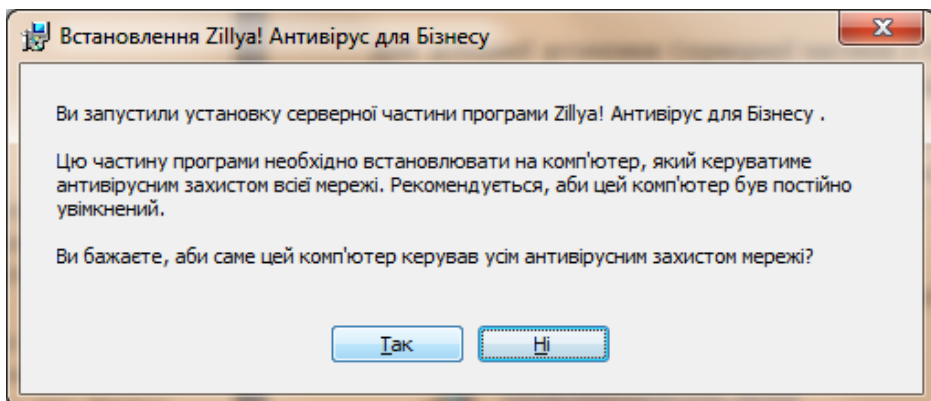
[ZillyaEnterpriseSecurity\\_ua.msi](http://download.zillya.com/ZillyaEnterpriseSecurity_ua.msi)

[http://download.zillya.com/ZillyaEnterpriseSecurity\\_ua.msi](http://download.zillya.com/ZillyaEnterpriseSecurity_ua.msi)

3. Дочекайтеся запуску інсталяційної програми:



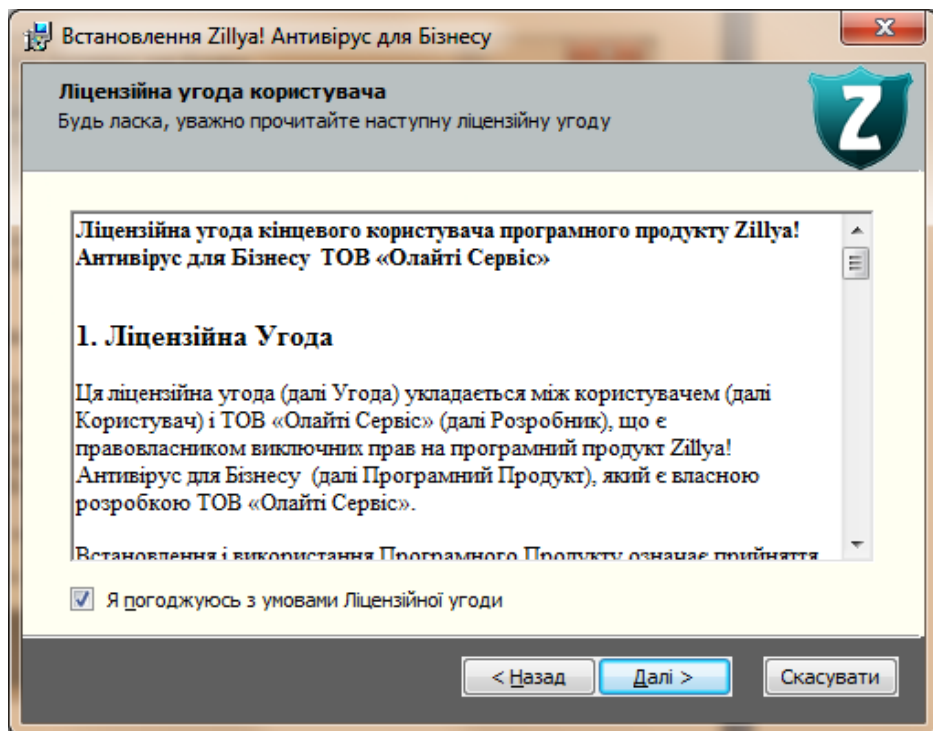
4. З'явиться вікно з запитом на затвердження цього комп'ютера у якості комп'ютера-адміністратора. Натисніть кнопку Так:



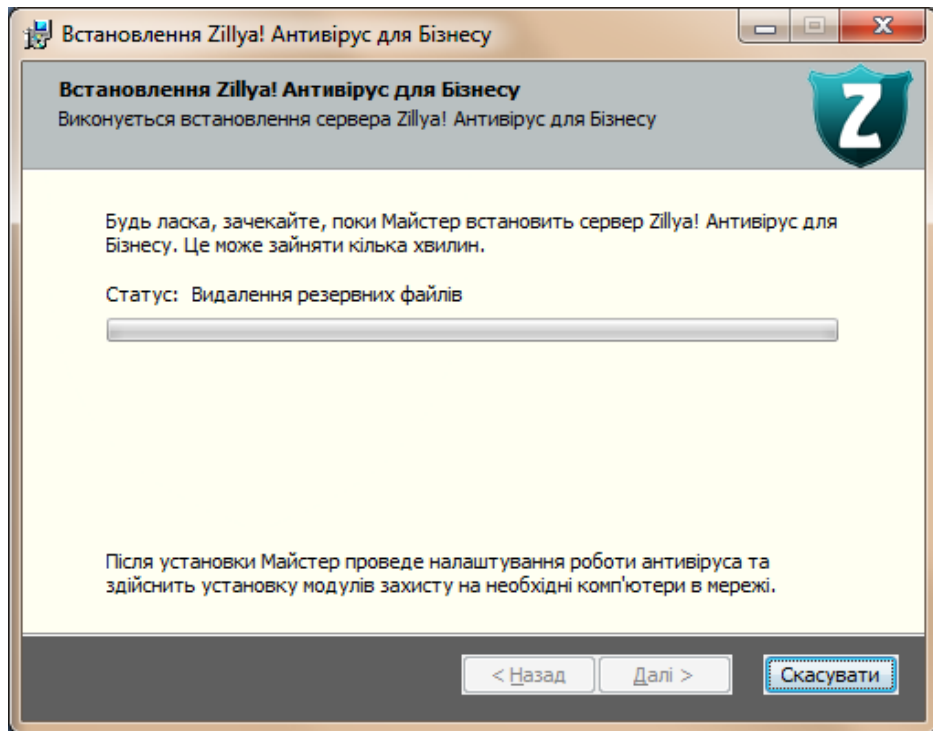
5. Після погодження запуститься **Майстер установки Сервера Zillya! Антивірус для Бізнесу**, який крок за кроком допоможе Вам встановити програму. Керуйте його вказівками. Натисніть Далі для продовження:



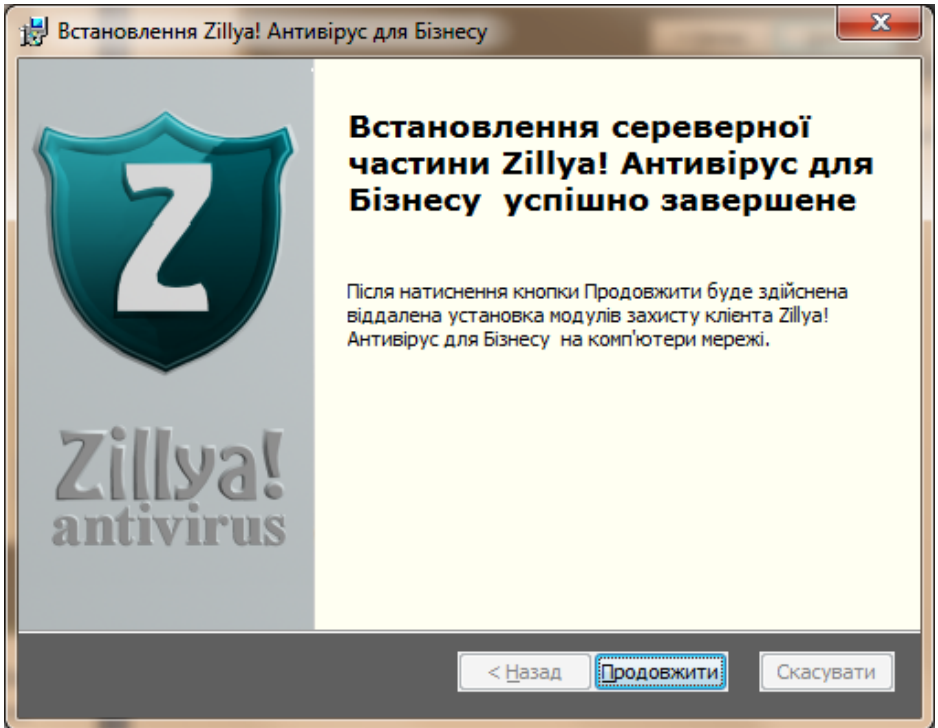
6. Уважно прочитайте **Ліцензійну угоду** та прийміть її умови, якщо Ви згодні з ними, відзначивши відповідний пункт галлюю внизу вікна. Натисніть Далі:



7. Розпочнеться процес встановлення програми. Це може зайняти деякий час.  
Будь ласка, зачекайте:



8. По завершенню процесу установки Серверної частини з Панеллю адміністратора Ви будете поінформовані відповідним повідомленням:



Натискання кнопки Продовжити завершить роботу даного Майстра установки та запустить наступний крок встановлення продукту Zillya! Антивірус для Бізнесу у Вашій локальній мережі.

### 3.1.3. Активація Ліцензії

Для використання програми Zillya! Антивірус для Бізнесу Вам необхідно активувати **ліцензію**. Ви можете активувати одну з 2 видів ліцензії:

1. **Комерційну ліцензію Zillya! Антивірус для Бізнесу** – це ліцензія, надана Користувачу після успішного здійснення ним транзакції для її придбання або на умовах окремої домовленості з Розробником.

Комерційна ліцензія може бути активована наступними двома шляхами:

- a) за допомогою **Коду активації з 32х символів**, через мережу Інтернет. Даний код видається користувачу автоматично та використовується для стандартної пріоритетної активації продукту. Він може бути

використаний повторно у разі зміни локальної мережі, переустановки Zillya! Антивірус для Бізнесу тощо.

- b) через **Ліцензійний ключ**, що не поребує Інтернет-з'єднання в момент активації. Цей Ліцензійний ключ видається користувачу за його запитом та використовується як екстренний, запасний метод. У разі його використання рекомендуємо Вам підключитися до Інтернету якомога швидше, адже для коректного функціонування продукту (оновлення вірусних баз, програмних модулів тощо) це є необхідним!

**2. Безкоштовну (пробну) ліцензію Zillya! Антивірус для Бізнесу** – це ліцензія, яка надається Користувачу на обмежену кількість комп'ютерів (5 комп'ютерів) з метою презентації можливостей продукту. Безкоштовна ліцензія не відрізняється від комерційної функціонально. Під час її активації вона призначається автоматично та не відображається Користувачу. Безкоштовна ліцензія розрахована на використання протягом **1 календарного місяця**.

Після завершення роботи Майстра установки Серверної частини з Панеллю адміністратора та натиснення кнопки Продовжити відобразиться вікно Активація ліцензії:

Активация ліцензії

**Активуйте продукт, використовуючи Ваш ліцензійний ключ або активаційний код.**

Виберіть тип ліцензії та введіть реєстраційну інформацію:

- Код активації з 32х символів
- Ліцензійний ключ (не потребує Інтернет-з'єднання в момент активації)
- Активувати пробну ліцензію (до 5 комп'ютерів)

Введіть Ваш активаційний код. Код активації має формат "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXX". Увага, при використанні даного методу активації комп'ютер має бути підключений до мережі Інтернет на момент активації продукту.

Код активації:

Назад Далі Відміна

Будь ласка, оберіть бажаний Вами спосіб, заповніть відповідне поле у разі необхідності та натисніть Далі.

Якщо Ви обрали активацію продукту за допомогою **Коду активації з 32х символів**, Вам може відобразитися вікно з проханням ввести Ваші реєстраційні дані:

Активация ліцензії

## Введіть реєстраційні дані:

Будь ласка, введіть Ваші дані в форму реєстрації. Введена інформація потрібна для подальшого продовження ліцензії на Zillya! Антивірус для Бізнесу та звернень до служби технічної підтримки.

Назва організації:  \*

Контактна особа (ПІБ)  \*

Ел. адреса:  \*

Контактний телефон:

Назад Далі Відміна

Дані, введені Вами у цьому вікні, будуть передані нам як Ваша персональна реєстраційна інформація та використовуватимуться для нашої подальшої взаємодії з Вами.

Будь ласка, заповніть усі поля даної форми та натисніть Далі для завершення процесу активації ліцензії!

## 3.2. Установка Клієнтських частин

### 3.2.1. Підготовка до встановлення Клієнтських частин

Як вже зазначено, Клієнтські частини встановлюються на комп'ютери, які планується захистити.

Для коректного функціонування Клієнтської частини радимо обирати ПК, які відповідають наступним **мінімальним системним вимогам**:

**Операційна система: Windows XP SP2/SP3, Windows Vista x86/x64, Windows 7 x86/x64, Windows 8 x86/x64, Windows 2003 Server x86/x64, Windows 2008 Server x86/x64.**

**Частота процесора: 1 ГГц або вище**

**Оперативна пам'ять: 512 Мб або більше**

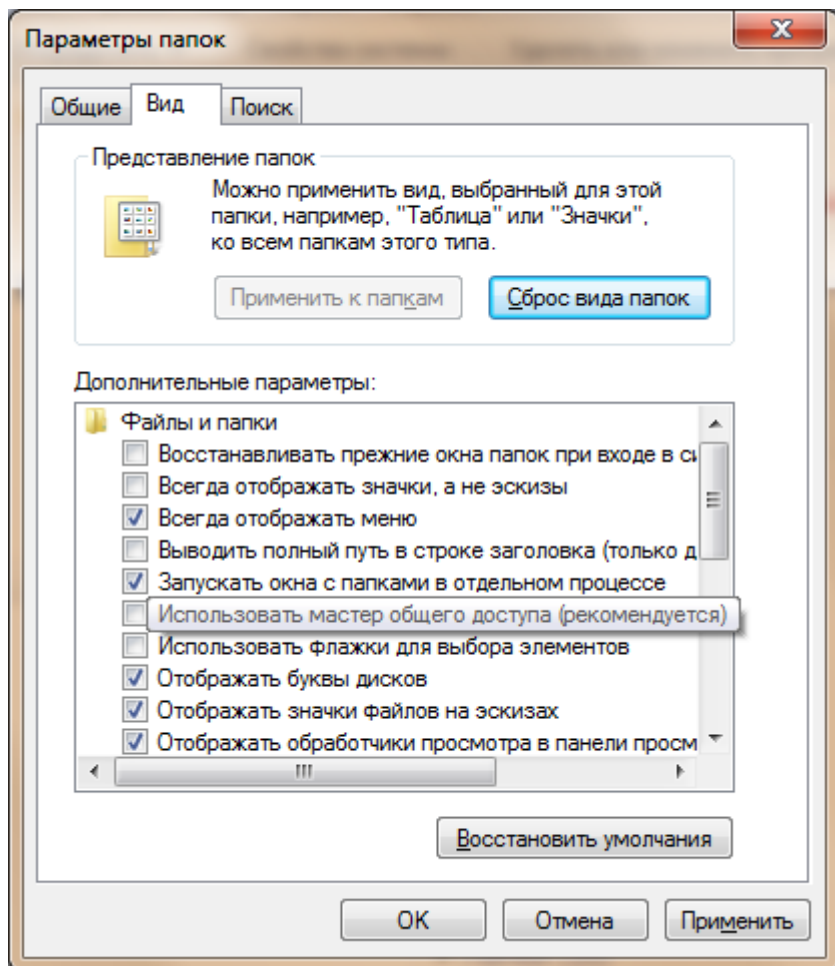
Налаштування операційної системи на комп'ютері-клієнті можуть значно вплинути на успішність централізованої віддаленої установки Клієнтської частини на даний ПК з комп'ютера-адміністратора.

Налаштування операційних систем на комп'ютерах-клієнтах мають відповідати наступним **нормам**:

- 1. Логін та пароль адміністратора операційної системи задані.** Перед початком процесу віддаленої установки Клієнтської частини назначте логін та пароль облікового запису Адміністратор на комп'ютері, на який планується встановити захист.
- 2. Брандмауер Windows вимкнений.** Вимкніть стандартний Брандмауер Windows та інші Брандмауери у разі їх наявності на комп'ютері-клієнті перед встановленням на нього Клієнтської частини.



3. **Простий загальний доступ до файлів вимкнено.** Будь ласка, вимкніть стандартний майстер загального доступу, як показано у вікні нижче, та натисніть Застосувати:



4. **Сторонні антивірусні рішення видалені.** Рекомендуємо впевнитись, що на усіх обраних Вами комп'ютерах не встановлено стороннього антивірусного ПО. В іншому разі ми не гарантуємо коректне функціонування продукту Zillya! Антивірус для Бізнесу.

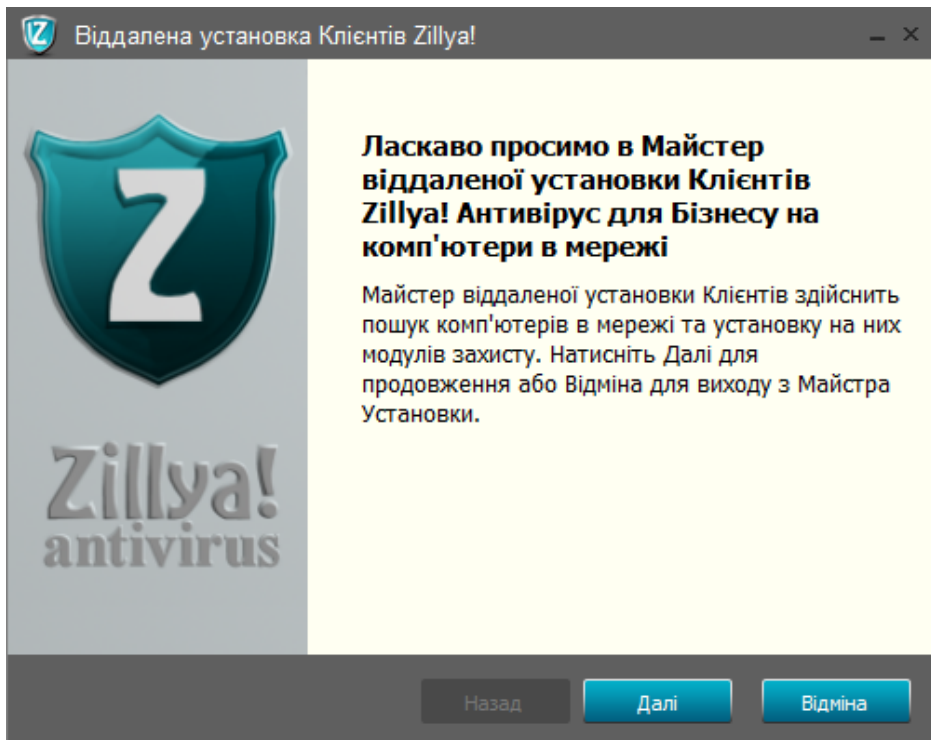
Вказані вище норми є необхідними умовами для централізованого віддаленого доступу до комп'ютерів-клієнтів та встановлені безпосередньо системою безпеки ОС Windows.

### 3.2.2. Централізована віддалена установка клієнтів

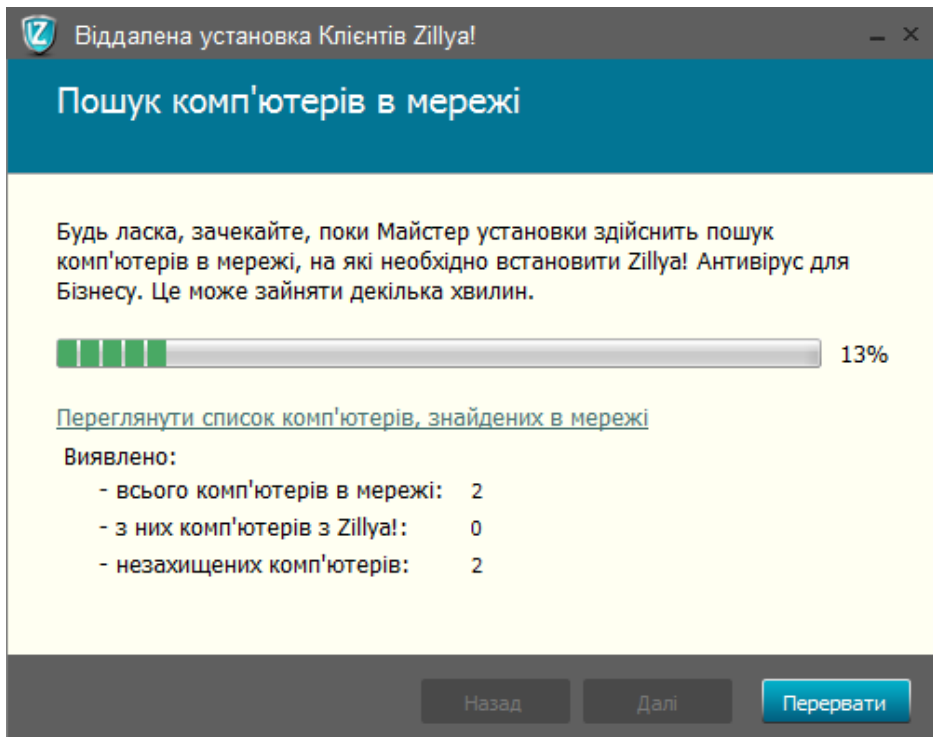
Після завершення активації ліцензії автоматично запуститься **Майстер віддаленої установки Клієнтів Zillya! Антивірус для Бізнесу**. Рекомендуємо слідувати його вказівкам.

**Будь ласка, дотримуйтесь наступних кроків для успішної віддаленої установки Клієнтських частин:**

1. **Натисніть Далі** у стартовому вікні Майстра:



2. Розпочнеться пошук усіх комп'ютерів в локальній мережі. Рекомендуємо зачекати деякий час:



3. Коли процес досягне 100 відсотків, кнопки Назад та Далі стануть активними. Ви можете переглянути результати пошуку, натиснувши на посилання [Переглянути список комп'ютерів, знайдених в мережі](#), та Далі для продовження:

Віддалена установка Клієнтів Zillya!

## Пошук комп'ютерів в мережі

Будь ласка, зачекайте, поки Майстер установки здійснить пошук комп'ютерів в мережі, на які необхідно встановити Zillya! Антивірус для Бізнесу. Це може зайняти декілька хвилин.

100%

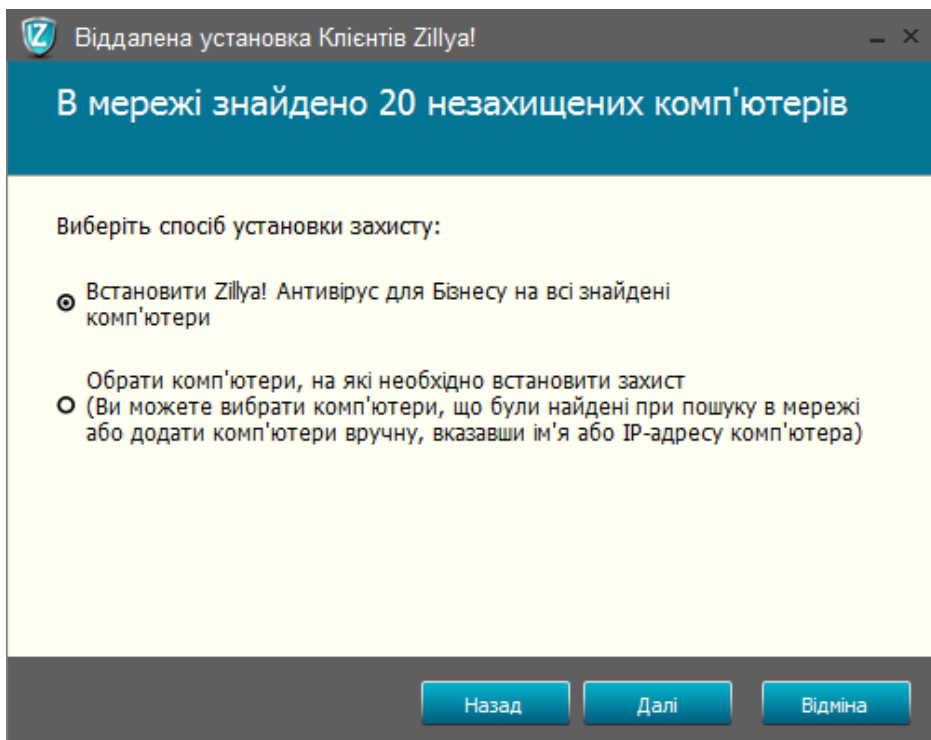
[Приховати список комп'ютерів, знайдених в мережі](#)

Комп'ютери:	Детально
192.168.0.157 (windowspc.zil...	встановлено Zillya! Антивірус дл...
192.168.0.159 (AVTEST3)	Антивірус не виявлено
192.168.0.161 (avtest.zillya)	Антивірус не виявлено
192.168.0.162 (AVSORT)	Антивірус не виявлено
192.168.0.172 (vmserver1.zil...	Антивірус не виявлено
192.168.0.178 (server.zillya)	Антивірус не виявлено


Назад    Далі    Відміна

4. Вам буде запропоновано обрати спосіб установки: встановити захист на всі знайдені комп'ютери або самостійно вибрати комп'ютери для встановлення захисту серед знайдених ПК в мережі.

Оберіть бажаний Вами спосіб та натисніть Далі.







Якщо Ви бажаєте самостійно обрати комп'ютери для встановлення захисту, оберіть другий спосіб та натисніть Далі:

 Віддалена установка Клієнтів Zillya!

## Знайдено 20 комп'ютерів, на які необхідно встановити захист

Виберіть комп'ютери, на які необхідно віддалено встановити Zillya! Антивірус для Бізнесу.

	Комп'ютери:	Статус
<input type="checkbox"/>	192.168.0.125 (TEST)	Антивірус не виявлено
<input type="checkbox"/>	192.168.0.147 (ZILLYA1.zillya)	Встановлено Zillya! Антивіру...
<input type="checkbox"/>	192.168.0.157 (WindoSPc.zill...	Встановлено Zillya! Антивіру...
<input type="checkbox"/>	192.168.0.159 (AVTEST3)	Антивірус не виявлено
<input type="checkbox"/>	192.168.0.161 (avtest.zillya)	Антивірус не виявлено
<input type="checkbox"/>	192.168.0.162 (AVSORT)	Антивірус не виявлено
<input type="checkbox"/>	192.168.0.163 (TV)	Антивірус не виявлено
<input type="checkbox"/>	192.168.0.164	Антивірус не виявлено
<input checked="" type="checkbox"/>	192.168.0.171 (TESTING_PC2)	Антивірус не виявлено

 Оновити     Додати ПК     Вибрати все     Зняти вибране

[Назад](#)    [Далі](#)    [Відміна](#)


Для встановлення захисту на окремих обраних Вами комп'ютерах натисніть, будь ласка, Зняти все, та відмітьте галками обрані Вами для захисту ПК. Після вибору комп'ютерів натисніть кнопку Далі для продовження.

5. Розпочнеться віддалена установка Клієнтських частин продукту на обрані Вами комп'ютери. Рекомендуємо зачекати її завершення:

Віддалена установка Клієнтів Zillya!

## Виконується установка Zillya! Антивірус для Бізнесу на комп'ютери мережі

Майстер встановлює Zillya! Антивірус для Бізнесу на комп'ютери. Це може зайняти деякий час. Будь ласка, зачекайте.

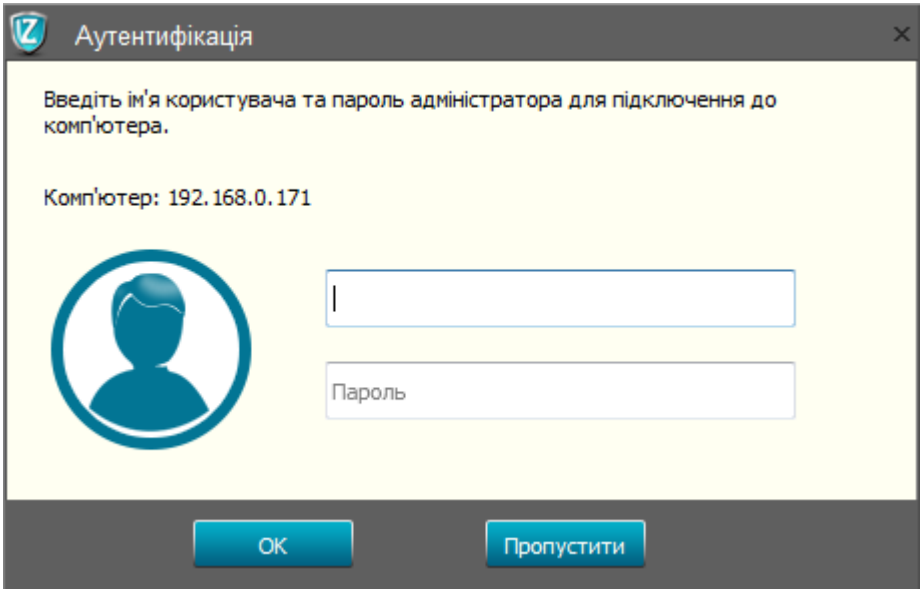
 68%

№	Комп'ютери:	Статус
1	192.168.0.171 (TESTING_PC2)	68% виконано

Назад   Далі   Відміна

6. В процесі установки Клієнтів може відобразитися вікно аутентифікації. Воно з'являтиметься щоразу з початком встановлення Клієнтської частини на комп'ютер з заданими логіном та паролем облікового запису Адміністратор.

Рекомендуємо Вам вказати логін та пароль для кожного комп'ютера, визначивши його за вказаним у даному вікні IP, та натиснути кнопку ОК для продовження:





7. Про завершення процесу віддаленої установки Клієнтських частин продукту Zillya! Антивірус для Бізнесу Ви будете поінформовані відповідним вікном. Натисніть Завершити для завершення роботи Майстера:

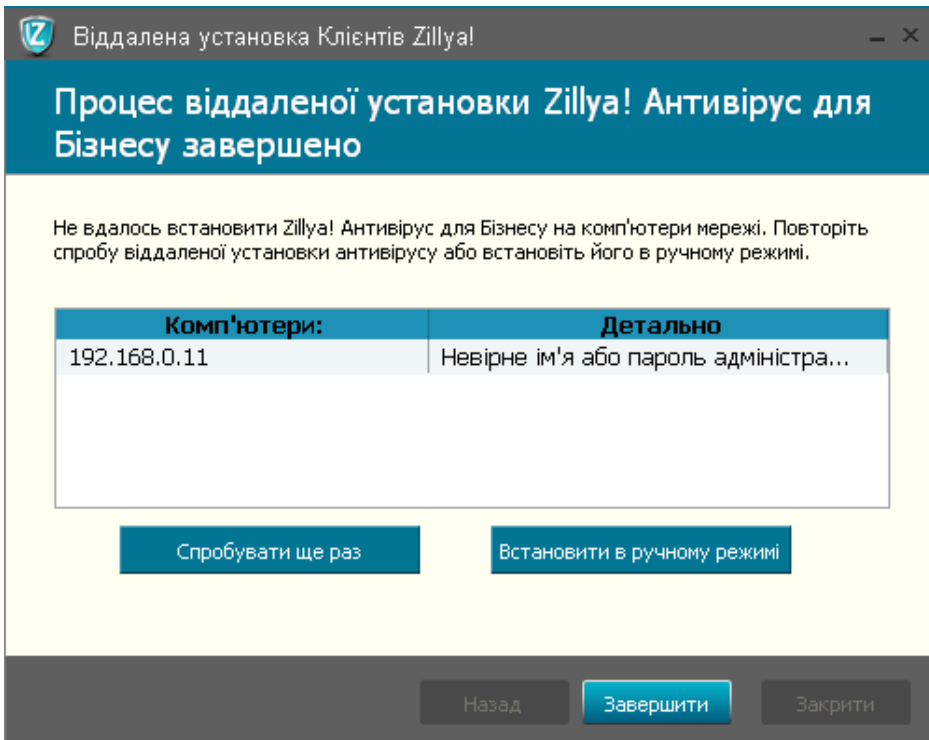


В процесі використання Zillya! Антивірус для Бізнесу Ви також можете викликати Майстер віддаленої установки Клієнтів за Вашим бажанням в будь який час у разі необхідності встановлення Клієнтських частин на додаткові комп'ютери.

Це можна зробити з Панелі адміністратора, натиснувши **Встановити захист на ПК**.

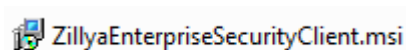
### 3.2.3. Установка клієнтів «вручну»

У випадку, якщо на певні обрані Вами для встановлення захисту комп'ютери не вдалось встановити Клієнтські частини віддалено, наприкінці процесу інсталяції Клієнтських частин Вам буде відображене наступне повідомлення:



Після натиснення кнопки **Встановити в ручному режимі**, відкриється папка з інсталяційним пакетом Клієнтської частини, який Ви можете використати для встановлення захисту «вручну» на обраних ПК.

Для встановлення Клієнта «вручну» Вам необхідно скористатися лише файлом `ZillyaEnterpriseSecurityClient.msi`:



Скопіюйте даний файл на обраний Вами комп'ютер-клієнт та запустіть його для встановлення Клієнтської частини.

Також Ви можете знайти інсталяційний пакет Клієнтської частини на системному диску комп'ютера, на якому встановлена Серверна частина Zillya! Антивірус для Бізнесу, за наступним шляхом:

`\Program Files\Common Files\Zillya! Enterprise Security\`

В даній папці розмішуватиметься 3 файли, з якого Вам для встановлення Клієнтської частини необхідним є лише `ZillyaEnterpriseSecurityClient.msi`.

## 4. Використання Zillya! Антивірус для Бізнесу

### 4.1. Сканування


#### 4.1.1. Види сканування

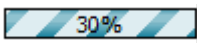
**Швидке сканування** – це перевірка найбільш уразливих ділянок системи на наявність зловмисним об'єктів.

**Повне сканування** – це повна перевірка комп'ютера на наявність зловмисних об'єктів. Zillya! перевіряє об'єкти на всіх дисках, в тому числі на змінних носіях.

**Вибіркове сканування** – це перевірка комп'ютера з урахуванням налаштувань користувача.

#### 4.1.2. Запуск сканування з Панелі адміністратора

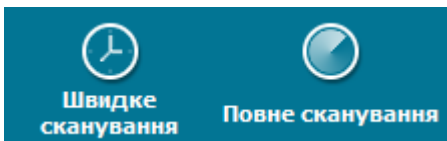
Запустити сканування на окремому комп'ютері Ви можете з Панелі адміністратора, натиснувши іконку з лупою  напроти обраного комп'ютера. У цьому випадку запуститься швидке сканування і на місці іконки та поточної дати з'явиться індикатор процесу сканування, напр.:



Одразу по завершенню процесу установки продукту Zillya! Антивірус для Бізнесу в локальній мережі на захищених комп'ютерах автоматично запускається швидке сканування.

Процес сканування графічно не відображається на комп'ютерах -клієнтах.

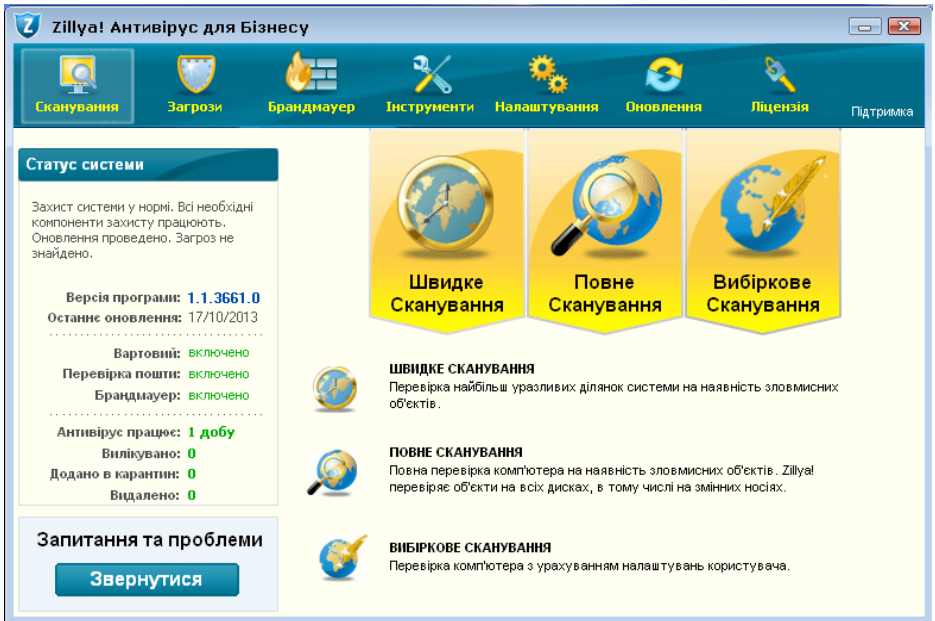
Кнопки для швидкого запуску різних видів сканування на обраних Клієнтах розміщені у верхньому меню Панелі адміністратора та такий мають вигляд:



Також Ви можете створити групу комп'ютерів за запустити сканування для цілої групи.

### 4.1.3. Запуск сканування з Клієнтської частини

Користувач може запустити сканування безпосередньо з Клієнтської частини, з Головного вікна програми, і його результати будуть передані Панелі адміністратора по завершенню процесу сканування:



По завершенню процесу сканування Користувач може дочекатися застосування дій над загрозами (у разі виявлення таких) з Панелі адміністратора адміністратором мережі або застосувати дії над загрозами самостійно, якщо це не заблоковано адміністратором.

## 4.2. Дії над загрозами:

### 4.2.1. Характеристика дій, що застосовуються до загроз

**Лікувати** – це видалення зловмисного коду з інфікованих файлах та відновлення їх коректного функціонування.

**Карантин** – це шифрування та переміщення інфікованих файлів до прихованих системних папок з можливістю їх відновлення у разі крайньої необхідності за бажанням і відповідною командою користувача у майбутньому.

**Видалити** – це повне та безповоротне видалення інфікованих файлів.

**Ігнорувати** – це ігнорування інфікованих файлів.

**Відновити** – це відновлення інфікованих файлів до початкового стану та початкового розміщення на диску.

**У винятки** – це переміщення файлів до списку таких, які ігноруються програмою Zillya! Антивірус для Бізнесу.

**Приховати** – це приховування інфікованих файлів до наступного сканування.


### 4.2.2. Застосування дій над загрозами з Панелі адміністратора

Усі дії щодо знайдених загроз на комп'ютерах-клієнтах Ви можете застосовувати з Панелі адміністратора.

У разі виявлення загроз на Клієнтах Панель адміністратора інформує Вас кількома шляхами:

1. Відповідним повідомленням у блоці Поточний стан мережі, наприклад:

**Поточний стан мережі: є проблеми (1 комп'ютерів)**

2. Відповідною іконкою  у блоці інфікованого комп'ютера.

Радимо застосовувати дії до знайдених загроз згідно наступних рекомендацій:

1. Оберіть інфікований ПК. Для цього рекомендуємо скористатися одним зі способів:

- а) зайти в Моя компанія -> Всі комп'ютери та знайти інфікований комп'ютер за допомогою відповідних іконок;

- b) відкрити Головне вікно Панелі адміністратора -> натиснути посилання Заражені комп'ютери у блоці Загрози в мережі;

2. Натиснути на блок зараженого комп'ютера. Він може виглядати так:



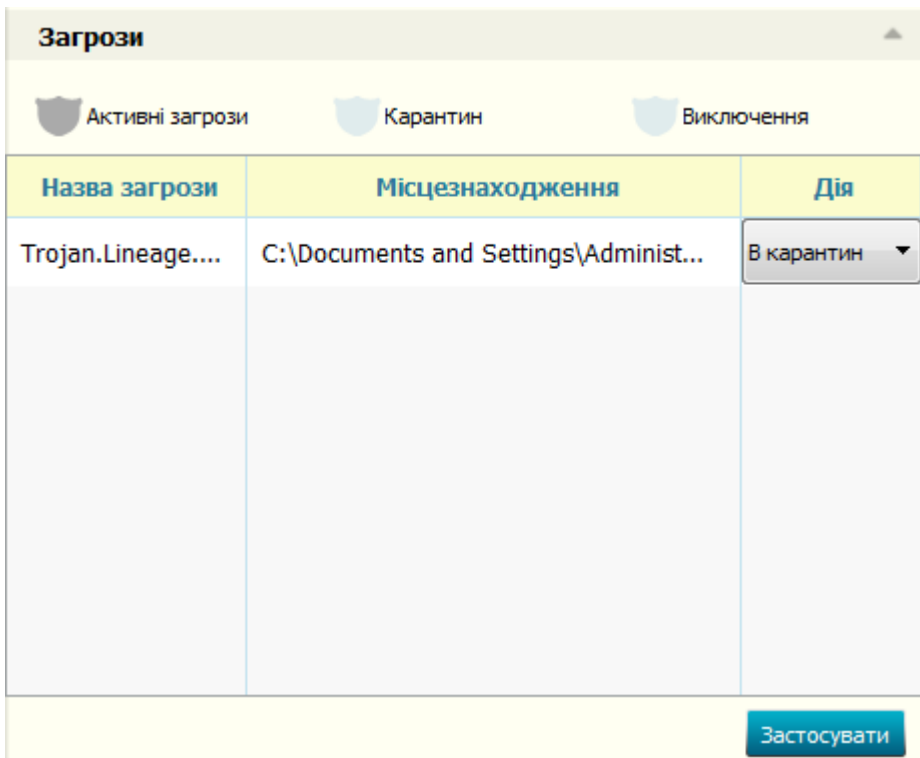
TESTING\_PC2 Всі комп'ютери  
192.168.0.171  
2.0.0.1556  17 жовт. 

3. Справа з'явиться 5 панелей, що розкриваються. Натисніть на Поточний стан: є проблеми:

Поточний стан: є проблеми	
Компонент захисту	Стан
Ліцензія	<a href="#">назначена</a>
Вартовий	<a href="#">увімкнено</a>
Перевірка пошти	<a href="#">увімкнено</a>
USB захист	<a href="#">увімкнено</a>
Брандмауер	<a href="#">увімкнено</a>
Web-фільтр	<a href="#">увімкнено</a>
Загрози	<a href="#">1 активних загроз</a>
Вірусні бази	<a href="#">нові</a>

4. Натисніть на посилання напроти Загрози (напр.: [1 активних загроз](#) );

5. Натисніть кнопку Застосувати у блоці Загрози, що відкриється:



Продукт Zillya! Антивірус для Бізнесу автоматично підбирає найбільш оптимальні дії для кожної знайденої загрози.

Після натиснення кнопки Застосувати знайдені загрози будуть знешкоджені і стан захисту знову прийде до норми, якщо немає інш завад цьому. Про безпеку в мережі Ви будете поінформовані відповідним повідомленням:

Поточний стан мережі: захист в нормі

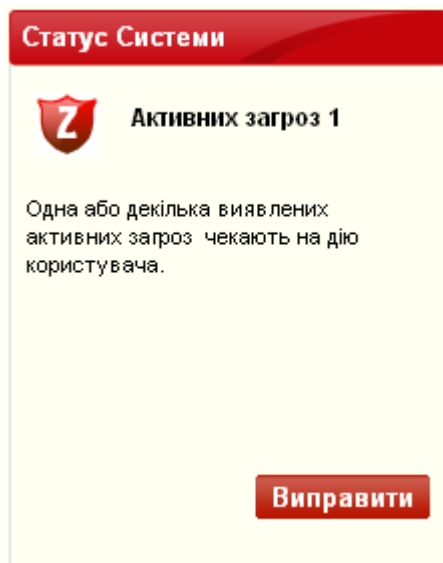
### 4.2.3. Застосування дій над загрозами з Клієнтської частини

Користувач комп'ютера-клієнта теж може застосовувати дії до знайдених загроз, якщо ці налаштування не заборонені адміністратором, тобто на них не встановлено пароль.


Для застосування дій до знайдених загроз на Клієнтських частинах необхідно перейти у закладку Загрози -> підпункт Активні загрози.

Перехід у вказаний підпункт здійснюється одним з наступних методів:

1. Натисненням кнопки Виправити у блоці Статус Системи:



**Статус Системи**

 **Активних загроз 1**

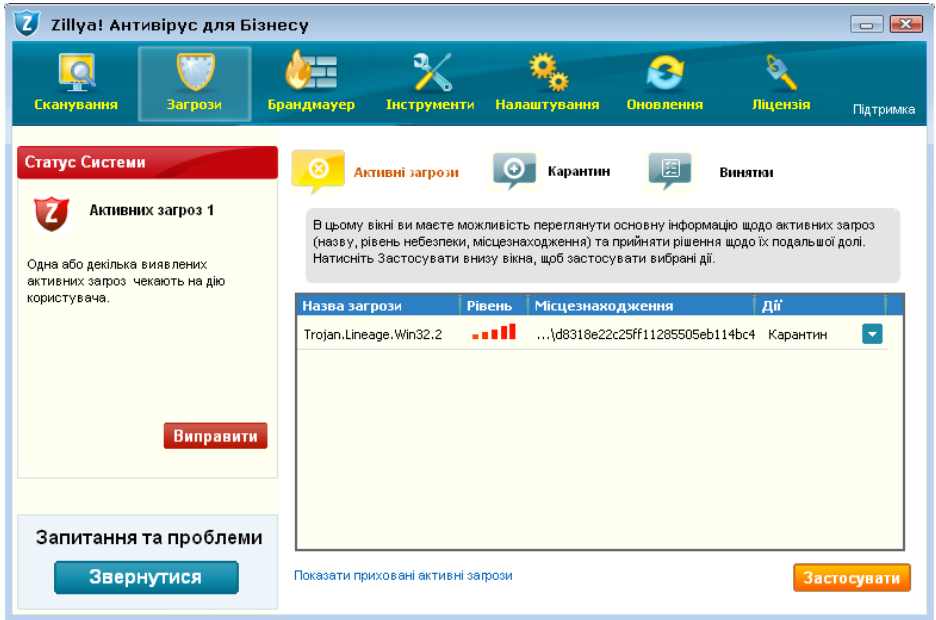
Одна або декілька виявлених активних загроз чекають на дію користувача.

**Виправити**



2. Натисненням закладки Загрози та переходом у підпункт Активні загрози (обраний за замовчуванням) у верхньому меню головного вікна програми.

У даному вікні необхідно натиснути кнопку Застосувати внизу вікна:



Таким чином дії до загроз будуть застосовані. Інформація про це також передається Панелі адміністратора, де її можна буде переглянути.

Навіть якщо дії до знайдених загроз не застосовуються одразу, продукт Zillya! Антивірус для Бізнесу **блокує знайдені загрози** та очікує подальших команд для них. Таким чином загрози не наносять шкоди, а «утримуються» антивірусом до застосування інших дій.

## 5. Оновлення продукту Zillya! Антивірус для Бізнесу


### 5.1. Вірусні бази

#### 5.1.1. Оновлення Вірусних баз з Панелі адміністратора

Оновлення Вірусних баз Zillya! викликається з Панелі адміністратора кількома способами:

1. Натисненням кнопки Оновити вірусні бази у головному верхньому меню:



2. Натисненням іконки  у блоці обраного Вами комп'ютера.

Зліва від даної іконки відображається поточна версія Вірусних баз на даному комп'ютері, напр.: **2.0.0.1556** .

3. Вибором комп'ютеру з застарілими базами та натисненням з панелі Поточний стан: є проблеми на посиланні напроти Вірусні бази.

Про необхідність оновлення Вірусних баз Zillya! на одному або кількох Клієнтах локальної мережі Ви будете поінформовані відповідним повідомленням у Поточному стані мережі та у блоках проблемних комп'ютерів.

### **5.1.2. Оновлення Вірусних баз з Клієнтської частини**


Оновлення Вірусних баз Zillya! за замовчуванням доступне з Клієнтської частини та може бути запущене Користувачем комп'ютера-клієнта, якщо ці налаштування не захищені паролем адміністратора з Панелі адміністратора.

Викликати оновлення Вірусних баз у разі їх застарівання з Клієнту можна наступними способами:

1. Зі сплеш-вікна, що відображається з трею та повідомляє про застарілість Вірусних баз Zillya!, натиснувши на посилання Виправити проблему:

**Zillya!**

**БАЗИ ЗАСТАРІЛИ!**



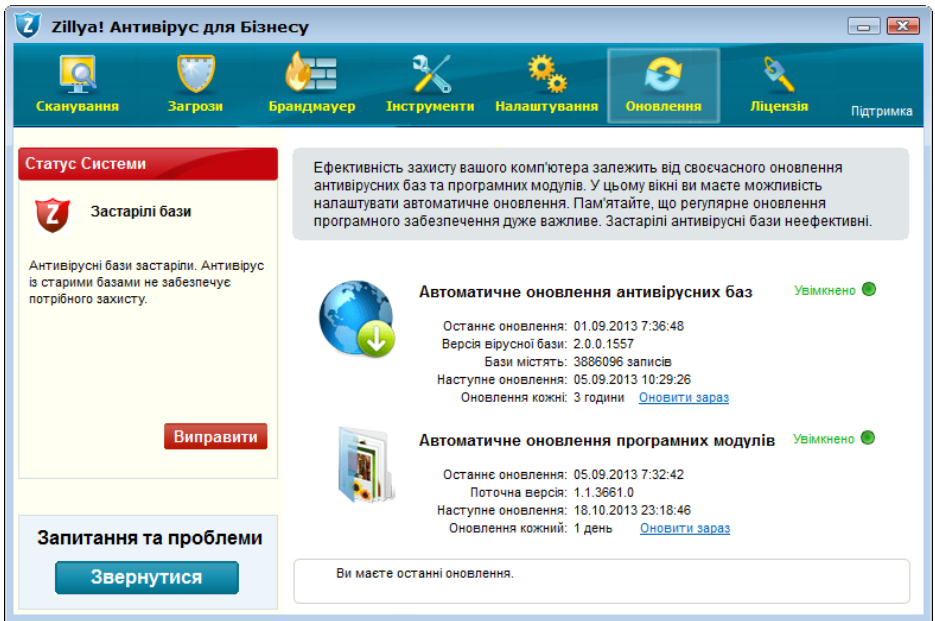
**УВАГА!**

Бази антивірусу на  
Вашому комп'ютері **ЗАСТАРІЛИ!**

Антивірус із застарілими базами  
не зможе знаходити нові віруси  
та шпигунські програми!

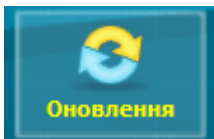
[Виправити  
проблему](#)      [Нагадати  
пізніше](#)

2. З головного вікна Клієнтської частини, натиснувши на кнопку виправити у Статусі системи та на посилання Оновити зараз в блоці Автоматичне оновлення антивірусних баз у вкладці Оновлення, яка відкриється після натиснення кнопки:



Інформація щодо оновлення Вірусних баз на даному комп'ютері-клієнті буде передана до Панелі адміністратора.

Також Користувач може запустити оновлення Вірусних баз на Клієнтській частині, не очікуючи повідомлення про їх застарівання, за власним бажанням. Запуск оновлення Вірусних баз Zillya! завжди доступний з вкладки Оновлення:



та викликається натисненням на посиланні Оновити зараз: [Оновити зараз](#) в блоці Автоматичне оновлення антивірусних баз, напр.:



### Автоматичне оновлення антивірусних баз

[Увімкнено](#)

Останнє оновлення: 03.10.2013 7:47:46

Версія вірусної бази: 2.0.0.1557

Бази містять: 3886096 записів

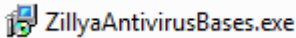
Наступне оновлення: 08.10.2013 10:58:54

Оновлення кожні: 3 години [Оновити зараз](#)

### 5.1.3. Оновлення Вірусних баз без підключення до Інтернет

У якості екстреного способу оновлення Вірусних баз на Клієнті, що не має підключення до мережі Інтернет, використовується офф-лайн оновлення Вірусних баз Zillya!

Офф-лайн оновлення Вірусних баз виконується за допомогою встановлення повного комплекту Вірусних баз. Файл, що є повним комплектом Вірусних баз Zillya!, має назву ZillyaAntivirusBases.exe:



Він доступний цілодобово на нашому офіційному сайті <http://www.zillya.ua> у розділі Підтримка та оновлюється щоденно мінімум 1 раз на добу.

Для оновлення Вірусних баз на комп'ютері-клієнті, що не має підключення до мережі Інтернет, необхідно завантажити файл ZillyaAntivirusBases.exe з нашого офіційного сайту, розділу Підтримка, напр.:



[Zillya! Антивірусні Бази 2.0.0.1557 від 18.10.2013](#)

Для оновлення вірусних баз та усунення несправностей

використовуючи комп'ютер, який підключений до Інтернету, скопіювати будь-яким методом даний файл на бажаний Вами комп'ютер та запустити цей файл. Далі рекомендуємо Вам дотримуватись інструкцій Майстра встановлення, який запуститься з запуском вказаного файлу.

## 5.2. Оновлення програмних модулів

### 5.2.1. Оновлення програмних модулів з Панелі адміністратора

Оновлення програмних модулів з Панелі адміністратора доступне з верхнього меню головного вікна та викликається натисненням на кнопку Оновити програму:

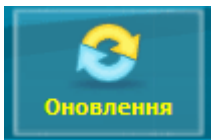


Також про застарівання програмних модулів на одному або кількох Клієнтах локальної мережі Ви будете поінформовані відповідним повідомленням у Поточному стані мережі та у блоках проблемних комп'ютерів.

### 5.2.2. Оновлення програмних модулів з Клієнтської частини

На кожній Клієнтській частині також за замовчуванням можна викликати оновлення програмних модулів.

Для цього рекомендуємо перейти у закладку Оновлення:



та натиснути на посиланні Оновити зараз: [Оновити зараз](#) у блоці Автоматичне оновлення програмних модулів, напр.:



#### Автоматичне оновлення програмних модулів

Останнє оновлення: 05.09.2013 7:32:42  
Поточна версія: 1.1.3661.0  
Наступне оновлення: 18.10.2013 23:18:46  
Оновлення кожний: 1 день [Оновити зараз](#)

Інформація про успішне оновлення програмних модулів буде передана до Панелі адміністратора.

## 6. Управління Ліцензією

### 6.1. Активація комерційної Ліцензії

Активація комерційної ліцензії на продукт Zillya! Антивірус для Бізнесу доступна Вам на 2-х етапах використання програми:

1. В процесі встановлення продукту у Вашій локальній мережі. Для цього рекомендуємо слідувати інструкціям, описаним в пункті **3.1.3.** даної Інструкції користувача.
2. В процесі використання продукту. Ви можете викликати вікно Активація ліцензії повторно, натиснувши на посиланні Активувати [Активувати](#) в блоці Ліцензія в головному вікні Панелі адміністратора, напр.:




Для активації нової ліцензії дотримуйтесь, будь ласка, рекомендацій, наданих в пункті **3.1.3.** даної Інструкції користувача.

### 6.2. Призначення Ліцензій на Клієнтських комп'ютерах

В процесі централізованого віддаленого встановлення Клієнтських частин продукту Zillya! Антивірус для Бізнесу у Вашій локальній мережі ліцензія призначається автоматично для максимально можливої кількості Клієнтів. В майбутньому Ви можете самостійно знімати, назначати та переназначати ліцензії для кожного комп'ютера-клієнта з Панелі адміністратора.

Про необхідність призначення ліцензії для одного або кількох Клієнтів Вашої локальної мережі Ви будете поінформовані стандартним повідомленням Поточний стан мережі: є проблеми, напр.:

Поточний стан мережі: є проблеми (1 комп'ютерів)

та відповідною іконкою  у блоці проблемного комп'ютера.

Призначення ліцензії для Клієнта здійснюється наступними способами:

1. З контекстного меню, натисненням на блок проблемного комп'ютера правою кнопкою миші, напр.:



Для призначення ліцензії для обраного Клієнта необхідно натиснути пункт Встановити ліцензію: **Встановити ліцензію** в контекстному меню.

2. З панелі Поточний стан: є проблеми:



Для встановлення ліцензії радимо натиснути на дану панель та на посилання відсутня: **ВІДСУТНЯ** напроти пункту Ліцензія:

Ліцензія **ВІДСУТНЯ**

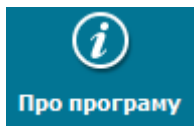
Ліцензія буде успішно призначена для обраного Клієнту у випадку, якщо ліміт комп'ютерів для Вашої ліцензії не перевищений.

Загальну інформацію по активовану у Вашій локальній мережі ліцензію для продукту Zillya! Антивірус для Бізнесу Ви можете переглянути у головному вікні Панелі адміністратора, блоці Ліцензія, напр.:

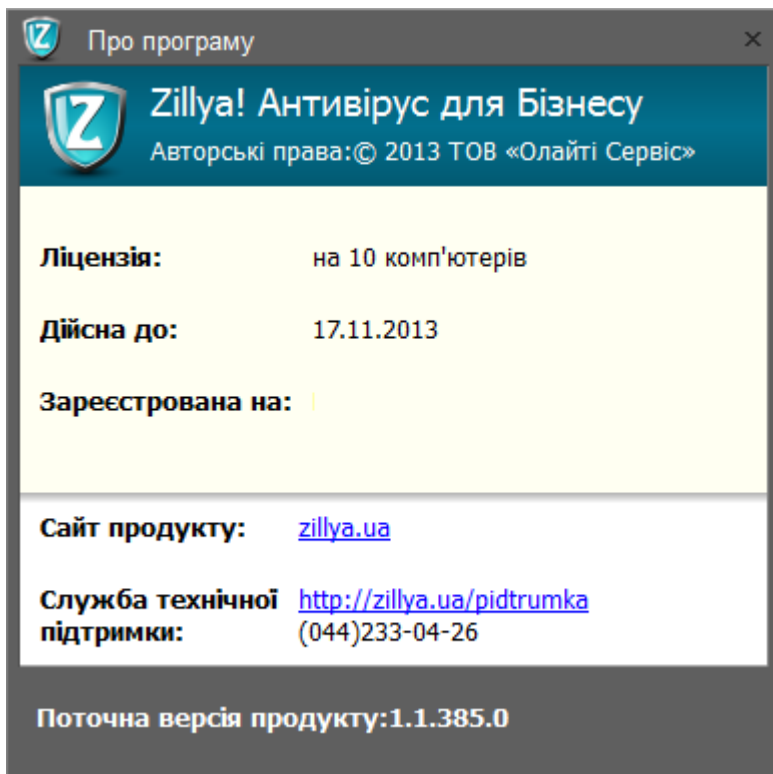




та у вікні Про програму, що викликається натисненням на кнопку Про програму:



у головному верхньому меню Панелі адміністратора, напр.:



## 7. Захист паролем Панелі адміністратора та Клієнтських частин

### 7.1. Встановлення та зміна паролю для Панелі адміністратора

Усі дії щодо встановлення та зміни паролів для захисту Сервера та Клієнтських частин застосовуються у вікні Налаштування, яке викликається натисненням на кнопку Налаштування у верхньому меню головного вікна Панелі адміністратора:



Призначити та змінити пароль для підключення до Серверу Ви можете в блоці Параметри захисту сервера у додатковому вікні, яке відобразиться після натиснення кнопки Налаштування:

### Параметри захисту сервера

Введіть пароль для підключення до серверу

Показати пароль

У наданих полях вкажіть, будь ласка, Ваш новий пароль та підтвердьте його повторним вводом.

Цей пароль разом з IP-адресою серверу використовується для аутентифікації адміністратора під час запуску Панелі адміністратора та для віддаленого доступу до Серверу.

## 7.2. Встановлення та зміна паролю для Клієнтських частин

Встановлення та зміна паролю для Клієнтів також доступні у вікні Налаштування:

### Параметри захисту клієнта

Введіть пароль для зміни налаштувань на клієнтських комп'ютерах

 Показати пароль

Для задання нового паролю на Клієнтські частини необхідно двічі ввести новий пароль у наданих для цього полях.

Заданий адміністратором пароль для Клієнтів використовується для захисту налаштувань адміністратора на них та запитуватиметься щоразу при спробі змін налаштувань Клієнта безпосередньо з комп'ютера-клієнта, на якому встановлено дану Клієнтську частину.

## 8. Компоненти захисту Zillya! Антивірус для Бізнесу:

### 8.1. Файловий монітор «Вартовий»

#### 8.1.1. Опис файлового монітору «Вартовий»

**Файловий монітор Вартовий** – це система перевірки файлів у реальному часі, що виявляє віруси та інші шкідливі програм, які намагаються проникнути на комп'ютер. Вартовий відстежує запущені процеси, файли, що створюються і відкриваються, ефективно блокує і видаляє загрози «на льоту», не даючи вірусу створити свої файли на диску.

Тобто, Вартовий є он-лайн сканером, що постійно убезпечує комп'ютер від можливих загроз з різних джерел.

#### 8.1.2. Налаштування «Вартового» з Панелі адміністратора

Файловий монітор Вартовий є увімкненим на кожному Клієнті згідно налаштувань «за замовчуванням» як важливий елемент захисту комп'ютера.

Вимкнення монітору Вартовий здійснюється з Панелі адміністратора двома способами:

1. Натисненням на блок обраного Вами комп'ютера, після чого на панель Поточний стан: захист у нормі. Серед компонентів захисту, що містить дана панель, Ви можете обрати Вартовий та натиснути на посилання увімкнуто напроти нього: [увімкнено](#).

Таким чином модуль Вартовий буде вимкнено на обраному Вами ПК, напр.:

Поточний стан мережі: є проблеми (1 комп'ютерів)

Всі комп'ютери TEST\_PC3 Всі комп'ютери

**TEST\_PC3** Всі комп'ютери  
192.168.0.149  
2.0.0.1550 10%

Zillya! Антивірус для Бізнесу

**Поточний стан: є проблеми**

Компонент захисту	Стан
Ліцензія	назначена
Вартовий	<b>вимкнено</b>
Перевірка пошти	<a href="#">увімкнено</a>
USB захист	<a href="#">увімкнено</a>
Брандмауер	<a href="#">увімкнено</a>
Web-фільтр	<a href="#">увімкнено</a>
Загрози	немає активних загроз
Вірусні бази	нові

2. Натисненням на блок обраного Вами комп'ютера, після чого на панель Налаштування. В даній панелі Ви можете обрати вкладку Сканування та у ній вимкнути Вартовий, натиснувши на посилання Увімкнуто напроти нього:

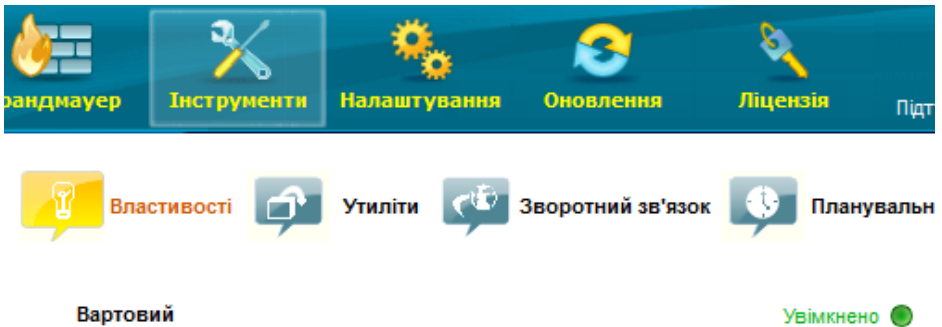
**Вартовий** [Увімкнуто](#)

Ми наполегливо не радимо вимикати Файловий монітор Вартовий зі зрозумілих причин без нагальної для цього потреби та, у разі зміни його налаштувань, повернути налаштування до базових, щойно з'явиться така можливість.

### 8.1.3. Налаштування «Вартового» з Клієнтської частини

Зміна налаштувань файлового монітору Вартовий доступна також у Клієнтській частині для кожного окремого комп'ютера-клієнта.

Для зміни налаштувань компоненту Вартовий Користувач може перейти у закладку Інструменти головного вікна Клієнтської частини, підпункт Властивості та натиснути на Увімкнено напроти компоненту Вартовий:



Вимкнення компоненту Вартовий будь-яким способом є небажаним!

## 8.2. Брандмауер

### 8.2.1. Опис Брандмауеру

Брандмауер Zillya! є брандмауером програмного рівня.

Він забезпечує:

1. Контроль за доступом додатків до мережі. Брандмауер відстежує всі спроби додатків отримати доступ до мережі – як вхідний трафік, так і вихідний.
2. Захист від несанкціонованих зовнішніх атак. За замовчуванням брандмауер дозволяє додаткам тільки вихідний трафік. Це дозволяє захистити систему від спроб отримати до неї доступ ззовні, оскільки будь-які вхідні запити блокуватимуться.
3. Вбудований набір правил. Програма містить вбудовану базу даних, яка містить усі необхідні правила дозволу або блокування (за бажанням користувача) стандартних системних сервісів або протоколів (NetBios, DHCP, DNS і т.п.) для роботи з мережею. З їхньою допомогою можна дозволяти або забороняти мережеву активність по таким протоколам та не розбиратися у тонкощах їхньої роботи.
4. Можливість встановлювати загальні налаштування для всіх додатків в системі. В Zillya! Антивірус для Бізнесу є можливість встановлювати загальні налаштування для всіх додатків. Наприклад, користувачу необхідно, щоб усі

додатки мали доступ до певного серверу. Для цього достатньо в цих налаштуваннях прописати правило, яке буде дозволяти доступ до певної IP-адреси по певному порту. І вже не буде потрібно для кожного додатку створювати окремі правила доступу до цього серверу.

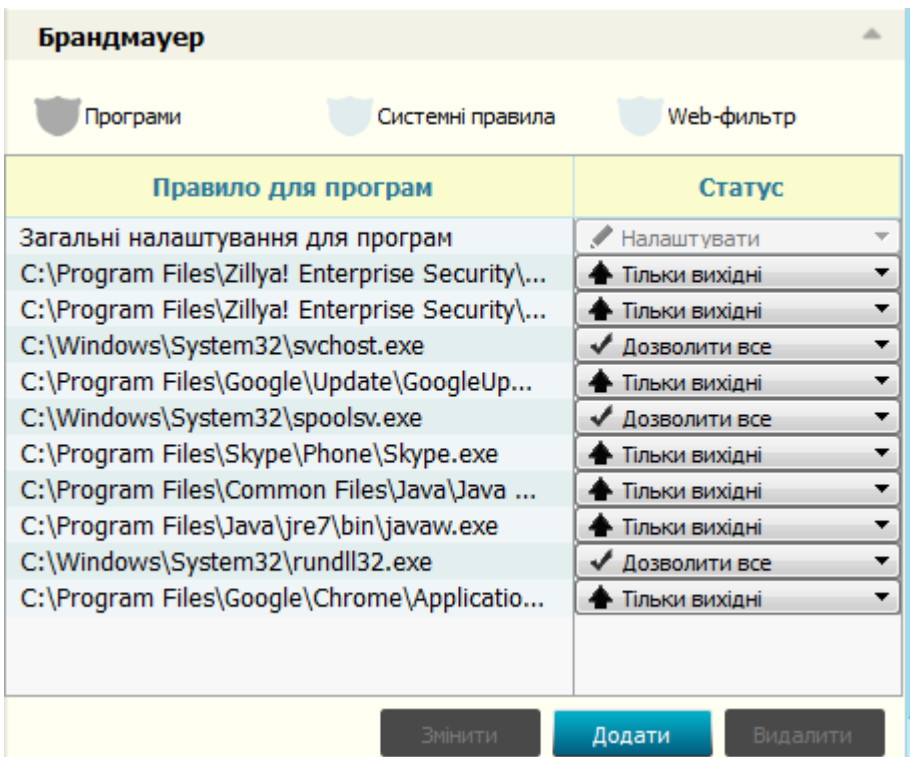
## 8.2.2. Налаштування Брандмауеру з Панелі адміністратора

Налаштування Брандмауеру з Панелі адміністратора здійснюється окремо для кожного Клієнта згідно наступної послідовності дій:

1. Натисніть на блок бажаного Вами комп'ютера.
2. Перейдіть у панель Брандмауер:



3. Змініть налаштування Брандмауера до бажаних Вами:

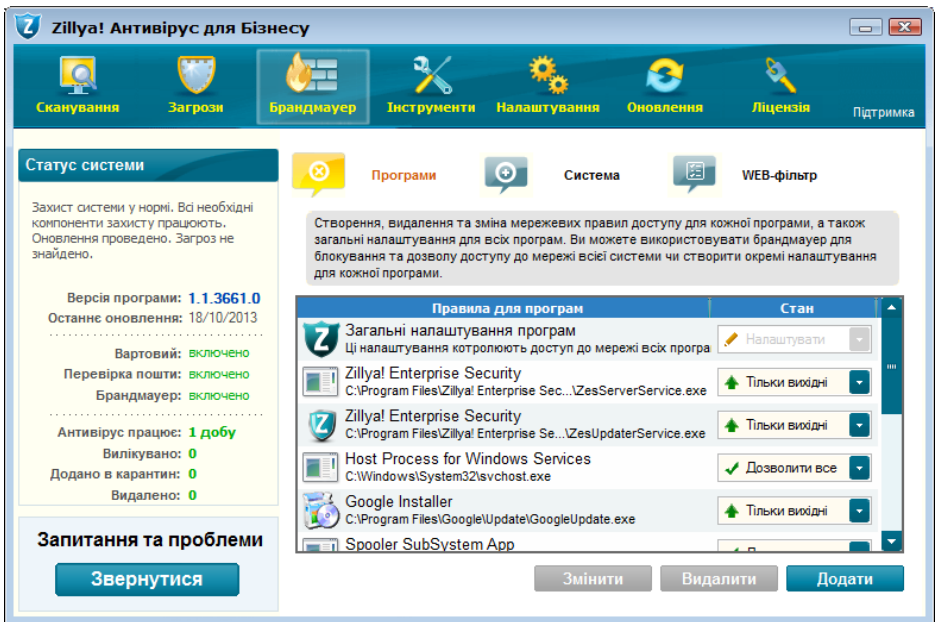


## 8.2.3. Налаштування Брандмауеру з Клієнтської частини

Налаштування Брандмауеру можуть бути змінені в Клієнтській частині, якщо це не заборонено адміністратором або якщо Користувач комп'ютера-клієнта володіє паролем, встановленим для Клієнтів адміністратором.

Змінити налаштування Брандмауера на Клієнті можна, дотримуючись наступної послідовності дій:

1. Відкрийте головне вікно Клієнтської частини продукту Zillya! Антивірус для Бізнесу та перейдіть у розділ Брандмауер:



2. Змініть налаштування Брандмауера до бажаних Вами.

Ми не радимо змінювати будь-які налаштування Брандмауера без нагальної потреби для цього!

## 8.3. WEB-фільтр:

### 8.3.1. Опис WEB-фільтру

WEB-фільтр Zillya! використовується для захисту HTTP-трафіку.

Його можливості:

1. Блокування небезпечних сайтів. В Zillya! Антивірус для Бізнесу є можливість блокувати доступ до потенційно небезпечних сайтів, блокуючи його завантаження при перегляді в браузері. При цьому користувач бачить відповідне повідомлення;
2. Блокування потенційно небезпечного контенту з підозрілих сайтів. Деякі сайти додаються до бази Zillya! Антивірус для Бізнесу як підозрілі, або як сайти, які мають шкідливий контент. Якщо сайт знаходиться в такому списку, ви матимете змогу його відвідувати, переглядати сторінки, зображення, але не матимете змогу завантажити з цього сайту програми, архіви, документи та інші файли, які потенційно можуть нести загрозу вашому комп'ютеру.
3. Створення власного списку сайтів, що блокуються. У WEB-фільтрі є можливість крім вбудованої бази сайтів, що блокуються, створити власний список таких сайтів, які користувач за певних причин вважатиме шкідливими. До власної бази застосовні ті ж самі правила, що і до загальної бази. Доступні два режими: повне блокування сайта та блокування завантажень з сайта.

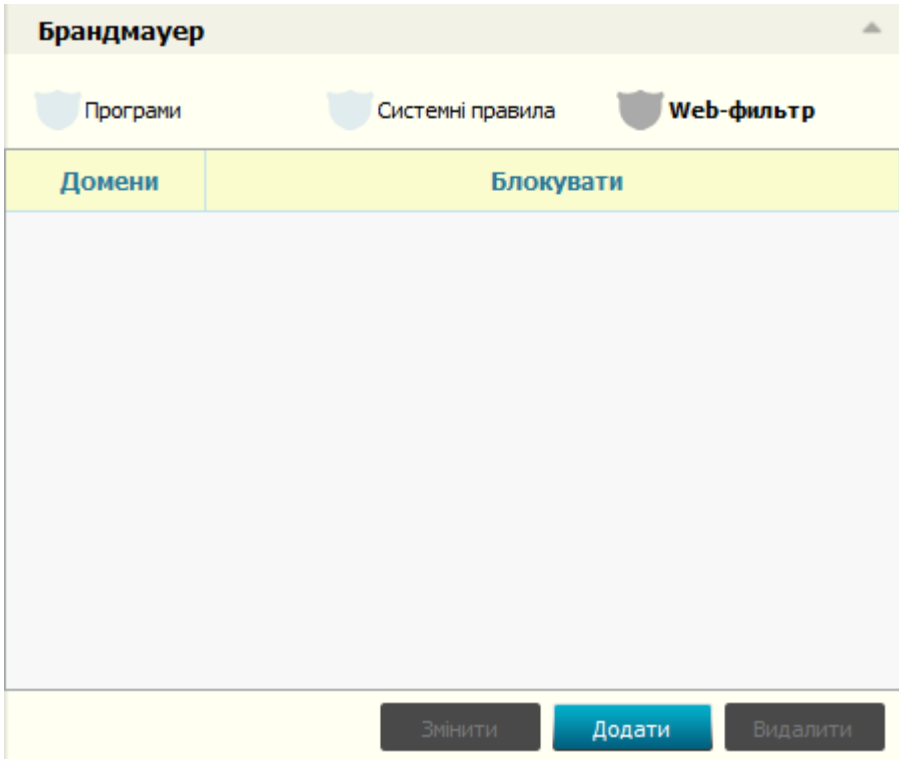
### 8.3.2. Налаштування WEB-фільтру з Панелі адміністратора

Зміна налаштувань WEB-фільтру в Панелі адміністратора доступна після реалізації наступних кроків:

1. Натисніть на блок бажаного Вами комп'ютера.
2. Перейдіть у панель Брандмауер.



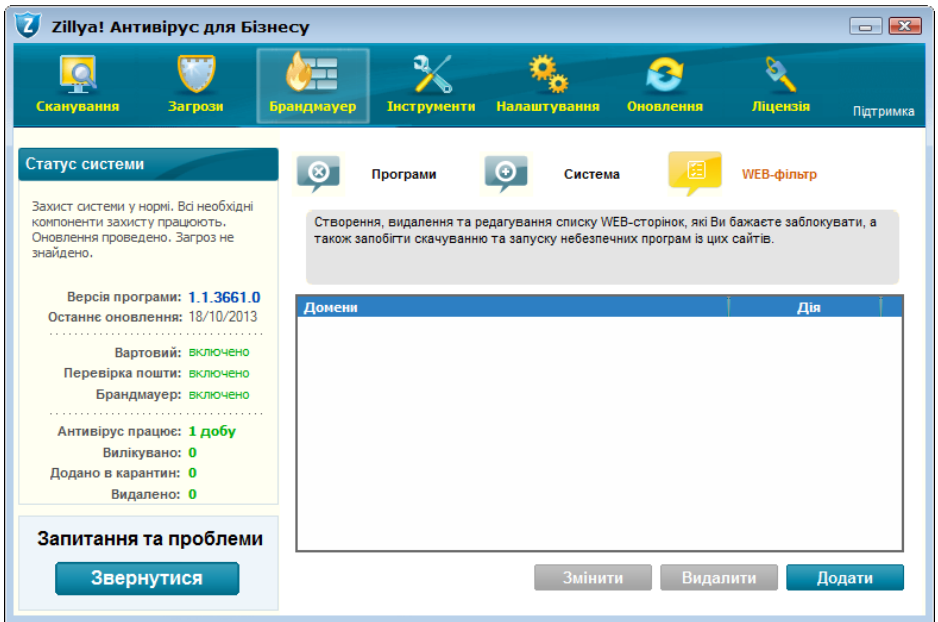
3. В панелі Брандмауера необхідно обрати підпункт WEB-фільтр:



Використовуючи дане вікно, Ви можете блокувати доступ до обраних Вами ресурсів для певних комп'ютерів-клієнтів.

### 8.3.3. Налаштування WEB-фільтру з Клієнтської частини

Налаштування WEB-фільтру доступні на Клієнтах у закладці Брандмауер, підпункті WEB-фільтр:



## 8.4. USB-захист

### 8.4.1. Опис USB-захисту

**USB-захист** – це додатковий модуль для захисту Клієнтів від загроз, що поширюються через підключення змінних носіїв інформації: Flash-накопичувачів тощо.

### 8.4.2. Налаштування USB-захисту з Панелі адміністратора

Зміна налаштувань USB-захисту з Панелі адміністратора здійснюється для кожного окремого комп'ютера-клієнта згідно наступної послідовності дій:

1. Натисніть на блок бажаного Вами комп'ютера.
2. Перейдіть у панель Поточний стан.
3. Серед Компонентів захисту у даній панелі оберіть USB-захист та натисніть посилання напроти нього:

USB захист


[увімкнено](#)

### 8.4.3. Налаштування USB-захисту з Клієнтської частини

Зміна налаштувань USB-захисту доступна також на кожному Клієнті. Для встановлення власних налаштувань модуля USB-захисту Користувач може відкрити головне вікно Клієнтської частини та перейти у закладку Інструменти.

В пункті перевіряти автозавантаження USB накопичувачів Користувач може обрати бажаний режим:

**Перевіряти автозавантаження USB накопичувачів**

Показувати вікно Zillya! Антивірус для Бізнесу 

## 9. Загальні налаштування продукту Zillya! Антивірус для Бізнесу

### 9.1. Сканування поштових повідомлень

Перевірка поштових повідомлень на Клієнтах здійснюється поштовим фільтром Zillya!

**Поштовий фільтр** перевіряє всі вхідні і вихідні поштові повідомлення на наявність шкідливих об'єктів, не допускаючи таким чином можливості для проникнення в систему загроз разом з електронним листом.

### 9.2. Зміна налаштувань з Панелі адміністратора

Для встановлення власних налаштувань Поштового фільтру з Панелі адміністратора радимо Вам використати один з наступних способів:

1. Натисніть на блок бажаного Вами комп'ютера. Перейдіть у панель Поточний стан та оберіть серед Компонентів компонент Перевірка пошти.

Після цього Вам стане доступною зміна налаштувань натисненням на посилання напроти даного Компоненту:

Перевірка пошти

увімкнено

2. Оберіть бажаний Вами комп'ютер. Розкрийте панель Налаштування напроти нього та, в закладці Сканування, змініть налаштування для Сканування поштових повідомлень до бажаних Вами:

Сканувати поштові повідомлення Увімкнено ●

Тільки вхідні

Тільки вихідні

Вихідні та вхідні

### 9.3. Зміна налаштувань з Клієнтської частини

Змінити налаштування для Поштового фільтру можна з Клієнту, перейшовши у закладку Інструменти, підрозділ Властивості та встановивши налаштування, бажані Користувачем:

Сканування поштових повідомлень Увімкнено ●

Виключно надіслані

Виключно вхідні

Вхідні та надіслані

## 10. Додаткові можливості Панелі адміністратора:

### 10.1. Управління групами комп'ютерів

В Панелі адміністратора доступна можливість формування різних груп комп'ютерів та призначення різних типів та часу сканування для кожної окремої групи.

Для формування групи комп'ютерів радимо використовувати блок Управління групами:

#### Управління групами

+ Створити групу

✎ Перейменувати

✕ Видалити групу

## 10.2. Статистика та історія

В головному вікні Панелі адміністратора доступний перегляд повної статистики щодо стану комп'ютерів локальної мережі. Для перегляду статистики радимо натиснути на заголовок Моя компанія:

Панель адміністратора Zillya! Антивірус для Бізнесу

Швидке сканування Повне сканування Оновити вірусні бази Оновити програму Журнал подій Встановити захист на ПК Налаштування Про програму

Виконати повне сканування для обраного комп'ютера (групи комп'ютерів)  
Поточний стан мережі: захист в нормі

**Моя компанія**  
Всі комп'ютери

**Управління групами**  
+ Створити групу  
✎ перейменувати  
✕ Видалити групу

**Загрози в мережі**

Заражені комп'ютери	0
Застарілі бази	0
Вимк. модулі захисту	0
Комп'ютери з проблемами	0

**Поширення загроз**

Trojan - 100.00%

**Ліцензія**

Тип ліцензії:	Комерційна
Дійсна:	17.11.2013
Призначено:	1 (з 10)
Активувати	Замовити

**Дії над загрозами**

Заблоковано:	0
Вилкнено:	0
У карантині:	2
Видалено:	0

**Вірусна активність**

**Безпека в мережі**

Оновлення на сервері:	-
Захищених ПК:	1
ПК он-лайн:	1

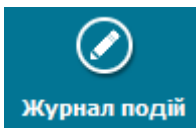
**Останні знайдені загрози**

№	Комп'ютер	Дата	Знайдено
1	TESTING_PC2	17/10/20...	4

**Загрози знайдені в мережі**

№	Вірус	Знайдено	Кіл-сть ПК
1	Trojan.Lineag...	4	1

Також переглянути історію по події у Вашій локальній мережі Ви можете, натиснувши на кнопку Журнал подій у верхньому меню головного вікна Панелі адміністратора:



Після натиснення на кнопку Журнал подій Вам відобразиться додаткове вікно з журналом та фільтрами, за допомогою яких Ви можете відкоригувати зручність перегляду інформації:

№	Статус	Дата та час	Комп'ютер	Подія
1	Інформ...	17/10/2013 ...		Вартовий увімкнений
2	Інформ...	17/10/2013 ...		Перевірка пошти увімкнена
3	Інформ...	17/10/2013 ...		Брандмауер увімкнений
4	Інформ...	17/10/2013 ...		Перевірка пошти увімкнена
5	Інформ...	17/10/2013 ...	TESTING_PC2	Перевірка пошти увімкнена
6	Інформ...	17/10/2013 ...	TESTING_PC2	Швидке сканування запущено
7	✓ Заверш...	17/10/2013 ...	TESTING_PC2	Швидке сканування завершено
8	! Попере...	17/10/2013 ...	TESTING_PC2	Виявлена загроза: Trojan.Lineage.Win32.2(C:\Documents and Se...
9	Інформ...	17/10/2013 ...	TESTING_PC2	Вартовий увімкнений
10	Інформ...	17/10/2013 ...	TESTING_PC2	Перевірка пошти увімкнена
11	Інформ...	17/10/2013 ...	TESTING_PC2	Брандмауер увімкнений

### 10.3. Вікно «Про програму»

У додатковому вікні Про програму, яке викликається способом, описаним у п. 6.2. даної Інструкції користувача, окрім зазначеної у п. 6.2. інформації Ви також можете переглянути такі дані:

- 1) Офіційний сайт продукту та Розробника;
- 2) Контакти Служби технічної підтримки користувачів;
- 3) Поточна версія Панелі адміністратора;
- 4) Вказані вище дані про Вашу ліцензію тощо.

## 11. Додаткові можливості Клієнтських частини:

### 11.1. Евристичний аналізатор

Технології евристичного аналізу використовуються для розпізнавання нових та невідомих загроз.

**Евристичний аналізатор** перевіряє файли за схожими характеристиками. При виявленні певної кількості схожих даних у файлі він приймає рішення, що дана програма схожа на шкідливу. Таким чином Zillya! Антивірус для Бізнесу може виявити шкідливі програми, які ще не були додані в антивірусну базу.

### 11.2. Диспетчер задач та Диспетчер автозавантаження

Zillya! Антивірус для Бізнесу містить додаткові модулі - **Диспетчер задач** та **Диспетчер автозавантаження**. Ці утиліти розширюють функціонал програми та допомагають користувачеві краще контролювати процеси в системі. Диспетчер задач необхідний для контролю над запущеними на комп'ютері програмами, а за допомогою Диспетчера автозавантаження можна переглядати інформацію про програми, які автоматично запускаються при старті Windows.

### 11.3. Планувальник

Вам не потрібно кожен день пам'ятати про те, що потрібно перевірити комп'ютер на наявність шкідливих програм.

Клієнти Zillya! Антивірус для Бізнесу містять функцію Планувальник.

**Планувальник** - це сканування персонального комп'ютера, яку можна налаштувати так, як буде найбільш зручно для Вас. Користувач може налаштувати автоматичне сканування одноразово, щодня, погодинно, щотижня або щомісяця.



## 12. Зворотній зв'язок

Наші спеціалісти завжди раді відповісти на усі Ваші питання та надати Вам всі бажані Вами консультації!

Якщо у вас виникли запитання стосовно продукту Zillya! Антивірус для Бізнесу, Ви до нас:

### **Відділ інтеграції корпоративних рішень Zillya!:**

- тел.: +38 (063) 233 04 26, +38 (044) 233 04 26

- email: [avcorp@zillya.com](mailto:avcorp@zillya.com)

### **Служба технічної підтримки користувачів Zillya!:**

- тел.: +38 (044) 233 05 24

- email: [support@zillya.com](mailto:support@zillya.com)

*Дякуємо Вам за довіру!*