Zillya!™ Антивірус для бізнесу

Інструкція користувача

Клієнтської частини

www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

ЗМІСТ

www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

1. Загальна характеристика Клієнтської частини

Клієнтська частина Zillya! Антивірус для Бізнесу – це складова продукту Zillya! Антивірус для Бізнесу, яка безпосередньо забезпечує захист комп'ютера, на якому вона встановлена, від шкідливого програмного забезпечення. Клієнтська частина забезпечує виявлення та знешкодження шкідливого програмного забезпечення, попереджає його проникнення на комп'ютер, тобто виконує функції антивірусного захисту на комп'ютері користувача.

Також клієнтська частина приймає через Сервер та виконує команди від Панелі адміністратора, звітує Серверу про події безпеки та інше.

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

Основними можливостями Клієнтської частини Zillya! Антивірус для Бізнесу є:

- **захист комп'ютера «он-лайн» в режимі реального часу** за допомогою системи перевірки файлів «на льоту», що виявляє віруси та інше шкідливе програмне забезпечення, яке намагаються проникнути на комп'ютер;
- **повний антивірусний функціонал**;
- **сканування знімних накопичувачів** (Flesh-карт тощо), що забезпечує технологія USB-захист;
- **контроль за доступом** встановлених на комп'ютері **додатків** до мережі та сторонніх додатків з мережі на комп'ютер. **Захист від несанкціонованих зовнішніх атак**. Брандмауер відстежує всі спроби додатків отримати доступ до мережі – як вхідний трафік, так і вихідний;
- **блокування небезпечних сайтів** та **потенційно небезпечного контенту** з підозрілих сайтів за допомогою WEB-фільтру. Доступна можливість створення власного списку сайтів, що блокуються.
- **перевірка усіх поштових повідомлень** на шкідливі об'єкти, яка гарантує, що жодна загроза не потрапить до системи разом з електронним листом;
- **евристичний аналіз**, який визначає нові віруси, записи для детектування яких ще відсутні в антивірусній базі та багато іншого.

www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

2. Системні вимоги

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

Операційна система:

- Windows XP (SP2, SP3) (32-х та 64-х бітні)
- Windows Vista (32-х та 64-х бітні)
- Windows 7 (також с SP1) (32-х та 64-х бітні)
- Windows 8 (також версія 8.1) (32-х та 64-х бітні)
- Windows 2003 Server (32-х та 64-х бітні)
- Windows 2008 Server (32-х та 64-х бітні)

Частота процесора: 1 ГГц або вище

Оперативна пам'ять: 512 Мб або більше

Місце на жорсткому диску: 120 Мб

www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

3. Компоненти Клієнтської частини

3.1. Файловий монітор 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.

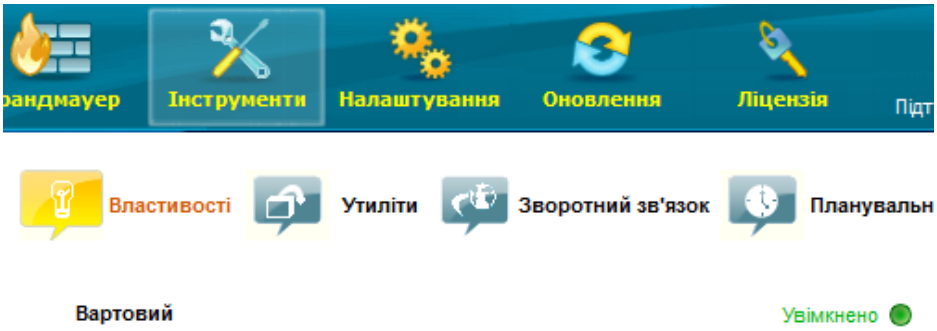
Тобто, Вартовий є он-лайн сканером, що постійно убезпечує комп’ютер від можливих загроз з різних джерел.

Налаштування «Вартового» з Клієнтської частини

Зміна налаштувань файлового монітору Вартовий доступна з Панелі Адміністратора програми Zillya! Антивірус для Бізнесу та з кожної Клієнтської частини для кожного окремого комп’ютера-клієнта (якщо зміна налаштувань не захищена паролем).

Адміністратор мережі може заборонити зміну налаштувань Вартового на Клієнтських комп’ютерах, встановивши пароль для зміни налаштувань на клієнтських комп’ютерах (Детальніше з цією можливістю можна ознайомитись в Інструкції для адміністратора).

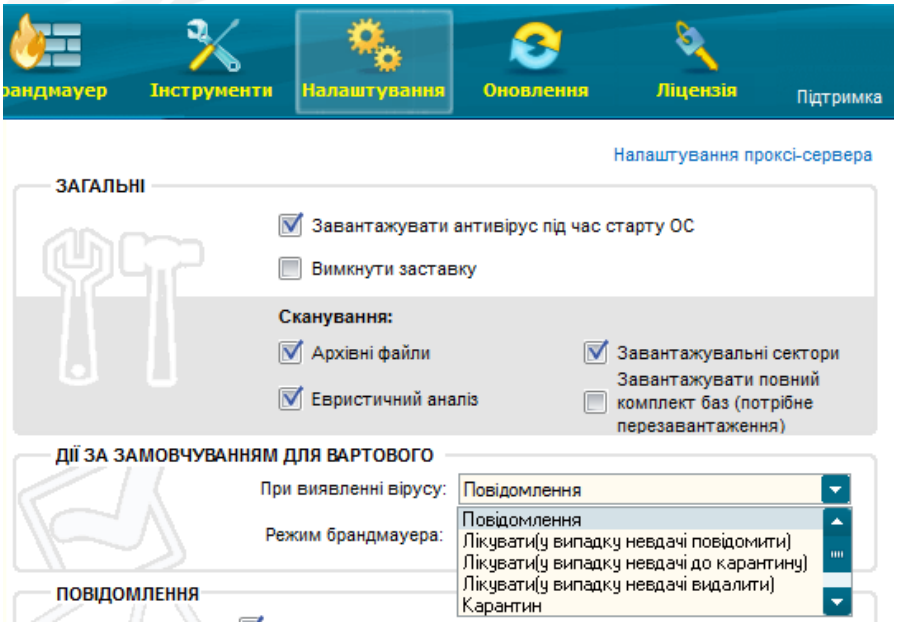
Для зміни налаштувань компоненту Вартовий користувач може перейти у закладку Інструменти головного вікна Клієнтської частини, підпункт Властивості та натиснути на Увімкнено напроти компоненту Вартовий:



Вимкнення компоненту Вартовий будь-яким способом є небажаним!

www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

Змінити налаштування даного модулю Ви можете з головного вікна Клієнтської частини, вкладки Налаштування, блок ДІЇ ЗА ЗАМОВЧУВАННЯМ ДЛЯ ВАРТОВОГО, пункт «При виявленні вірусу»:



www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

3.2. Брандмауер

Брандмауер Zillya! є брандмауером програмного рівня.

Він забезпечує:

- Контроль за доступом встановлених на комп'ютері додатків до мережі. Брандмауер відстежує всі спроби додатків отримати доступ до мережі – як вхідний трафік, так і вихідний;

- 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;

- 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 и 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;

- 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.

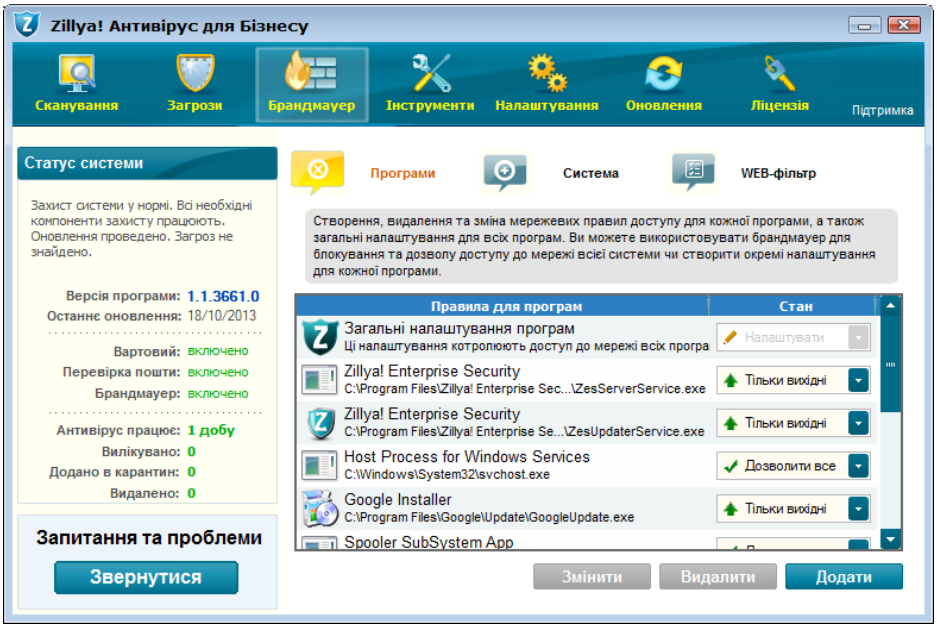
Налаштування Брандмауеру з Клієнтської частини

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.

www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

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

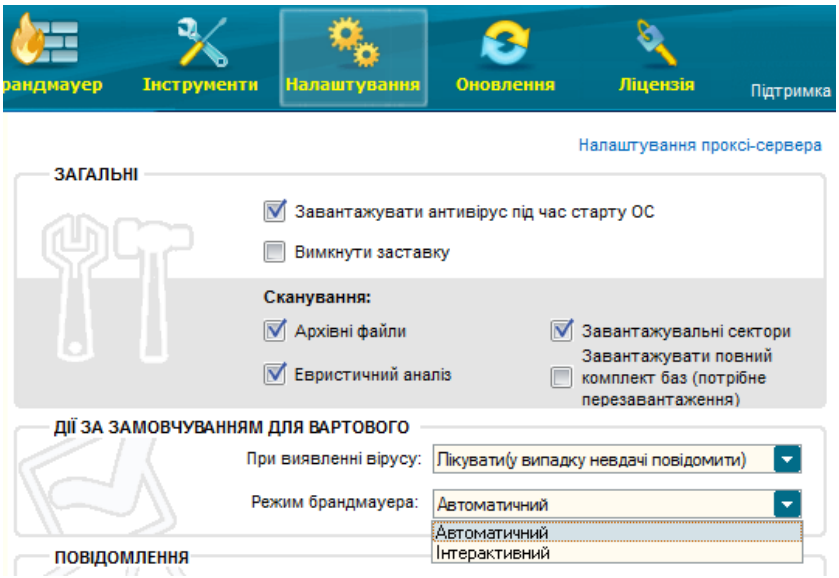
1. Відкрийте головне вікно Клієнтської частини продукту Zillya! Антивірус для Бізнесу та перейдіть у розділ Брандмауер:



2. Змініть налаштування Брандмауера для кожного додатку до бажаних Вами.

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

Змінити налаштування для Брандмауера користувач може з головного вікна Клієнтської частини, вкладки Налаштування, блок ДІЇ ЗА ЗАМОВЧУВАННЯМ ДЛЯ ВАРТОВОГО, пункт «Режим брандмауера»:



www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

3.3. WEB-фільтр

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

Його можливості:

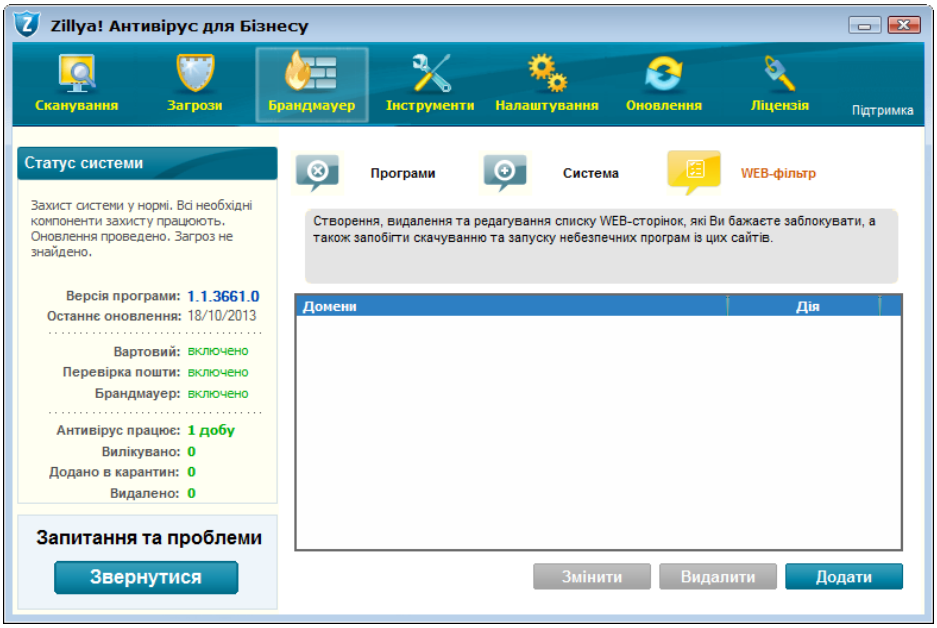
- Блокування небезпечних сайтів. В Zillya! Антивірус для Бізнесу є можливість блокувати доступ до потенційно небезпечних сайтів, блокуючи його завантаження при перегляді в браузері. При цьому користувач бачить відповідне повідомлення;

- 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.

- 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 сами правила, що і до загальної бази. Доступні два режими: повне блокування сайта та блокування завантажень з сайта.

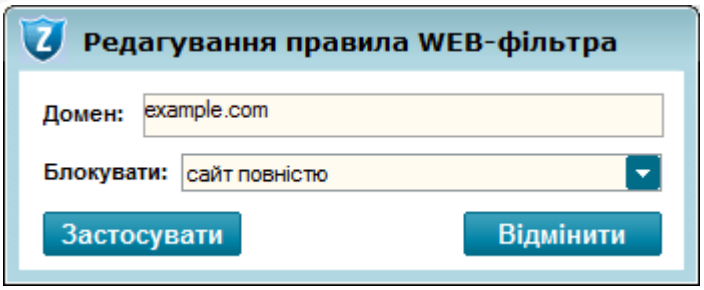
Налаштування WEB-фільтру з Клієнтської частини

Налаштування WEB-фільтру також можуть бути захищені паролем адміністратора! Налаштування доступні в Клієнтських частинах у закладці Брандмауер, підпункті WEB-фільтр:



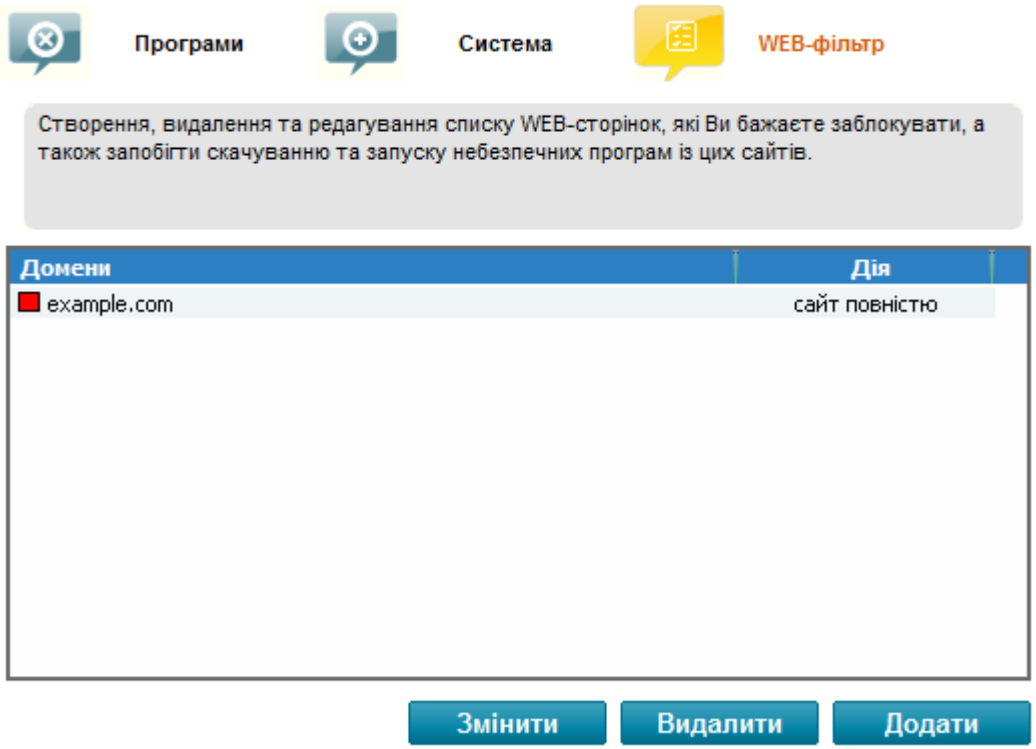
www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

Натиснувши кнопку Додати, користувач може додати у список заблокованих ресурсів певні сайти. Для блокування бажаних сайтів необхідно вказати їх доменні імена у додатковому вікні, що з'виться, та натиснути на кнопку Застосувати:



Ви можете заблокувати сайт повністю або тільки небезпечні об'єкти, які можуть міститися на даному сайті, обравши відповідний параметр в випадаючому списку Блокувати.

Після додання сайт з'явиться в переліку заблокованих WEB-фільтром:



Виділивши сайт у списку та натиснувши на кнопку Видалити, ти можете видалити сайт зі списку заблокованих.

"All IT Service" Ltd
www.zillya.com
+38 (044) 233-05-24
04053 Kyiv, str. Observatorna, 23, office # 17

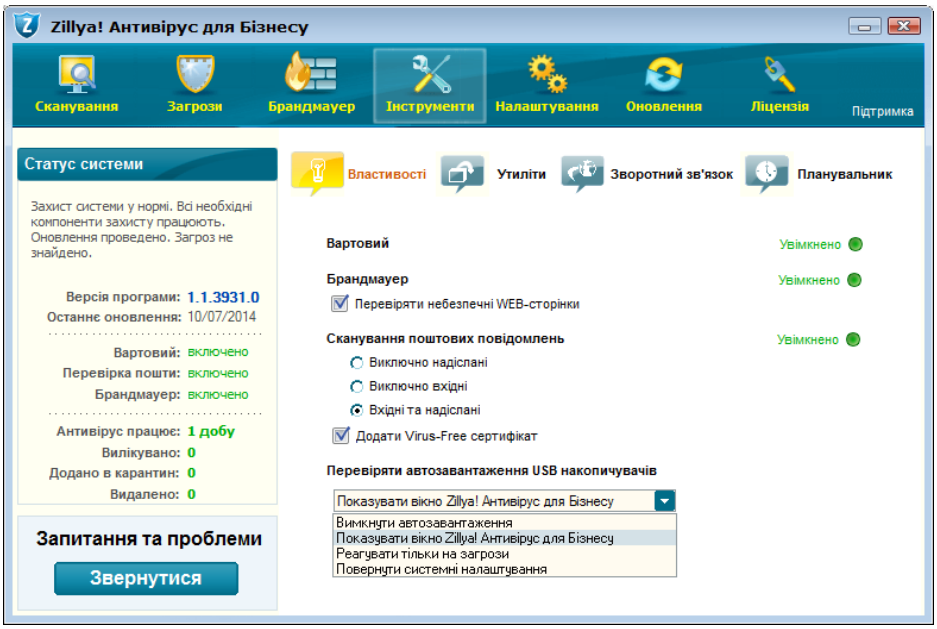
3.4. USB-захист

USB-захист – це модуль для захисту комп'ютерів-клієнтів від загроз, що поширюються через підключення змінних носіїв інформації: Flesh-накопичувачів тощо. USB-захист здійснює перевірку флеш-накопичувачів на наявність вірусів, аналізує ймовірність зараження носія та пропонує виконати сканування за вимогою.

Налаштування USB-захисту

Зміна налаштувань USB-захисту доступна в кожній Клієнтській частині продукту Zillya! Антивірус для Бізнесу. 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 в випадаючому списку користувач може обрати бажаний режим:



В процесі використання режиму USB-захисту «за замовчуванням» «Показувати вікно Zillya! Антивірус для Бізнесу» під час підключення знімного носія до комп'ютера користувач побачить одне з додаткових вікон, яке поінформує його про рівень безпеки даного носія та запропонує оптимальні дії для нього.

"All IT Service" Ltd
www.zillya.com
+38 (044) 233-05-24
04053 Kyiv, str. Observatorna, 23, office # 17

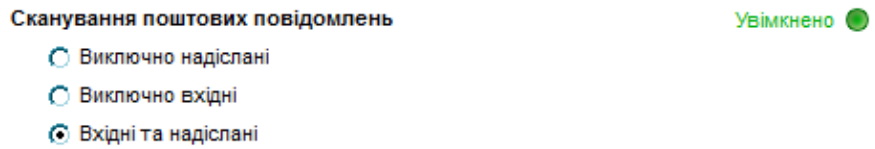
3.5. Сканування поштових повідомлень

Перевірка поштових повідомлень на комп'ютерах-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.

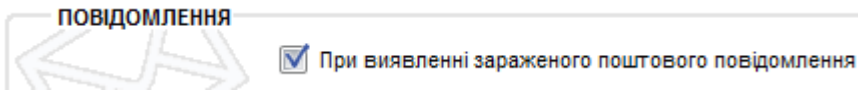
Налаштування Поштового фільтру

Змінити налаштування для Поштового фільтру можна в кожній Клієнтській частині, перейшовши у закладку Інструменти, підрозділ Властивості та встановивши налаштування, бажані користувачем:



Налаштування поштового фільтру також можуть бути захищені паролем адміністратора.

Зміна налаштувань для повідомлень поштового фільтру доступна в кожній в Клієнтській частині в головному вікні програми у вкладці Налаштування, блок ПОВІДОМЛЕННЯ, пункт «При виявленні зараженого поштового повідомлення»:



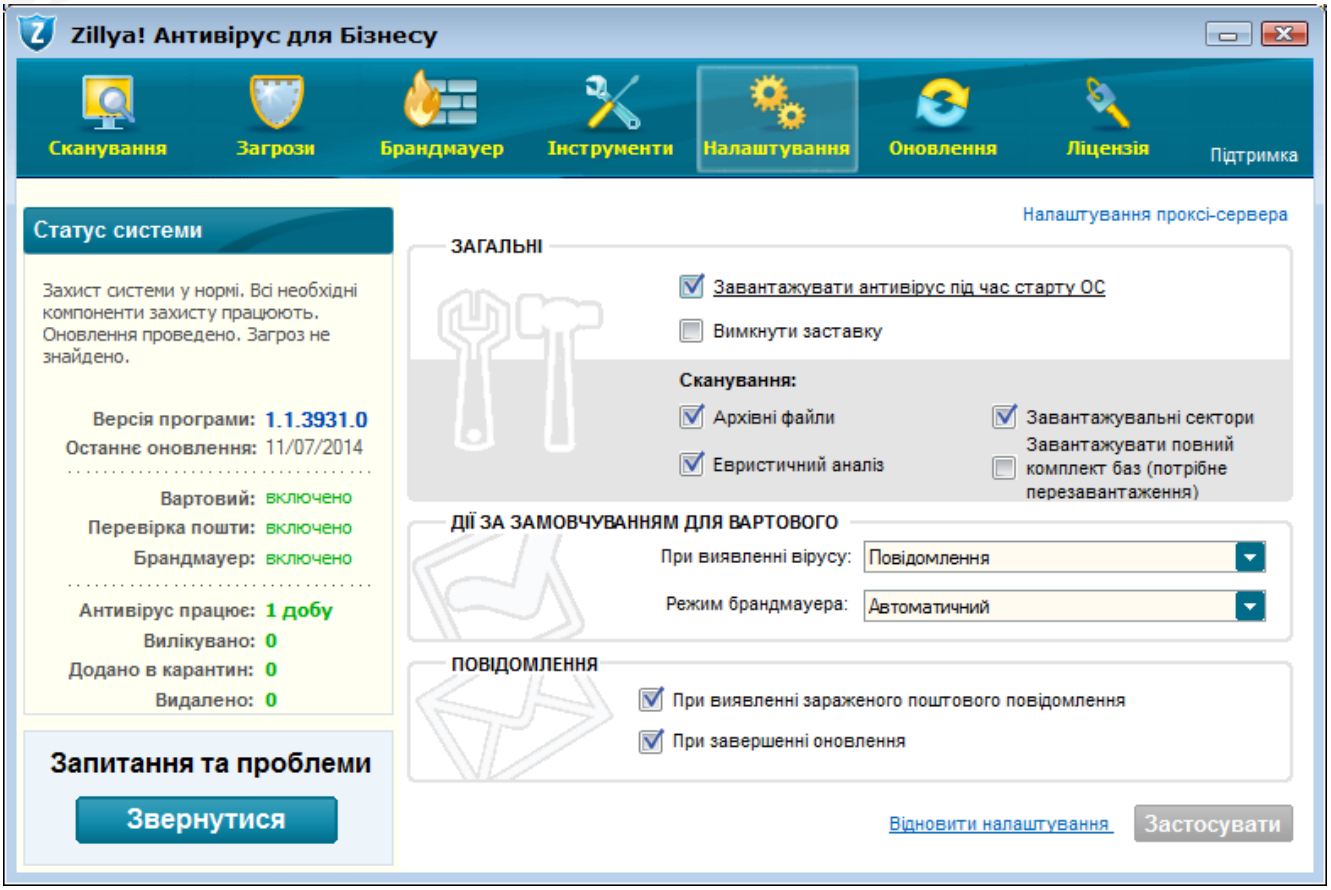
Увімкнення даної опції забезпечує відображення повідомлення при виявленні e-mail повідомлення, що містить зловмисне ПО, і завтосування програмою оптимальної дії до виявленої загрози.

Вимкнення даної опції ніяк не впливає на якість функціонування Клієнтської частини Zillya! Антивірус для Бізнесу на даному комп'ютері.

"All IT Service" Ltd
www.zillya.com
+38 (044) 233-05-24
04053 Kyiv, str. Observatorna, 23, office # 17

3.6. Загальні налаштування

Загальні налаштування Клієнтських частин доступні в головному вікні програми у вкладці Налаштування:



Завантажувати антивірус під час старту ОС – ця опція відповідає за запуск Клієнтської частини одразу з запуском операційної системи Windows на даному комп'ютері. У разі її увімкнення служби антивірусу запускаються одразу після старту операційної системи до запуску усіх додатків та драйверів з автозапуску. Таким чином Клієнтська частина Zillya! Антивірус для Бізнесу перевіряє усі програмні рішення з автозапуску та попереджає запуск вірусів і іншого зловмисного ПО з автозапуску, що є популярним проявом зловмисного ПО. Ми наполегливо не рекомендуємо нашим користувачам вимикати дану опцію!

Вимкнути заставку – дана можливість дозволяє вимкнути «сплеш», який відображається під час завантаження графічної оболонки програми або самої програми:

Вимкнення даної опції жодним чином не впливає на якість функціонування Клієнтської частини Zillya! Антивірус для Бізнесу на комп'ютері користувача.

www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

Сканування

Архівні файли – увімкнення опції вмикає сканування усіх файлів, що є архівами: ZIP, RAR, 7Zip, ACE, ARJ, MS CAB, IS CAB, GZ, BZ2, RPM, DEB, LZH, TAR, CPIO, ISO і деякі інші, MSI, Nullsoft Installer, WISE Installer та різні типи архівів, що самостійно розпаковуються, CHM (Windows Help Files), OLE2-контейнери (офіс складені файли) та інші.

Завантажувальні сектори – увімкнення даної опції вмикає перевірку завантажувальних секторів кожного логічного диску на комп'ютері користувача. Ми також не рекомендуємо вимикати її без нагальної потреби.

Завантажувати повний комплект баз (потрібне перезавантаження) – увімкнення даної опції вмикає завантаження повного комплекту баз разом з запуском Клієнтської частини Zillya! Антивірус для Бізнесу на комп'ютері користувача. З налаштуваннями «за замовчуванням» Клієнтська частина використовує оптимізований пакет антивірусних баз, що містить записи про актуальні віруси та зловмисні програми. У разі увімкнення даної опції Клієнтська частина завантажуватиме повний комплект антивірусних баз, що містить понад 10 мільйонів вірусних баз. Але використання повного комплекту антивірусних баз може вплинути на швидкодію роботи комп'ютера, тому «за замовчуванням» дана опція вимкнена.

Повідомлення

При завершенні оновлення – дана опція відповідає за відображення повідомлення про успішне оновлення антивірусних баз та програмних модулів Клієнтської частини Zillya! Антивірус для Бізнесу. Її вимкнення також не впливає на якість функціонування програми.

Про інші налаштування, які доступні на вкладці Налаштування головного вікна клієнтської частини, будь ласка, читайте в описі відповідного їм компоненту (наприклад, налаштування для модулю Вартовий описані в описі модулю Вартовий, п. 3.1 на стр. 4 даної Інструкції).

Відновити налаштування – натиснення на дане посилання призведе до повернення налаштувань даної Клієнтської частини програми Zillya! Антивірус для Бізнесу до таких, що встановлені розробником, тобто до «налаштувань за замовчуванням».

Застосувати – натиснення даної кнопки застосує зміни налаштувань, внесені користувачем для даної Клієнтської частини.

www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

4. Використання Клієнтської частини

4.1. Сканування

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.

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.

"All IT Service" Ltd
www.zillya.com
+38 (044) 233-05-24
04053 Kyiv, str. Observatorna, 23, office # 17

4.2. Дії над загрозами

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.

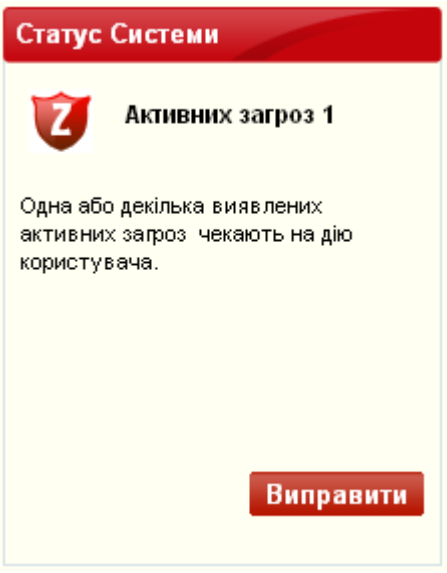
Застосування дій над загрозами з Клієнтської частини

Користувач комп'ютера-клієнта 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:

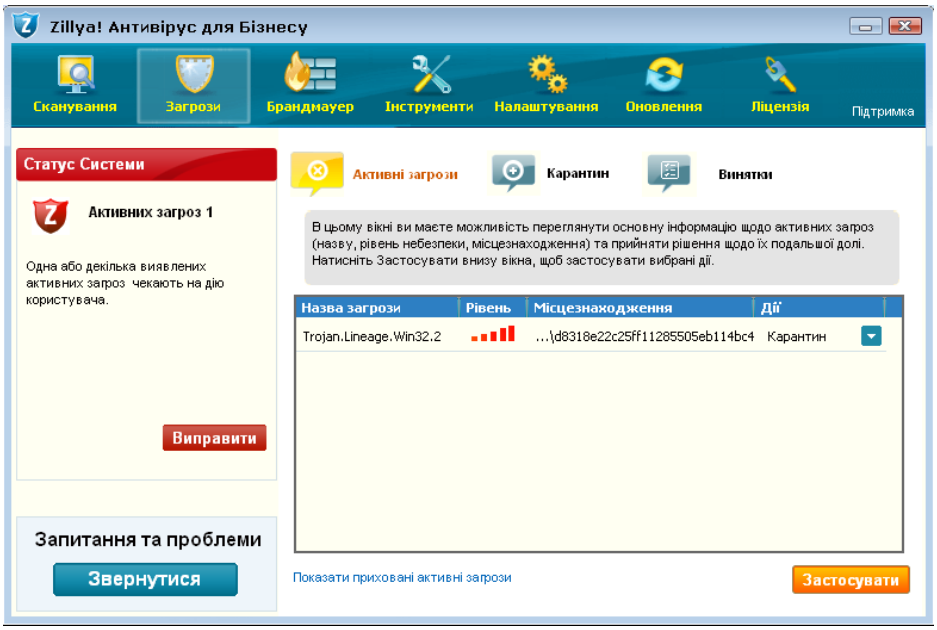
a) Натисненням кнопки Виправити у блоці Статус Системи:



"All IT Service" Ltd
www.zillya.com
+38 (044) 233-05-24
04053 Kyiv, str. Observatorna, 23, office # 17

b) 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 передасться Панелі адміністратора, де її можна буде переглянути.

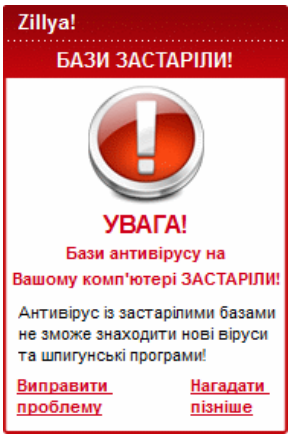
Навіть якщо дії до знайдених загроз не застосовуються одразу, продукт Zillya! Антивірус для Бізнесу **блокує знайдені загрози** та очікує подальших команд для них. Таким чином загрози не наносять шкоди, а «утримуються» антивірусом до застосування інших дій.

www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

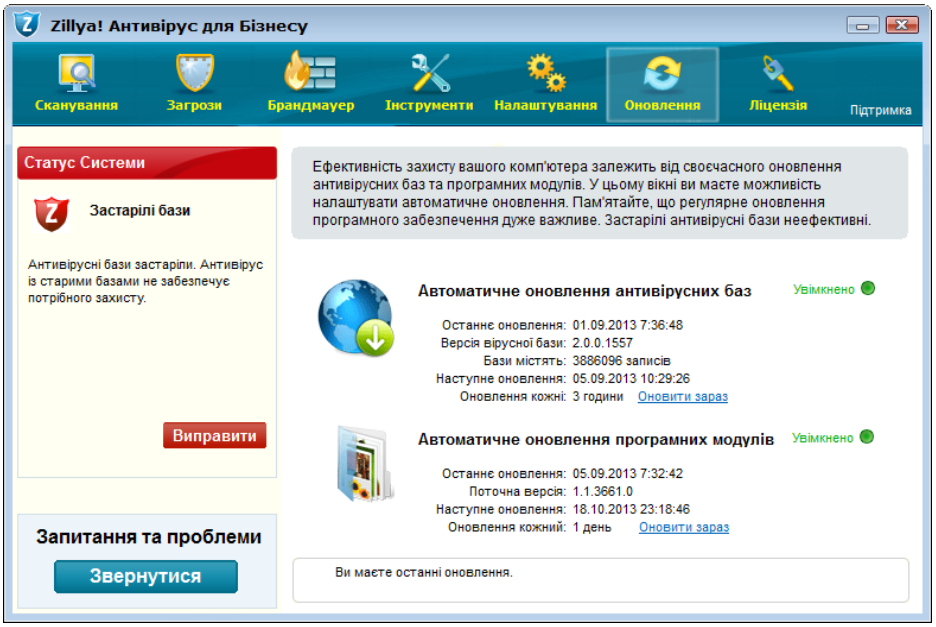
5. Оновлення

5.1. Оновлення антивірусних базОновлення антивірусних баз Zillya! доступне з Клієнтської частини та може бути запущене користувачем комп'ютера-клієнта. Викликати оновлення антивірусних баз у разі їх застарівання з Клієнтської частини можна наступними способами:

a) Зі сплеш-вікна, що відображається з трею та повідомляє про застарілість антивірусних баз Zillya!, натиснувши на посилання Виправити проблему:



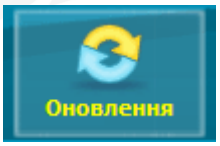
b) З головного вікна Клієнтської частини, натиснувши на кнопку Виправити у Статусі системи та на посилання Оновити зараз в блоці Автоматичне оновлення антивірусних баз у вкладці Оновлення, яка відкриється після натиснення кнопки:



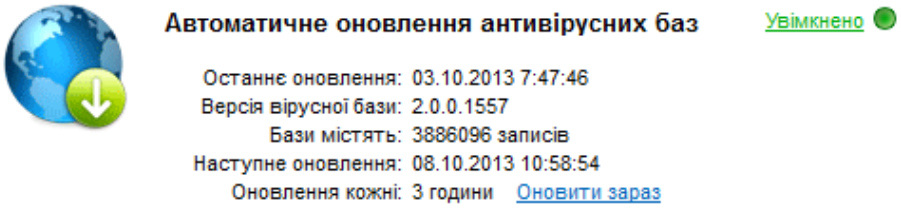
Інформація щодо оновлення антивірусних баз на даному комп'ютері-клієнті буде передана до Панелі адміністратора.

www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

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



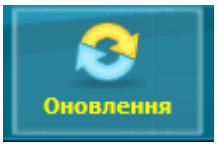
та викликається натисненням на посиланні Оновити зараз: Оновити зараз в блоці Автоматичне оновлення антивірусних баз, напр.:



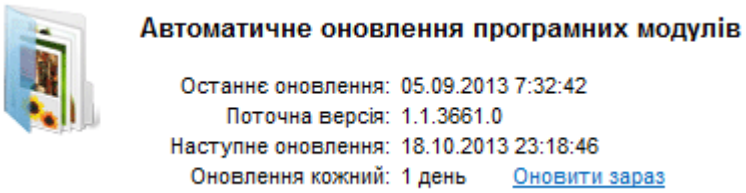
www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

5.2. Оновлення програмних модулів

З кожної Клієнтської частини 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:



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

"All IT Service" Ltd
www.zillya.com
+38 (044) 233-05-24
04053 Kyiv, str. Observatorna, 23, office # 17

6. Додаткові можливості Клієнтської частини

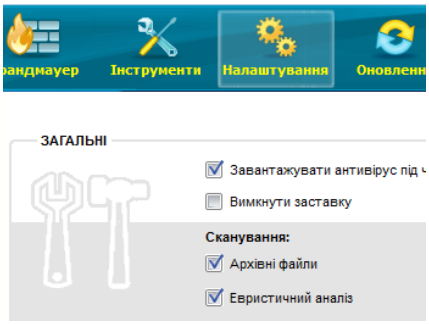
6.1. Евристичний аналізатор

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.

Налаштування Евристичного аналізатору

Змінити налаштування для Евристичного аналізатору користувач може з головного вікна Клієнтської частини, вкладки Налаштування, блок СКАНУВАННЯ, пункт «Евристичний аналіз»:

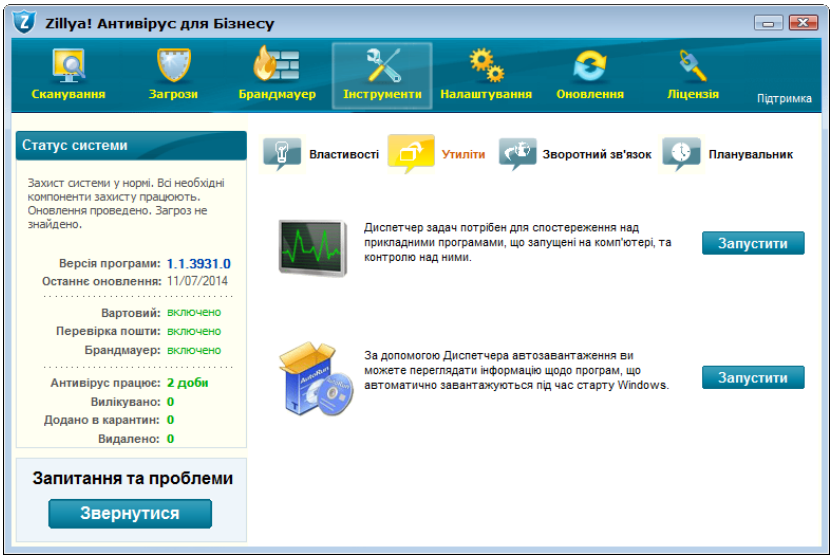


Евристичний аналіз – увімкнення даної опції вмикає евристичний аналізатор. Дана технологія визначає нові віруси, записи для детектування яких ще відсутні в антивірусній базі.

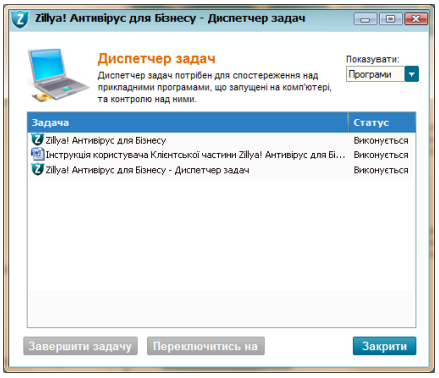
"All IT Service" Ltd
www.zillya.com
+38 (044) 233-05-24
04053 Kyiv, str. Observatorna, 23, office # 17

6.2. Диспетчер задач та Диспетчер автозавантаження

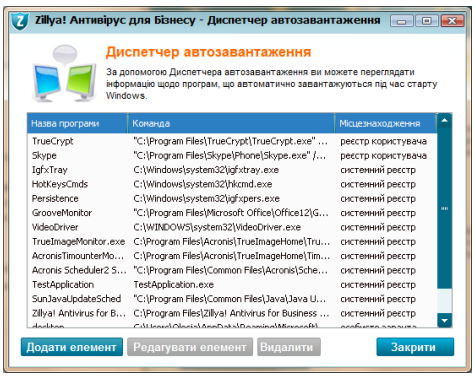
Zillya! Антивірус для Бізнесу містить додаткові модулі - **Диспетчер задач** та **Диспетчер автозавантаження**. Ці утиліти розширюють функціонал програми та допомагають користувачеві краще контролювати процеси в системі. Дані утиліти доступні з головного вікна кожної Клієнтської частини продукту Zillya! Антивірус для Бізнесу, вкладки Інструменти, підпункт Утиліти:



Диспетчер задач необхідний для контролю над запущеними на комп'ютері програмами:



За допомогою Диспетчера автозавантаження можна переглядати інформацію про програми, які автоматично запускаються при старті ОС Windows.



www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

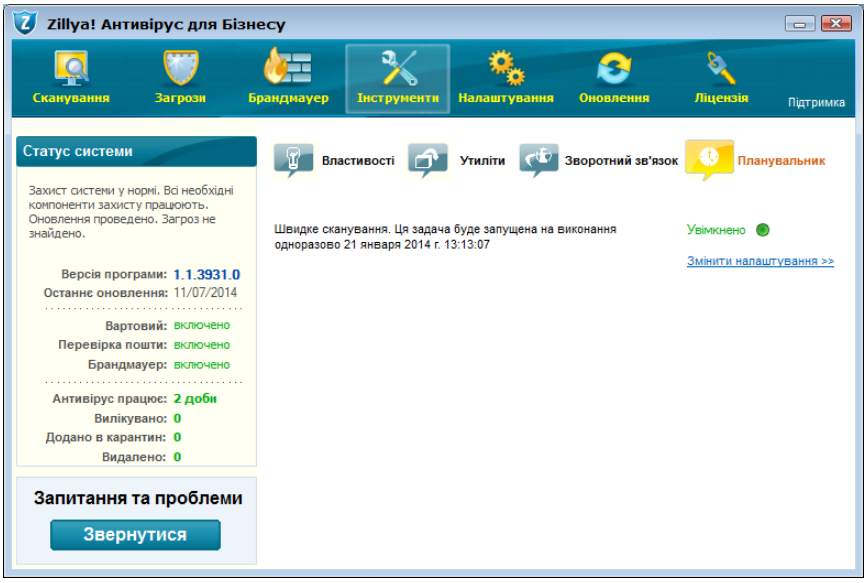
6.3. Планувальник

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

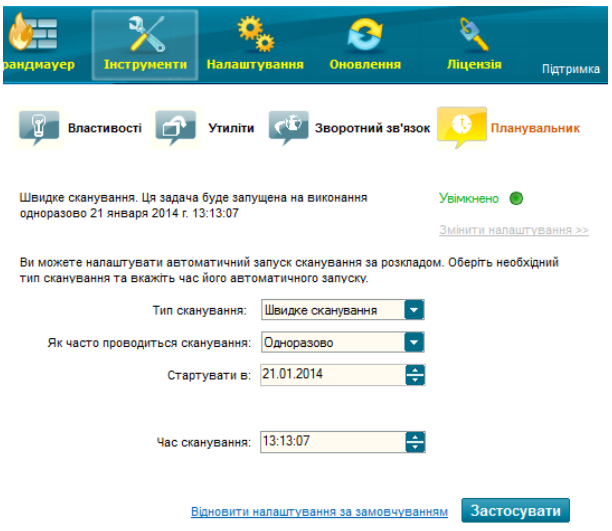
Клієнтські частини Zillya! Антивірус для Бізнесу містять функцію Планувальник.

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.

Функція Планувальник доступна з головного вікна кожної клієнтської частини, вкладки Інструменти, підпункту Планувальник:



Натиснувши на посиланні Змінити налаштування >>, в новому вікні програми користувач може запланувати будь-яке сканування в зручний для нього час:



www.zillya.com
+38 (044) 233-05-24
"All IT Service" Ltd
04053 Kyiv, str. Observatorna, 23, office # 17

7. Зворотній зв'язок

Всі користувачі Клієнтських частин продукту Zillya! Антивірус для Бізнесу можуть звернутися за консультацією щодо продукту до адміністратора їх локальної мережі.

Наші спеціалісти також 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 завжди можете звернутися до нас:

Відділ інтеграції корпоративних рішень Zillya!:

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

- email: avcorp@zillya.com

Служба технічної підтримки користувачів Zillya!:

- тел.: +38 (044) 233 05 24

- email: support@zillya.com

Дякуємо Вам за довіру!