Dr.WEB

для Linux

Посібник користувача

Dr.Web для Linux
Версія 11.1
Посібник користувача
03.11.2020

ТОВ «Доктор Веб», Центральний офіс в Росії

Адреса: 125124, Росія, Москва, 3-я вулиця Ямського поля, вол. 2, корп.12А

Веб-сайт: https://www.drweb.com/

Телефон: +7 (495) 789-45-87

Інформацію про регіональні представництва та офіси Ви можете знайти на офіційному сайті компанії.

«Доктор Веб»

«Доктор Веб» — російський розробник засобів інформаційної безпеки.

«Доктор Веб» пропонує ефективні антивірусні та антиспам-рішення як для державних організацій та великих компаній, так і для приватних користувачів.

Антивірусні рішення сімейства Dr.Web розробляються з 1992 року та незмінно демонструють чудові результати детектування шкідливих програм, відповідають світовим стандартам безпеки.

Сертифікати та нагороди, а також широка географія користувачів свідчать про виключну довіру до продуктів компанії.

Ми вдячні користувачам за підтримку рішень сімейства Dr.Web!

Зміст

Умовні позначення та скорочення

В даному посібнику використовуються такі позначення:

Позначення	Коментар
	Важливе зауваження або вказівка.
	Попередження про можливі помилкові ситуації, а також про важливі моменти, на які слід звернути особливу увагу.
Антивірусна мережа	Новий термін або акцент на терміни в описах.
<IP-address>	Поля для заміни функціональних назв фактичними значеннями.
Зберегти	Назви екранних кнопок, вікон, пунктів меню та інших елементів програмного інтерфейсу.
CTRL	Позначення клавіш клавіатури.
`/home/user`	Назви файлів та каталогів, фрагменти програмного коду.
Додаток А	Перехресні посилання на глави документу або гіперпосилання на зовнішні ресурси.

Командам, які необхідно ввести з клавіатури в командний рядок операційної системи (в терміналі або емуляторі терміналу), в Посібнику передує символ запрошення до введення `$` або `#`, який вказує, які повноваження користувача необхідні для виконання даної команди. Стандартним для UNIX-систем мається на увазі, що:

`$` — для виконання команди достатньо звичайних прав користувача.

`#` — для виконання команди необхідні права суперкористувача (зазвичай — *root*). Для підвищення прав можна використовувати команди **su** та **sudo**.

Вступ

Дякуємо вам за придбання Dr.Web для Linux. Він дозволить вам забезпечити надійний захист вашого комп'ютера від комп'ютерних загроз всіх можливих типів, використовуючи найсучасніші технології виявлення та знешкодження загроз.

Даний посібник призначений для допомоги користувачам комп'ютерів, що працюють під управлінням операційних систем сімейства **GNU/Linux** (далі в документі буде використане позначення **Linux**), у встановленні та використанні Dr.Web для Linux версії 11.1.

Якщо у вас вже встановлений Dr.Web для Linux попередньої версії, та ви бажаєте оновити його до версії 11.1, виконайте процедуру переходу на нову версію (див. розділ Перехід на нову версію).

Про продукт

В цьому розділі міститься така інформація про продукт:

- Призначення.
- Основні функції.
- Структура Dr.Web для Linux.
- Розташування карантину.
- Повноваження для роботи з файлами.
- Режими роботи.

Призначення

Dr.Web для Linux створений для захисту комп'ютерів, що працюють під управлінням ОС сімейства **GNU/Linux**, від вірусів та інших видів шкідливого програмного забезпечення, призначених для різних платформ.

Основні компоненти програми (антивірусне ядро та вірусні бази) є не тільки вкрай ефективними та невимогливими до системних ресурсів, але й крос-платформеними, що дозволяє спеціалістам компанії «Доктор Веб» створювати надійні антивірусні рішення, які забезпечують захист комп'ютерів та мобільних пристроїв, що працюють під управлінням поширених операційних систем, від загроз, призначених для різних платформ. В даний час, поряд з Dr.Web для Linux, в компанії «Доктор Веб» розроблені також антивірусні рішення для операційних систем сімейства **UNIX** (таких, як **FreeBSD**), **IBM OS/2**, **Novell NetWare**, **macOS** та **Windows**. Окрім того, розроблені антивірусні рішення, які забезпечують захист мобільних пристроїв, що працюють під управлінням ОС **Andorid**, **Symbian**, **BlackBerry**.

Компоненти Dr.Web для Linux постійно оновлюються, а вірусні бази Dr.Web регулярно доповнюються новими сигнатурами загроз, що забезпечує актуальний рівень захищеності комп'ютера, програм та даних користувачів. Для додаткового захисту від невідомого шкідливого програмного забезпечення використовуються методи евристичного аналізу, реалізовані в антивірусному ядрі, а також звернення до сервісу Dr.Web Cloud, який збирає свіжу інформацію про актуальні загрози та здатен захистити користувачів від відвідання небажаних веб-сайтів, а також захистить операційні системи від інфікованих файлів.

Основні функції

Основні функції Dr.Web для Linux:

1. **Пошук та знешкодження загроз**. Виявляються та знешкоджуються як безпосередньо шкідливі програми всіх можливих типів (різні віруси, включаючи віруси, що інфікують поштові файли та завантажувальні записи дисків, троянські програми, поштові

хробаки тощо), так і небажані програми (рекламні програми, програми-жарти, програми автоматичного додзвону). Докладніше про види загроз див. Додаток А. Види комп'ютерних загроз.

Для виявлення шкідливих та небажаних програм використовуються:

- *Сигнатурний аналіз*. Метод перевірки, який дозволяє виявити вже відомі загрози, інформація про які міститься в вірусних базах.
- *Евристичний аналіз*. Набір методів перевірки, які дозволяють виявити загрози, які ще невідомі.
- *Хмарні технології виявлення загроз*. Звернення до сервісу Dr.Web Cloud, який збирає свіжу інформацію про актуальні загрози, що розсилається різними антивірусними продуктами Dr.Web.

Зверніть увагу, що евристичний аналізатор може помилково реагувати на програмне забезпечення, що не є шкідливим. Тому об'єкти, що містять виявлені ним загрози, отримують спеціальний статус «підозрілі». Рекомендується поміщати такі файли до карантину, а також передавати на аналіз до антивірусної лабораторії «Доктор Веб». Докладніше про методи знешкодження див. Додаток Б. Усунення комп'ютерних загроз.

Перевірка файлової системи може запускатися як вручну, за запитом користувача, так і автоматично — відповідно до заданого розкладу. Є можливість як повної перевірки всіх об'єктів файлової системи, доступних користувачу, так і вибіркової перевірки тільки вказаних об'єктів (окремих каталогів або файлів). Окрім того, доступна можливість окремої перевірки завантажувальних записів томів та виконуваних файлів, з яких запущені процеси, активні в системі в даний момент. В останньому випадку при виявленні загрози проводиться не тільки знешкодження шкідливого виконуваного файла, але й примусове завершення роботи всіх процесів, запущених з нього.

Для операційних систем, що мають середовище графічного робочого столу, реалізована інтеграція функцій перевірки файлів як з панеллю задач, так і з графічним файловим менеджером. В системах, що реализують мандатну модель доступу до файлів з набором різних рівнів доступу, сканування файлів, недоступних на поточному рівні доступу, может проводитися в спеціальному режимі автономної копії.

Всі об'єкти з загрозами, виявлені в файловій системі, реєструються в реєстрі загроз, який постійно зберігається, за виключенням тих загроз, які були виявлені в режимі автономної копії.

Утиліта управління з командного рядка, що входить до складу Dr.Web для Linux, дозволяє також проводити перевірку на наявність загроз файлових систем віддалених вузлів мережі, які надають віддалений доступ до них через SSH або Telnet.

Ви можете використовувати віддалене сканування тільки для виявлення шкідливих або підозрілих файлів на віддаленому вузлі. Для усунення виявлених загроз на віддаленому вузлі скористайтеся засобами управління, які надаються безпосередньо цим вузлом. Наприклад, для роутерів та інших «розумних» пристроїв ви можете оновити прошивку, а для обчислювальних машин — підключитися до них (у тому числі — у віддаленому термінальному режимі) та виконати відповідні операції в їх файловій системі (видалення або переміщення файлів тощо) або запустити антивірусне ПЗ, встановлене на них.

2. **Моніторинг звернень до файлів**. Відстежуються звернення до файлів з даними та спроби запуску виконуваних файлів. Це дозволяє виявляти та нейтралізовувати шкідливі програми безпосередньо при спробах інфікування ними комп'ютера. Окрім стандартного режиму моніторингу, є можливість включити посилений («агресивний») режим, в якому доступ до файлів блокуватиметься монітором до моменту завершення їх перевірки (це дозволяє попередити випадки доступу до файла, коли він містить загрозу, але результат його перевірки стає відомим вже після того, як програма отримала доступ до файла). Посилений режим моніторингу підвищує рівень безпеки, але уповільнює доступ програм до ще не перевірених файлів.
3. **Моніторинг мережних з'єднань**. Відстежуються спроби звернення до серверів в мережі Інтернет (веб-серверів, файлових серверів) за протоколами HTTP та FTP для блокування доступу користувачів до веб-сайтів та вузлів, адреси яких позначені як небажані для відвідування, а також для попередження завантаження щкідливих файлів.
4. **Перевірка повідомлень електронної пошти** для попередження отримання та відправлення повідомлень електронної пошти, що містять інфіковані файли та небажані посилання, а також таких, що класифіковані як спам.

   Перевірка повідомлень електронної пошти та файлів, що завантажуються по мережі, на наявність в них вірусів та інших загроз проводиться «на льоту». Залежно від поставки, компонент Dr.Web Anti-Spam може бути відсутнім у складі Dr.Web для Linux. В цьому випадку перевірка повідомлень на спам не проводиться.

   Для визначення небажаних посилань використовуються як база даних категорій веб-ресурсів, що постачається разом з Dr.Web для Linux та автоматично оновлюється, так і чорні та білі списки, що складаються користувачем вручну. Додатково Dr.Web для Linux може звертатися до сервісу Dr.Web Cloud, щоб перевірити, чи не позначений веб-сайт, до якого намагається звернутися користувач, або посилання на який міститься в повідомленні електронної пошти, як шкідливий іншими антивірусними продуктами Dr.Web.

Якщо будь-які повідомлення електронної пошти неправильно розпізнаються компонентом Dr.Web Anti-Spam, рекомендується пересилати на спеціальні поштові адреси для аналізу та підвищення якості роботи спам-фільтра. Для цього кожне таке повідомлення збережіть в окремий файл типу `.eml`. Збережені файли прикріпіть до повідомлення електронної пошти, яке відправте на відповідну службову адресу.

- vrnonspam@drweb.com — якщо воно містить файли листів, *помилково розпізнаних як спам*;
- vrspam@drweb.com — якщо воно містить файли листів, *помилково не визначених як спам*.

5. **Надійна ізоляція інфікованих або підозрілих об'єктів** в спеціальному сховищі — карантині, щоб вони не могли заподіяти шкоди системі. При переміщенні об'єктів до карантину вони спеціальним чином перейменовуються та за необхідності можуть бути відновлені в вихідне місце тільки за командою користувача.
6. **Автоматичне оновлення** вмісту вірусних баз Dr.Web та антивірусного ядра для підтримки високого рівня надійності захисту від шкідливих програм.
7. **Збір статистики** перевірок та вірусних інцидентів; ведення журналу виявлених загроз (доступний тільки через утиліту управління з командного рядка), а також відправлення статистики вірусних інцидентів хмарному сервісу Dr.Web Cloud.
8. **Забезпечення роботи під управлінням сервера централізованого захисту** (такого, як Dr.Web Enterprise Server або в рамках сервісу Dr.Web AV-Desk) для застосування на захищуваному комп'ютері єдиних політик безпеки, прийнятих в мережі, до складу якої він входить. Це може бути як мережа підприємства (корпоративна мережа) або приватна мережа VPN, так і мережа, організована провайдером послуг, наприклад, доступу до мережі Інтернет.

Оскільки для використання інформації, що міститься в хмарному сервісі Dr.Web Cloud, необхідно передавати дані про активність користувача (наприклад, передавати на перевірку адреси відвідуваних ним веб-сайтів), то звернення до Dr.Web Cloudпроводиться тільки після отримання відповідного дозволу користувача. За необхідності, використання Dr.Web Cloud можна заборонити в будь-який момент в налаштуваннях програми.

Структура Dr.Web для Linux

Dr.Web для Linux складається з таких компонентів:

Компонент	Опис
Сканер	Компонент, що проводить за запитом користувача або за заданим розкладом перевірку об'єктів файлової системи (файли, каталоги та завантажувальні записи) на наявність в них загроз. Користувач може запускати перевірку як в графічному режимі, так і з командного рядка.

Компонент	Опис
SpIDer Guard	Компонент, що працює в резидентному режимі та відстежує операції з файлами (такі, як створення, відкриття, закриття та запуск файла). Відправляє Сканеру запити на перевірку вмісту нових та змінених файлів, а також виконуваних файлів в момент запуску програм. Працює з файловою системою ОС через системний механізм **fanotify** або через спеціальний модуль ядра (*LKM — Linux Kernel Module*), розроблений компанією «Доктор Веб». При роботі через системний механізм **fanotify** монітор може працювати в посиленому режимі, блокуючи доступ до файлів (всіх типів або тільки до виконуваних файлів), які ще не перевірені, до моменту завершення їх перевірки. За замовчуванням посилений режим моніторингу відключений.
SpIDer Gate	Компонент, що працює в резидентному режимі та відстежує всі мережні з'єднання. • Перевіряє наявність URL в базах категорій веб-ресурсів та чорних списках користувача; блокує доступ до веб-сайтів, якщо їхні URL зареєстровані в чорному списку користувача або в категоріях, позначених як небажані для відвідування. • Блокує відправлення та приймання повідомлень електронної пошти, якщо вони містять шкідливі об'єкти або небажані посилання. • Відправляє Сканеру на перевірку файли, що завантажуються з мережі Інтернет (з серверів, доступ до яких був дозволений), та блокує їхнє завантаження, якщо вони містять загрози. Додатково, за наявності відповідного дозволу від користувача, відправляє запитувані ним URL на перевірку в сервіс Dr.Web Cloud.
Антивірусне ядро	Центральний компонент антивірусного захисту. Використовується Сканером для пошуку й виявлення вірусів та шкідливих програм, а також аналізу підозрілої поведінки.
Dr.Web Anti-Spam	Компонент перевірки повідомлень електронної пошти на наявність ознак спаму. В версіях для ARM64 компонент відсутній.
Вірусні бази	Автоматично оновлювана база даних, що містить інформацію про відомі загрози. Використовується антивірусним ядром для виявлення та знешкодження загроз.
База категорій веб-ресурсів	Автоматично оновлювана база даних, що містить список веб-ресурсів, розбитих за категоріями. Використовується SpIDer Gate для блокування доступу до небажаних ресурсів.
Компонент оновлення	Компонент, що відповідає за автоматичне завантаження з серверів оновлень компанії «Доктор Веб» оновлень для вірусних баз та антивірусного ядра та бази категорій веб-ресурсів (як автоматично за розкладом, так і безпосередньо за командою користувача).
Графічний інтерфейс управління	Компонент, що надає віконний графічний інтерфейс управління Dr.Web для Linux. Дозволяє користувачу в графічному режимі запускати перевірку обєктів файлової системи, управляти роботою моніторів SpIDer Guard та

Компонент	Опис
	SpIDer Gate, переглядати вміст карантину, запускати отримання оновлень, а також налаштовувати роботу Dr.Web для Linux.
Агент сповіщень	Компонент, що працює у фоновому режимі. Відображає спливаючі сповіщення про події, що виникають, та індикатор програми Dr.Web для Linux в області сповіщень, запускає перевірки за розкладом. За замовчуванням запускається на початку сеансу роботи користувача в середовищі робочого столу.
Менеджер ліцензій	Компонент, що спрощує роботу з ліцензіями в графічному режимі. Дозволяє активувати ліцензію або демонстраційний період, переглянути дані про поточну ліцензію, подовжити її, а також встановити та видалити ліцензійний ключовий файл.

Окрім наведених в таблиці, до складу Dr.Web для Linux входять також додаткові сервісні компоненти, що працюють у фоновому режимі та не потребують втручання користувача.

Монітор файлової системи SpIDer Guard може використовувати два режими роботи:

- *FANOTIFY* – робота через системний механізм **fanotify** (підтримується не всіма ОС сімейства **GNU/Linux**).
- *LKM* – робота з використанням завантажуваного модуля ядра **Linux**, розробленого компанією «Доктор Веб» (може бути використаний в будь-якій ОС сімейства **GNU/Linux** з ядром версії 2.6.x та вище). Для архітектури ARM64 можливість роботи з LKM не підтримується.

За замовчуванням монітор файлової системи автоматично вибирає потрібний режим роботи, виходячи з можливостей оточення. Якщо SpIDer Guard не запускається, виконайте збірку та встановлення завантажуваного модуля ядра з вихідних кодів, що постачаються.

Розташування карантину

Карантин Dr.Web для Linux є системою каталогів, призначених для надійної ізоляції файлів, що містять виявлені загрози, які в даний момент не можуть бути знешкоджені з будь-яких причин. Наприклад, виявлена загроза може бути невиліковною, тому що ще невідома Dr.Web для Linux (наприклад, вона була виявлена евристичним аналізатором, а в вірусних базах її сигнатура, а отже — й метод лікування, відсутній), або при спробі її лікування виникають помилки. Окрім того, файл може бути переміщений до карантину безпосередньо за бажанням користувача, якщо він вибрав відповідну дію у списку виявлених загроз або вказав його як реакцію Сканера або монітора файлової системи SpIDer Guard на загрози визначеного типу.

Коли файл, що містить загрозу, переміщується до карантину, він спеціальним чином перейменовується, щоб унеможливити його ідентифікацію користувачами та програмами та ускладнити доступ до нього, оминаючи інструменти роботи з

карантином, реалізовані в Dr.Web для Linux. Окрім того, при переміщенні файла до карантину у нього завжди скидається біт виконання, щоб запобігти його запуску.

Каталоги карантину розміщуються:

- *в домашньому каталозі користувача* (якщо на цьому комп'ютері є декілька облікових записів різних користувачів, то в домашньому каталозі кожного з цих користувачів може бути створений свій власний каталог карантину).
- *в кореневому каталозі кожного логічного тому,* змонтованого в файлову систему операційної системи.

Каталоги карантину Dr.Web для Linux завжди мають ім'я `.com.drweb.quarantine` та створюються за необхідності, в той момент, коли до будь-якої загрози застосовується дія *«До карантину» (Quarantine)*, тобто доти, поки загрози не виявлені, каталоги карантину не створюються. При цьому завжди створюється тільки той каталог карантину, який потребується для ізоляції файла. Щоб визначити, в який з каталогів необхідно ізолювати файл, використовується ім'я власника файла. Якщо під час руху до кореня файлової системи `/` від каталогу, що містить файл, досягається домашній каталог власника, файл ізолюється до каталогу карантину, що знаходиться в ньому. В іншому випадку файл буде ізольований до каталогу карантину, створеного в корені тому, що містить файл (кореневий каталог тому необов'язково збігається з коренем файлової системи). Таким чином, будь-який інфікований файл, що переміщується до карантину, завжди залишається на тому томі, на якому він бил виявлений. Це забезпечує коректну роботу карантину за наявності в системі змінних накопичувачів та інших томів, які можуть монтуватися в файлову систему операційної системи періодично та в різні точки.

Користувач може управляти вмістом карантину як в графічному режимі роботи, так і з командного рядка. При цьому завжди опрацьовується консолідований карантин, який об'єднує в собі всі каталоги з ізольованими об'єктами, доступні в даний момент. З точки зору користувача, який переглядає вміст консолідованого карантину, каталог, що розташовується в його домашньому каталозі, називається карантином *Користувача*, а решта каталогів вважається *Системним* карантином.

> Робота з карантином можлива навіть тоді, коли відсутня активна ліцензія, але в цьому випадку лікування ізольованих об'єктів унеможливлюється.

Повноваження для роботи з файлами

При скануванні об'єктів файлової системи та нейтралізації загроз Dr.Web для Linux (точніше, користувач, від імені якого він запущений) повинен мати такі повноваження:

Дія	Необхідні повноваження
Виведення всіх виявлених загроз	Без обмежень. Спеціальних повноважень не потребується.

Дія	Необхідні повноваження
Виведення вмісту контейнера (архіву, поштового файла тощо) (Відображення тільки елементів, які містять помилку або загрозу)	Без обмежень. Спеціальних повноважень не потребується.
Переміщення до карантину	Без обмежень. Користувач може відправляти до карантину всі інфіковані файли, незалежно від наявності у нього прав на читання та запис для переміщуваного файла.
Видалення загроз	Користувач повинен мати права на запис в файл, що видаляється. Якщо загроза виявлена в файлі, що знаходиться в контейнері (архів, поштове повідомлення тощо), замість видалення виконується переміщення контейнера до карантину.
Лікування файлів	Без обмежень. Після виконання лікування залишається зцілений файл з вихідними правами доступу та власником. Файл може бути видалений, якщо видалення є методом лікування виявленої в ньому загрози.
Відновлення файла з карантину	Користувач повинен мати права на читання відновлюваного файла та мати права на запис до каталогу відновлення.
Видалення файла з карантину	Користувач повинен мати права на запис у вихідний файл, який був переміщений до карантину.

Для тимчасового підвищення прав запущеного в графічному режимі Dr.Web для Linux ви можете скористатися відповідною кнопкою у вікні Dr.Web для Linux (вона доступна та відображається, тільки якщо підвищення прав може знадобитися для успішного виконання будь-якої операції). Для запуску Dr.Web для Linux в графічному режимі або утиліти управління з командного рядка з правами суперкористувача ви можете скористатися командою зміни користувача **su** або командою виконання від імені іншого користувача **sudo**.

Сканер не може працювати з файлами, розмір яких перевищує 4 ГБайт (при спробі перевірки таких файлів видаватиметься помилка *«Файл занадто великий»*).

Режими роботи

Dr.Web для Linux може працювати як автономно, так і у складі корпоративної або приватної *антивірусної мережі,* що управляється будь-яким *сервером централізованого захисту*. Такий режим роботи називається *режимом централізованого захисту*. Використання цього режиму не потребує встановлення додаткового програмного забезпечення, перевстановлення або видалення Dr.Web для Linux.

- *В одиночному режимі (standalone mode)* захищуваний комп'ютер не входить до антивірусної мережі та управляється локально. В цьому режимі конфігураційний та ліцензійний ключовий файли знаходяться на локальних дисках, а Dr.Web для Linux повністю управляється з захищуваного комп'ютера. Оновлення вірусних баз отримуються з серверів оновлень компанії «Доктор Веб».
- *В режимі централізованого захисту (central protection mode)* захистом комп'ютера управляє сервер централізованого захисту. В цьому режимі деякі функції та налаштування Dr.Web для Linux можуть бути змінені або заблоковані відповідно до загальної (корпоративної) стратегії антивірусного захисту, прийнятої в антивірусній мережі. В цьому режимі на комп'ютері використовується особливий ліцензійний ключовий файл, отриманий з вибраного сервера централізованого захисту, до якого підключений Dr.Web для Linux. Ліцензійний або демонстраційний ключовий файл користувача, якщо він наявний на локальному комп'ютері, не використовується. На сервер централізованого захисту відсилається статистика роботи Dr.Web для Linux, включаючи статистику вірусних інцидентів. Оновлення вірусних баз також проводиться з сервера централізованого захисту.
- *В мобільному режимі (mobile mode)* Dr.Web для Linux отримує оновлення вірусних баз з серверів оновлень компанії «Доктор Веб», але використовує локальні налаштування та особливий ліцензійний ключовий файл, отримані з сервера централізованого захисту.

При роботі Dr.Web для Linux під управлінням сервера централізованого захисту (у тому числі й в мобільному режимі) блокуються такі можливості:

1. Можливість видалення ліцензійного ключового файла в Менеджері ліцензій.
2. Можливість запуску оновлень вручну та налаштування параметрів оновлення.
3. Можливість налаштування параметрів перевірки об'єктів файлової системи Сканером.

Можливість налаштування монітора файлової системи SplDer Guard, а також його включення та відключення при роботі Dr.Web для Linux під управлінням сервера централізованого захисту залежить від дозволів, заданих на сервері.

В режимі централізованого захисту недоступна перевірка файлів за заданим розкладом.

Якщо на сервері централізованого захисту включена заборона запуску перевірки файлів користувачем, то сторінка запуску сканування та кнопка **Сканер** у вікні Dr.Web для Linux будуть недоступні.

Принципи централізованого захисту

Рішення компанії «Доктор Веб» з організації централізованого антивірусного захисту мають клієнт-серверну архітектуру (див. ілюстрацію нижче).

Комп'ютери компанії або користувачів постачальника IT-послуг захищені від загроз *локальними антивірусними компонентами* (в даному випадку — Dr.Web для Linux), які забезпечують антивірусний захист та підтримують з'єднання з сервером централізованого захисту.

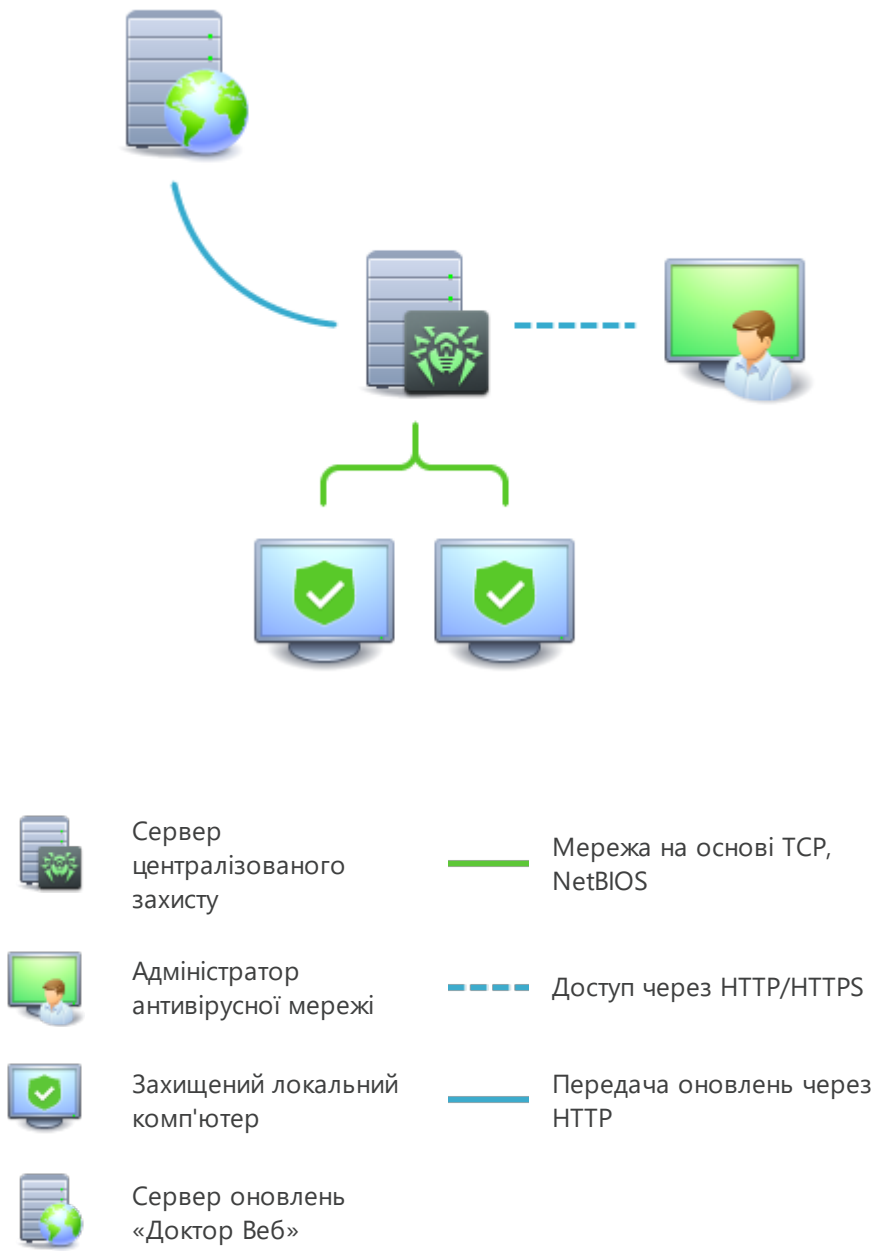


Рисунок 1. Логічна структура антивірусної мережі.

Оновлення та конфігурація локальних компонентів проводиться через *сервер централізованого захисту*. Весь потік команд, даних та статистичної інформації в антивірусній мережі також проходить через сервер централізованого захисту. Обсяги трафіку між захищеними комп'ютерами та сервером централізованого захисту може бути достатньо значним, тому передбачена можливість його стиснення. Використання шифрування при передачі даних дозволяє уникнути розголошення особистих відомостей та підміни програмного забезпечення, що завантажується на захищені комп'ютери.

Всі необхідні оновлення завантажуються на сервер централізованого захисту з серверів оновлень компанії «Доктор Веб».

Змінення в конфігурації локальних антивірусних компонентів та передача команд проводиться сервером централізованого захисту за вказівкою адміністраторів антивірусної мережі. Адміністратори управляють конфігурацією сервера централізованого захисту та формуванням антивірусної мережі (зокрема, підтверджують підключення локальної станції до мережі), а також, за необхідності, задають налаштування роботи конкретних локальних антивірусних компонентів.

Локальні антивірусні компоненти несумісні з антивірусним програмним забезпеченням як інших компаній, так і антивірусними рішеннями Dr.Web, що не підтримують режим централізованого захисту (наприклад, Dr.Web для Linux версії 5.0). Встановлення двох антивірусних програм на одному комп'ютері може призвести до відмови системи та до втрати важливих даних.

В режимі централізованого захисту можливий експорт та збереження звітів про функціонування Dr.Web для Linux за допомогою сервера централізованого захисту. Підтримується експорт та збереження звітів у форматах HTML, CSV, PDF та XML.

Підключення до антивірусної мережі

Dr.Web для Linux може бути підключений до антивірусної мережі таким чином:

- На вкладці **Режим** сторінки налаштувань вікна Dr.Web для Linux.
- За допомогою команди `esconnect` утиліти управління з командного рядка **drweb-ctl**.

Відключення від антивірусної мережі

Dr.Web для Linux може бути відключений від антивірусної мережі таким чином:

- На вкладці **Режим** сторінки налаштувань вікна Dr.Web для Linux.
- За допомогою команди `esdisconnect` утиліти управління з командного рядка **drweb-ctl**.

Системні вимоги та сумісність

В цьому розділі:

Системні вимоги

Використання Dr.Web для Linux можливе на комп'ютері, що задовольняє таким вимогам:

Компонент	Вимога
Платформа	Підтримуються процесори таких архітектур та систем команд: • **Intel/AMD**: 32-розрядні (*IA-32, x86*); 64-розрядні (*x86-64, x64, amd64*); • **ARM64**
Оперативна пам'ять (RAM)	Не менше 500 МБ вільної оперативної пам'яті (рекомендується 1 ГБ та більше).
Місце на жорсткому диску	Не менше 512 МБ вільного дискового простору на томі, на якому розміщуються каталоги Dr.Web для Linux.
Операційна система	**Linux** на основі ядра з версією 2.6.37 або вище, що використовує **PAM** та бібліотеку **glibc** версії 2.13 та вище. Список протестованих дистрибутивів **Linux** наведений нижче. Для коректної роботи компонента SpIDer Gate ядро ОС має бути зібране з включенням таких опцій: • *CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;* • *CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS;* • *CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.* Конкретний набір необхідних опцій з указаного списку може залежати від використовуваного дистрибутиву ОС **GNU/Linux**.
Інше	Наявність мережного підключення:

Компонент	Вимога
	• Підключення до мережі Інтернет для завантаження оновлень, а також для звернення до Dr.Web Cloud (за наявності відповідного дозволу від користувача). • При роботі в режимі централізованого захисту достатньо тільки підключення до використовуваного сервера в межах локальної мережі, доступ до Інтернету не потребується.

Для забезпечення правильної роботи Dr.Web для Linux мають бути відкриті такі порти:

Призначення	Напрямок	Номери портів
Для отримання оновлень	вихідний	80
Для з'єднання з хмарним сервісом Dr.Web Cloud	вихідний	2075 (у тому числі для UDP)

Dr.Web для Linux несумісний з іншими антивірусними програмами. Через те, що встановлення двох антивірусів на один комп'ютер може призвести до помилок в системі та до втрати важливих даних, перед встановленням Dr.Web для Linux видаліть з комп'ютера інші антивірусні програми.

Список протестованих дистрибутивів ОС

Працездатність Dr.Web для Linux протестована на таких дистрибутивах **Linux**:

Назва дистрибутиву Linux	Версії	Платформи
Astra Linux Special Edition (Смоленськ)	1.4, 1.5, 1.6	x86_64
ALT Linux Workstation	9	ARM64
ALT Linux Server	9	ARM64
CentOS	6.9, 7.7, 8	x86, x86_64. ARM64
Debian	7.11, 8.10, 9.3	x86_64
Fedora	27–29	x86, x86_64
Red Hat Enterprise Linux	7.4	x86_64
SUSE Linux Enterprise Server	11 SP4, 12 SP3	x86_64
Ubuntu	14.04, 16.04, 18.04	x86_64, ARM64

Інші дистрибутиви **Linux**, що відповідають описаним вимогам, не проходили тестування на сумісність з Dr.Web для Linux, але можуть бути сумісними. При виникненні проблем з сумісністю вашого дистрибутиву зверніться до Служби технічної підтримки.

Для архітектури ARM64 тестування на сумісність з Dr.Web for Linux проходили наступні дистрибутиви **GNU/Linux**: Ubuntu 18.04 , CentOS 7.7, ALT Linux Workstation 9 і ALT Linux Server 9. Інші дистрибутиви тестування не проходили, але можуть бути сумісні. При виникненні проблем з сумісністю вашого дистрибутиву зверніться до Служби технічної підтримки.

Необхідні додаткові компоненти та пакети

- Для роботи Dr.Web для Linux в графічному режимі, а також для запуску програм встановлення та видалення продукту для графічного режиму необхідна наявність графічної підсистеми **X Window System** та будь-якого менеджера вікон. Окрім того, для коректного відображення індикатора в графічному оточенні **Ubuntu Unity** можуть знадобитися додаткові бібліотеки (за замовчуванням необхідна бібліотека **libappindicator1**).
- Для роботи в графічному режимі програм встановлення та видалення, розрахованих на режим командного рядка, необхідна наявність в системі будь-якого емулятора терміналу (наприклад, **xterm** або **xvt**).
- Для підвищення привілеїв програм встановлення та видалення необхідна наявність будь-якої з утиліт підвищення прав: **su**, **sudo**, **gksu**, **gksudo**, **kdesu**, **kdesudo**. Для коректної роботи Dr.Web для Linux також необхідно, щоб в системі використовувався механізм аутентифікації **PAM**.

Для зручної роботи з Dr.Web для Linux з командного рядка рекомендується включити автодоповнення команд у використовуваній командній оболонці, якщо воно не включене.

При виникненні проблем зі встановленням необхідних додаткових пакетів та компонентів зверніться до довідкових посібників використовуваного вами дистрибутиву операційної системи.

Сумісність з компонентами операційних систем

- Монітор SpIDer Guard за замовчуванням використовує системний механізм **fanotify**, а в тих ОС, в яких механізм **fanotify** не реалізований або недоступний з інших причин — спеціальний *завантажуваний модуль ядра (LKM-модуль)*, який постачається в зібраному виді. До складу Dr.Web для Linux входять LKM-модулі для всіх систем **GNU/Linux**, вказаних вище. За необхідності ви можете зібрати модуль ядра самостійно з вихідних кодів, що постачаються для будь-якої ОС, яка використовує ядро **GNU/Linux** версії 2.6.x та вище.
  Для архітектури ARM64 можливість роботи з LKM не підтримується.

Робота SpIDer Guard через модуль ядра **GNU/Linux** (LKM-модуль) не підтримується для ОС, запущених в середовищі гіпервізора **Xen**. Спроба завантаження модуля ядра SpIDer Guard при роботі ОС в середовищі **Xen** може призвести до критичної помилки ядра (так звана помилка «*Kernel panic*»).

Робота SpIDer Guard в посиленому («агресивному») режимі з попереднім блокуванням доступу до ще не перевірених файлів можлива тільки через **fanotify** та за умови, що ядро ОС зібране з активною опцією `CONFIG_FANOTIFY_ACCESS_PERMISSIONS`.

- Монітор SpIDer Gate може конфліктувати з іншими міжмережними екранами, встановленими в вашій ОС:
  - Конфлікт з **Shorewall** та **SuseFirewall2** (в ОС **SUSE Linux Enterprise Server**). Ознакою конфлікту з цими міжмережними екранами є повідомлення про помилку SpIDer Gate з кодом `x109`. Спосіб усунення конфлікту описаний у розділі «Опис відомих помилок».
  - Конфлікт з **FirewallD** (в ОС **Fedora**, **CentOS**, **Red Hat Enterprise Linux**). Ознакою конфлікту з цим міжмережним екраном є повідомлення про помилку SpIDer Gate з кодом `x102`. Спосіб усунення конфлікту описаний у розділі «Опис відомих помилок».
- Якщо до складу ОС включений **NetFilter** версії *нижче 1.4.15*, при роботі SpIDer Gate можливе виникнення такої проблеми, пов'язаної з внутрішньою помилкою в реалізації **NetFilter**: при відключенні SpIDer Gate порушується робота мережі. Рекомендується оновити ОС до версії, що містить **NetFilter** версії 1.4.15 або вище. Спосіб усунення вказаної проблеми наведений у розділі «Опис відомих помилок».
- В штатному режимі роботи монітор SpIDer Gate сумісний з усіма програмами користувача, що використовують мережу, включаючи веб-браузери та поштові клієнти. Для коректної перевірки захищених з'єднань необхідно додати сертифікат Dr.Web для Linux до списку довірених сертифікатів тих програм, які використовують захищені з'єднання (наприклад, веб-браузери та поштові клієнти).
- Після внесення змінень в роботу монітора SpIDer Gate (включення раніше відключеного монітора, змінення режиму перевірки захищених з'єднань) необхідно *перезапускати поштові клієнти*, що використовують протокол IMAP для отримання повідомлень електронної пошти з поштового сервера.

Сумісність з підсистемами безпеки

При налаштуваннях за замовчуванням Dr.Web для Linux не сумісний з підсистемою поліпшення безпеки **SELinux**. Окрім того, за замовчуванням Dr.Web для Linux працює в режимі обмеженої функціональності в системах **GNU/Linux**, що використовують мандатні моделі доступу (наприклад, в системах, оснащених підсистемою мандатного доступу **PARSEC**, основаній на присвоєнні користувачам та файлам різних рівнів привілеїв, які називаються мандатними рівнями).

Для встановлення Dr.Web для Linux в системи з **SELinux**, а також в системи, що використовують мандатні моделі доступу, може знадобитися додаткове налаштування підсистем безпеки, щоб зняти обмеження у функціонуванні Dr.Web для Linux. Докладніше див. у розділі Налаштування підсистем безпеки.

Ліцензування

Права користувача на використання копії Dr.Web для Linux підтверджуються та регулюються ліцензією, яка придбана користувачем у компанії «Доктор Веб» або у її партнерів. Параметри ліцензії, що регулюють права користувача, встановлені відповідно до Ліцензійної угоди (див. https://license.dataprotection.com.ua/agreement/), умови якої приймаються користувачем при встановленні Dr.Web для Linux на свій комп'ютер. В ліцензії фіксується інформація про користувача та продавця, а також параметри використання придбаної копії продукту, зокрема:

- Список компонентів, дозволених використовувати даному користувачу.
- Період, протягом якого дозволене використання Dr.Web для Linux.
- Інші обмеження (зокрема, кількість комп'ютерів, на яких дозволено використовувати придбану копію Dr.Web для Linux).

З метою ознайомлення з можливостями продукту ви можете активувати *демонстраційний період*. Після активації демонстраційного періоду ви отримуєте право на повноцінне використання встановленої копії Dr.Web для Linux протягом усього цього періоду.

Кожній ліцензії на використання програмних продуктів компанії «Доктор Веб» зіставлений унікальний серійний номер, а на локальному комп'ютері з ліцензією пов'язується спеціальний файл, що регулює роботу компонентів Dr.Web для Linux відповідно до параметрів ліцензії. Він називається *ліцензійним ключовим файлом*. При активації демонстраційного періоду також автоматично формується спеціальний ключовий файл, що називається *демонстраційним*.

За відсутності діючої ліцензії або активованого демонстраційного періоду (у тому числі, якщо термін дії раніше придбаної ліцензії або демонстраційного періоду завершився), антивірусні функції Dr.Web для Linux блокуються. Окрім того, недоступний сервіс отримання оновлень вірусних баз Dr.Web з серверів оновлень компанії «Доктор Веб». Проте є можливість активувати Dr.Web для Linux, підключивши його до сервера централізованого захисту антивірусної мережі підприємства або антивірусної мережі, організованої інтернет-провайдером. В цьому випадку управління антивірусними функціями та оновленнями копії продукту, встановленого на комп'ютері, покладається на сервер централізованого захисту.

Встановлення та видалення

В цьому розділі описуються процедури встановлення та видалення Dr.Web для Linux версії 11.1, а також процедура отримання поточних оновлень та процедура переходу на нову версію, якщо на вашому комп'ютері вже встановлений Dr.Web для Linux попередньої версії.

Окрім того, в цьому розділі описана процедура вибіркового встановлення та видалення компонентів Dr.Web для Linux (наприклад, для усунення помилок, що виникли у процесі його експлуатації, або для отримання встановлення з обмеженим набором функцій) та налаштування розширених підсистем безпеки (таких, як **SELinux**), що може знадобитися при встановленні або у процесі експлуатації Dr.Web для Linux.

- Встановлення Dr.Web для Linux.
- Оновлення Dr.Web для Linux.
- Видалення Dr.Web для Linux.
- Налаштування підсистем безпеки.
- Додатково:
  - Розташування файлів Dr.Web для Linux.
  - Вибіркове встановлення та видалення компонентів.

Для проведення цих операцій необхідні права суперкористувача (користувача *root*). Щоб отримати права суперкористувача, скористайтеся командою зміни користувача **su** або командою виконання від імені іншого користувача **sudo**.

Не гарантується сумісність Dr.Web для Linux з іншими антивірусними програмами інших виробників. Через те, що встановлення двох антивірусів на один комп'ютер може призвести до *помилок в системі та до втрати важливих даних*, перед встановленням Dr.Web для Linux *необхідно* видалити з комп'ютера інші антивірусні програми.

Якщо на вашому комп'ютері *вже є* інший антивірусний продукт Dr.Web, встановлений з універсального пакета (`.run`), та ви бажаєте встановити ще один антивірусний продукт Dr.Web (наприклад, у вас з універсального пакета встановлений продукт Dr.Web для файлових серверів UNIX, й ви хочете додатково до нього встановити продукт Dr.Web для Linux), попередньо переконайтеся, що версія вже встановленого продукту *збігається* з версією Dr.Web для Linux, яку ви плануєте встановити. Якщо версія, яку ви збираєтесь встановити, новіша, ніж версія продукту, вже встановленого на вашому комп'ютері, *перед початком* встановлення оновіть вже встановлений продукт до версії того продукту Dr.Web, який ви хочете встановити додатково.

Встановлення Dr.Web для Linux

Ви можете встановити Dr.Web для Linux в один з двох способів:

1. Завантаживши з сайта компанії «Доктор Веб» інсталяційний файл, що містить універсальний пакет для UNIX-систем та програми встановлення в графічному режимі та режимі командного рядка (на початку встановлення буде запущена одна з них, залежно від можливостей оточення).
2. Встановивши Dr.Web для Linux в виді набору нативних пакетів (для цього необхідно підключитися до відповідного репозиторію пакетів компанії «Доктор Веб»).

Після встановлення Dr.Web для Linux в будь-який з указаних в цьому Посібнику способів, на початку роботи вам необхідно або активувати ліцензію, або встановити ключовий файл, якщо він у вас вже є, або підключити Dr.Web для Linux до сервера централізованого захисту. Поки ви цього не зробите, *функції антивірусного захисту будуть відключені.*

Якщо в системі запущений поштовий клієнт (такий, як **Mozilla Thunderbird**), що використовує для отримання повідомлень електронної пошти протокол IMAP, його необхідно перезапустити після завершення встановлення антивірусу, щоб забезпечити перевірку вхідних листів.

Dr.Web для Linux, встановлений в будь-який з розглянутих в даному розділі способів, ви можете у подальшому видалити або оновити за наявності виправлень для компонентів, що входять до його складу, або при виході нової версії продукту. За необхідності проведіть також налаштування підсистем безпеки **Linux** для коректної роботи Dr.Web для Linux. При виникненні проблем з функціонуванням окремих компонентів ви можете провести їх вибіркове встановлення та видалення, не видаляючи Dr.Web для Linux цілком.

Встановлення універсального пакета

Dr.Web для Linux розповсюджується в виді інсталяційного файла з іменем `drweb-<версія>-av-linux-<платформа>.run`, де <*платформа*> — рядок, що вказує тип платформи, для якої призначений продукт (`x86` для 32-розрядних платформ та `amd64` для 64-розрядних платформ). Наприклад:

```
drweb-11.1-av-linux-amd64.run
```

Надалі ім'я інсталяційного файла вказуватиметься як <*ім'я_файла*>`.run`.

Щоб встановити компоненти Dr.Web для Linux:

1. Завантажте інсталяційний файл з офіційного сайта компанії «Доктор Веб».
2. Збережіть його на жорсткий диск комп'ютера в будь-який доступний каталог (наприклад, `/home/`<*username*>, де <*username*> — ім'я поточного користувача).

3. Перейдіть до каталогу зі збереженим файлом та запустіть його на виконання, наприклад, командою:

```
# chmod +x <ім'я_файла>.run
```

4. Запустіть його на виконання командою:

```
# ./<ім'я_файла>.run
```

або скористайтеся стандартним файловим менеджером вашої графічної оболонки як для змінення властивостей файла, так і для його запуску.

> При встановленні Dr.Web для Linux в середовищі ОС **Astra Linux SE** версії 1.6, що працює в режимі *ЗПС*, може статися відмова в запуску програми встановлення через відсутність відкритого ключа компанії «Доктор Веб» у списку довірених ключів. В цьому випадку необхідно провести попереднє налаштування режиму ЗПС (див. Налаштування запуску в режимі ЗПС (Astra Linux SE, версія 1.6)), після чого запустити програму встановлення повторно.

Спочатку буде перевірена цілісність архіву, потім файли, що містяться в архіві, будуть розпаковані в тимчасовий каталог та автоматично запуститься програма встановлення. Якщо запуск був проведений не з правами суперкористувача, то програма встановлення автоматично спробує підвищити свої права, запитавши пароль (використовується **sudo**). Якщо спроба підвищення прав завершиться невдало, встановлення буде завершене.

> Якщо в частині файлової системи, що містить тимчасовий каталог, немає достатнього вільного місця для розпакування дистрибутиву, процес встановлення буде завершений після видачі відповідного повідомлення. В цьому випадку повторіть розпакування, змінивши значення системної перемінної оточення `TMPDIR` таким чином, щоб вона вказувала на каталог з достатньою кількістю вільного місця. Також ви можете скористатися ключем розпакування в указаний каталог `--target` (див. у розділі Вибіркове встановлення та видалення компонентів).

Залежно від можливостей поточного оточення, в якому проведений запуск дистрибутиву, запуститься одна з програм встановлення, що входять до складу дистрибутиву:

- Програма встановлення для графічного режиму.
- Програма встановлення для режиму командного рядка.

При цьому програма встановлення для режиму командного рядка запуститься автоматично, якщо неможливо запустити програму встановлення для графічного режиму.

5. Слідуйте інструкціям програми встановлення.

Існує можливість запустити програму встановлення повністю в автоматичному режимі, виконавши команду:

```
# ./<ім'я_файла>.run -- --non-interactive
```

В цьому випадку програма встановлення буде запущена повністю в автоматичному режимі, без показу інтерфейсу користувача (включаючи діалоги програми встановлення для режиму командного рядка).

Зверніть увагу, що можна:

- Використання цієї опції означає, що ви *погоджуєтеся* з умовами Ліцензійної угоди Dr.Web. Ознайомитися з текстом Ліцензійної угоди після встановлення продукту ви можете, прочитавши файл `/opt/drweb.com/share/doc/LICENSE`. Розширення файла вказує мову, якою написаний текст Ліцензійної угоди. Файл `LICENSE` без розширення містить текст Ліцензійної угоди Dr.Web англійською мовою. Якщо ви *не згодні* з умовами Ліцензійної угоди, ви маєте видалити Dr.Web для Linux після встановлення.
- Запуск програми встановлення повністю в автоматичному режимі потребує прав суперкористувача. Щоб підвищити права, ви можете використати команду **su** та **sudo**.

Якщо ваш дистрибутив **Linux** оснащений підсистемою безпеки **SELinux**, то можлива ситуація, коли робота програми встановлення буде перерване підсистемою безпеки. В цьому випадку вам необхідно тимчасово перевести **SELinux** в режим *дозволу (Permissive)*, для чого виконайте команду:

```
# setenforce 0
```

Після цього перезапустіть програму встановлення. Також в цьому випадку після завершення процесу встановлення необхідно виконати налаштування політик безпеки **SELinux**, щоб у подальшому антивірусні компоненти працювали коректно.

Всі інсталяційні файли, витягнуті з архіву, будуть автоматично видалені після завершення встановлення.

Рекомендується зберегти завантажений файл *<ім'я_файла>*`.run`, з якого проводилося встановлення, з метою можливого перевстановлення Dr.Web для Linux або його компонентів у подальшому без оновлення його версії.

Після завершення встановлення в графічній оболонці робочого столу в меню **Програми**, з'явиться група **Dr.Web**, що містить два пункти:

- **Dr.Web для Linux** для запуску Dr.Web для Linux в графічному режимі.
- **Удалить компоненты Dr.Web** для його видалення.

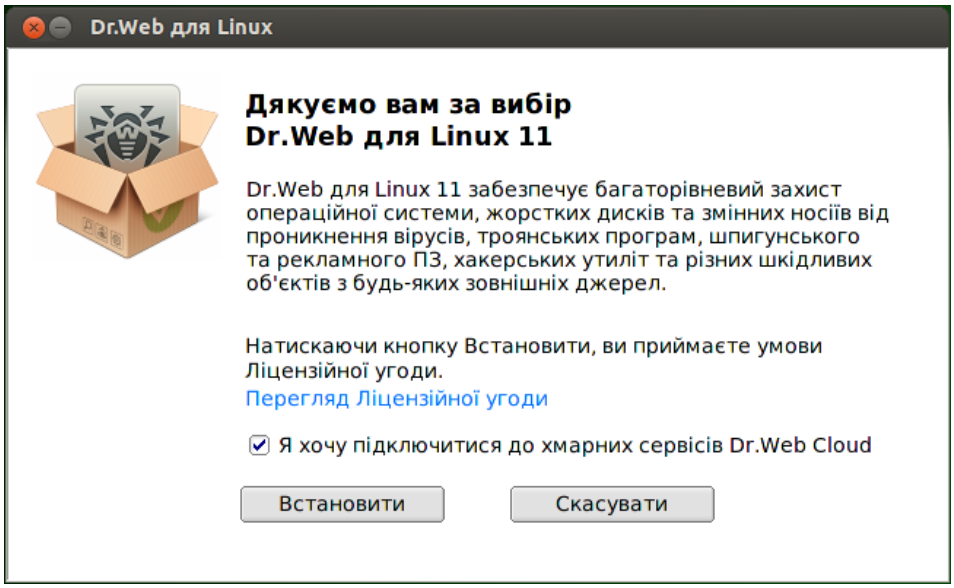
Значок індикатора стану програми з'явиться в області сповіщень робочого столу автоматично після повторного входу користувача в систему.

Для коректної роботи Dr.Web для Linux додатково може знадобитися встановлення пакетів, наведених у розділі Системні вимоги та сумісність (наприклад, бібліотеку підтримки виконання 32-розрядних програм для 64-розрядної платформи, а також бібліотеку **libappindicator1** для коректного відображення індикатора стану програми в області сповіщень робочого столу).

Встановлення в графічному режимі

Якщо програма встановлення на початку своєї роботи виявить наявність на комп'ютері ряду проблем, які можуть у подальшому призвести до повної або часткової непрацездатності Dr.Web для Linux, на екрані з'явиться відповідне вікно зі списком виявлених проблем. Ви можете перервати встановлення, натиснувши **Вихід**, щоб усунути виявлені проблеми до початку встановлення. В цьому випадку після розв'язання виявлених проблем (встановлення необхідних додаткових бібліотек, тимчасового відключення **SELinux** тощо), програму встановлення необхідно запустити повторно. Ви можете не переривати встановлення Dr.Web для Linux, для цього натисніть **Продовжити**. В цьому випадку програма встановлення продовжить свою роботу та покаже вікно майстра встановлення. Проте вам необхідно усунути виявлені проблеми пізніше, після завершення процесу встановлення, або при виявленні помилок в роботі Dr.Web для Linux.

Після запуску програми встановлення, яка працює в графічному режимі, на екрані з'явиться вікно майстра встановлення.



Малюнок 2. Сторінка привітання майстра встановлення.

Для встановлення Dr.Web для Linux на свій комп'ютер необхідно послідовно виконати такі дії:

1. Ознайомтеся з умовами Ліцензійної угоди компанії «Доктор Веб». Для цього клацніть по відповідному посиланню на стартовій сторінці майстра встановлення. Після цього

відкриється сторінка з текстом Ліцензійної угоди та відомостями по авторські права на компоненти, які будуть встановлені на ваш комп'ютер.

За необхідності, якщо в вашій системі встановлений та налаштований принтер, ви можете роздрукувати текст Ліцензійної угоди та відомості про авторські права. Для цього відкрийте потрібну вкладку на сторінці та натисніть кнопку **Друк**.

Щоб закрити сторінку ознайомлення з Ліцензійною угодою та авторськими правами, натисніть кнопку **ОК**.

2. Перед початком встановлення ви можете погодитися з тим, що після встановлення Dr.Web для Linux автоматично підключиться до хмарного сервісу Dr.Web Cloud. Для цього встановіть відповідний прапорець (за замовчуванням він встановлений в момент запуску майстра встановлення). Якщо ви не хочете дозволити Dr.Web для Linux використовувати хмарний сервіс Dr.Web Cloud, скиньте прапорець. За необхідності, ви в будь-який момент зможете дозволити або заборонити Dr.Web для Linux використовувати сервіс Dr.Web Cloud в налаштуваннях програми.
3. Щоб розпочати встановлення, натисніть **Встановити**. Тим самим ви одночасно підтверджуєте, що приймаєте умови Ліцензійної угоди компанії «Доктор Веб». Якщо ви вирішили відмовитися від встановлення Dr.Web для Linux на свій комп'ютер, натисніть **Скасувати**. Майстер встановлення завершить роботу.
4. Після початку встановлення відкриється сторінка майстра з індикатором, що показує прогрес процесу встановлення. Якщо ви хочете ознайомитися з записами в журналі встановлення, натисніть **Докладніше**.
5. Після успішного завершення процесу копіювання файлів програми та внесення необхідних змінень в системні файли, відкриється фінальна сторінка майстра, що відображає результат встановлення.
6. Щоб закрити вікно майстра встановлення, натисніть кнопку **ОК**. Якщо дана операція підтримується можливостями оточення, на фінальному кроці з'явиться сторінка з запрошенням запустити Dr.Web для Linux в графічному режимі. Для запуску встановіть прапорець **Запустити Dr.Web для Linux зараз** та натисніть **ОК**.

Якщо встановлення було перерване через помилку, фінальна сторінка майстра міститиме відповідне повідомлення. В цьому випадку закрийте майстер встановлення, натиснувши кнопку **ОК**. Після усунення проблеми, що спричинила помилку встановлення, запустіть встановлення знову.

Встановлення в режимі командного рядка

Після запуску програми встановлення, що працює з режимі командного рядка, на екрані з'явиться текст запрошення до встановлення.

1. Щоб розпочати встановлення, введіть *Yes* або *Y* на запит «Ви хочете продовжити?». Щоб відмовитися від встановлення, введіть *No* або *N*. В цьому випадку робота програми встановлення буде завершена.
2. Далі вам необхідно ознайомитися з текстом Ліцензійної угоди компанії «Доктор Веб», який буде виведений на екран. Щоб перегортати текст ліцензійної угоди, скористайтеся клавішами ENTER (перегортання тексту на один рядок вниз) та ПРОБІЛ

(перегортання тексту вниз на екран). Зверніть увагу, що перегортання тексту Ліцензійної угоди назад (вгору) не передбачене.

3. Після читання Ліцензійної угоди вам буде запропоновано прийняти її умови. Введіть *Yes* або *Y*, якщо ви приймаєте умови, та *No* або *N*, якщо ви не згодні з умовами Ліцензійної угоди. Після відмови від прийняття умов Ліцензійної угоди робота програми встановлення буде завершена.
4. Після погодження з умовами Ліцензійної угоди автоматично буде запущений процес встановлення на комп'ютер компонентів Dr.Web для Linux. При цьому на екран виводитиметься інформація про процес встановлення, що містить список встановлюваних компонентів (журнал встановлення).
5. Після завершення процесу встановлення програма встановлення завершить свою роботу автоматично. При виникненні помилок на екран буде виведене відповідне повідомлення з описом помилки, після чого робота програми встановлення також буде завершена.
6. Щоб розпочати роботу зі встановленим Dr.Web для Linux, скористайтеся будь-яким зручним для вас способом запуску.

Якщо встановлення було перерване через помилки, усуньте проблеми, що спричинили помилку встановлення, та повторіть процес встановлення знову.

Встановлення з репозиторію

Нативні пакети Dr.Web для Linux знаходяться в офіційному репозиторії Dr.Web https://repo.drweb.com. Після додавання репозиторію Dr.Web до списку репозиторіїв, що використовуються менеджером пакетів вашої операційної системи, ви зможете встановлювати його в виді нативних пакетів для операційної системи так само, як і будь-якої іншої програми з репозиторіїв вашої операційної системи. Необхідні залежності розв'язуватимуться автоматично. Окрім того, в цьому випадку підтримується процедура виявлення пакетним менеджером ОС оновлень всіх компонентів Dr.Web, встановлених з підключеного репозиторію, та пропозиція встановлення всіх виявлених оновлень.

Для доступу до репозиторію Dr.Web необхідне підключення до мережі Інтернет.

Все наведенні нижче команди для підключення репозиторіїв, імпортування ключів, встановлення та видалення пакетів мають бути виконані з правами суперкористувача (користувача *root*). Щоб отримати відповідні права, використовуйте команду зміни користувача **su** або команду виконання від імені іншого користувача **sudo**.

Нижче наведені процедури для таких ОС (менеджерів пакетів):

- Debian, Mint, Ubuntu (apt).
- ALT Linux, PCLinuxOS (apt-rpm).
- Mageia, OpenMandriva Lx (urpmi).
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf).

- SUSE Linux (zypper).

Debian, Mint, Ubuntu (apt)

1. Репозиторій для цих ОС захищений цифровим підписом «Доктор Веб». Для доступу до репозиторію імпортуйте та додайте ключ цифрового підпису у сховище пакетного менеджера, виконавши команду:

```
# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
8C42FC58D8752769
```

2. Щоб підключити репозиторій, додайте такий рядок в файл `/etc/apt/sources.list`:

```
deb https://repo.drweb.com/drweb/debian 11.1 non-free
```

Ви можете виконати пункти 1 та 2, завантаживши з репозиторію та встановивши спеціальний DEB-пакет.
Посилання на завантаження пакета: https://repo.drweb.com/drweb/drweb-repo11.1.deb.

3. Для встановлення Dr.Web для Linux з репозиторію виконайте команди:

```
# apt-get update
# apt-get install drweb-workstations
```

Встановлення також може проводитися за допомогою альтернативних менеджерів (наприклад, **Synaptic** або **aptitude**). Окрім того, альтернативні менеджери, такі, як **aptitude**, рекомендується використовувати для розв'язання конфлікту пакетів, якщо він виникне.

ALT Linux, PCLinuxOS (apt-rpm)

1. Щоб підключити репозиторій, додайте такий рядок в файл `/etc/apt/sources.list`:

```
rpm https://repo.drweb.com/drweb/altlinux 11.1/<arch> drweb
```

де <*arch*> — позначення використовуваної архітектури пакетів:

- Для **32-розрядної** версії: `i386`
- Для **64-розрядної** версії: `x86_64`
- Для **архитектурі ARM64**: `aarch64`

2. Для встановлення Dr.Web для Linux з репозиторію виконайте команди:

```
# apt-get update
# apt-get install drweb-workstations
```

Встановлення також може проводитися за допомогою альтернативних менеджерів (наприклад, **Synaptic** або **aptitude**).

Mageia, OpenMandriva Lx (urpmi)

1. Підключіть репозиторій за допомогою команди:

```
# urpmi.addmedia drweb https://repo.drweb.com/drweb/linux/11.1/<arch>/
```

де <*arch*> — позначення використовуваної архітектури пакетів:

- Для **32-розрядної** версії: `i386`
- Для **64-розрядної** версії: `x86_64`

2. Для встановлення Dr.Web для Linux з репозиторію виконайте команду:

```
# urpmi drweb-workstations
```

Встановлення також може проводитися за допомогою альтернативних менеджерів (наприклад, **rpmdrake**).

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

1. Додайте файл `drweb.repo` з таким вмістом до каталогу `/etc/yum.repos.d`:

```
[drweb]
name=DrWeb - 11.1
baseurl=https://repo.drweb.com/drweb/linux/11.1/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```

Якщо планується записати наведений вище вміст в файл за допомоги команди типу **echo** з перенаправленням виведення, символ `$` необхідно екранувати: `\$`.

Ви можете виконати пункт 1, завантаживши з репозиторію та встановивши спеціальний RPM-пакет.
Посилання на завантаження пакета: https://repo.drweb.com/drweb/drweb-repo11.1.rpm.

2. Для встановлення Dr.Web для Linux з репозиторію виконайте команду:

```
# yum install drweb-workstations
```

В ОС **Fedora**, починаючи з версії 22, рекомендується замість менеджера **yum** використовувати менеджер **dnf**, наприклад:

```
# dnf install drweb-workstations
```

Встановлення також може проводитися за допомогою альтернативних менеджерів (наприклад, **PackageKit** або **Yumex**).

SUSE Linux (zypper)

1. Щоб підключить репозиторій, запустіть таку команду:

```
# zypper ar https://repo.drweb.com/drweb/linux/11.1/\$basearch/ drweb
```

2. Для встановлення Dr.Web для Linux з репозиторію виконайте команди:

```
# zypper refresh
# zypper install drweb-workstations
```

Встановлення також може проводитися за допомогою альтернативних менеджерів (наприклад, **YaST**).

Оновлення Dr.Web для Linux

Передбачено два режими оновлення Dr.Web для Linux:

1. Отримання оновлень пакетів та компонентів, випущених в рамках експлуатації поточної версії Dr.Web для Linux (як правило, такі оновлення містять виправлення помилок та дрібні покращення в функціонуванні компонентів);
2. Перехід на нову версію продукту. Цей спосіб оновлення використовується, якщо компанія «Доктор Веб» випустила нову версію Dr.Web для Linux , що відрізняється новими можливостями.

Отримання поточних оновлень

Після встановлення Dr.Web для Linux в будь-який зі способів, описаних у відповідному розділі, проходить автоматичне підключення менеджера пакетів до репозиторію пакетів Dr.Web:

- Якщо встановлення проводилося з універсального пакета (файл `.run`), а в системі використовуються пакети у форматі DEB (наприклад, ОС **Debian**, **Mint**, **Ubuntu**), для роботи з пакетами Dr.Web використовується окрема версія менеджера пакетів **zypper**, автоматично встановлена в рамках встановлення Dr.Web для Linux.

  Щоб отримати та встановити оновлені пакети Dr.Web цим менеджером, перейдіть до каталогу <*opt_dir*>`/bin` (для **GNU/Linux** — `/opt/drweb.com/bin`), та виконайте такі команди:

  ```
  # ./zypper refresh
  # ./zypper update
  ```

- В решті випадків використовуйте команди оновлення пакетного менеджера, що використовується в вашій ОС, наприклад:
  - В **Red Hat Enterprise Linux** та **CentOS** використовуйте команду **yum** ;
  - В **Fedora** використовуйте команду **yum** або **dnf** ;
  - В **SUSE Linux** використовуйте команду **zypper** ;
  - В **Mageia**, **OpenMandriva Lx** використовуйте команду **urpmi** ;
  - В **Alt Linux**, **PCLinuxOS**, **Debian**, **Mint**, **Ubuntu** використовуйте команду **apt-get**.

Також ви можете використовувати й альтернативні менеджери пакетів, розроблені для вашої операційної системи. За необхідності зверніться до довідкового посібника з використовуваного вами менеджера пакетів.

При випуску нової версії Dr.Web для Linux пакети, що містять його компоненти, поміщуються у розділ репозиторію Dr.Web, відповідний новій версії продукту. В цьому випадку для оновлення необхідно переключити менеджер пакетів на новий розділ репозиторію Dr.Web (див. Перехід на нову версію).

Перехід на нову версію

Попередні зауваження

Підтримується процедура оновлення попередніх версій Dr.Web для Linux до версії 11.1. Перехід на нову версію Dr.Web для Linux проводьте в той самий спосіб, в який була встановлена версія Dr.Web для Linux, яку необхідно оновити:

- Якщо версія Dr.Web для Linux, яку необхідно оновити, була встановлена з репозиторію, то перехід на нову версію проводьте оновленням з репозиторію.
- Якщо версія Dr.Web для Linux, яку необхідно оновити, була встановлена з універсального пакета, то для переходу на нову версію встановіть універсальний пакет, що містить нову версію продукту.

Щоб уточнити спосіб, в який була встановлена версія Dr.Web для Linux, яку необхідно оновити, перевірте в каталозі виконуваних файлів Dr.Web для Linux наявність сценарію програми видалення `remove.sh`. Якщо цей файл наявний, поточна версія Dr.Web для Linux була встановлена з універсального пакета, а в іншому випадку — з репозиторію.

Якщо неможливо оновити Dr.Web для Linux в той самий спосіб, в який він був встановлений первісно, вам попередньо видаліть поточну версію продукту, а потім проведіть встановлення нової версії продукту в доступний для вас спосіб. Способи встановлення та видалення попередніх версій продукту Dr.Web для Linux аналогічні способам встановлення та видалення, розглянутим в цьому Посібнику для версії 11.1. За додатковою інформацією зверніться до Посібника користувача встановленої у вас версії Dr.Web для Linux.

Зверніть увагу, що перехід з Dr.Web для Linux версії 6.0.2 та нижче на версію 11.1 можливий *тільки* шляхом попереднього видалення старої версії Dr.Web для Linux з подальшим встановленням продукту версії 11.1.

Якщо версія Dr.Web для Linux, яку необхідно оновити, працює під управлінням сервера централізованого захисту, то перед початком оновлення рекомендується зберегти адресу сервера централізованого захисту, до якого підключений Dr.Web для Linux. Щоб отримати адресу сервера централізованого захисту, до якого підключений Dr.Web для Linux з версією вище 6.0.2, скористайтеся командою:

```
$ drweb-ctl appinfo
```

з рядка виведення команди:

```
ESAgent; <PID>; RUNNING 1; Connected <адреса>, on-line
```

збережіть частину <*адреса*> (може виглядати як рядок виду `tcp://`<*IP-адреса*>`:`<*порт*>, наприклад: `tcp://10.20.30.40:1234`). Окрім того, рекомендується зберегти файл сертифікату сервера.

При виникненні ускладнень з отриманням параметрів поточного підключення зверніться до Посібника адміністратора зі встановленої версії Dr.Web для Linux, а також до адміністратора вашої антивірусної мережі.

Оновлення з версії 9.0 та вище

Оновлення встановленням універсального пакета

Проведіть встановлення Dr.Web для Linux версії 11.1 з універсального пакета. У процесі встановлення за необхідності вам буде запропоновано автоматично видалити наявні компоненти старої версії Dr.Web для Linux.

Оновлення з репозиторію

Щоб оновити поточну версію Dr.Web для Linux, встановлену з репозиторію компанії «Доктор Веб», залежно від типу використовуваних пакетів виконайте такі дії:

- **При використанні пакетів RPM (yum)**:
  1. Змініть використовуваний репозиторій (з репозиторію пакетів поточної версії на репозиторій пакетів версії 11.1).

     Ім'я репозиторію, що містить пакети версії 11.1, див. у розділі Встановлення з репозиторію. Щоб уточнити спосіб змінення репозиторіїв, зверніться до довідкових посібників використовуваного вами дистрибутиву операційної системи.

  2. Встановіть нову версію Dr.Web для Linux з репозиторію, виконавши команду:

     ```
     # yum update
     ```

     або, якщо використовується менеджер **dnf** (як, наприклад, в ОС **Fedora** версії 22 та вище):

     ```
     # dnf update
     ```

     Якщо у процесі оновлення пакетів станеться помилка, то проведіть видалення та подальше повторне встановлення Dr.Web для Linux. За необхідності див. розділи Видалення Dr.Web для Linux, встановленого з репозиторію та Встановлення з репозиторію (пункти, відповідні використовуваній вами ОС та менеджеру пакетів).

- **При використанні пакетів DEB (apt-get)**:

1. Змініть використовуваний репозиторій (з репозиторію пакетів поточної версії на репозиторій пакетів версії 11.1).
2. Оновіть пакети Dr.Web для Linux, виконавши команду:

```
# apt-get update
# apt-get dist-upgrade
```

Зверніть увагу, що в ОС **Ubuntu** 14.04 (64-розрядна версія) виконання команди **apt-get** `dist-upgrade` для оновлення дистрибутиву може завершитися невдачею. В цьому випадку скористайтеся менеджером пакетів **aptitude** (для оновлення дистрибутива використовуйте команду **aptitude** `dist-upgrade`).

Перенесення ключового файла

При будь-якому способі оновлення Dr.Web для Linux наявний у вас ліцензійний ключовий файл буде автоматично встановлений в потрібне місце для використання новою версією Dr.Web для Linux.

При виникненні проблем з автоматичним встановленням ліцензійного ключового файла, ви можете виконати його встановлення вручну. Dr.Web для Linux, починаючи з версії 9.0, зберігає ключовий файл в каталозі `/etc/opt/drweb.com`. При втраті діючого ліцензійного ключового файла зверніться до Служби технічної підтримки компанії «Доктор Веб».

Повторне підключення до сервера централізованого захисту

Якщо це можливо, то після оновлення (якщо оновлювана версія була підключена до сервера централізованого захисту) підключення буде відновлене автоматично. Якщо підключення не відновилося автоматично, для підключення оновленої версії Dr.Web для Linux до антивірусної мережі скористайтеся будь-яким з таких способів (зверніть увагу, що вам доведеться вказати попередньо збережені адресу та файл публічного ключа сервера):

- Встановіть прапорець на вкладці **Режим** вікна налаштувань Dr.Web для Linux.
- Виконайте команду:

```
$ drweb-ctl esconnect <адреса> --Certificate <шлях до файла сертифікату сервера>
```

При виникненні ускладнень з підключенням зверніться до адміністратора вашої антивірусної мережі.

Особливості процесу оновлення

- При оновленні з репозиторію при працюючому Dr.Web для Linux оновлюваної версії, після завершення встановлення пакетів нової версії Dr.Web для Linux, процеси старої

версії Dr.Web для Linux залишаться запущеними до виходу користувача з системи, у тому числі — в області сповіщень робочого столу (якщо ви працюєте в графічному режимі) може бути доступний значок індикатора старої версії Dr.Web для Linux.

- При оновленні Dr.Web для Linux налаштування SplDer Gate можуть бути скинуті в значення за замовчуванням.
- Якщо в системі запущений поштовий клієнт (такий, як **Mozilla Thunderbird**), що використовує для отримання повідомлень електронної пошти протокол IMAP, перезапустіть його після завершення оновлення, щоб забезпечити перевірку вхідних листів.

Оновлення з версії 6.0.2 та нижче

Перехід з Dr.Web для Linux версії 6.0.2 та нижче на версію 11.1 можливий тільки шляхом попереднього видалення старої версії Dr.Web для Linux з подальшим встановленням продукту версії 11.1. За додатковою інформацією про способи видалення старої версії Dr.Web для Linux зверніться до Посібника користувача встановленої у вас версії Dr.Web для Linux.

Перенесення ключового файла

Наявний у вас ліцензійний ключовий файл старої версії Dr.Web для Linux не буде автоматично встановлений для використання новою версією, але ви можете провести його встановлення вручну. Dr.Web для Linux версії 6.0.2 та нижче зберігає ключовий файл в каталозі `/home/<user>/.drweb` (каталог має атрибут «прихований»). При втраті діючого ліцензійного ключового файла зверніться до Служби технічної підтримки компанії «Доктор Веб».

Dr.Web для Linux версії 11.1 не підтримує карантин Dr.Web для Linux версій, нижчих за 9.0. За наявності в карантині цієї версії продукту ізольованих файлів ви можете витягнути їх звідти або остаточно видалити вручну. Dr.Web для Linux версії 6.0.2 (та нижче) використовує як карантин такі каталоги:

- `/var/drweb/infected` — системний карантин;
- `/home/<user>/.drweb/quarantine` — карантин користувача (де *<user>* — ім'я користувача).

Щоб спростити обробку карантину, рекомендується провести ревізію його вмісту безпосередньо з ранньої версії Dr.Web для Linux перед початком переходу на нову версію.

Видалення Dr.Web для Linux

Залежно від способу встановлення, ви можете видалити Dr.Web для Linux в один з двох способів:

1. Запустивши програму видалення універсального пакета (для графічного режиму або режиму командного рядка, залежно від можливостей оточення).
2. Видаливши пакети, встановлені з репозиторію компанії «Доктор Веб», використовуючи системний менеджер пакетів.

Видалення універсального пакета

Видалення Dr.Web для Linux, встановленого з універсального пакета, можна провести як через меню програм оточення графічного робочого столу, так і за допомогою командного рядка.

Зверніть увагу, що програма видалення видалить не тільки Dr.Web для Linux, але й *всі інші* продукти Dr.Web, встановлені на вашому комп'ютері.

Якщо на вашому комп'ютері, окрім Dr.Web для Linux, встановлені й інші продукти Dr.Web, для видалення тільки Dr.Web для Linux замість запуску програми автоматичного видалення скористайтеся процедурою вибіркового встановлення та видалення компонентів.

Видалення Dr.Web для Linux через меню програм

Для цього в меню програм виберіть групу **Dr.Web**, в якій виберіть пункт меню **Удалить компоненты Dr.Web**. Далі буде запущена програма видалення для графічного режиму.

Видалення Dr.Web для Linux з командного рядка

Запуск програми видалення виконується сценарієм `remove.sh`, розташованим в каталозі `/opt/drweb.com/bin`. Таким чином, щоб запустити видалення Dr.Web для Linux, необхідно виконати таку команду:

```
# /opt/drweb.com/bin/remove.sh
```

Далі запуститься програма видалення (що використовує графічний режим або режим командного рядка, залежно від можливостей поточного оточення).

Щоб безпосередньо запустити програму видалення для режиму командного рядка, використовуйте таку команду:

```
# /opt/drweb.com/bin/uninst.sh
```

Процедура видалення Dr.Web для Linux розглянута у відповідних розділах:

- Видалення в графічному режимі.
- Видалення в режимі командного рядка.

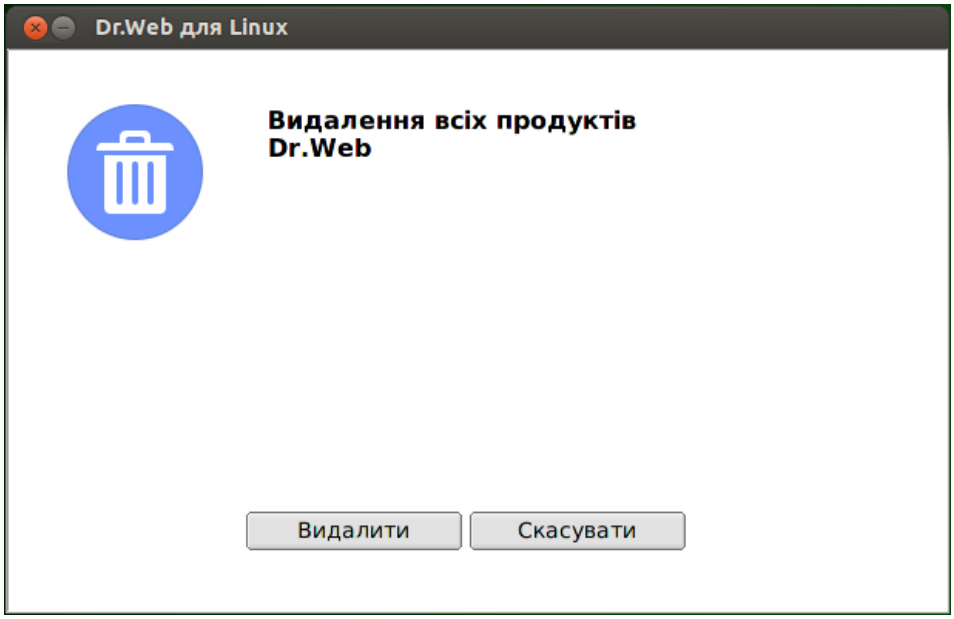
Існує можливість запустити програму видалення повністю в автоматичному режимі, виконавши команду:

```
# /opt/drweb.com/bin/remove.sh --non-interactive
```

В цьому випадку програма видалення буде запущена повністю в автоматичному режимі, без показу інтерфейсу користувача (включаючи діалоги програми видалення для режиму командного рядка). Зверніть увагу, що запуск програми видалення повністю в автоматичному режимі потребує наявності прав суперкористувача. Для підвищення прав ви можете використовувати команди **su** та **sudo**.

Видалення в графічному режимі

Після запуску програми видалення для графічного режиму, на екрані з'явиться вікно майстра видалення.



Малюнок 3. Сторінка привітання майстра видалення.

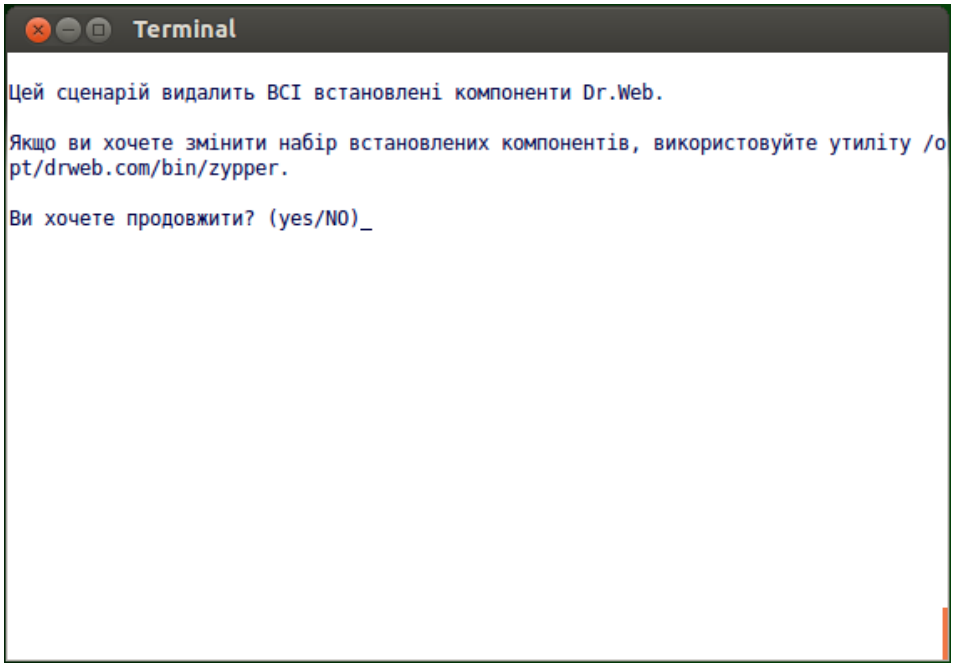
1. Щоб видалити продукти Dr.Web, натисніть **Видалити**. Щоб припинити роботу майстра видалення та відмовитися від видалення продуктів Dr.Web з вашого комп'ютера, натисніть **Скасувати**.
2. Після початку процесу видалення відкриється сторінка майстра, що відображає хід процесу видалення та містить відповідний індикатор прогресу. Щоб переглянути повідомлення журналу видалення, натисніть **Докладніше**.

3. Після успішного завершення процесу видалення файлів Dr.Web для Linux та внесення необхідних змінень в системні налаштування відкриється фінальна сторінка майстра з повідомленням про успішне видалення.
4. Щоб закрити вікно майстра видалення, натисніть кнопку **OK**.

Видалення в режимі командного рядка

Після запуску програми видалення, що працює в режимі командного рядка, на екрані з'явиться текст запрошення до видалення.

1. Щоб розпочати видалення, введіть *Yes* або *Y* на запит «Ви хочете продовжити?». Щоб відмовитися від видалення продуктів Dr.Web з вашого комп'ютера, введіть *No* або *N*. В цьому випадку робота програми видалення буде завершена.



Малюнок 4. Запрошення до видалення.

2. Після підтвердження запуститься процедура видалення всіх встановлених пакетів Dr.Web. На екран видаватимуться записи, що фіксуються в журналі та відображають хід процесу видалення.
3. Після завершення процесу програма видалення завершить свою роботу автоматично.

Видалення Dr.Web для Linux, встановленого з репозиторію

Всі наведені нижче команди для видалення пакетів мають виконуватися з правами суперкористувача. Для цього використовуйте команду зміни користувача **su** або команду виконання від імені іншого користувача **sudo**.

Нижче наведені процедури для таких ОС (менеджерів пакетів):

- Debian, Mint, Ubuntu (apt).
- ALT Linux, PCLinuxOS (apt-rpm).
- Mageia, OpenMandriva Lx (urpmi).
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf).
- SUSE Linux (zypper).

Debian, Mint, Ubuntu (apt)

Щоб видалити кореневий метапакет Dr.Web для Linux, виконайте команду:

```
# apt-get remove drweb-workstations
```

Для видалення всіх встановлених пакетів Dr.Web виконайте команду (в деяких системах символ '*' необхідно екранувати: '*'):

```
# apt-get remove drweb*
```

Для автоматичного видалення з системи всіх більше не використовуваних пакетів можна додатково скористатися командою:

```
# apt-get autoremove
```

Зверніть увагу на такі особливості видалення з використанням **apt-get**:

1. Перша команда видалить тільки кореневий метапакет `drweb-workstations`, а решта пакетів, які могли бути автоматично встановлені при встановленні цього пакета для задоволення його залежностей, залишаться в системі.
2. Друга команда видалить з системи всі пакети, назва яких починається на "`drweb`" (стандартне найменування для пакетів програмних продуктів Dr.Web). Зверніть увагу, що ця команда видалить з системи всі пакети з таким іменем, а не тільки пакети Dr.Web для Linux.
3. Третя команда видалить з системи всі пакети, які були автоматично встановлені для задоволення залежностей інших пакетів, но більше не потрібні (наприклад, через видалення вихідного пакета). Зверніть увагу, що ця команда видалить з системи всі більше не потрібні пакети, а не тільки пакети Dr.Web для Linux.

Видалити пакети Dr.Web для Linux також можна за допомогою альтернативних менеджерів (наприклад, **Synaptic** або **aptitude**).

ALT Linux, PCLinuxOS (apt-rpm)

Видалення Dr.Web для Linux в цьому випадку проводиться так само, як і в **Debian**, **Ubuntu** (див. вище).

Видалити пакети Dr.Web для Linux також можна за допомогою альтернативних менеджерів (наприклад, **Synaptic** або **aptitude**).

Mageia, OpenMandriva Lx (urpme)

Для видалення Dr.Web для Linux виконайте команду:

```
# urpme drweb-workstations
```

Для автоматичного видалення з системи всіх більше не використовуваних пакетів можна додатково скористатися командою:

```
# urpme --auto-orphans drweb-workstations
```

Зверніть увагу на такі особливості видалення з використанням **urpme**:

1. Перша команда видалить тільки кореневий метапакет `drweb-workstations`, а решта пакетів, які могли бути автоматично встановлені при встановленні цього пакета для задоволення його залежностей, залишаться в системі.
2. Друга команда видалить з системи пакет `drweb-workstations`, а також всі пакети, які були автоматично встановлені для задоволення залежностей інших пакетів, но більше не потрібні (наприклад, через видалення вихідного пакета). Зверніть увагу, що ця команда видалить з системи всі більше не потрібні пакети, а не тільки пакети Dr.Web для Linux.

Видалити пакети Dr.Web для Linux також можна за допомогою альтернативних менеджерів (наприклад, **rpmdrake**).

Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf)

Для видалення всіх встановлених пакетів Dr.Web виконайте команду (в деяких системах символ '*' необхідно екранувати: '*'):

```
# yum remove drweb*
```

В ОС **Fedora**, починаючи з версії 22, рекомендується замість менеджера **yum** використовувати менеджер **dnf**, наприклад:

```
# dnf remove drweb*
```

Зверніть увагу на такі особливості видалення з використанням **yum** (**dnf**):

Вказана команда видалить з системи всі пакети, назва яких починається на "drweb" (стандартне найменування для пакетів програмних продуктів Dr.Web). Зверніть увагу, що ця команда видалить з системи всі пакети з таким іменем, а не тільки пакети Dr.Web для Linux.

Видалити пакети Dr.Web для Linux також можна за допомогою альтернативних менеджерів (наприклад, **PackageKit** або **Yumex**).

SUSE Linux (zypper)

Для видалення Dr.Web для Linux виконайте команду:

```
# zypper remove drweb-workstations
```

Для видалення всіх встановлених пакетів Dr.Web виконайте команду (в деяких системах символ '*' необхідно екранувати: '*'):

```
# zypper remove drweb*
```

Зверніть увагу на такі особливості видалення з використанням **zypper**:

1. Перша команда видалить тільки кореневий метапакет `drweb-workstations`, а решта пакетів, які могли бути автоматично встановлені при встановленні цього пакета для задоволення його залежностей, залишаться в системі.
2. Друга команда видалить з системи всі пакети, назва яких починається на "drweb" (стандартне найменування для пакетів програмних продуктів Dr.Web). Зверніть увагу, що ця команда видалить з системи всі пакети з таким іменем, а не тільки пакети Dr.Web для Linux.

Видалити пакети Dr.Web для Linux також можна за допомогою альтернативних менеджерів (наприклад, **YaST**).

Додатково

Розташування файлів Dr.Web для Linux

Файли Dr.Web для Linux після встановлення розташовуються в каталогах `/opt`, `/etc` та `/var` дерева файлової системи.

Структура використовуваних каталогів:

Каталог	Вміст
`/opt/drweb.com`	Виконувані файли компонентів та основні бібліотеки, необхідні для роботи Dr.Web для Linux.
`/etc/opt/drweb.com`	Файли налаштувань компонентів (за замовчуванням) та ліцензійний ключовий файл для роботи Dr.Web для Linux в одиночному режимі («Standalone mode»).
`/var/opt/drweb.com`	Вірусні бази, антивірусне ядро, а також тимчасові файли та додаткові бібліотеки, необхідні для роботи Dr.Web для Linux.

Вибіркове встановлення та видалення компонентів

За необхідності ви можете провести вибіркове встановлення та видалення окремих компонентів Dr.Web для Linux, встановивши або видаливши відповідні пакети. Вибіркове встановлення та видалення необхідно проводити в той самий спосіб, в який був встановлений Dr.Web для Linux.

Щоб перевстановити будь-який компонент, ви можете спочатку видалити його, а потім встановити знову.

Встановлення та видалення компонентів Dr.Web для Linux:

- встановленого з репозиторію;
- встановленого з універсального пакета.

1. Встановлення та видалення компонентів Dr.Web для Linux, встановленого з репозиторію

Якщо Dr.Web для Linuxбув встановлений з репозиторію, для встановлення та видалення окремого компонента скористайтеся відповідною командою менеджера пакетів, що використовується в вашій ОС. Наприклад:

1. Щоб видалити компонент SplDer Gate (пакет `drweb-gated`) зі складу Dr.Web для Linux, встановленого в ОС **CentOS**, виконайте команду:

```
# yum remove drweb-gated
```

2. Щоб додати компонент SplDer Gate (пакет `drweb-gated`) до складу Dr.Web для Linux, встановленого в ОС **Ubuntu Linux**, виконайте команду:

```
# apt-get install drweb-gated
```

   За необхідності скористайтеся довідкою з менеджера пакетів, що використовується в вашій ОС.

2. Встановлення та видалення компонентів Dr.Web для Linux, встановленого з універсального пакета

Якщо Dr.Web для Linux був встановлений з універсального пакета, та ви бажаєте додатково встановити або перевстановити пакет будь-якого компонента, вам знадобиться інсталяційний файл (з розширенням `.run`), з якого був встановлений Dr.Web для Linux. Якщо ви не зберегли цей файл, завантажте його з сайта компанії «Доктор Веб».

Розпакування інсталяційного файла

При запуску run-файла ви можете скористатися такими параметрами командного рядка:

`--noexec` — замість запуску процесу встановлення просто розпакувати інсталяційні файли Dr.Web для Linux. Файли будуть розпаковані в каталог, вказаний в системній перемінній `TMPDIR` (зазвичай це каталог `/tmp`).

`--keep` — не видаляти інсталяційні файли Dr.Web для Linux та журнал встановлення після завершення встановлення.

`--target` <*каталог*> — розпакувати інсталяційні файли Dr.Web для Linux в указаний каталог <*каталог*>.

С повним списком параметрів командного рядка, які можуть бути використані для інсталяційного файла, можна ознайомитися, виконавши команду:

```
$ ./<ім'я_файла>.run --help
```

Для вибіркового встановлення компонентів Dr.Web для Linux перейдіть до каталогу, що містить розпаковані файли пакетів Dr.Web для Linux. Якщо цей каталог відсутній, виконайте команду:

```
$ ./<ім'я_файла>.run --noexec --target <каталог>
```

В результаті в каталозі <*каталог*> з'явиться вкладений каталог <*ім'я_файла*>, що містить розпаковані файли пакетів Dr.Web для Linux.

Вибіркове встановлення компонентів

Інсталяційний run-файл містить пакети всіх компонентів, з яких складається Dr.Web для Linux (у форматі RPM), а також допоміжні файли. Файли пакетів кожного компонента мають вид:

```
<ім'я_компонента>_<версія>~linux_<платформа>.rpm
```

де <*версія*> — це рядок, що містить версію та дату випуску пакета, а <*платформа*> — рядок, що вказує тип платформи, для якої призначений Dr.Web для Linux. Імена всіх пакетів, що містять компоненти Dr.Web для Linux, починаються з префіксу «drweb».

Для встановлення пакетів до складу інсталяційного комплекту включений менеджер пакетів **zypper**. Для вибіркового встановлення скористайтеся службовим сценарієм `installpkg.sh`. Для цього необхідно попередньо розпакувати вміст інсталяційного пакета в будь-який каталог.

Для встановлення пакетів необхідні права суперкористувача (користувача *root*). Щоб отримати права суперкористувача, скористайтеся командою зміни користувача **su** або командою виконання від імені іншого користувача **sudo**.

Щоб провести встановлення або перевстановлення компонента, необхідно перейти до каталогу, що містить розпакований інсталяційний комплект, та виконати в консолі (або в емуляторі консолі — терміналі для графічного режиму) команду:

```
# ./scripts/installpkg.sh <ім'я_пакета>
```

Наприклад:

```
# ./scripts/installpkg.sh drweb-gated
```

Якщо необхідно запустити програму встановлення Dr.Web для Linux цілком, запустіть сценарій автоматичного встановлення, виконавши команду:

```
$ ./install.sh
```

Окрім того, ви можете встановити всі пакети Dr.Web для Linux (у тому числі, щоб встановити відсутні або помилково видалені компоненти), запустивши встановлення кореневого метапакета:

```
# ./scripts/installpkg.sh drweb-workstations
```

Вибіркове видалення компонентів

Для вибіркового видалення пакета будь-якого компонента використовуйте відповідну команду видалення менеджера пакетів вашої операційної системи, якщо ваша ОС використовує формат пакетів RPM:

- В **Red Hat Enterprise Linux** та **CentOS** використовуйте команду **yum** `remove` *<ім'я_пакета>*
- В **Fedora** використовуйте команду **yum** `remove` *<ім'я_пакета>* або **dnf** `remove` *<ім'я_пакета>*
- В **SUSE Linux** використовуйте команду **zypper** `remove` *<ім'я_пакета>*
- В **Mageia**, **OpenMandriva Lx** використовуйте команду **urpme** *<ім'я_пакета>*
- В **Alt Linux** та **PCLinuxOS** використовуйте команду **apt-get** `remove` *<ім'я_пакета>*.

Наприклад (для **Red Hat Enterprise Linux**):

```
# yum remove drweb-gated
```

Якщо ваша ОС використовує пакети у форматі DEB, для вибіркового видалення скористайтеся менеджером пакетів **zypper**, автоматично встановленим в межах встановлення Dr.Web для Linux. Для цього перейдіть до каталогу `/opt/drweb.com/bin` та виконайте таку команду:

```
# ./zypper rm <ім'я_пакета>
```

Наприклад:

```
# ./zypper rm drweb-gated
```

Якщо ви хочете видалити Dr.Web для Linux цілком, запустіть сценарій автоматичного видалення, виконавши команду:

```
# ./uninst.sh
```

Щоб перевстановити будь-який компонент, ви можете спочатку видалити його, а потім встановити, запустивши вибіркове або повне встановлення з інсталяційного комплекту.

Налаштування підсистем безпеки

Наявність у складі ОС підсистеми забезпечення додаткової безпеки **SELinux**, а також використання систем мандатного управління доступом (на відміну від класичної дискреційної моделі UNIX), таких, як **PARSEC**, призводить до проблем у функціонуванні Dr.Web для Linux при налаштуваннях за замовчуванням. Щоб забезпечити коректну роботу Dr.Web для Linux в цьому випадку, необхідно внести додаткові змінення в налаштування підсистеми безпеки та/або Dr.Web для Linux.

В цьому розділі розглядаються такі налаштування, що забезпечують коректну роботу Dr.Web для Linux:

- Налаштування політик безпеки **SELinux**.
- Налаштування дозволів для системи мандатного доступу **PARSEC** (ОС **Astra Linux SE**).
- Налаштування запуску в режимі ЗПС (замкненого програмного середовища) (ОС **Astra Linux SE**, версія 1.6).

Налаштування дозволів системи мандатного доступу **PARSEC** для Dr.Web для Linux дозволить компонентам антивірусу обходити обмеження встановлених політик безпеки та отримувати доступ до файлів різних рівнів привілеїв.

Зверніть увагу, що навіть якщо ви не налаштуєте дозволи системи мандатного доступу **PARSEC** для компонентів Dr.Web для Linux, то ви все одно зможете запускати перевірку файлів, використовуючи графічний інтерфейс Dr.Web для Linux в режимі автономної копії. Для цього виконайте команду **drweb-gui** з параметром `--Autonomous`. Також ви можете запускати переверку файлів безпосередньо з командного рядка. Для цього виконайте команду **drweb-ctl** з цим самим параметром (`--Autonomous`). При цьому буде можлива перевірка файлів, для доступу до яких необхідний рівень привілеїв не вище рівня, з яким працює користувач, який запустив сеанс перевірки. Даний режим має такі особливост:

- Для запуску в режимі автономної копії необхідна наявність діючого ключового файла, робота під управлінням сервера централізованого захисту не підтримується (існує можливість встановити ключовий файл, експортований з сервера централізованого захисту). При цьому, навіть якщо Dr.Web для Linux підключений до сервера централізованого захисту, автономна копія *не повідомляє* серверу централізованого захисту про загрози, виявлені при запуску в режимі автономної копії.
- Всі допоміжні компоненти, що обслуговують роботу автономної копії, будуть запущені від імені поточного користувача та працюватимуть зі спеціально сформованим файлом конфігурації.
- Всі тимчасові файли та сокети UNIX, що використовуються для взаємодії компонентів між собою, створюватимуться тільки в каталозі з унікальним іменем, створеним запущеною автономною копією в каталозі тимчасових файлів (вказаному в системній перемінній оточення `TMPDIR`).

- Автономно запущена копія графічного інтерфейсу управління *не запускає* монітори SpIDer Guard та SpIDer Gate, працюють тільки функції перевірки файлів та управління карантином, які підтримуються Сканером.
- Шляхи до файлів вірусних баз, антивірусного ядра та виконуваних файлів сервісних компонентів задані за замовчуванням або беруться зі спеціальних перемінних оточення.
- Кількість одночасно працюючих автономних копій не обмежена.
- При завершенні роботи автономно запущеної копії також завершує роботу і комплект обслуговуючих її сервісних компонентів.

Налаштування політик безпеки для SELinux

Якщо використовуваний вами дистрибутив **Linux** оснащений підсистемою безпеки **SELinux** (*Security-Enhanced Linux — Linux з поліпшеною безпекою*), то для того, щоб службові компоненти Dr.Web для Linux (такі, як скануюче ядро) працювали коректно після встановлення компонентів програми, вам, можливо, буде необхідно внести змінення в політики безпеки, що використовуються **SELinux**.

1. Проблеми при встановленні універсального пакета

При включеному **SELinux** встановлення Dr.Web для Linux в виді універсального пакета з інсталяційного файла (`.run`) може завершитися невдало, оскільки буде заблокована спроба створення в системі спеціального користувача *drweb*, з повноваженнями якого працюють копоненти Dr.Web для Linux.

Якщо спроба встановлення Dr.Web для Linux з інсталяційного файла (`.run`) була перервана через неможливість створення користувача *drweb*, перевірте режим роботи **SELinux**, для чого виконайте команду **getenforce**. Ця команда виводить на екран поточний режим захисту:

- *Permissive* — захист активний, але використовується дозвільна стратегія: дії, що порушують політики безпеки, не забороняються, а тільки фіксуються в журналі аудиту.
- *Enforced* — захист активний, використовується стратегія заборони: дії, що порушують політики безпеки, реєструються в журналі аудиту та блокуються.
- *Disabled* — **SELinux** встановлений, але неактивний.

Якщо **SELinux** працює в режимі *Enforced*, тимчасово (на період встановлення) переведіть її в режим *Permissive*. Для цього виконайте команду

```
# setenforce 0
```

яка тимчасово (до першого перезавантаження системи) переведе **SELinux** в режим *Permissive*.

Який режим захисту ви б не встановили за допомогою команди **setenforce**, після перезавантаження операційної системи **SELinux** повернеться в режим захисту, заданий в її налаштуваннях (зазвичай файл налаштувань **SELinux** знаходиться в каталозі `/etc/selinux`).

Після успішного встановлення Dr.Web для Linux з інсталяційного файла, але до його запуску та активації поверніть режим *Enforced*, для чого виконайте команду:

```
# setenforce 1
```

2. Проблеми функціонування Dr.Web для Linux

В деяких випадках при працюючому **SELinux** окремі допоміжні компоненти Dr.Web для Linux (такі, як **drweb-se** та **drweb-filecheck**, що використовуються Сканером і SpIDer Guard) не зможуть запуститися, внаслідок чого сканування об'єктів та моніторинг файлової системи унеможливляться. Ознакою того, що ці допоміжні модулі не можуть бути запущені, є поява повідомлень про помилки *119* та *120* в головному вікні Dr.Web для Linux та в системному журналі **syslog** (зазвичай розташований в каталозі `/var/log/`).

При спрацюванні системи безпеки **SELinux** інформація про відмови фіксується також в системному журналі аудиту. Загалом, при використанні в системі демона **audit**, журнал аудиту розташовується в файлі `/var/log/audit/audit.log`. В іншому випадку повідомлення про заборону операції записуються в загальний файл журналу `/var/log/messages` або `/var/log/syslog`.

Якщо встановлено, що допоміжні модулі не функціонують через те, що вони блокуються **SELinux**, скомпілюйте для них спеціальні політики безпеки.

В деяких дистрибутивах **Linux** вказані нижче утиліти можуть бути за замовчуванням не встановлені. В цьому випадку вам, можливо, знадобиться додатково встановити пакети, що їх містять.

Створення політик безпеки SELinux:

1. Створіть новий файл з вихідним кодом політики **SELinux** (файл з розширенням `.te`). Даний файл визначає обмеження, що відносяться до описуваного модуля. Вихідний файл політики може бути створений в два способи:
   1) За допомогою утиліти **audit2allow**. Це найпростіший спосіб, оскільки дана утиліта генерує дозвільні правила на основі повідомлень по відмову в доступі в файлах системних журналів. Можна задати автоматичний пошук повідомлень в файлах журналів або вказати шлях до файла журналу вручну.

      Зверніть увагу, що цей спосіб можна використовувати, тільки коли в системному журналі аудиту вже зареєстровані інциденти порушення політик безпеки **SELinux**

компонентами Dr.Web для Linux. Якщо це не так, або дочекайтеся таких інцидентів у процесі роботи продукту Dr.Web для Linux, або створіть дозвільні політики примусово, скориставшись утилітою **policygentool** (див. нижче).

Утиліта **audit2allow** міститься в пакеті `policycoreutils-python` або `policycoreutils-devel` (для ОС **RedHat Enterprise Linux**, **CentOS**, **Fedora**, залежно від версії) або в пакеті `python-sepolgen` (для ОС **Debian**, **Ubuntu**).

Приклад використання **audit2allow**:

```
# grep drweb-se.real /var/log/audit/audit.log | audit2allow -M drweb-se
```

В цьому прикладі утиліта **audit2allow** проводить пошук в файлі `audit.log` повідомлень про відмову в доступі для модуля **drweb-se**.

В результаті роботи утиліти створюються два файла: вихідний файл політики `drweb-se.te` та готовий до встановлення модуль політики `drweb-se.pp`.

Якщо потрібні інциденти в системному журналі не виявлені, утиліта поверне повідомлення про помилку.

В більшості випадків вам не потрібно вносити змінення в файл політики, створений утилітою **audit2allow**. Тому рекомендується одразу переходити до пункту 4 для встановлення отриманого модуля політики `drweb-se.pp`. Зверніть увагу, що за замовчуванням утиліта **audit2allow** як результат своєї роботи виводить на екран готовий виклик команди **semodule**. Скопіювавши його в командний рядок та виконавши, ви виконайте пункт 4. Перейдіть до пункту 2, тільки якщо ви хочете внести змінення в політики, автоматично сформовані для компонентів Dr.Web для Linux.

2) За допомогою утиліти **policygentool**. Для цього вкажіть в якості параметрів ім'я модуля, роботу з яким ви хочете налаштувати, та повний шлях до його виконуваного файла.

Зверніть увагу, що утиліта **policygentool**, що входить до складу пакета `selinux-policy` для ОС **RedHat Enterprise Linux** та **CentOS Linux**, може працювати некоректно. В такому випадку скористайтеся утилітою **audit2allow**.

Приклад створення політик за допомогою **policygentool**:

- Для **drweb-se**:

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- Для **drweb-filecheck**:

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```

Вам буде запропоновано вказати декілька загальних характеристик домену, після чого для кожного модуля будуть створені три файла, що визначають політику:

<module_name>.te, <module_name>.fc та *<module_name>.if*.

2. За необхідності відредагуйте згенерований вихідний файл політики *<module_name>.te*, а потім, використовуючи утиліту **checkmodule**, створіть бінарне представлення (файл з розширенням `.mod`) вихідного файла локальної політики.

   Зверніть увагу, що для успішної роботи цієї команди в системі має бути встановлений пакет `checkpolicy`.

   Приклад використання:

   ```
   # checkmodule -M -m -o drweb-se.mod drweb-se.te
   ```

3. Створіть встановлюваний модуль політики (файл з розширенням `.pp`) за допомогою утиліти **semodule_package**.

   Приклад:

   ```
   # semodule_package -o drweb-se.pp -m drweb-se.mod
   ```

4. Для встановлення створеного модуля політики скористайтеся утилітою **semodule**.

   Приклад:

   ```
   # semodule -i drweb-se.pp
   ```

Щоб отримати додаткову інформацію про принципи роботи та налаштування **SELinux**, зверніться до документації з використовуваного вами дистрибутиву **Linux**.

Налаштування дозволів PARSEC (Astra Linux SE)

В системах, оснащених підсистемою безпеки **PARSEC** (система управління мандатним доступом) через різні рівні привілеїв, необхідні для доступу до файлів, за замовчуванням SpIDer Guard не може перехоплювати події про доступ до файлів з більш високими рівнями привілеїв, ніж рівень привілеїв, на якому запущений SpIDer Guard. Окрім того, якщо користувач працює не на нульовому рівні привілеїв, інтерфейс користувача Dr.Web для Linux не може взаємодіяти з SpIDer Guard та сервісними компонентами антивірусу, що працюють на інших рівнях привілеїв, у тому числі може бути відсутнім доступ до консолідованого карантину.

Якщо в ОС використовується **PARSEC** та наявні облікві дані користувачів, які працюють не на нульовому рівні, необхідно провести спеціальне налаштування Dr.Web для Linux, щоб забезпечити взаємодію його компонентів, які запускаються на різних рівнях привілеїв.

В цьому розділі розглядаються такі налаштування **PARSEC**, що забезпечують коректну роботу Dr.Web для Linux:

- Налаштування взаємодії компонентів, запущених на різних рівнях привілеїв.
- Налаштування автоматичного запуску компонентів Dr.Web для Linux на рівні привілеїв користувача.

- Налаштування SplDer Guard для перехоплення подій доступу до файлів.

Для проведення цих операцій необхідні права суперкористувача (користувача *root*). Щоб отримати права суперкористувача, скористайтеся командою зміни користувача **su** або командою виконання від імені іншого користувача **sudo**.

Налаштування взаємодії компонентів, запущених на різних рівнях привілеїв

Для ОС Astra Linux SE версії 1.6:

Внесіть змінення в системний файл `/etc/parsec/privsock.conf`, надавши демону управління конфігурацієюDr.Web для Linux (**drweb-configd**) право на використання механізму *privsock*. **drweb-configd** — сервісний компонент продукту, що забезпечує взаємодію всіх антивірусних компонентів між собою. Механізм *privsock* призначений для забезпечення функціонування системних мережних сервісів, що не проводять обробку інформації з використанням мандатного контексту, але взаємодіють з процесами, що працюють в мандатному контексті суб'єкта доступу. Для цього виконайте такі дії:

1. В будь-якому текстовому редакторі відкрийте файл `/etc/parsec/privsock.conf`. Додайте в цей файл вказані рядки:

```
/opt/drweb.com/bin/drweb-configd
/opt/drweb.com/bin/drweb-configd.real
```

2. Збережіть файл та перезавантажте систему.

Для ОС Astra Linux SE версії 1.5 та нижче:

Внесіть змінення в сценарій запуску демона управління конфігурацією Dr.Web для Linux (**drweb-configd**). Для цього виконайте такі дії:

1. Ввійдіть в систему під обліковим записом з нульовим рівнем привілеїв.
2. В будь-якому текстовому редакторі відкрийте файл сценарію `/etc/init.d/drweb-configd`.
3. Знайдіть в цьому файлі визначення функції `start_daemon()`, в якому замініть рядок

```
"$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
```

на рядок

```
execaps -c 0x100 -- "$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
```

4. В деяких ОС (наприклад, **Astra Linux SE** 1.3) може знадобитися вказати додатково залежність запуску компонента від підсистеми **PARSEC**. В такому випадку також необхідно модифікувати в цьому файлі рядок:

```
# Required-Start: $local_fs $network
```

Змініть даний рядок таким чином:

```
# Required-Start: $local_fs $network parsec
```

5. Збережіть файл та перезавантажте систему.

Налаштування автоматичного запуску компонентів на рівні привілеїв користувача

Щоб компоненти Dr.Web для Linux, з якими взаємодіє користувач, були доступні в його оточенні (при роботі користувача не на нульовому рівні привілеїв), внесіть змінення в файли налаштувань PAM, щоб забезпечити автоматичний запуск необхідних компонентів Dr.Web для Linux на початку сесії користувача та їх завершення при завершенні сесії (використовується спеціальний PAM-модуль **pam_drweb_session.so**, розроблений «Доктор Веб», що запускає компонент-посередник **drweb-session**, який пов'язує між собою локальні копії компонентів, запущених в оточенні користувача, з компонентами, що працюють на нульовому рівні привілеїв та запускаються автоматично при завантаженні ОС).

Щоб внести змінення в налаштування PAM, скористайтеся утилітою конфігурування **drweb-configure**, яка входить да складу Dr.Web для Linux (рекомендується), або внесіть змінення в необхідні файли конфігурації вручну.

1. Використання утиліти drweb-configure

Для зручності налаштування деяких складних параметрів, що забезпечують працездатність Dr.Web для Linux, розроблена спеціальна допоміжна утиліта **drweb-configure**.

1. Щоб включити або відключити автоматичний запуск необхідних компонентів Dr.Web для Linux в оточенні користувача при його роботі не на нульовому рівні привилеїв, скористайтеся такою командою:

   ```
   $ sudo drweb-configure session <режим>
   ```

   де *<режим>* може приймати одне з таких значень:

   - `enable` — включити режим автоматичного запуску необхідних компонентів в сесії користувача на його рівні привілеїв.
   - `disable` — відключити режим автоматичного запуску необхідних компонентів в сесії користувача на його рівні привілеїв (при цьому ряд функцій Dr.Web для Linux виявиться недоступним).
2. Перезавантажте систему.

Щоб отримати довідку з використання **drweb-configure** для налаштування PAM, скористайтеся командою:

```
$ drweb-configure --help session
```

2. Змінення файлів конфігурації PAM вручну

1. В файли конфігурації PAM (розташовані в каталозі `/etc/pam.d`), в яких викликається модуль PAM **pam_parsec_mac.so**, додайте такі записи типу *session*:
   - Перед першим записом типу *session*:

   ```
   session optional pam_drweb_session.so type=close
   ```

   - Після останнього запису типу *session*:

   ```
   session optional pam_drweb_session.so type=open
   ```

2. Збережіть змінені файли.
3. Створіть символічне посилання на файл `pam_drweb_session.so` з системного каталогу, що містить PAM-модулі. Файл `pam_drweb_session.so` розташовується в каталозі бібліотек Dr.Web для Linux `/opt/drweb.com/lib/`(наприклад, для 64-розрядних ОС — в каталозі `/opt/drweb.com/lib/x86_64-linux-gnu/pam/`).
4. Перезавантажте систему.

Налаштування SpIDer Guard для перехоплення подій доступу до файлів

Щоб надати файловому монітору SpIDer Guard можливість виявляти доступ до файлів з будь-яким рівнем привілеїв доступу, необхідно перевести SpIDer Guard в режим роботи *Fanotify*.

Щоб перевести SpIDer Guard в режим роботи *Fanotify*, виконайте таку команду:

```
# drweb-ctl cfset LinuxSpider.Mode Fanotify
```

Щоб отримати додаткову інформацію використовуйте команду:

```
$ man drweb-spider
```

Налаштування запуску в режимі ЗПС (Astra Linux SE, версія 1.6)

В ОС **Astra Linux SE** підтримується особливий режим *замкненого програмного середовища* (ЗПС), в якому запускаються тільки програми, виконувані файли яких підписані цифровим підписом розробника, чий відкритий ключ доданий до списку ключів, яким довіряє ОС.

За замовчуванням компоненти Dr.Web для Linux, що постачаються для виконання в середовищі **Astra Linux SE**, підписані цифровим підписом компанії «Доктор Веб», а відкритий ключ для цього цифрового підпису автоматично додається до списку довірених при встановленні програми, через що Dr.Web для Linux має коректно запускатися при активізації режиму ЗПС в ОС **Astra Linux SE** версії 1.5 та нижче.

Проте, через те, що в версії 1.6 ОС **Astra Linux SE** механізм підпису був змінений, для забезпечення запуску Dr.Web для Linux в режимі ЗПС в ОС версії 1.6 необхідно провести попереднє налаштування системи.

Налаштування Astra Linux SE версії 1.6 для запуску Dr.Web для Linux в режимі ЗПС

1. Встановіть пакет `astra-digsig-oldkeys` з інсталяційного диска ОС, якщо він ще не встановлений;
2. Помістіть відкритий ключ компанії «Доктор Веб» до каталогу `/etc/digsig/keys/legacy/keys` (за відсутності каталогу його необхідно створити).
3. Виконайте команду:

```
# update-initramfs -k all -u
```

4. Перезавантажте систему.

Початок роботи

1. Виконайте активацію Dr.Web для Linux.
2. Перевірте його працездатність.
3. Задайте режим моніторингу файлів.
4. Визначте виключення, якщо вони є.

Реєстрація та активація

В цьому розділі:

- Придбання та реєстрація ліцензій.
- Активація Dr.Web для Linux
  - Запит демонстраційного періоду.
  - Встановлення ключового файла.
  - Підключення до сервера централізованого захисту.
- Повторна реєстрація.

Придбання та реєстрація ліцензій

При придбанні ліцензії клієнт отримує можливість протягом всього терміну її дії отримувати оновлення з серверів оновлень компанії «Доктор Веб», а також отримувати стандартну технічну підтримку компанії «Доктор Веб» та її партнерів.

Придбати будь-який антивірусний продукт Dr.Web або серійний номер для нього ви можете у наших партнерів (див. список партнерів за адресою https://partners.dataprotection.com.ua/) або через інтернет-магазин https://estore.dataprotection.com.ua/. Додаткову інформацію про можливі варіанти ліцензій можна знайти на офіційному сайті компанії «Доктор Веб» https://www.dataprotection.com.ua/.

Реєстрація ліцензії підтверджує, що ви є повноправним користувачем Dr.Web для Linux, та активує його функції, включаючи функції оновлення вірусних баз. Рекомендується провести реєстрацію та активацію ліцензії одразу після встановлення.

Активація Dr.Web для Linux

Придбана ліцензія може бути активована в будь-який з указаних нижче способів:

- За допомогою майстра реєстрації, що входить до складу Менеджера ліцензій.
- Безпосередньо на сайті компанії «Доктор Веб» за адресою https://products.dataprotection.com.ua/register/.

При активації або подовженні ліцензії необхідно вказати серійний номер. Цей номер може постачатися разом з Dr.Web для Linux або електронною поштою, при придбанні або подовженні ліцензії онлайн.

При подовженні ліцензії необхідно також вказати серійний номер або ліцензійний ключовий файл попередньої ліцензії, в іншому випадку термін дії нової ліцензії буде скорочений на 150 днів.

Якщо є комплект ліцензій, виданих для використання Dr.Web для Linux на декількох комп'ютерах, то при реєстрації існує можливість вказати, що Dr.Web для Linux буде використовуватися тільки на одному комп'ютері. В такому випадку всі ліцензії з комплекту будуть об'єднані в одну, а термін її дії буде автоматично збільшений.

Запит демонстраційного періоду

Користувачам продуктів Dr.Web доступно два типи демонстраційного періоду:

- Терміном на 3 місяці.
- Терміном на 1 місяць.

Щоб отримати демонстраційний період терміном на 3 місяці, пройдіть процедуру реєстрації на офіційному сайті компанії «Доктор Веб» та вкажіть свої персональні дані. В цьому випадку ви отримаєте електронною поштою серійний номер для активації вашої копії Dr.Web для Linux. Демонстраційний період терміном на 1 місяць можна отримати безпосередньо у вікні майстра реєстрації Менеджера ліцензій, не вказуючи персональних даних.

Вікно майстра реєстрації Менеджера ліцензій з'являється на екрані при першому запуску Dr.Web для Linux (як правило, він автоматично запускається одразу після завершення встановлення). Також ви можете в будь-який момент запустити процес реєстрації або запиту демонстраційного періоду з вікна Менеджера ліцензій, натиснувши **Отримати нову ліцензію** на сторінці перегляду інформації про поточну ліцензію.

Для активації за допомогою серійного номера, а також для запиту демонстраційного періоду необхідне підключення до мережі Інтернет.

Демонстраційний період використання Dr.Web для Linux може бути виданий повторно для того самого комп'ютера тільки після завершення визначеного періоду часу.

При активації ліцензії або демонстраційного періоду за допомогою Менеджера ліцензій ключовий файл (ліцензійний або демонстраційний) буде сформований на локальному комп'ютері та встановлений в належне місце автоматично. Після отримання ключового файла електронною поштою при реєстрації на сайті встановіть його вручну.

За відсутності можливості скористатися майстром реєстрації (наприклад, через відсутність графічної оболонки ОС), ви можете скористатися командою управління ліцензією утиліти командного рядка **drweb-ctl**, яка дозволяє автоматично отримати демонстраційний ключовий файл або ліцензійний ключовий файл для серійного номера зареєстрованої ліцензії (у тому числі — й для серійного номера демонстраційного періоду, отриманого на адресу електронної пошти). Опис утиліти **drweb-ctl** наведений в Посібнику користувача.

Повна версія Посібника користувача Dr.Web для Linux доступна:

- На сайті компанії «Доктор Веб» за адресою https://download.drweb.com/doc/ (необхідне підключення до мережі Інтернет).
- В виді документу PDF в каталозі `/opt/drweb.com/share/doc` (суфікс в імені файла вказує на мову Посібника).

Встановлення ключового файла

Якщо вже є ключовий файл, відповідний діючій ліцензії (наприклад, він був отриманий від продавця електронною поштою після реєстрації або Dr.Web для Linux переноситься на інший комп'ютер), існує можливість активувати Dr.Web для Linux, просто вказавши шлях до наявного ключового файла. Це можна зробити таким чином:

- В Менеджері ліцензій, перейшовши на першому кроці майстра реєстрації за посиланням **Інші види активації** та вказавши шлях до наявного ключового файла або до zip-архіву, що містить його.
- Вручну, для цього:
  1. Розпакуйте ключовий файл, якщо він був отриманий вами в архіві.
  2. Скопіюйте його в каталог `/etc/opt/drweb.com` та за необхідності перейменуйте в `drweb32.key`.
  3. Виконайте команду:

     ```
     # drweb-ctl reload
     ```

     щоб застосувати внесені змінення.

Ви можете також скористатися командою:

```
# drweb-ctl cfset Root.KeyPath <шлях до ключового файла>
```

Зверніть увагу, що в останньому випадку ключовий файл не буде скопійований в каталог `/etc/opt/drweb.com`, а залишиться в своєму вихідному каталозі.

Якщо ключовий файл не буде скопійований в каталог `/etc/opt/drweb.com`, користувач сам несе відповідальність за збереження ключового файла. Такий спосіб встановлення ключового файла не рекомендується через можливість його випадкового видалення (наприклад, якщо він був розташований в каталозі, що автоматично очищується системою). Пам'ятайте, що при втраті ви можете запитати ключовий файл повторно, але кількість запитів на його отримання обмежена.

Підключення до сервера централізованого захисту

Якщо провайдер або адміністратор мережі підприємства надав файл налаштувань підключення до сервера централізованого захисту, ви можете активувати Dr.Web для Linux, просто вказавши шлях до наявного файла налаштувань підключення. Це можна зробити таким чином:

- У вікні налаштувань програми на вкладці **Режим** встановіть прапорець **Включити режим централізованого захисту**, виберіть у вікні, що з'явилося, пункт зі списку, що випадає, *Завантажити з файла*, вкажіть шлях до наявного файла налаштувань підключення та натисніть **Підключити.**

Повторна реєстрація

Повторна реєстрація може знадобитися при втраті ліцензійного ключового файла за наявності активної ліцензії. При повторній реєстрації вкажіть ті самі персональні дані, які ви ввели при першій реєстрації ліцензії. Допускається використовувати іншу адресу електронної пошти — в такому випадку ліцензійний ключовий файл буде надісланий за новою адресою.

Кількість запитів на отримання ліцензійного ключового файла обмежена — реєстрація ліцензії з одним тим самим серійним номером допускається *не більше 25 разів*. Якщо це число перевищене, ліцензійний ключовий файл не буде висланий. В цьому випадку зверніться до Служби технічної підтримки (в запиті докладно опишіть ситуацію та вкажіть персональні дані, введені при реєстрації, та серійний номер ліцензії). Ліцензійний ключовий файл буде висланий Службою технічної підтримки електронною поштою.

Ключовий файл

Ключовий файл — це спеціальний файл, який зберігається на локальному комп'ютері та відповідає придбаній ліцензії або активованому демонстраційному періоду для програмного продукту Dr.Web для Linux. В ключовому файлі фіксуються параметри використання Dr.Web для Linux відповідно до придбаної ліцензії або активованим демонстраційним періодом.

Ключовий файл має розширення `.key` та є дійсним за одночасного виконання таких умов:

- Термін дії ліцензії або демонстраційного періоду, яким він відповідає, не минув.
- Дозвіл, що визначається ліцензією або активним демонстраційним періодом, поширюється на всі використовувані модулі.
- Цілісність файла не порушена.

При порушенні будь-якого з цих умов ключовий файл стає недійсним.

При роботі Dr.Web для Linux ключовий файл за замовчуванням має знаходитися в каталозі `/etc/opt/drweb.com` та мати ім'я `drweb32.key`.

Компоненти Dr.Web для Linux регулярно перевіряють наявність та коректність ключового файла. Його вміст захищений від редагування за допомогою механізму електронного цифрового підпису, тому редагування робить ключовий файл недійсним. Не рекомендується відкривати ключовий файл в текстових редакторах, щоб уникнути випадковому пошкодженню його вмісту.

За відсутності дійсного ключового файла (ліцензійного або демонстраційного), а також після завершення терміну його дії, антивірусні функції всіх компонентів блокуються до встановлення діючого ключового файла.

Рекомендується зберегти наявний ліцензійний ключовий файл до завершення терміну його дії. В такому випадку при перевстановленні Dr.Web для Linux або перенесенні його на інший комп'ютер повторна реєстрація серійного номера ліцензії не потребується, та ви зможете використовувати ліцензійний ключовий файл, отриманий при першому проходженні процедури реєстрації.

Електронною поштою ключові файли Dr.Web зазвичай передаються упакованими в zip-архіви. Архів, що містить ключовий файл для активації Dr.Web для Linux, зазвичай має ім'я `agent.zip` (зверніть увагу, що якщо в листі міститься *декілька* архівів, то необхідно використовувати саме архів `agent.zip`). В майстрі реєстрації можна вказувати шлях безпосередньо до архіву, не виконуючи його попереднього розпакування. Також перед встановленням ключового файла ви можете розпакувати архів в будь-який спосіб та витягнути з нього ключовий файл, зберігши його в будь-який доступний каталог (наприклад — в домашній каталог або на змінний носій USB flash).

Файл налаштувань підключення

Файл налаштувань підключення є спеціальним файлом, що містить параметри підключення Dr.Web для Linux до сервера централізованого захисту. Цей файл може бути наданий адміністратором антивірусної мережі або інтернет-провайдером (якщо він забезпечує підтримку послуги централізованого антивірусного захисту).

Ви можете використовувати цей файл для активації Dr.Web для Linux через підключення його до сервера централізованого захисту (в цьому випадку ви не зможете використовувати Dr.Web для Linux в автономному режимі, не придбавши додатково ліцензію).

Перевірка працездатності

Існує стандартний тест, що дозволяє перевірити працездатність антивірусних програм, які використовують сигнатурні методи виявлення загроз. З цією метою застосовується спеціальний тест *EICAR* (*European Institute for Computer Anti-Virus Research*), розроблений однойменною організацією. Цей тест розроблений для того, щоб користувач, не наражаючи свій комп'ютер на небезпеку, міг побачити, як встановлений антивірус сигналізуватиме про виявлення вірусу.

Програма, що використовується для тесту *EICAR*, не є шкідливою, але спеціально визначається більшістю антивірусних програм як вірус. Антивірусні продукти Dr.Web називають цей «вірус» таким чином: **EICAR Test File (NOT a Virus!)**. Приблизно так його називають й інші антивірусні програми. Тестова програма **EICAR** є послідовністю з 68 байт, що створюють тіло виконуваного COM-файла для ОС **MS DOS**/**MS Windows**, в результаті виконання якого на консоль виводиться текстове повідомлення:

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

Тіло тестової програми складається тільки з текстових символів, які формують такий рядок:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Якщо ви створите файл, що містить наведений вище рядок, то в результаті вийде програма, яка і буде описаним «вірусом».

За коректної роботи Dr.Web для Linux цей файл має виявлятися при перевірці об'єктів файлової системи в будь-який доступний спосіб зі сповіщенням про виявлення загрози **EICAR Test File (NOT a Virus!)**.

Приклад команди для перевірки працездатності Dr.Web для Linux за допомогою тестової програми **EICAR** з командного рядка:

```
$ tail /opt/drweb.com/share/doc/drweb-se/readme.eicar | grep X5O > testfile
&& drweb-ctl scan testfile && rm testfile
```

Дана команда виділяє з файла `/opt/drweb.com/share/doc/drweb-se/readme.eicar` (постачається разом з Dr.Web для Linux) рядок, що є тілом тестової програми **EICAR**, записує його в файл `testfile` в поточному каталозі, проводить перевірку отриманого файла, після чого видаляє створений файл.

Для успішного проведення цього тесту вам необхідні права запису в поточний каталог. Окрім того, переконайтеся, що в ньому відсутній файл з іменем `testfile` (за необхідності змініть ім'я файла в команді).

При успішному виявленні тестового «вірусу» на екран буде виведене таке повідомлення:

```
<шлях до поточного каталогу>/testfile - infected with EICAR Test File (NOT a Virus!)
```

Якщо при перевірці буде отримане повідомлення про помилку, зверніться до опису відомих помилок.

Якщо в системі працює монітор файлової системи SpIDer Guard, при виявленні загрози файл може бути одразу видалений або переміщений до карантину (залежно від налаштувань компонента). В цьому випадку після повідомлення про виявлену загрозу команда **rm** повідомить про відсутність файла. Ця ситуація не є помилкою, а сигналізує про коректну роботу монітора.

Режими моніторингу файлів

Загальні відомості

Монітор файлової системи SpIDer Guard, що проводить контроль доступу до файлів, може використовувати три режими моніторингу:

- *Звичайний* (встановлений за замовчуванням) — відстежуються операції доступу до файлів (створення, відкриття, закриття та запуск файла). Проводиться перевірка файла, до якого був запитаний доступ, за результатами перевірки до файла можуть бути застосовані дії з нейтралізації загрози, якщо вона в ньому виявлена. До завершення перевірки доступ до файла з боку програм, що запитали доступ, не обмежується.
- *Посилений контроль виконуваних файлів* — для файлів, що не вважаються виконуваними, — так само, як і в звичайному режимі. Для файлів, що вважаються виконуваними, при спробі доступу SpIDer Guard блокує запитану операцію доступу доти, поки не стануть відомі результати перевірки файла на наявність загроз.

  Виконуваними файлами вважаються двійкові файли форматів PE та ELF, а також текстові файли сценаріїв, що містять преамбулу «`#!`».

- *«Агресивний» режим* — при спробі доступу до будь-якого файла SpIDer Guard блокує запитану операцію доступу доти, поки не стануть відомі результати перевірки цього файла на наявність загроз.

Сканер протягом визначеного часу зберігає результати перевірки файлів в спеціальному кеші, тому при повторному доступі до того самого файла за наявності інформації в кеші

повторна перевірка файла не проводиться, за результат перевірки цього файла приймається результат з кешу. Незважаючи на це, використання «агресивного» режиму моніторингу призводить до суттєвого уповільнення роботи при доступі до файлів.

Змінення режиму моніторингу файлів

Режими посиленого моніторингу файлів з попереднім блокуванням доступні, тільки якщо SplDer Guard працює в режимі `FANOTIFY`, а ядро ОС зібране з включеною опцією `CONFIG_FANOTIFY_ACCESS_PERMISSIONS`.

Переключення режимів роботи SplDer Guard проводиться тільки за допомогою команди **`cfset`** утиліти **drweb-ctl**.

Для переключення режимів роботи SplDer Guard необхідні права суперкористувача. Щоб отримати права суперкористувача, скористайтеся командою зміни користувача **su** або командою виконання від імені іншого користувача **sudo**.

- Щоб перевести SplDer Guard в режим роботи `FANOTIFY`, виконайте таку команду:

```
$ sudo drweb-ctl cfset LinuxSpider.Mode FANOTIFY
```

- Щоб змінити режим моніторингу, виконайте таку команду:

```
$ sudo drweb-ctl cfset LinuxSpider.BlockBeforeScan <режим>
```

де <*режим*> визначає режим блокування:

  - `Off` — блокування доступу не проводиться, SplDer Guard працює в звичайному (не блокуючому) режимі моніторингу;
  - `Executables` — проводиться блокування доступу до виконуваних файлів, SplDer Guard проводить посилений контроль виконуваних файлів;
  - `All` — проводиться блокування доступу до будь-яких файлів, SplDer Guard проводить «агресивний» режим моніторингу.

- Щоб змінити термін актуальності результатів перевірки файлів, що містяться в кеші Сканера, виконайте таку команду:

```
$ sudo drweb-ctl cfset FileCheck.RescanInterval <період>
```

де <*період*> визначає період актуальності попередніх результатів перевірки, що містяться в кеші. Допустимі значення від `0s` до `1m` (включно). Якщо вказаний період менше 1 секунди, то файл перевірятиметься при будь-якому запиті.

Робота з Dr.Web для Linux

Робота користувача з Dr.Web для Linux може проводитися як в графічному режимі, за допомогою компонента, що надає графічний інтерфейс управління, так і з командного рядка (включаючи роботу через емулятори терміналу в графічному режимі).

- Для запуску графічного інтерфейсу управління Dr.Web для Linux виберіть пункт **Dr.Web для Linux** в системному меню **Програми** або виконайте в командному рядку операційної системи команду:

  ```
  $ drweb-gui
  ```

  Після цього, якщо оточення графічного робочого столу доступне, буде запущений графічний інтерфейс управління Dr.Web для Linux. Для запуску перевірки при старті графічного інтерфейсу або для запуску його в режимі автономної копії можна скористатися викликом даної команди з аргументами.
- Управління роботою Dr.Web для Linux з командного рядка розглянуте у розділі Робота з командного рядка.
- Для графічних середовищ робочого столу також підтримується запуск перевірки файлів з панелі задач (такої, як **Unity Launcher** в ОС **Ubuntu**) та з графічного файлового менеджера (такого, як **Nautilus**). Окрім того, в області сповіщень робочого столу відображається індикатор стану, який використовується для показу спливаючих сповіщень та доступу до контекстного меню програми. Індикатор відображається агентом сповіщень, який, як і інші сервісні компоненти програми, запускається автоматично та не потребує ручного втручання в свою роботу. Докладніше див. у розділі Інтеграція з середовищем робочого столу.
- Включення режиму посиленого моніторингу файлів монітором SpIDer Guard описане у розділі Режими моніторингу файлів.

Після встановлення Dr.Web для Linux в будь-який з описаних в цьому Посібнику способів, на початку роботи вам необхідно активувати ліцензію, або встановити ключовий файл, якщо він у вас вже є, або підключити Dr.Web для Linux до сервера централізованого захисту (див. розділ Реєстрація та активація). Поки ви цього не зробите, *функції антивірусного захисту будуть відключені.*

Зверніть увагу, що поштовий протокол IMAP, який в більшості випадків використовується поштовими клієнтами (такими, як **Mozilla Thunderbird**) для отримання повідомлень електронної пошти з поштового сервера, є сеансовим. Тому після внесення змінень в роботу монітора SpIDer Gate (включення раніше відключеного монітора, змінення режиму перевірки захищених з'єднань) необхідно обов'язково перезапустити поштовий клієнт, щоб монітор SpIDer Gate зміг перевіряти вхідні повідомлення після змінення режиму своєї роботи.

Робота в графічному режимі

В цьому розділі:

- Загальні відомості.
- Агент сповіщень.
- Графічний інтерфейс управління.

Загальні відомості

За роботу Dr.Web для Linux в оточенні робочого столу відповідають два компоненти:

- Агент сповіщень — компонент, що запускається автоматично на початку сеансу роботи користувача в оточенні робочого столу. Цей компонент показує спливаючі сповіщення про події в роботі Dr.Web для Linux, а також надає індикатор стану Dr.Web для Linux в області системних сповіщень та основне меню для взаємодії з ним.
- Графічний інтерфейс — компонент, що працює в оточенні графічного робочого столу та надає віконний інтерфейс для управління роботою Dr.Web для Linux.

Агент сповіщень

Агент сповіщень Dr.Web для Linux призначений для:

1. Відображення індикатора стану Dr.Web для Linux.
2. Управління моніторами та оновленням, запуску графічного інтерфейсу управління.
3. Показу спливаючих сповіщень про події.
4. Запуску перевірок за заданим розкладом.

Графічний інтерфейс управління

Графічний інтерфейс управління Dr.Web для Linux дозволяє вирішувати такі задачі:

1. Перегляд стану роботи Dr.Web для Linux, включаючи актуальність наявних вірусних баз та терміну дії ліцензії.
2. Запуск та зупинення монітора файлової системи SplDer Guard.
3. Запуск та зупинення монітора мережних з'єднань SplDer Gate.
4. Запуск перевірки файлів на вимогу, в тому числі:
   - *Швидка перевірка* системних файлів та найуразливіших системних об'єктів.
   - *Повна перевірка* всіх файлів системи.
   - *Вибіркова перевірка* тільки вказаних файлів та каталогів або спеціалізованих об'єктів (завантажувальних записів дисків, активних процесів).

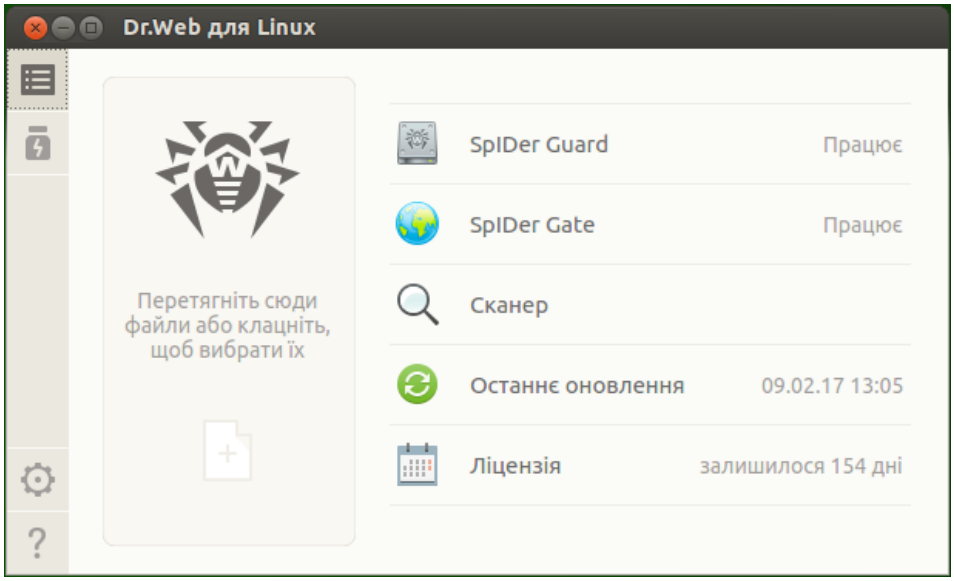
Вибір файлів для перевірки проводиться як вказанням цільових каталогів або файлів перед запуском перевірки, так і перетягуванням їх («*drag and drop*») мишею з вікна файлового менеджера на головну сторінку (див. нижче) або сторінку **Сканер** вікна Dr.Web для Linux.

5. Огляд всіх загроз, виявлених Dr.Web для Linux під час поточного сеансу роботи в графічному режимі, включаючи огляд нейтралізованих та пропущених загроз, а також об'єктів, переміщених до карантину.
6. Огляд об'єктів, переміщених до карантину з можливістю їхнього остаточного видалення або відновлення.
7. Налаштування параметрів роботи компонентів Dr.Web для Linux, включаючи такі параметри:
   - Дії, які Сканер та SplDer Guard автоматично застосовуватимуть до виявлених загроз (залежно від їх типу).
   - Список каталогів та файлів, які не перевірятимуться Сканером та не контролюватимуться монітором файлової системи SplDer Guard.
   - Чорні та білі списки веб-сайтів та небажаних категорій веб-ресурсів, що використовуються монітором SplDer Gate, а також параметри перевірки файлів, що завантажуються з мережі Інтернет або отримуються електронною поштою.
   - Розклад планових перевірок файлової системи, включаючи періодичність та тип перевірки, а також список об'єктів для вибіркової перевірки відповідно до заданого розкладу.
   - Режим роботи (підключення до сервера централізованого захисту та відключення від нього).
   - Параметри моніторингу мережної активності, включаючи аналіз зашифрованого трафіку.
   - Дозвіл на використання сервісу Dr.Web Cloud.
8. Управління ліцензіями (проводиться через Менеджер ліцензій).
9. Перегляд повідомлень про стан антивірусної мережі, які розсилаються сервером централізованого захисту (тільки якщо Dr.Web для Linux працює у складі антивірусної мережі та тільки якщо адміністратор антивірусної мережі задасть відповідне налаштування на сервері централізованого захисту).

Для коректної роботи Dr.Web для Linux необхідно, щоб попередньо були запущені його сервісні компоненти, в іншому випадку він завершить свою роботу безпосередньо після запуску, видавши відповідне попередження. В штатному режимі всі необхідні сервісні компоненти запускаються автоматично та не потребують втручання користувача.

Зовнішній вигляд графічного інтерфейсу управління

Вигляд головного вікна графічного інтерфейсу управління Dr.Web для Linux наведений на малюнку нижче.



Малюнок 5. Графічний інтерфейс управління Dr.Web для Linux.

В лівій частині вікна розташована навігаційна панель, кнопки якої дозволяють виконати такі дії.

Кнопка	Опис
1. Постійно доступні	
	Відкриває головну сторінку, на якій є можливість: • Включити або відключити монітор файлової системи SpIDer Guard. • Включити або відключити монітор мережних з'єднань SpIDer Gate. • Запустити перевірку об'єктів файлової системи (файлів, завантажувальних записів) та запущених процесів. • Переглянути стан актуальності вірусних баз та провести їхнє оновлення за необхідності. • Запустити Менеджер ліцензій для перегляду стану поточної ліцензії та реєстрації нової за необхідності.
	Відкриває сторінку роботи з карантином, що дозволяє переглянути файли, поміщені до карантину, а також видалити їх або відновити з карантину.
	Відкриває вікно налаштування роботи Dr.Web для Linux, зокрема: • Сканера об'єктів файлової системи. • Монітора файлової системи SpIDer Guard. • Монітора мережних з'єднань SpIDer Gate. • Запуску перевірок за розкладом.

Кнопка	Опис
	Окрім того, тут може бути налаштована робота в режимі централізованого захисту.
	Надає доступ до довідкових матеріалів та допоміжних ресурсів компанії «Доктор Веб»: • Інформація про продукт. • Посібник користувача. • Форум Dr.Web. • Технічна підтримка. • Персональний кабінет користувача **Мій Dr.Web**. Всі посилання відкриваються в браузері, встановленому в системі.
2. З'являються залежно від умов	
	Відкриває сторінку списку задач перевірки файлів, в якому є незавершені (або що виконуються) задачі перевірки. *Відображається на навігаційній панелі, тільки якщо хоча б одна перевірка проводиться.*
  	Відкриває сторінку списку результатів завершених перевірок. Забарвлюється залежно від результату: 1) Зелена — все перевірки завершилися успішно, всі загрози, якщо були виявлені, знешкоджені. 2) Червона — є незнешкоджені загрози. 3) Жовта — будь-яка з перевірок завершилася через помилки. *Відображається на навігаційній панелі, тільки якщо запускалась хоча б одна перевірка.*
	Відкриває сторінку перегляду загроз, виявлених при перевірці файлів сканером або монітором файлової системи SplDer Guard. *Відображається на навігаційній панелі, тільки якщо є виявлені загрози.*
	Відображається на навігаційній панелі, тільки якщо відкрита та активна сторінка запуску сканування. *При переході на будь-яку іншу сторінку головного вікна, а також при запуску сканування сторінка запуску сканування буде автоматично закрита, а кнопка прибрана з навігаційної панелі.*
	Відображається на навігаційній панелі, тільки якщо відкрита та активна сторінка управління SplDer Guard. *При переході на будь-яку іншу сторінку головного вікна сторінка управління SplDer Guard буде автоматично закрита, а кнопка прибрана з навігаційної панелі.*
	Відображається на навігаційній панелі, тільки якщо відкрита та активна сторінка управління SplDer Gate.

Кнопка	Опис
	При переході на будь-яку іншу сторінку головного вікна сторінка управління SplDer Gate буде автоматично закрита, а кнопка прибрана з навігаційної панелі.
	Відображається на навігаційній панелі, тільки якщо відкрита та активна сторінка управління оновленнями. *При переході на будь-яку іншу сторінку головного вікна сторінка управління оновленнями буде автоматично закрита, а кнопка прибрана з навігаційної панелі.*
	Відображається на навігаційній панелі, тільки якщо відкрита та активна сторінка Менеджера ліцензій. *При переході на будь-яку іншу сторінку головного вікна сторінка Менеджера ліцензій буде автоматично закрита, а кнопка прибрана з навігаційної панелі.*
	Відкриває сторінку перегляду повідомлень від сервера централізованого захисту. *Відображається на навігаційній панелі, тільки якщо Dr.Web для Linux працює в режимі централізованого захисту та адміністратор антивірусної мережі налаштував відправлення повідомлень на цю робочую станцію.*

Головна сторінка

На головній сторінці вікна графічного інтерфейсу управління Dr.Web для Linux розташована цільова область («мішень») для перетягування файлів та каталогів, які необхідно перевірити. Вона позначена написом **Перетягніть сюди файли або клацніть, щоб вибрати їх**. При перетягуванні файлів та каталогів з вікна файлового менеджера на головну сторінку вікна Dr.Web для Linux запускається їх вибіркова перевірка (якщо Сканер вже проводить будь-яку перевірку, то задача перевірки вказаних файлів ставиться в чергу).

Також на головній сторінці вікна розташовані такі кнопки:

- **SplDer Guard** — відображає поточний стан, в якому знаходиться монітор файлової системи SplDer Guard. При натисненні відкриває сторінку управління, на якій можна запустити або зупинити SplDer Guard, а також переглянути статистику його роботи.
- **SplDer Gate** — відображає поточний стан, в якому знаходиться монітор мережних з'єднань SplDer Gate. При натисненні відкриває сторінку управління, на якій можна запустити або зупинити SplDer Gate, а також переглянути статистику його роботи.
- **Сканер** — дозволяє відкрити сторінку запуску перевірки файлів, каталогів та інших об'єктів файлової системи (наприклад, завантажувальні записи).
- **Останнє оновлення** — відображає поточний стан оновлення вірусних баз. При натисненні відкриває сторінку управління оновленням, на якій можна запустити процес оновлення вручну.
- **Ліцензія** — відображає стан поточної ліцензії. При натисненні відкриває сторінку Менеджера ліцензій, на якій можна ознайомитися з більш докладною інформацією

про поточну ліцензію, а також провести процедуру придбання та реєстрації нової ліцензії, якщо це необхідно.

Інтеграція з середовищем робочого столу

Dr.Web для Linux підтримує чотири способи інтеграції з графічним оточенням робочого столу:

- Відображення в області сповіщень робочого столу значка програми, що відіграє роль індикатора стану, та дозволяє відкрити контекстне меню програми;
- Виклик контекстного меню з основними командами перевірки файлів при натисненні правою клавіші миші на значок програми в панелі задач;
- Запуск перевірки файлів та каталогів за допомогою команди контекстного меню в графічному файловому менеджері;
- Запуск перевірки файлів та каталогів при перетягуванні їх мишею на головну сторінку вікна Dr.Web для Linux.

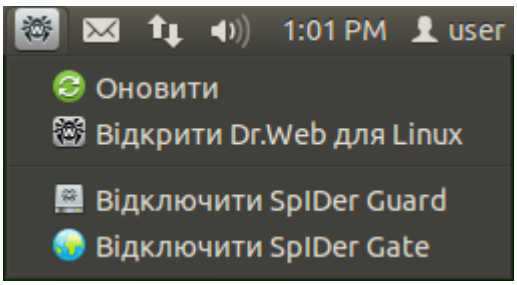
Індикатор програми в області сповіщень

Після входу користувача в систему, в області сповіщень робочого столу (якщо вона підтримується використовуваним графічним середовищем) агент сповіщень відображає індикатор в виді значка з логотипом Dr.Web для Linux. Індикатор використовується для відображення статусу програми, а також для доступу до контекстного меню Dr.Web для Linux. За наявності будь-яких проблем в роботі (наприклад, застарілі вірусні бази або завершується термін дії ліцензії) на індикаторі поверх логотипу Dr.Web для Linux відображається знак оклику:  .

Окрім індикатора стану, агент сповіщень також відображає спливаючі сповіщення, які інформують користувача про важливі події в роботі Dr.Web для Linux, такі, як:

- Виявлена загроза (в тому числі — резидентними моніторами SpIDer Guard та SpIDer Gate).
- Завершується термін дії ліцензії.

При натисненні мишею на значок індикатора на екрані відкривається контекстне меню Dr.Web для Linux.



Малюнок 6. Контекстне меню індикатора Dr.Web для Linux.

При виборі пункту меню **Відкрити за допомогою Dr.Web для Linux** на екрані з'являється вікно графічного інтерфейсу управління Dr.Web для Linux, тобто проводиться його запуск. Вибір пунктів меню **Включити SpIDer Gate/Відключити SpIDer Gate** та **Включити SpIDer Guard/Відключити SpIDer Guard** дозволяє запустити або завершити роботу відповідного монітора. Зверніть увагу, що для відключення роботи будь-якого монітора вам буде необхідно пройти аутентифікацію, вказавши логін та пароль користувача з адміністративними правами (див. Управління правами програми). Вибір пункту **Оновити** примусово запускає процедуру отримання оновлень.

Якщо індикатор вказує на наявність проблем в функціонуванні Dr.Web для Linux, то в меню значок відповідного пункту, що спричинив проблему, також супроводжується знаком оклику, наприклад:  .

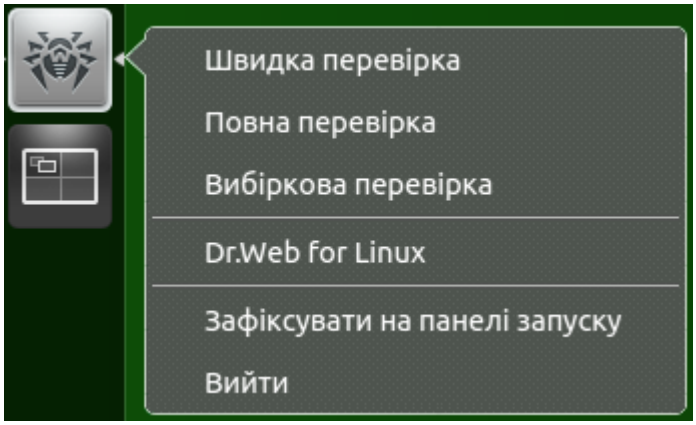
Проблеми в роботе індикатора програми

1. Якщо індикатор відображається з символом критичної помилки  , а у меню, що випадає, містить тільки неактивний пункт **Завантаження**, це означає, що Dr.Web для Linux не може запуститься через те, що деякі сервісні компоненти недоступні. Якщо цей стан триває значний час, то спробуйте усунути цю помилку самостійно або зверніться до Технічної підтримки.
2. Якщо після входу користувача в систему індикатор не відобразився в області сповіщень робочого столу, спробуйте усунути цю помилку самостійно або зверніться до Технічної підтримки.

В деяких оточеннях робочого столу зовнішній вигляд та поведінка індикатора можуть відрізнятися від описаного, наприклад, можуть не відображатися значки в меню, що випадає.

Контекстне меню значка панелі задач

Якщо оточення робочого столу підтримує використання панелі задач, наприклад, такої, як **Unity Launcher** в ОС **Ubuntu**, то при запуску графічного інтерфейсу Dr.Web для Linux на панелі задач з'явиться кнопка зі значком програми. Для цього рекомендується запускати програму через вибір пункту **Dr.Web для Linux** в меню **Програми**. Натиснення правої клавіші миші на кнопку запущеної програми відкриє на екрані контекстне меню, приблизний вигляд якого показаний на малюнку нижче.



Малюнок 7. Контекстне меню Dr.Web для Linux в панелі задач.

- Вибір пунктів меню **Швидка перевірка**, **Повна перевірка** та **Вибіркова перевірка** дозволяє запустити відповідну задачу перевірки (для **Вибіркова перевірка** — відкрити сторінку вибору об'єктів, що необхідно перевірити).
- Вибір пункту меню **Dr.Web для Linux** запускає графічний інтерфейс (якщо не запущений), а пункту **Вийти** — завершує роботу графічного інтерфейсу (якщо він запущений в даний момент).
- Вибір пункту меню **Зафіксувати на панелі запуску** дозволяє закріпити кнопку програми на панелі задач для швидкого доступу до запуску графічного інтерфейсу та основних задач перевірки.

Якщо в черзі задач є виконувані задачі перевірки файлової системи, поверх кнопки зі значком програми в панелі задач відображається індикатор сумарного виконання активних задач перевірки.

В різних оточеннях робочого столу зовнішній вигляд панелі задач, контекстного меню та поведінка пунктів меню, окрім **Швидка перевірка**, **Повна перевірка** та **Вибіркова перевірка**, можуть відрізнятися від описаного.

Проблеми в роботі значка панелі задач

Якщо значок запущеного графічного інтерфейсу відображається на панелі задач, але меню, що випадає, не містить пунктів запуску задач перевірки, спробуйте запустити програми через вибір пункту **Dr.Web для Linux** в меню **Програми** (замість запуску виконанням команди **drweb-gui** в емуляторі терміналу або вибору пункту **Відкрити за допомогою Dr.Web для Linux** в меню індикатора програми в області сповіщень).

Перевірка файлів та каталогів через контекстне меню файлового менеджера

Dr.Web для Linux дозволяє проводити перевірку файлів та каталогів безпосередньо з вікна огляду файлів та каталогів графічного файлового менеджера (такого, як **Nautilus**). Для перевірки файлів та каталогів необхідно:

1. Виділити їх у вікні файлового менеджера та натиснути праву клавішу миші.
2. В контекстному меню, що з'явилося, вибрати пункт **Відкрити через іншу програму**.
3. У списку встановлених програм, що з'явився, знайти **Dr.Web для Linux**.

Як правило, після першого використання Dr.Web для Linux в якості програми для відкриття файлів ця асоціація буде запам'ятована файловим менеджером та у подальшому в контекстному меню буде доступний пункт **Відкрити за допомогою Dr.Web для Linux**.

В різних графічних файлових менеджерах вказана назва пункту контекстного меню для вибору програми, також як і спосіб вибору програми зі списку встановлених в системі можуть відрізнятися від описаного.

Проблеми з використанням контекстного меню файлового менеджера

Деякі графічні середовища для ОС **GNU/Linux** можуть автоматично налаштувати асоціацію файлів або каталогів (за MIME-типом цих об'єктів) з **Dr.Web для Linux**, вибраним в файловому менеджері для перевірки за допомогою пункту контекстного меню **Відкрити через іншу програму**. В цьому випадку у подальшому для таких файлів та каталогів подвійне натиснення лівою кнопкою миші призводитиме до запуску **Dr.Web для Linux**. Щоб виправити цю ситуацію скасуйте налаштовану асоціацію між файлами та **Dr.Web для Linux**.

Перетягування файлів та каталогів у вікно графіченго інтерфейсу управління

Dr.Web для Linux дозволяє проводити перевірку файлів та каталогів перетягуванням їх курсором миші з вікна огляду файлів та каталогів графічного файлового менеджера у вікно запущеного графічного інтерфейсу управління Dr.Web для Linux. Для того щоб розпочати перевірку файлів та каталогів, що перетягнені мишею у вікно програми, необхідно, щоб вікно було відкрите на головній сторінці або на сторінці вибору типу перевірки. Ознакою того, що на дану сторінку вікна Dr.Web для Linux можна перетягувати файли та каталоги для перевірки, служить наявність на сторінці «мішені», що містить напис **Перетягніть сюди файли або клацніть, щоб вибрати їх**.

Запуск та завершення роботи

Запуск графічного інтерфейсу управління Dr.Web для Linux.

Щоб запустити графічний інтерфейс управління Dr.Web для Linux, необхідно:

- Вибрати в системному меню **Програми** пункт **Dr.Web для Linux**.

або

- Натиснути правою кнопкою миші на індикатор Dr.Web для Linux в області сповіщень робочого столу та вибрати в меню, що випадає, пункт **Відкрити за допомогою Dr.Web для Linux**.

Ви також можете запустити графічний інтерфейс управління Dr.Web для Linux з командного рядка. Це можливе, тільки якщо графічне оточення доступне при роботі з командним рядком, наприклад — з вікна емулятора терміналу.

Завершення роботи графічного інтерфейсу управління Dr.Web для Linux

Щоб завершити роботу графічного інтерфейсу управління Dr.Web для Linux, необхідно закрити його вікно, використовуючи стандартну кнопку закриття, розташовану в заголовку вікна.

Зверніть увагу, що при завершенні роботи графічного інтерфейсу Dr.Web для Linux сервісні компоненти, включаючи агент сповіщень і монітори SpIDer Guard та SpIDer Gate (якщо вони не були відключені користувачем) продовжують свою роботу.

В штатному режимі всі необхідні сервісні компоненти не потребують втручання користувача в свою роботу.

Пошук та знешкодження загроз

Пошук та знешкодження загроз проводиться як Сканером (на вимогу користувача або за заданим розкладом), так і в процесі роботи моніторів файлової системи SpIDer Guard та мережних з'єднань SpIDer Gate.

- Включення та відключення SpIDer Guard та SpIDer Gate проводиться як з меню області сповіщень, так і на відповідних сторінках управління їхньою роботою (див. Моніторинг файлової системи та Моніторинг мережних з'єднань).
- Огляд поточних задач на перевірку Сканером об'єктів файлової системи та управління ними проводиться на сторінці управління списком перевірок.
- Всі загрози, виявлені Сканером або монітором файлової системи SpIDer Guard, відображаються в виді списку на сторінці перегляду виявлених загроз.
- Управління загрозами, поміщеними до карантину, проводиться на сторінці роботи з карантином.
- Налаштування реакції Dr.Web для Linux на виявлення загрози проводиться у вікні налаштувань. Там також існує можливість включити та налаштувати розклад періодичних перевірок, а також налаштувати перевірку зашифрованих з'єднань.

Якщо Dr.Web для Linux працює під управлінням сервера централізованого захисту, на якому включена заборона запуску перевірки файлів користувачем, то сторінка **Сканер** вікна Dr.Web для Linux буде недоступною. Окрім того, в цьому випадку агент сповіщень та графічний інтерфейс управління не запускатимуть перевірки за розкладом.

Перевірка об'єктів на вимогу

В цьому розділі:

- Типи виконуваних перевірок.
- Запуск перевірки.
- Додавання та видалення об'єктів зі списку вибіркової перевірки.
- Запуск вибіркової перевірки зі списку.

Типи виконуваних перевірок

На вимогу користувача Сканер може проводити такі типи перевірок:

- *Швидка перевірка* — перевірка тільки жорстко визначеного набору критичних системних об'єктів, що піддаються найбільшому ризику (завантажувальні записи дисків, системні файли тощо).
- *Повна перевірка* — перевірка всіх об'єктів локальної файлової системи, доступних користувачу, від імені якого запущений Dr.Web для Linux.
- *Вибіркова перевірка* — перевірка об'єктів файлової системи або деяких об'єктів спеціального типу, безпосередньо вказаних користувачем.

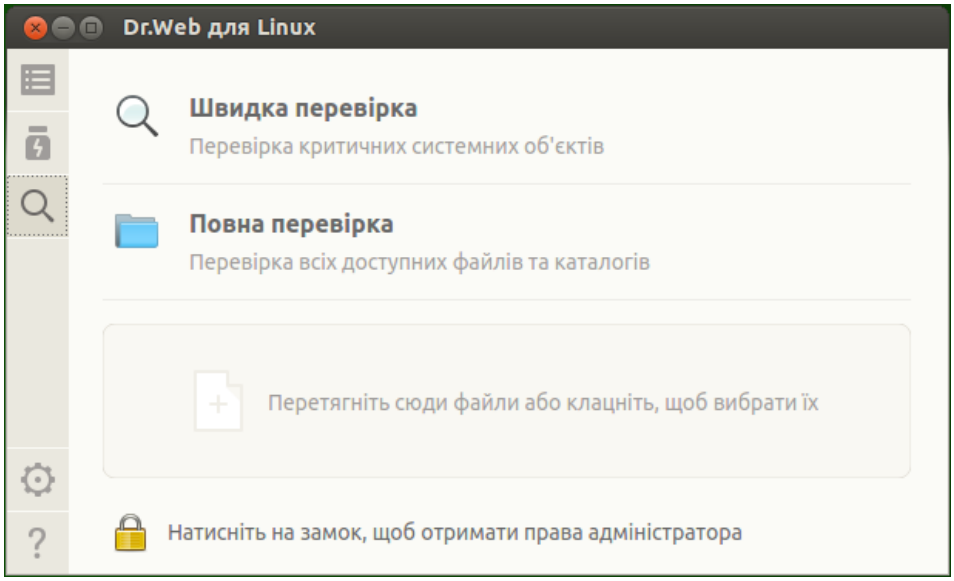
Якщо Dr.Web для Linux працює під управлінням сервера централізованого захисту, на якому включена заборона запуску перевірки файлів користувачем, то ця сторінка вікна Dr.Web для Linux буде недоступною.

При перевірці об'єктів збільшується навантаження на процесор, що може призвести до швидкої розрядки акумулятора на мобільних пристроях. Тому на портативних комп'ютерах рекомендується проводити перевірку системи при живленні від мережі.

Запуск перевірки

Запустити процес перевірки об'єктів файлової системи ви можете, натиснувши **Сканер** на головній сторінці вікна.

При цьому відкриється сторінка вибору типу перевірки. Щоб ініціювати *Швидку* або *Повну* перевірку, натисніть відповідну кнопку. Після цього перевірка розпочнеться автоматично.



Малюнок 8. Сторінка вибору типу перевірки.

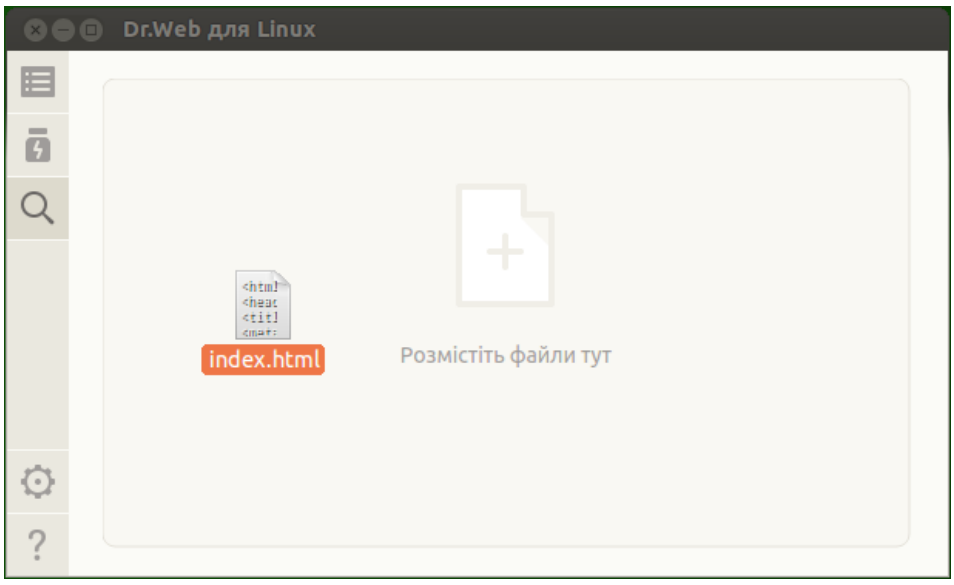
Перевірка об'єктів завжди проводиться Сканером з поточними правами програми. Якщо у програми немає підвищених прав, то при перевірці будуть пропущені всі файли та каталоги, недоступні користувачу, що запустив Dr.Web для Linux. Щоб забезпечити перевірку всіх необхідних файлів, власником яких ви не є, перед початком перевірки підвищіть права програми. Див. Управління правами програми.

Якщо необхідно *Вибіркова перевірка* тільки вибраних файлів та каталогів, то це можна зробити в будь-який зі способів, вказаних нижче:

- **Перетягування курсором**.

  Файли та каталоги, які необхідно перевірити, можна перетягнути мишею з вікна файлового менеджера на відкриту сторінку вибору типу перевірки (в зону, позначену написом **Перетягніть сюди файли або клацніть, щоб вибрати їх**). Також можна перетягнути їх на головну сторінку вікна Dr.Web для Linux.

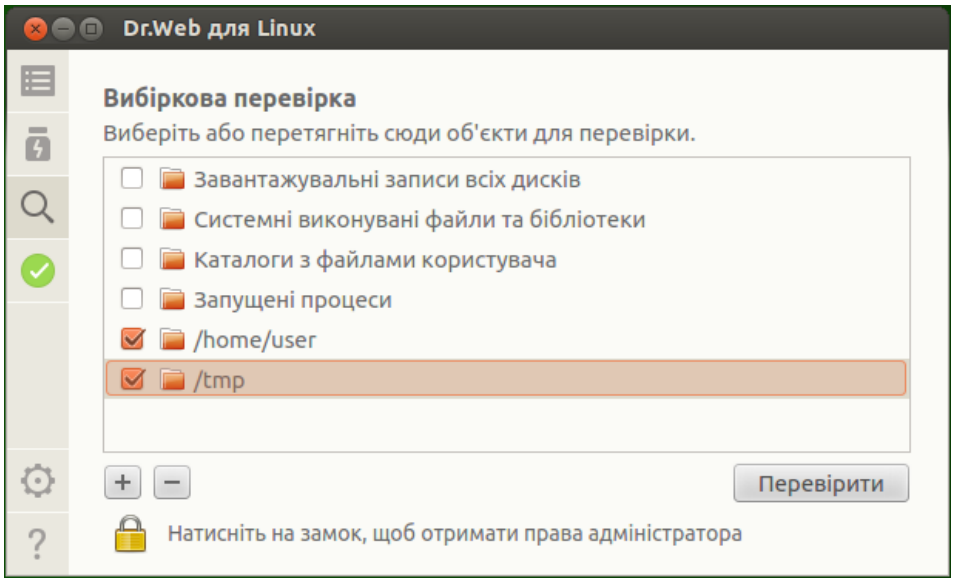
  При наведенні переміщуваних файлів та/або каталогів курсором миші на вікно, на ньому відображається мішень, що містить напис **Розмістіть файли тут**. Для початку перевірки вибраних файлів достатньо «кинути» їх на сторінку, відпустивши кнопку миші. Після цього перевірка розпочнеться автоматично.



Малюнок 9. Мішень для файлів, які необхідно перевірити.

- **Формування списку об'єктів для вибіркової перевірки**.

  Для формування списку об'єктів для вибіркової перевірки необхідно клацнути мишею по мішені для вибору файлів. На екрані відкриється список об'єктів для вибіркової перевірки.



Малюнок 10. Список об'єктів для вибіркової перевірки.

У списку також є чотири спеціальних пункти, що задають передвизначені групи об'єктів:

- *Завантажувальні записи всіх дисків*. При виборі цього пункту автоматично виділяються для перевірки всі завантажувальні записи всіх доступних в системі дисків.
- *Системні виконувані файли та бібліотеки*. При виборі цього пункту автоматично вибираються для перевірки всі каталоги, що містять системні виконувані файли (`/bin`, `/sbin` тощо).

- *Каталоги з файлами користувача*. При виборі цього пункту автоматично вибираються для перевірки каталоги, що містять файли користувача та поточного сеансу роботи (домашній каталог `/home/<username>` (~), `/tmp`, `/var/mail`, `/var/tmp`).
- *Запущені процеси*. При виборі цього пункту автоматично перевіряються виконувані файли, з яких були запущені процеси, активні в системі в даний момент. Якщо в виконуваному файлі виявляється загроза, то всі процеси, запущені з цього файла, примусово завершуються, а до файла застосовуються заходи з нейтралізації загрози.

Додавання та видалення об'єктів зі списку вибіркової перевірки

За необхідності ви можете додати до списку вибіркової перевірки власні шляхи для перевірки. Для цього перетягніть необхідні об'єкти мишею (шляхи, що ведуть до вказаних об'єктів, автоматично будуть додані до списку вибіркової перевірки), або натисніть `+` під списком. Відкриється стандартне вікно вибору файлів та каталогів. Виберіть необхідний об'єкт (файл або каталог) та натисніть **Відкрити**.

> Файли та каталоги зі встановленим атрибутом «прихований» за замовчуванням не відображаються у вікні вибору файлів та каталогів. Щоб відобразити їх, натисніть  на панелі інструментів вікна вибору файлів та каталогів.

Натисніть `–` під списком, щоб видалити зі списку всі виділені шляхи (шлях вважається виділеним, якщо виділений рядок списку, що містить шлях). Якщо необхідно виділити більше одного шляху, використовуйте виділення елементів списку, утримуючи клавішу CTRL або SHIFT. Зверніть увагу, що неможливо видалити зі списку перші чотири передвизначених пункти.

Запуск вибіркової перевірки зі списку

Щоб розпочати вибіркову перевірку, встановіть у списку прапорці для всіх об'єктів, які необхідно перевірити, та натисніть **Перевірити**. Після цього запуститься перевірка.

Після запуску створена задача перевірки поміщується в чергу, яка містить всі перевірки, що проводяться Сканером в поточному сеансі роботи, як завершені, так і такі, що виконуються в даний момент або ще тільки очікують свого виконання. Перегляд списку задач перевірки та управління ним проводиться на сторінці перегляду списку задач перевірки.

Перевірка об'єктів за розкладом

Dr.Web для Linux може виконувати автоматичний запуск періодичних перевірок заданого списку об'єктів файлової системи за вказаним розкладом.

Якщо Dr.Web для Linux працює під управлінням сервера централізованого захисту, на якому включена заборона запуску перевірки файлів користувачем, то ця можливість Dr.Web для Linux буде недоступною.

Типи виконуваних перевірок

За розкладом можна проводити такі типи перевірок:

- *Швидка перевірка* — перевірка тільки жорстко визначеного набору критичних системних об'єктів, що піддаються найбільшому ризику (завантажувальні записи дисків, системні файли тощо).
- *Повна перевірка* — перевірка всіх об'єктів локальної файлової системи, доступних користувачу, від імені якого запущений Dr.Web для Linux.
- *Вибіркова перевірка* — перевірка об'єктів файлової системи або деяких об'єктів спеціального типу, безпосередньо вказаних користувачем.

Запуск перевірки

Перевірки запускаються автоматично, відповідно до заданого розкладу. Запуск проверки проводиться:

1. Самим графічним інтерфейсом, якщо він запущений в момент початку перевірки.
2. Агентом сповіщень, якщо в момент початку перевірки графічний інтерфейс недоступний.

На початку перевірки за розкладом автоматично запускається графічний інтерфейс управління (якщо він ще не запущений), створена задача перевірки поміщується в чергу, яка містить всі перевірки, що проводяться Сканером в поточному сеансі роботи, як завершені, так і такі, що виконуються в даний момент або ще тільки очікують свого виконання. Перегляд списку задач перевірки та управління ним проводиться на сторінці перегляду списку задач перевірки.

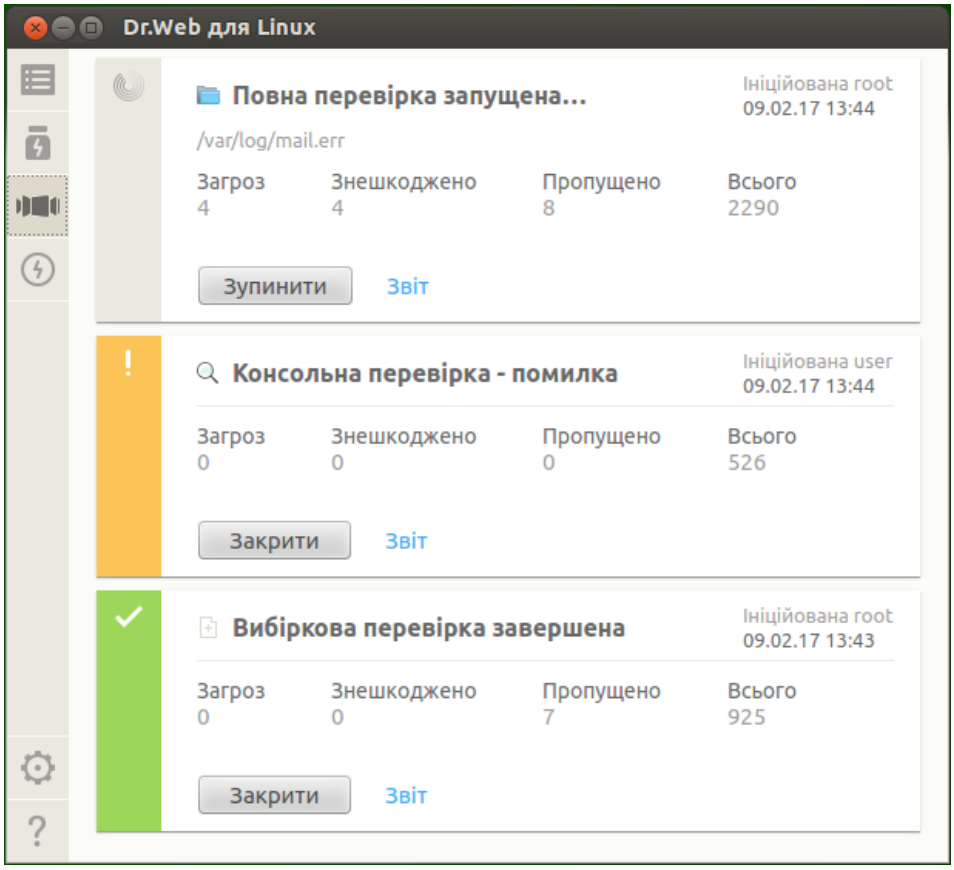
Управління списком перевірок

Список задач перевірки об'єктів файлової системи, що створені або виконуються Сканером, а також результати перевірок доступні на спеціальній сторінці вікна Dr.Web для Linux. За наявності в черзі Сканера хоча б однієї задачі, на навігаційній панелі вікна з'являється спеціальна кнопка, натиснення якої призводить до відкриття сторінки огляду списку задач перевірки. Залежно від стану задач перевірки ця кнопка має такий вигляд:

	У списку задач є незавершені перевірки (використовується анімація).

	Всі наявні у списку перевірки завершені або були зупинені користувачем, загрози не виявлені або всі виявлені загрози знешкоджені.
	Всі наявні у списку перевірки завершені або були зупинені користувачем, є незнешкоджені загрози.
	Всі наявні у списку перевірки завершені або були зупинені користувачем, є перевірки, що завершилися з помилками.

Задачі у списку упорядковані у міру їх створення згори вниз (від останньої до першої).



Малюнок 11. Сторінка перегляду списку перевірок.

Для кожної задачі виводиться така інформація:

- Тип перевірки (у списку можуть бути не тільки *Швидка перевірка, Повна перевірка* та *Вибіркова перевірка*, але й перевірки додаткових типів, див. нижче).
- Ім'я користувача, що ініціював перевірку (якщо ім'я користувача невідоме, виводиться його системний ідентифікатор — *UID*).
- Дата створення задачі та її завершення, якщо вона вже завершена.
- Кількість виявлених загроз, знешкоджених загроз, пропущених файлів та загальна кількість перевірених об'єктів.

Стан, в якому знаходиться задача, вказується за допомогою кольорової мітки, що присвоєна задачі у списку. Використовуються такі кольори:

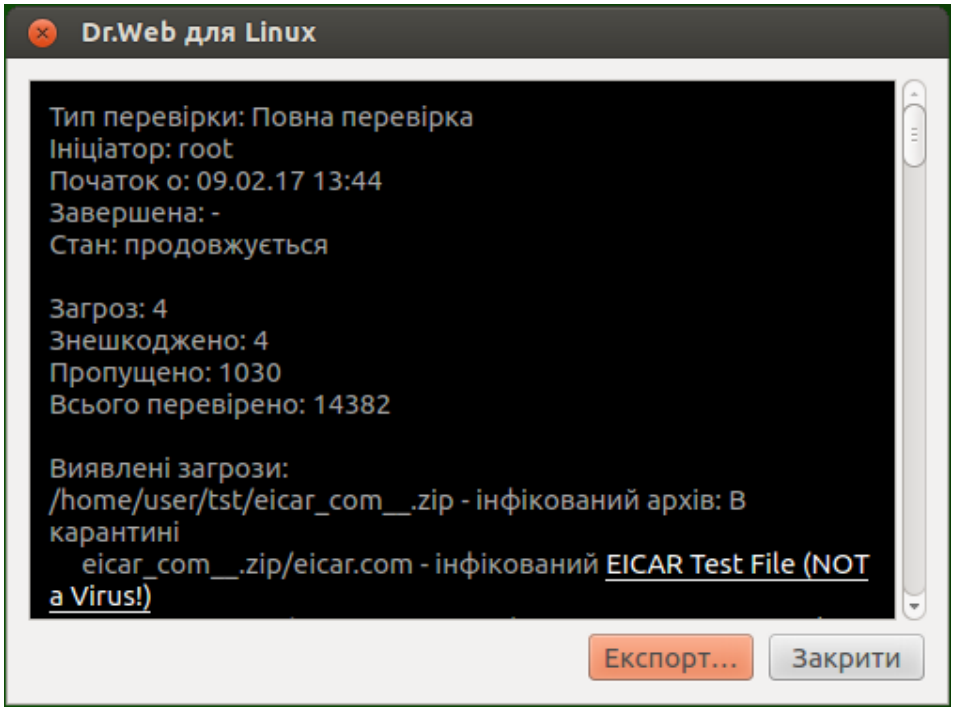
	Перевірка ще не завершена або очікує своєї черги.
	Перевірка завершена або зупинена користувачем, загрози не виявлені, або всі виявлені загрози знешкоджені.
	Перевірка зупинена через помилку.
	Перевірка завершена або виявлені користувачем, є незнешкоджені загрози.

Зверніть увагу, що у списку відображаються тільки ті перевірки, що виконуються Сканером, які були безпосередньо ініційовані користувачем у вікні Dr.Web для Linux, а також перевірки, запущені автоматично за заданим розкладом.

В області опису задачі може розташовуватися одна з таких кнопок:

- **Скасувати** — скасувати перевірку, що очікує своєї черги. Доступна, якщо задача очікує виконання. Після натиснення задача завершується. Інформація про задачу залишається у списку.
- **Зупинити** — зупинити розпочату перевірку без можливості її поновлення. Доступна, якщо задача виконується. Після натиснення задача завершується, а у списку залишається інформація про задачу, що містить результати перевірки, отримані до моменту зупинення.
- **Закрити** — закрити інформацію про завершену задачу та видалити її зі списку. Доступна, якщо задача завершена та немає незнешкоджених загроз.
- **Знешкодити** — провести знешкодження загроз. Доступна, якщо задача перевірки завершена та є незнешкоджені загрози.
- **Докладніше** — перейти до перегляду списку загроз. Доступна, якщо за результатами знешкодження деякі загрози залишилися незнешкодженими.

Натиснення на посилання **Звіт** відкриває на екрані вікно звіту з докладною інформацією про перевірку, що містить як загальну інформацію про задачу, так і список виявлених загроз, якщо вони були виявлені у процесі цієї перевірки.



Малюнок 12. Детальна інформація про перевірку.

В файловій системі UNIX-подобних операційних систем, до яких відносяться та ОС **GNU/Linux**, можуть зустрічатися спеціальні об'єкти, які виглядають як файли, та мають ім'я, але за своєю природою не є файлами, що містять дані (наприклад, це символічні посилання, сокети, іменовані канали та файли пристроїв). На противагу до *звичайних* (*регулярних*) файлів такі об'єкти носять назву *спеціальних файлів*. Спеціальні файли *завжди* пропускаються Dr.Web для Linux при перевірці.

Натиснення на посилання з іменем загрози відкриє у встановленому в системі веб-браузері сторінку на сайті компанії «Доктор Веб» з описом загрози (необхідне підключення до мережі Інтернет).

Натисніть **Експорт**, якщо ви хочете зберегти звіт про перевірку в текстовий файл. Щоб закрити вікно з докладною інформацією про перевірку, натисніть **Закрити**.

До загроз, виявлених Сканером у процесі будь-якої перевірки, запущеної через вікно Dr.Web для Linux (включаючи перевірку за розкладом), застосовуються дії з їх знешкодження відповідно до налаштувань, заданих на вкладці **Сканер**.

Налаштування знешкодження загроз, задані на вкладці **Сканер**, не використовуються для *Централізованої* та *Консольної* перевірок.

Загальний список всіх виявлених загроз доступний на сторінці Перегляду виявлених загроз.

Моніторинг файлової системи

В цьому розділі:

- Загальні відомості.
- Управління роботою монітора файлової системи.
- Налаштування роботи монітора файлової системи.
- Проблеми в роботі SpIDer Guard.

Загальні відомості

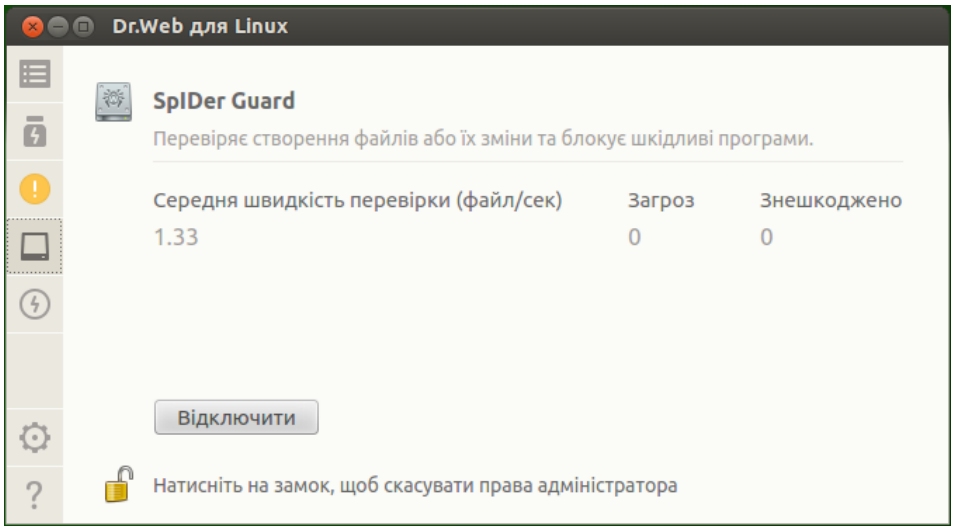
Функція постійного контролю над об'єктами файлової системи реалізується монітором файлової системи SpIDer Guard.

Графічний інтерфейс управління Dr.Web для Linux дозволяє управляти роботою SpIDer Guard, а саме:

- Запускати та зупиняти монітор файлової системи.
- Переглядати статистику роботи компонента та список виявлених загроз.
- Налаштовувати такі параметри роботи монітора файлової системи:
  - Реакція на виявлення загроз.
  - Список виключень з перевірки.

Управління роботою монітора файлової системи

Запуск та зупинення монітора файлової системи SpIDer Guard, а також перегляд статистики його роботи проводяться зі спеціальної сторінки вікна Dr.Web для Linux. Щоб перейти на сторінку управління моніторингом, натисніть **SpIDer Guard** на головній сторінці.



Малюнок 13. Сторінка управління роботою SpIDer Guard.

На сторінці управління моніторингом файлової системи виводиться така інформація:

- Стан монітора файлової системи SpIDer Guard (включений або відключений), а також, можливо, відомості про помилку, що сталася у процесі його роботи.
- Статистика моніторингу файлової системи:
  - Середня швидкість перевірки файлів.
  - Кількість виявлених та знешкоджених загроз.

Щоб включити моніторинг, якщо він відключений, натисніть кнопку **Включити**. Щоб відключити моніторинг, якщо він включений, натисніть **Відключити**.

Щоб відключити моніторинг файлової системи, необхідно, щоб програма мала підвищені права. Див. Управління правами програми.

Можливість включення та відключення монітора файлової системи SpIDer Guard при роботі Dr.Web для Linux під управлінням сервера централізованого захисту може бути заблокована, якщо це заборонено сервером.

Стан SpIDer Guard (включений або відключений) відображається індикатором:

	Монітор файлової системи SpIDer Guard включений та захищає файлову систему.
	Монітор файлової системи SpIDer Guard не захищає файлову систему, тому що відключений користувачем або через помилку, що сталася.

Щоб закрити сторінку управління моніторингом файлової системи, достатньо перейти до будь-якої іншої сторінки за допомогою кнопок навігаційної панелі.

Список загроз, виявлених SpIDer Guard в поточному сеансі роботи Dr.Web для Linux, відображається на сторінці перегляду виявлених загроз (ця сторінка доступна, тільки якщо є виявлені загрози).

Налаштування роботи монітора файлової системи

Налаштування роботи монітора файлової системи SpIDer Guard проводиться у вікні налаштувань:

- На вкладці **SpIDer Guard** — реакція на виявлені загрози.
- На вкладці **Виключення** — виключення об'єктів з перевірки.

Включення режиму посиленого моніторингу файлів монітором SpIDer Guard описане у розділі Режими моніторингу файлів.

Проблеми в роботі SpIDer Guard

При виникненні помилок функціонування SpIDer Guard на сторінці управління відображається повідомлення про помилку, що сталася. Щоб усунути помилки, скористайтеся описом відомих помилок, наведеним в Додатку Г.

Моніторинг мережних з'єднань

В цьому розділі:

- Загальні відомості.
- Управління роботою монітора мережних з'єднань.
- Налаштування роботи SpIDer Gate.
- Проблеми в роботі SpIDer Gate.

Загальні відомості

Функція постійного контролю встановлених мережних з'єднань реалізується монітором SpIDer Gate. Він дозволяє запобігати доступу до сайтів, внесених до чорного списку користувача, а також до таких, що відносяться до категорій сайтів, вказаних як небажані для відвідування. Окрім того, SpIDer Gate проводить перевірку:

- вхідних та вихідних повідомлень електронної пошти (у тому числі — на наявність ознак спаму)
- файлів, що завантажуються з Інтернету.

При виявленні загроз в об'єкті, що перевіряється, SpIDer Gate блокує їх завантаження або передачу.

Графічний інтерфейс управління Dr.Web для Linux дозволяє управляти роботою SpIDer Gate:

- Запускати та зупиняти моніторинг мережних з'єднань.
- Переглядати кількість перевірених та заблокованих об'єктів та спроб доступу до сайтів.
- Налаштовувати такі параметри моніторингу мережних з'єднань:
  - Вибирати тип трафіку для перевірки (веб-трафік, FTP-трафік).
  - Список категорій сайтів та вузлів, доступ до яких забороняється.
  - Персональні чорні та білі списки користувача для сайтів та вузлів.
  - Параметри перевірки файлів, що завантажуються з мережі Інтернет.

Загрози, що містяться в повідомленнях електронної пошти, можуть бути виявлені працюючим монітором файлової системи SpIDer Guard в момент збереження файлів поштовим клієнтом в локальну файлову систему.

Управління роботою монітора мережних з'єднань

Запуск та зупинення монітора мережних з'єднань SpIDer Gate, а також перегляд статистики його роботи проводяться зі спеціальної сторінки вікна Dr.Web для Linux. Щоб перейти на сторінку управління моніторингом мережних з'єднань, натисніть **SpIDer Gate** на головній сторінці.

Малюнок 14. Сторінка управління роботою SpIDer Gate.

На сторінці управління моніторингом мережних з'єднань виводиться така інформація:

- Стан монітора мережних з'єднань SpIDer Gate (включений або відключений), а також, можливо, відомості про помилку, що сталася у процесі його роботи.
- Статистика моніторингу:
  - Середня швидкість перевірки повідомлень електронної пошти та завантажуваних з Інтернет файлів.
  - Кількість перевірених об'єктів (повідомлень електронної пошти, файлів, завантажених з Інтернету, а також URL).
  - Кількість заблокованих звернень до сайтів та об'єктів, що містять загрози.

Щоб включити моніторинг, якщо він відключений, натисніть кнопку **Включити**. Щоб відключити моніторинг, якщо він включений, натисніть **Відключити**.

Щоб відключити моніторинг мережних з'єднань, необхідно, щоб програма мала підвищені права. Див. Управління правами програми.

Можливість включення та відключення монітора мережних з'єднань SpIDer Gate при роботі Dr.Web для Linux під управлінням сервера централізованого захисту може бути заблокована, якщо це заборонено сервером.

Стан монітора мережних з'єднань SpIDer Gate (включений або відключений) відображається індикатором:

	SpIDer Gate включений та контролює мережні з'єднання (приймання та передачу електронної пошти), а також доступ до мережі Інтернет).
	SpIDer Gate не контролює мережні з'єднання (доступ до сайтів не обмежується, повідомлення електронної пошти, а також завантажувані з мережі файли не перевіряються), тому що відключений користувачем або через помилку, що сталася.

Якщо в системі запущений поштовий клієнт (такий, як **Mozilla Thunderbird**), що використовує для отримання повідомлень електронної пошти протокол IMAP, його необхідно перезапустити після включення монітора SpIDer Gate, щоб забезпечити перевірку вхідних листів.

Щоб закрити сторінку управління моніторингом мережних з'єднань, достатньо перейти до будь-якої іншої сторінки за допомогою кнопок навігаційної панелі.

Налаштування роботи SpIDer Gate

Налаштування роботи монітора мережних з'єднань SpIDer Gate проводиться у вікні налаштувань:

- на вкладці **SpIDer Gate** — список заблокованих категорій сайтів та реакція на виявлені загрози.
- на вкладці **Виключення** — управління чорними та білими списками сайтів, а також виключення з перевірки мережної активності програм.
- на вкладці **Мережа** — управління перевіркою захищених мережних з'єднань (SSL/TLS).

Проблеми в роботі SpIDer Gate

При виникненні помилок функціонування монітора мережних з'єднань SpIDer Guard на сторінці управління відображається повідомлення про помилку, що сталася. Щоб усунути помилки, скористайтеся описом відомих помилок, наведеним у розділі Додаток Г. Опис відомих помилок.

Залежно від поставки, компонент Dr.Web Anti-Spam може бути відсутнім у складі Dr.Web для Linux. В цьому випадку перевірка повідомлень на спам не проводиться.

Якщо будь-які повідомлення електронної пошти неправильно розпізнаються компонентом Dr.Web Anti-Spam, рекомендується пересилати на спеціальні поштові адреси для аналізу та підвищення якості роботи спам-фільтра. Для цього кожне таке повідомлення збережіть в окремий файл типу `.eml`. Збережені файли прикріпіть до повідомлення електронної пошти, яке відправте на відповідну службову адресу.

- vrnonspam@drweb.com — якщо воно містить файли листів, *помилково розпізнаних як спам*;
- vrspam@drweb.com — якщо воно містить файли листів, *помилково не визначених як спам*.

Перегляд виявлених загроз

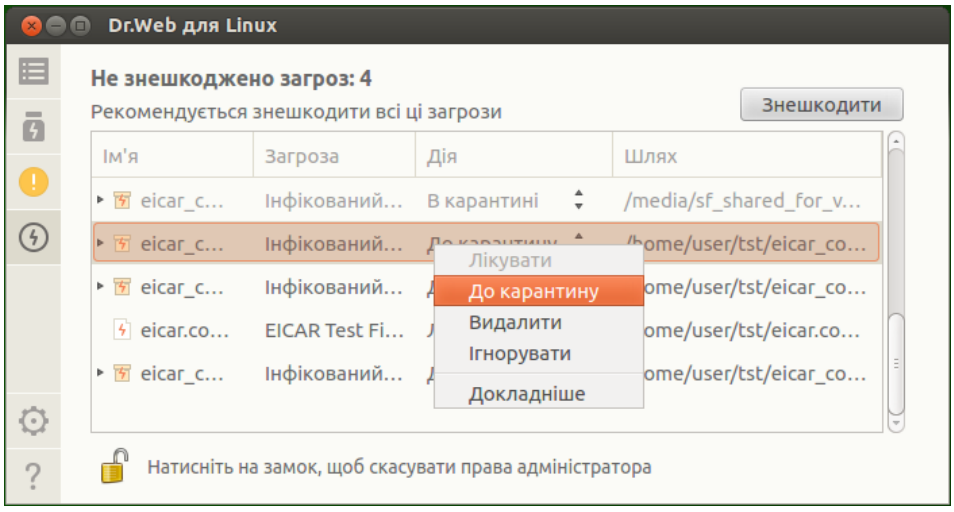
В цьому розділі:

- Загальні відомості.
- Знешкодження виявлених загроз
- Перегляд інформації про загрози

Загальні відомості

Список загроз, виявлених Сканером та монітором файлової системи SplDer Guard у поточному сеансі роботи Dr.Web для Linux, відображається на спеціальній сторінці вікна, що доступна, тільки якщо була виявлена хоча б одна загроза.

Якщо були виявлені загрози, то, щоб відкрити сторінку зі списком загроз, натисніть  на навігаційній панелі.



Малюнок 15. Сторінка огляду загроз.

У списку для кожної виявленої загрози виводиться така інформація:

- Ім'я об'єкта, що містить загрозу.
- Ім'я загрози, що міститься в об'єкті (за класифікацією «Доктор Веб»).
- Дія, що буде застосована до об'єкта для нейтралізації загрози (або вже була застосована, якщо загроза нейтралізована).
- Шлях до об'єкта файлової системи, в якому ця загроза була виявлена.

Вже знешкоджені загрози у списку наведені у списку неактивними рядками.

Знешкодження виявлених загроз

Якщо у списку є незнешкоджені загрози, на сторінці, безпосередньо над списком, доступна кнопка **Знешкодити**, при натисненні якої до всіх загроз, наведених у списку, будуть застосовані дії зі знешкодження, вказані у полі **Дія** у кожної незнешкодженої загрози. Якщо загроза знешкоджується успішно, її рядок в таблиці стає неактивним. Якщо спроба виявляється невдалою, рядок, що містить відомості про загрозу, залишається активним, текст в рядку забарвлюється в червоний колір, а у полі **Дія** виводиться інформація про помилку.

За замовчуванням у списку в якості дій вибираються дії, задані в якості реакцій на загрозу в налаштуваннях компонента, що виявив загрозу. Дії, які за замовчуванням вибираються для загроз, що знешкоджуються Сканером та монітором файлової системи SpIDer Guard, можуть бути змінені на відповідних вкладках вікна налаштувань.

> Якщо в налаштуваннях Сканера або SpIDer Guard для будь-яких типів загроз була вибрана дія *Report*, то всі загрози цього типу відображатимуться у списку загроз з дією *No action*. Щоб нейтралізувати такі загрози, необхідно вказати для кожної з них дію у полі **Дія**.

Якщо необхідно застосувати до загрози дію, відмінну від наведеної у списку, клацніть мишею по полю **Дія** в рядку загрози та виберіть необхідну дію в контекстному меню.

> Якщо загроза виявлена в файлі, що знаходиться в контейнері (архів, поштове повідомлення тощо), замість видалення виконується переміщення контейнера до карантину.

Існує можливість виділення набору загроз у списку. Для цього необхідно виділяти їх мишею, утримуючи клавішу CTRL або SHIFT:

- При утриманні клавіші CTRL загрози додаватимуться до списку виділення по одній.
- При утриманні клавіші SHIFT загрози виділятимуться неперервним списком.

Після вибору загроз, щоб застосувати до них будь-яку дію, натисніть правую кнопку миші в області списку та виберіть необхідну дію у списку, в меню, що випадає. Дія, вибрана в меню, буде застосована до всіх виділених загроз.

Зверніть увагу, що можна:

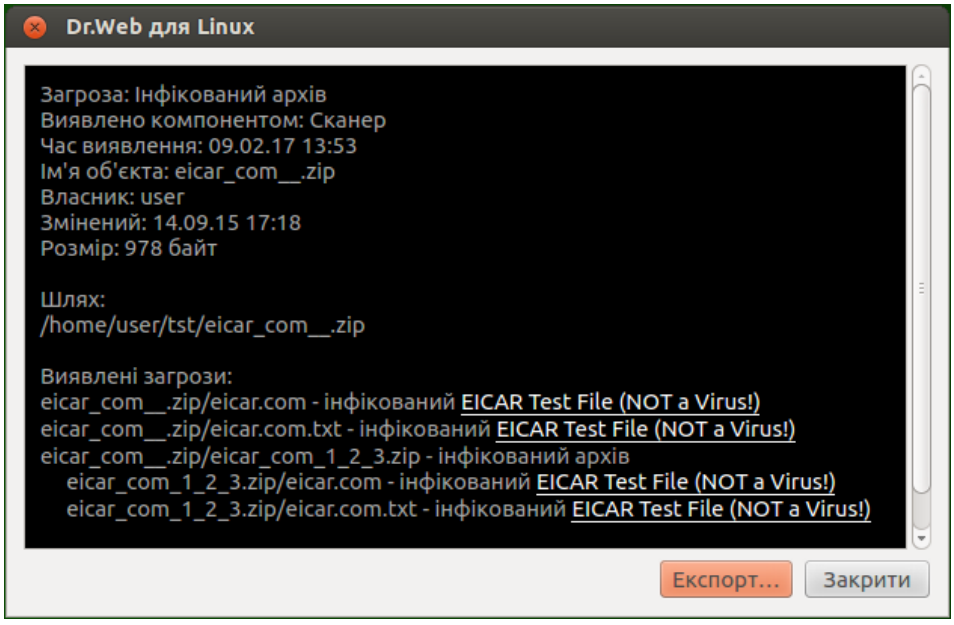
- Якщо загроза була виявлена в складеному об'єкті (архів, повідомлення електронної пошти тощо), то вибрана дія застосовується не до вкладеного інфікованого об'єкта, а до всього контейнера цілком.
- Дія *Лікувати* може бути застосована не до всіх типів загроз.

За необхідності, для успішного застосування дій до загроз, підвищіть права програми.

Загрози, до яких застосована дія *Ігнорувати*, відображатимуться у списку до перезапуску графічного інтерфейсу управління.

Перегляд інформації про загрози

Щоб отримати детальну інформацію про будь-яку виявлену загрозу, натисніть праву кнопку миші в рядку інформації про загрозу та виберіть в контекстному меню, що з'явилося, пункт **Докладніше**. Після цього на екрані з'явиться вікно з докладною інформацією про загрозу та об'єкт, що її містить. Якщо необхідно отримати докладну інформацію одразу про декілька загроз, перед викликом контекстного меню виділіть їх у списку мишею, утримуючи клавішу CTRL.



Малюнок 16. Інформація про загрозу.

В цьому вікні відображається така інформація:

- Ім'я загрози (за класифікацією «Доктор Веб»).
- Назва компонента Dr.Web для Linux, що виявив загрозу.

- Дата та час виявлення загрози.
- Інформація про об'єкт файлової системи, в якому ця загроза була виявлена: ім'я, користувач-власник об'єкта, дата останнього змінення та шлях до об'єкта в файловій системі.
- Остання дія, яка застосовувалася до загрози, та її результат (якщо в налаштуваннях компонента, що виявив загрозу, задане автоматичне застосування дій, наприклад, для Сканера вона може бути задана на відповідній вкладці вікна налаштувань).

Натиснення на посилання з іменем загрози відкриє у встановленому в системі веб-браузері сторінку на сайті компанії «Доктор Веб» з описом загрози (необхідне підключення до мережі Інтернет).

Натисніть **Експорт**, якщо ви хочете зберегти інформацію, наведену у вікні, в текстовий файл (відкриється вікно вибору файла для збереження інформації). Щоб закрити вікно докладної інформації про загрозу та об'єкт, що її містить, натисніть **Закрити**.

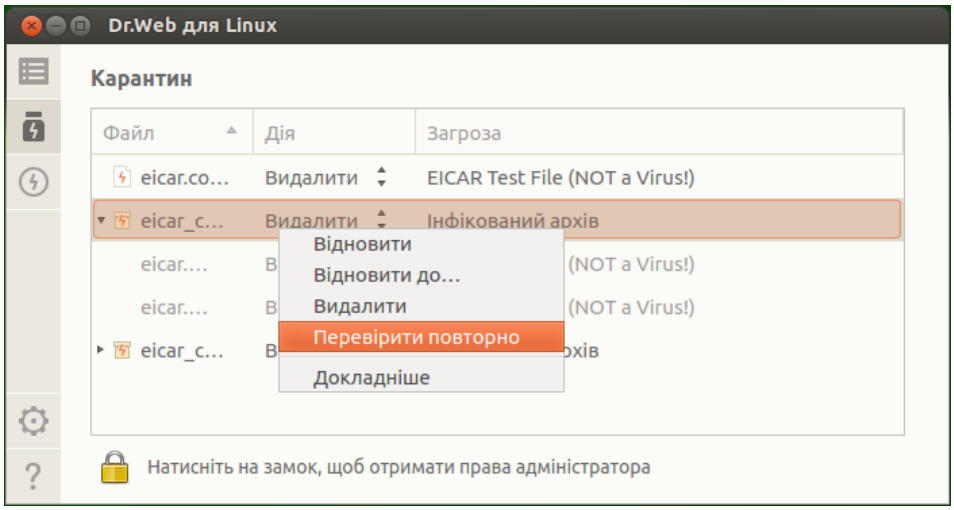
Управління карантином

В цьому розділі:

- Загальні відомості.
- Застосування дій до ізольованих об'єктів.
- Перегляд інформації про ізольовані об'єкти.

Загальні відомості

Список об'єктів, ізольованих Dr.Web для Linux до карантину, відображається на спеціальній сторінці. Щоб відкрити її, натисніть  на навігаційній панелі.



Малюнок 17. Сторінка управління карантином.

Якщо карантин не порожній, у списку для кожної виявленої загрози виводиться така інформація:

- Ім'я об'єкта, що містить загрозу.
- Дія, яку необхідно застосувати до об'єкта в карантині.
- Ім'я загрози, що міститься в об'єкті (за класифікацією «Доктор Веб»).

Застосування дій до ізольованих об'єктів

Щоб виконати будь-яку дію з ізольованим до карантину об'єктом, клацніть правою кнопкою миші в рядку, що містить інформацію про об'єкт, та виберіть необхідну дію в контекстному меню. Якщо необхідно провести будь-які дії з декількома ізольованими об'єктами, перед викликом контекстного меню виділіть їх у списку, утримуючи клавішу CTRL або SHIFT:

- При утриманні клавіші CTRL ізольовані об'єкти додаватимуться до списку виділення по одному.
- При утриманні клавіші SHIFT ізольовані об'єкти виділятимуться неперервним списком.

В меню доступні такі дії:

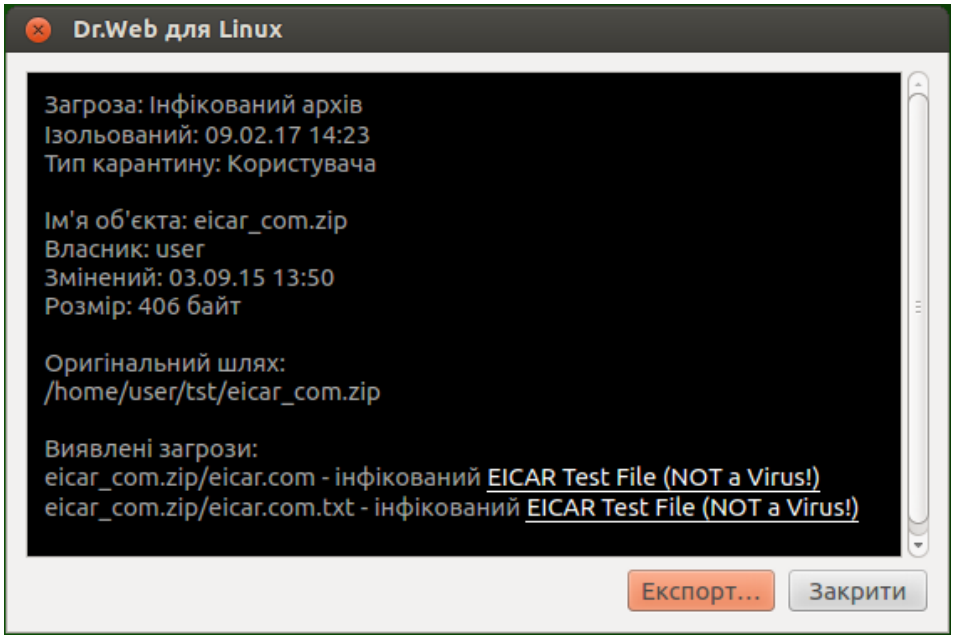
- **Відновити** — відновлення виділених об'єктів в їхні вихідні місця в файловій системі.
- **Відновити до** — відновлення виділених об'єктів в вибране місце в файловій системі (відкриється вікно вибору каталогу для відновлення).
- **Видалити** — безповоротне видалення виділених об'єктів.
- **Перевірити повторно** — повторна перевірка виділених об'єктів та їхнє лікування, якщо це можливо.

Якщо вибрана дія застосовується до виділеного об'єкта успішно, його рядок в таблиці стає неактивним. Якщо спроба виявляється невдалою, рядок, що містить відомості про ізольований об'єкт, залишається активним, текст в рядку забарвлюється в червоний колір, а у полі **Дія** виводиться інформація про помилку.

Для успішного застосування дій до ізольованих об'єктів може знадобитися підвищення прав програми. Наприклад, підвищення прав необхідне, щоб застосовувати дії до об'єктів, поміщених до карантину будь-яким з користувачів.

Перегляд інформації про ізольовані об'єкти

Щоб отримати докладну інформацію про будь-який ізольований об'єкт, натисніть праву кнопку миші на рядок інформації про цей об'єкт та виберіть в контекстному меню, що з'явилося, пункт **Докладніше**. Після цього на екрані з'явиться вікно з докладною інформацією про об'єкт. Якщо необхідно отримати докладну інформацію одразу про декілька ізольованих об'єктів, перед викликом контекстного меню виділіть їх у списку.



Малюнок 18. Інформація про ізольований об'єкт.

В цьому вікні відображається така інформація:

- Ім'я загрози (за класифікацією «Доктор Веб»).
- Дата та час ізоляції об'єкта до карантину.
- Тип карантину, до якого ізольований об'єкт.
- Найменування та результат останньої дії, що застосовувалася до об'єкта.
- Інформація про ізольований об'єкт файлової системи: ім'я, користувач-власник об'єкта, дата останнього змінення та шлях до об'єкта в файловій системі.

Натиснення на посилання з іменем загрози відкриє у встановленому в системі веб-браузері сторінку на сайті компанії «Доктор Веб» з описом загрози (необхідне підключення до мережі Інтернет).

Натисніть **Експорт**, якщо ви хочете зберегти інформацію, наведену у вікні, в текстовий файл (відкриється вікно вибору файла для збереження інформації). Щоб закрити вікно докладної інформації про загрозу та об'єкт, що її містить, натисніть **Закрити**.

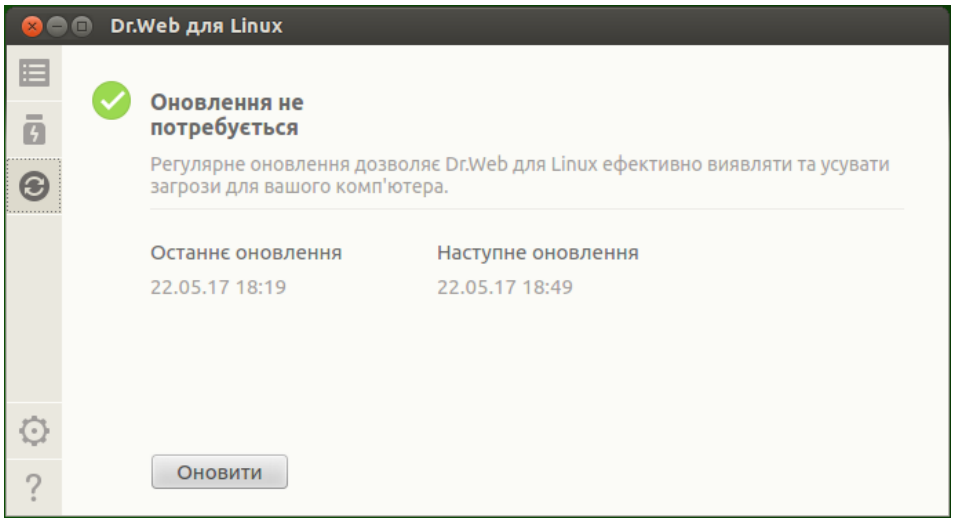
Оновлення антивірусного захисту

В цьому розділі:

- Загальні відомості.
- Налаштування оновлень.
- Проблеми в роботі компонента оновлень.

Загальні відомості

Періодичне оновлення вірусних баз, антивірусного ядра та баз категорій веб-ресурсів проводиться Компонентом оновлення автоматично. Перегляд стану оновлень та примусовий запуск оновлення на вимогу проводяться зі спеціальної сторінки вікна Dr.Web для Linux. Щоб перейти на сторінку управління оновленням, натисніть **Останнє оновлення** на головній сторінці.



Малюнок 19. Сторінка управління оновленням.

На сторінці управління оновленням виводиться така інформація:

- Актуальність вірусних баз, антивірусного ядра та баз категорій веб-ресурсів.
- Інформація про останнє проведене оновлення та час наступного планового оновлення.

Щоб провести примусове оновлення, натисніть **Оновити**. Щоб закрити сторінку управління оновленням, достатньо перейти на будь-яку іншу сторінку за допомогою кнопок навігаційної панелі.

Якщо Dr.Web для Linux працює в режимі централізованого захисту, ця сторінка буде заблокована.

Налаштування оновлень

Налаштування оновлень Dr.Web для Linux проводиться у вікні налаштувань на вкладці **Основні**.

Проблеми в роботі компонента оновлень

При виникненні помилок функціонування Компонента оновлення на сторінці управління оновленням відображається повідомлення про помилку, що сталася. Щоб усунути помилки, скористайтеся описом відомих помилок, наведеним в Додатку Г.

Менеджер ліцензій

В цьому розділі:

- Загальні відомості.
- Запуск Менеджера ліцензій.
- Активація ліцензії.
- Видалення ліцензійного ключового файла.

Загальні відомості

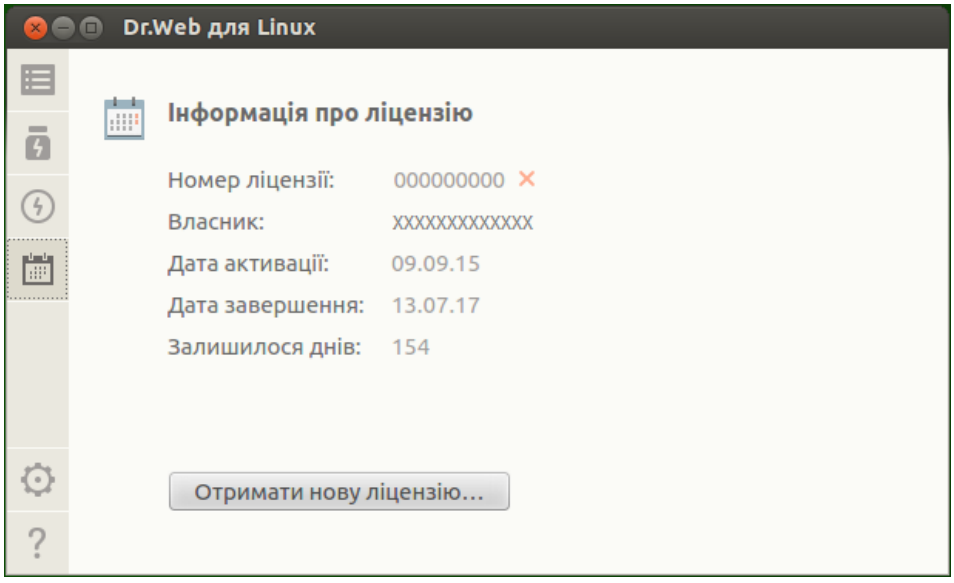
Менеджер ліцензій дозволяє переглянути в графічному режимі інформацію про поточну ліцензію, що видана користувачу Dr.Web для Linux. Дані ліцензії, виданої користувачу, зберігаються в ліцензійному ключовому файлі, який забезпечує роботу Dr.Web для Linux на комп'ютері користувача. За відсутності на комп'ютері ліцензійного або демонстраційного ключового файла все антивірусні функції Dr.Web для Linux (перевірка та моніторинг об'єктів файлової системи, оновлення вірусних баз) будуть заблоковані.

Запуск Менеджера ліцензій

Менеджер ліцензій інтегрований у вікні Dr.Web для Linux. Щоб відкрити сторінку Менеджера ліцензій, натисніть **Ліцензія** на головній сторінці вікна.

Якщо на комп'ютері вже встановлений ключовий файл, пов'язаний з будь-якою виданою користувачу ліцензією на використання Dr.Web для Linux, або з активним демонстраційним періодом, то на початковій сторінці Менеджера ліцензій відображаються данні про ліцензії, такі, як її номер, ім'я власника, а також термін дії, витягнуті з ключового файла.

Вид сторінки перегляду даних про ліцензії наведений на малюнку нижче.



Малюнок 20. Інформація про ліцензію.

Натиснення на символ ✕ праворуч від номера ліцензії дозволяє видалити ключовий файл.

Щоб закрити сторінку Менеджер ліцензій, достатньо перейти до будь-якої іншої сторінки за допомогою кнопок навігаційної панелі.

Активація ліцензії

Щоб за допомогою Менеджера ліцензій активувати ліцензію (у тому числі — придбати нову ліцензію або подовжити поточну) або демонстраційний період та отримати на комп'ютер відповідний ключовий файл, що забезпечує роботу Dr.Web для Linux, натисніть **Отримати нову ліцензію**. Після цього на екрані з'явиться майстер реєстрації. Зверніть увагу, що майстер реєстрації також відображається автоматично при першому запуску Dr.Web для Linux після його інсталяції.

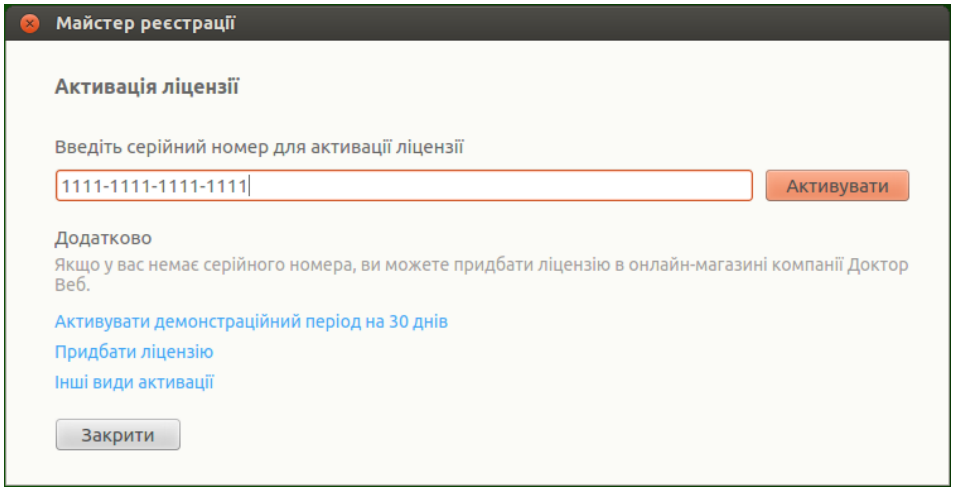
На першому етапі активації необхідно вибрати спосіб активації. Доступні три способи:

1. Активація ліцензії або демонстраційного періоду за наявним серійним номером.
2. Отримання демонстраційного періоду.
3. Встановлення ключового файла, отриманого раніше.

> Для реєстрації серійного номера та для отримання демонстраційного періоду необхідна наявність підключення до мережі Інтернет.

1. Активація ліцензії або демонстраційного періоду за допомогою серійного номера

Для активації ліцензії або демонстраційного періоду за допомогою серійного номера введіть символи наявного у вас серійного номера у поле введення та натисніть **Активувати**.



Малюнок 21. Реєстрація за допомогою серійного номера.

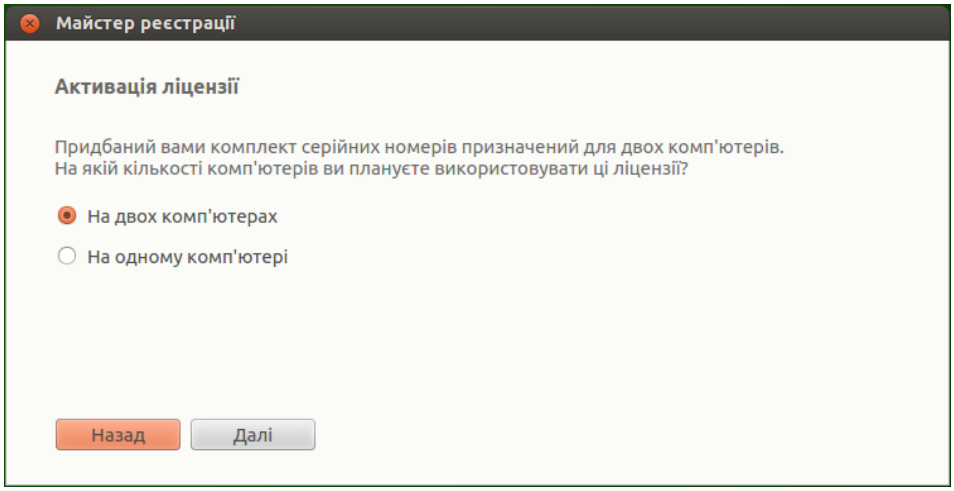
Якщо у вас немає серійного номера або діючого ключового файла, то ви можете придбати ліцензію в онлайн-магазині компанії «Доктор Веб», перейшовши за посиланням **Придбати ліцензію**.

Про додаткові способи придбання ліцензії на продукти Dr.Web див. у розділі Реєстрація та активація.

Після натиснення **Активувати** буде проведене підключення до сервера реєстрації компанії «Доктор Веб».

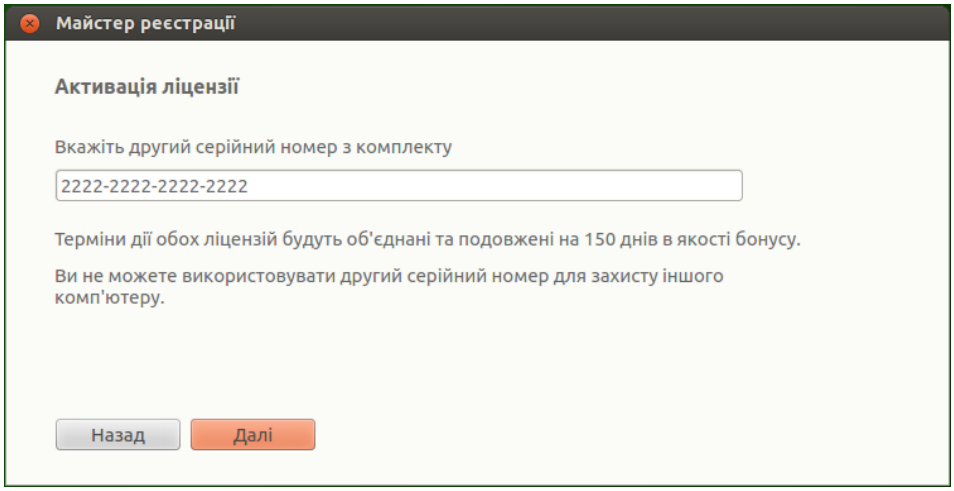
Якщо вказаний вами серійний номер був отриманий на сайті компанії «Доктор Веб» для активації демонстраційного періоду терміном на 3 місяці, то додаткових кроків для активації не потребується.

Якщо вказаний на першому кроці серійний номер входить в комплект з двох серійних номерів, то далі вам необхідно вибрати, на якій кількості комп'ютерів ви плануєте використовувати Dr.Web для Linux. Якщо ви виберете варіант **На двох комп'ютерах**, то другий серійний номер з цього комплекту ви зможете активувати ще на одному комп'ютері та отримати другий ліцензійний ключовий файл. При цьому для обох комп'ютерів видані ліцензії будуть дійсними протягом однакового терміну (наприклад, на рік). Якщо ви виберете варіант **На одному комп'ютері**, то вам необхідно буде вказати другий серійний номер з комплекту. У подальшому ви вже не зможете зареєструвати цей серійний номер на другому комп'ютері (також як і використовувати на ньому копію ліцензійного ключового файла, отриманого вами в результаті активації об'єднаної ліцензії), але для поточного комп'ютера термін дії ліцензії буде збільшений вдвічі (наприклад, до двох років, якщо ліцензія була видана терміном на рік).



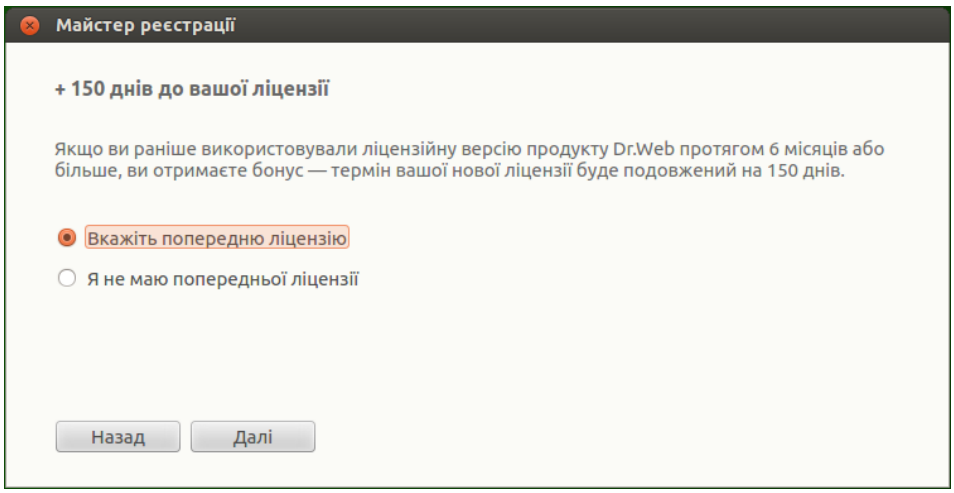
Малюнок 22. Вибір кількості комп'ютерів.

Після вибору кількості комп'ютерів, для яких може бути активована ліцензія, натисніть **Далі**, та, якщо ви вибрали варіант **На одному комп'ютері**, вкажіть сторінці майстра, що з'явилася, другий серійний номер з комплекту, після чого також натисніть **Далі**.



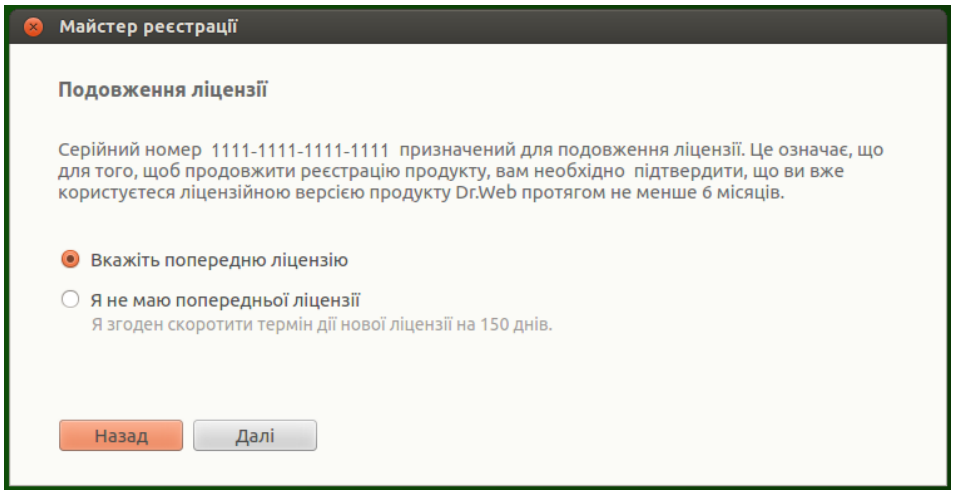
Малюнок 23. Вказання другого серійного номера з комплекту.

Далі вам буде запропоновано отримати бонус в 150 днів до терміну дії ліцензії, що активується. Для цього буде необхідно вказати інформацію про попередню придбану вами ліцензії, якщо вона у вас є. Якщо ви хочете отримати бонус, то виберіть пункт **Вкажіть попередню ліцензію**, а якщо ви не хочете отримувати бонус, або у вас немає попередньої ліцензії, виберіть пункт **Я не маю попередньої ліцензії**, після чого натисніть **Далі**.



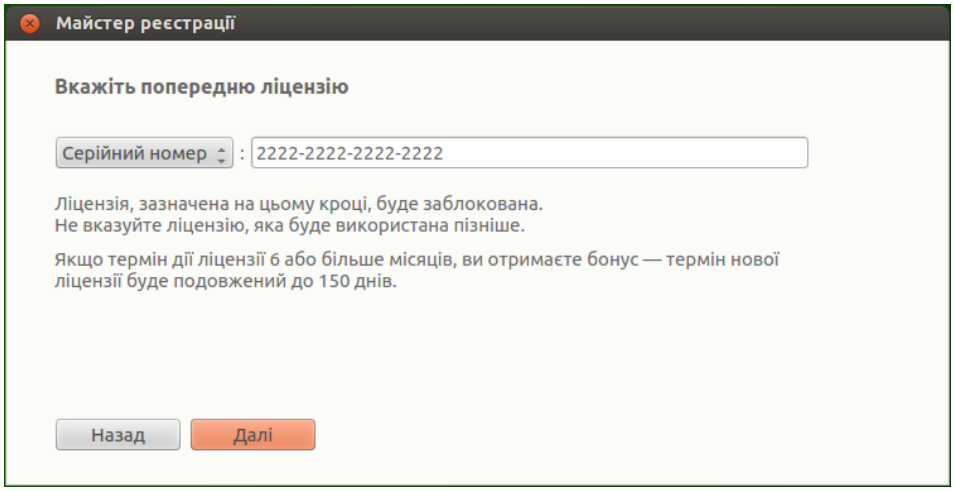
Малюнок 24. Отримання бонусу.

Якщо на першому кроці ви вказали спеціальний *серійний номер подовження,* то замість пропозиції отримати бонус вам буде запропоновано вказати попередню ліцензію, щоб не втратити 150 днів з терміну дії ліцензії, що активується. Якщо в цьому випадку ви виберете пункт **Я не маю попередньої ліцензії**, то ви зменшите термін дії нової ліцензії на 150 днів.



Малюнок 25. Подовження ліцензії.

Якщо ви вибрали пункт **Вкажіть попередню ліцензію**, то у вікні, що з'явилося, вкажіть серійний номер попередньої ліцензії або шлях до пов'язаного з нею ключового файла.



Малюнок 26. Вказання попередньої ліцензії.

Якщо ви вкажете на цьому кроці ліцензію, термін дії якої ще не завершився, то термін дії нової ліцензії буде додатково подовжений та на залишок терміну дії старої ліцензії. При активації комплекту з двох серійних номерів, порядок обробки бонусу залежить від того, який варіант використання був вибраний на попередньому кроці майстра реєстрації:

- **На двох комп'ютерах**, *та це перший комп'ютер*. Щоб отримати бонус для першого комп'ютера, ви маєте використати на цьому кроці попередню ліцензію, видану для цього комп'ютера, якщо вона є. *Другий серійний номер з комплекту тут вказувати не можна*.
- **На двох комп'ютерах**, *та це другий комп'ютер*. Щоб отримати бонус для другого комп'ютера, ви маєте використати на цьому кроці попередню ліцензію, видану для цього комп'ютера, якщо вона є. *Перший серійний номер з комплекту тут вказувати не можна*.
- **На одному комп'ютері**. В цьому випадку не тільки подвоюється термін дії нової ліцензії, але до нього також автоматично додається бонус (перший серійний номер дає бонус для другого номера). Окрім того, якщо ви на цьому кроці додатково вкажете попередню ліцензію, видану для цього комп'ютера, якщо вона є, то до подвоєного терміну дії нової ліцензії також додасться бонус та залишок терміну дії вказаної ліцензії, якщо він є.

Щоб вказати попередню ліцензію, можна ввести її серійний номер у відповідне поле або вказати пов'язаний з нею ключовий файл. Тип інформації про попередню ліцензію вибирається зі списку, що випадає, який розташований ліворуч від поля введення. Щоб вказати ключовий файл ви можете:

- Ввести шлях до нього безпосередньо в рядку введення.
- Скористатися стандартним вікном вибору файлів графічної оболонки, натиснувши **Огляд**.
- Перетягнути його мишею на сторінку майстра з вікна файлового менеджера.

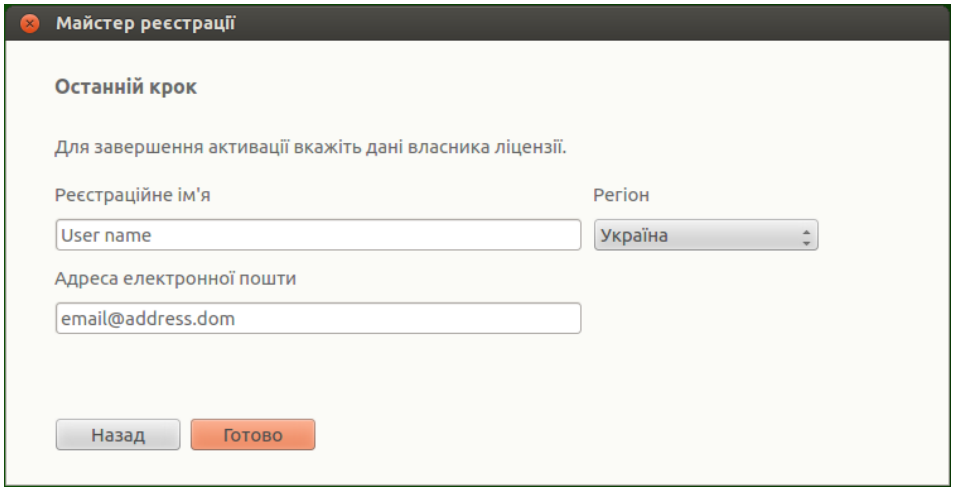
Вказати замість ключового файла файл zip-архіву, що містить ключовий файл, розпакування архіву при цьому не потребується.

Щоб продовжити активацію, натисніть **Далі**.

На наступному кроці необхідно вказати коректну реєстраційну інформацію, що включає такі дані:

- Реєстраційне ім'я.
- Регіон (країна) перебування, вибирається зі списку.
- Коректна адреса електронної пошти.

Всі поля реєстраційної форми є обов'язковими для заповнення.



Малюнок 27. Реєстраційна інформація користувача.

Після заповнення всіх полів форми натисніть **Готово**, щоб підключитися до сервера та отримати ліцензійний ключовий файл. За необхідності ви зможете перенести отриманий ліцензійний ключовий файл на будь-який комп'ютер за умови, що ви припините використовувати його на цьому комп'ютері.

2. Отримання демонстраційного періоду

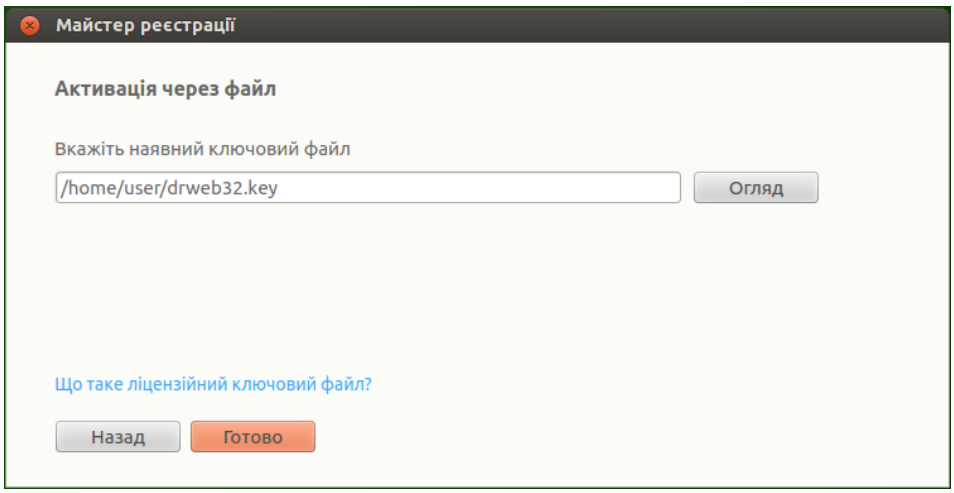
Якщо необхідно отримати демонстраційний період для роботи Dr.Web для Linux протягом 30 днів, перейдіть на першому кроці активації за посиланням **Активувати демонстраційний період на 30 днів**.

При отримання демонстраційного періоду терміном на 1 місяць через Менеджер ліцензій вам не потрібно вказувати свої персональні дані. Проте ви можете зареєструватися на офіційному сайті компанії «Доктор Веб» та отримати серійний номер, що надає демонстраційний період терміном на 3 місяці.

Демонстраційний період для одного того самого комп'ютера може бути виданий повторно тільки після завершення визначеного періоду часу. Докладніше див. у розділі Реєстрація та активація.

3. Встановлення наявного ключового файла

Якщо ви вже маєте діючу ліцензію та пов'язаний з нею ключовий файл (можливо, отриманий від компанії «Доктор Веб» або її партнерів електронною поштою), то ви можете активувати Dr.Web для Linux, встановивши цей ключовий файл. Для цього на першому кроці активації перейдіть за посиланням **Інші види активації**, після чого вкажіть у полі введення, що з'явилося, шлях до наявного у вас ключового файла.



Малюнок 28. Активація через ключовий файл.

Щоб вказати ключовий файл, ви можете:

- Ввести шлях до нього безпосередньо в рядку введення.
- Скористатися стандартним вікном вибору файлів графічної оболонки, натиснувши **Огляд**.
- Перетягнути його мишею на сторінку майстра з вікна файлового менеджера.

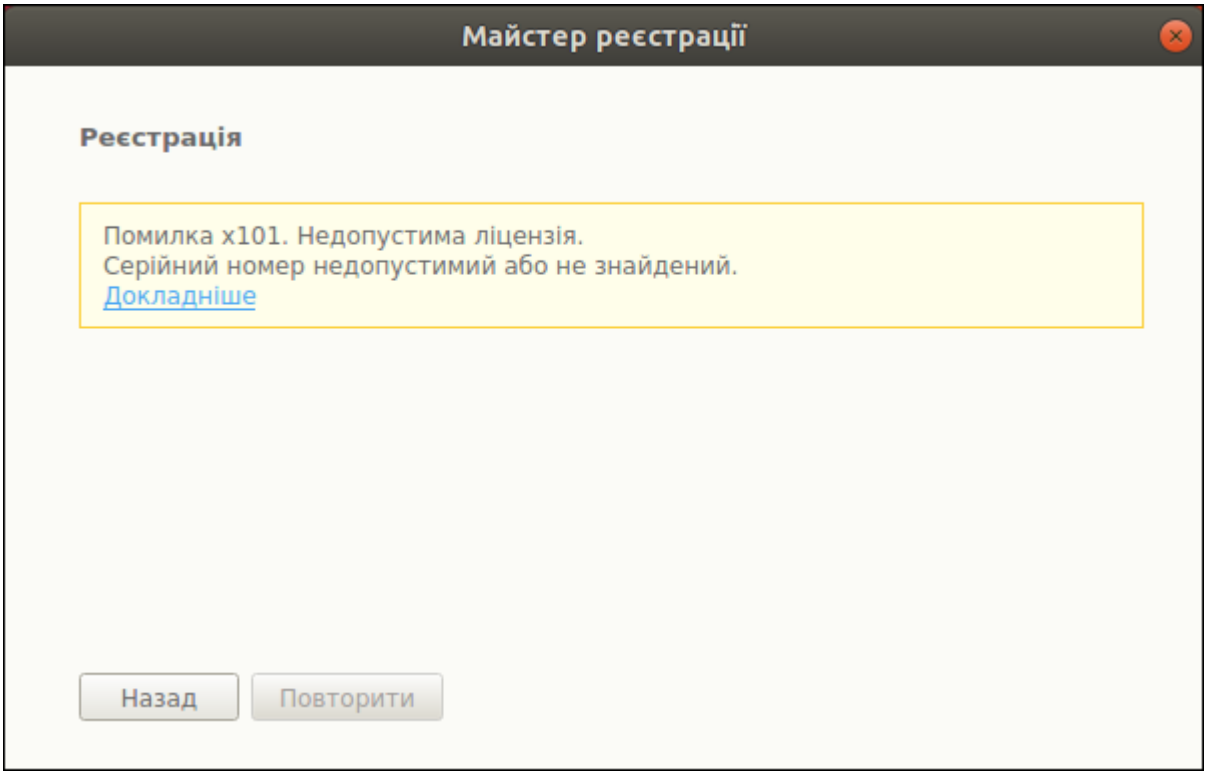
Вказати замість ключового файла файл zip-архіву, що містить ключовий файл, розпакування архіву при цьому не потребується.

Після вказання шляху до ключового файла (або до архіву, що його містить) натисніть кнопку **Готово** для автоматичного встановлення ключового файла. Ключовий файл буде за необхідності розпакований та скопійований до каталогу службових файлів Dr.Web для Linux. Підключення до мережі Інтернет в цьому випадку не потрібне.

Після успішного завершення процесу активації (в будь-який з описаних вище способів) на екрані буде показана фінальна сторінка майстра реєстрації з повідомленням про успішну активацію ліцензії або демонстраційного періоду. Натисніть **ОК**, щоб закрити майстер реєстрації та повернутися на головну сторінку вікна Dr.Web для Linux.

Малюнок 29. Повідомлення про успішну активацію.

Якщо на будь-якому з етапів реєстрації виникне помилка, з'явиться сторінка з відповідним повідомленням та стислим описом помилки. Приклад такої сторінки показаний нижче.

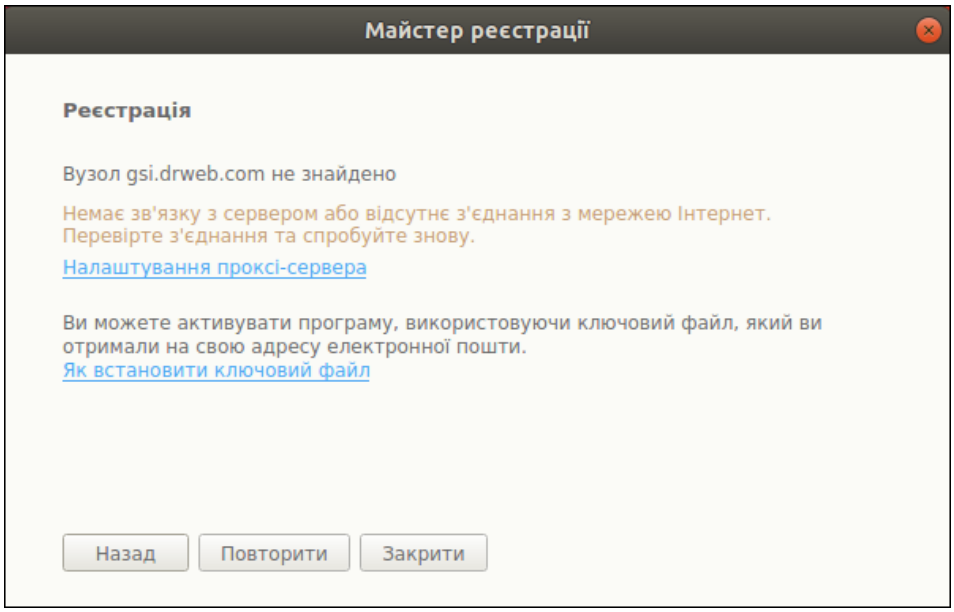


Малюнок 30. Повідомлення про помилку.

В цьому випадку у вас є можливість повернутися на попередній крок реєстрації, щоб внести виправлення (наприклад, виправити серійний номер або вказати вірний шлях до файла). Для цього натисніть **Назад**.

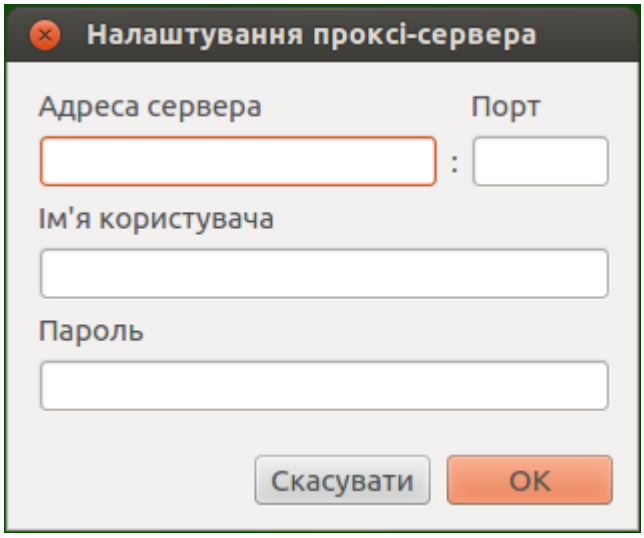
Якщо помилка пов'язана з тимчасовими несправністю, наприклад, тимчасовим збоєм в мережі, то ви можете спробувати повторити цей крок, натиснувши **Повторити**. За необхідності ви можете натиснути **Закрити**, щоб перервати реєстрацію та закрити

майстер реєстрації. Вам доведеться пізніше повторити процедуру реєстрації знову. Якщо майстер реєстрації не зможе встановити з'єднання з сервером реєстрації компанії «Доктор Веб» для перевірки введеного серійного номера, буде показана сторінка з відповідним повідомленням про помилку.



Малюнок 31. Помилка підключення до сервера реєстрації.

Якщо помилка пов'язана з тим, що у вас відсутня можливість прямого підключення до мережі Інтернет, але можна встановити з'єднання через проксі-сервер, то перехід за посиланням **Налаштування проксі-сервера** відкриває на екрані вікно налаштувань використання проксі-сервера:



Малюнок 32. Налаштування проксі-сервера.

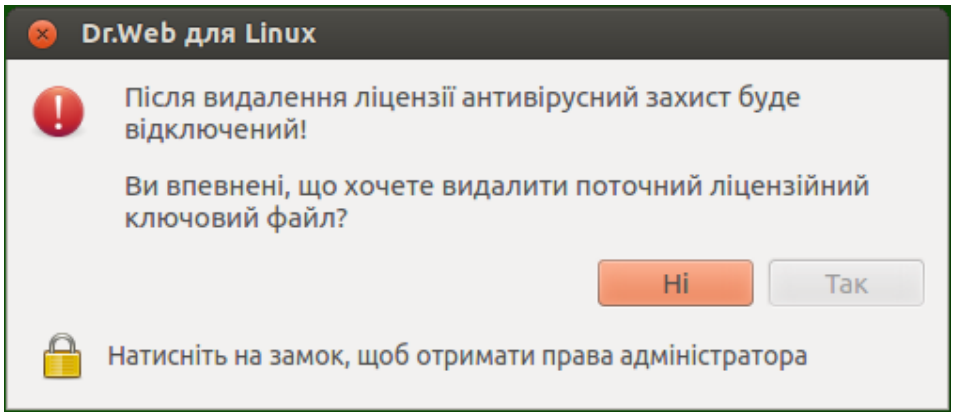
В цьому вікні вкажіть параметри доступу до проксі-сервера та натисніть **OK**. Далі повторіть спробу підключення до сервера реєстрації компанії «Доктор Веб», натиснувши **Повторити**.

При активації нової ліцензії та формуванні нового ключового файла, попередній ключовий файл, що використовувався Dr.Web для Linux, автоматично зберігається в виді файла резервної копії в каталозі `/etc/opt/drweb.com`. За необхідності ви можете повернутися до його використання, виконавши процедуру встановлення ключового файла.

Видалення ліцензійного ключового файла

За необхідності (наприклад, ви вирішили більше не використовувати Dr.Web для Linux на цьому комп'ютері, а перенести його на інший комп'ютер) можна видалити встановлений на комп'ютері ліцензійний ключовий файл, що управляє роботою Dr.Web для Linux. Для цього відкрийте сторінку інформації про ліцензії (початкова сторінка Менеджера ліцензій) та клацніть мишею по символу ✕ праворуч від номера поточної ліцензії.

Після цього вам необхідно у вікні, що з'явилося, підтвердити видалення ліцензійного ключового файла з даного комп'ютера. Для цього натисніть **Так**. Якщо ви вирішили відмовитися від видалення з даного комп'ютера ліцензійного ключового файла, натисніть **Ні**.



Малюнок 33. Вікно підтвердження видалення ліцензійного ключового файла.

Для видалення ліцензійного ключового файла у програми мають бути підвищені права. Якщо в момент спроби видалення права програми не підвищені, кнопка **Так** буде недоступна. За необхідності ви можете підвищити права програми, та за успішного підвищення кнопка **Так** стане доступною.

Видалення з комп'ютера ліцензійного ключового файла не впливає на термін дії ліцензії. Якщо термін дії ліцензії ще не минув, то ви зможете отримати новий ключовий файл для цієї ліцензії на термін, що залишився.

Після видалення ліцензійного ключового файла та до моменту активації нової ліцензії або демонстраційного періоду всі антивірусні функції Dr.Web для Linux (перевірка файлів, оновлення вірусних баз, антивірусного ядра та баз категорій веб-ресурсів, моніторинг файлової системи) будуть заблоковані.

Перегляд повідомлень від сервера централізованого захисту

В цьому розділі:

- Загальні відомості.
- Застосування дій до повідомлень.
- Фільтрація повідомлень.

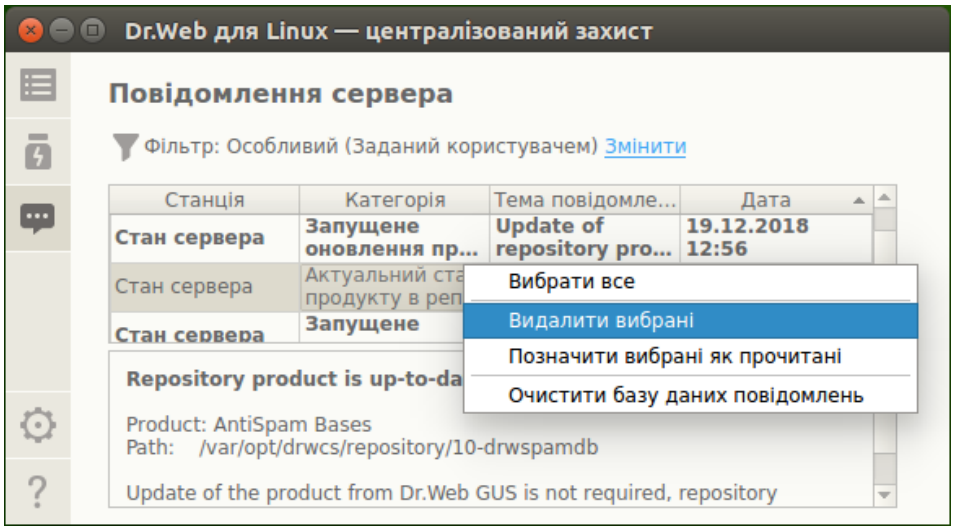
Загальні відомості

Якщо Dr.Web для Linux працює під управлінням сервера централізованого захисту, доступний інтерфейс для перегляду повідомлень про стан антивірусної мережі, які розсилаються сервером на станції під його управлінням. Даний інструмент може бути використаний адміністратором антивірусної мережі для відстеження стану мережі та важливих подій в роботі сервера централізованого захисту.

> Повідомлення про стан та події антивірусної мережі надходитимуть, тільки якщо адміністратор антивірусної мережі налаштував відправлення повідомлень на вашу станцію на тому сервері централізованого захисту, до якого підключений Dr.Web для Linux. В іншому випадку перегляд повідомлень недоступний та відповідна сторінка не відображається в головному вікні Dr.Web для Linux.

Інтерфейс перегляду повідомлень від сервера відображається на спеціальній сторінці.

Щоб відкрити її, натисніть  на навігаційній панелі.



Малюнок 34. Сторінка перегляду повідомлень від сервера централізованого захисту.

У списку для кожного повідомлення виводиться така інформація:

- Ім'я (адреса) станції, інформація про яку міститься в повідомленні.
- Категорія повідомлення.

- Заголовок (тема) повідомлення.
- Дата та час відправлення повідомлення сервером.

Для перегляду повідомлень необхідно виділити його у списку, після цього текст виділеного повідомлення буде відображений в панелі під списком повідомлень. Не переглянуті повідомлення виділяються у списку жирним шрифтом.

Текст повідомлень про стан та події антивірусної мережі формується тією мовою, яка задана в налаштуваннях сервера централізованого захисту.

Застосування дій до повідомлень

Щоб виконати будь-яку дію з повідомленням, клацніть правою кнопкою миші в рядку, що містить інформацію про повідомлення, та виберіть необхідну дію в контекстному меню, що з'явилося. Якщо необхідно провести будь-яку дію з декількома повідомленнями, перед викликом контекстного меню виділіть їх у списку, утримуючи клавішу CTRL або SHIFT:

- При утриманні клавіші CTRL повідомлення додаватимуться до списку виділення по одному.
- При утриманні клавіші SHIFT повідомлення виділятимуться неперервним списком.

Щоб виділити всі повідомлення натисніть комбінацію клавіш CTRL+A.

В меню доступні такі дії:

- Позначення у списку всіх повідомлень, що підпадають під поточний фільтр.
- Видалення виділених повідомлень.
- Позначення виділених повідомлень як прочитані.
- Очищення бази даних повідомлень.

При очищенні бази даних повідомлень будуть видалені всі повідомлення (у тому числі — непрочитані).

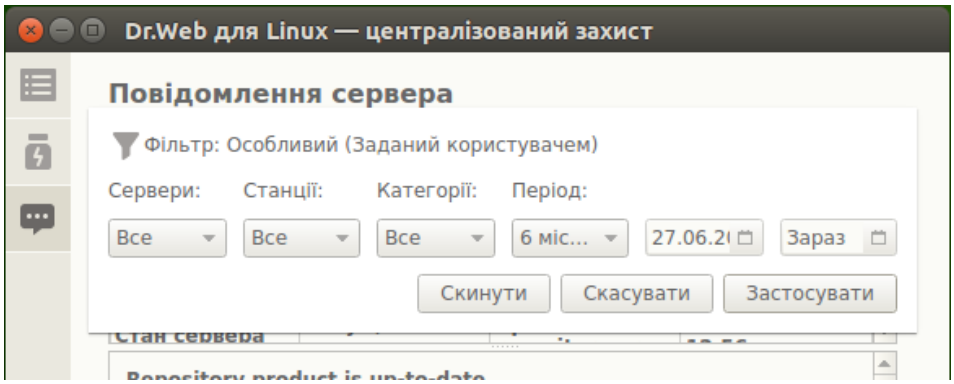
Зверніть увагу, що для повідомлень, що надійшли від сервера централізованого захисту, в налаштуваннях задається граничний термін зберігання їх в базі даних, після чого вони видаляються автоматично.

Фільтрація повідомлень

Через те, що від сервера може надходити значна кількість повідомлень, передбачена можливість їх фільтрації як за адресою сервера-відправника або за іменем станції антивірусної мережі, так і за категорією необхідних повідомлень та за періодом часу їх

надходження. За замовчуванням заданий фільтр відображає у списку повідомлення всіх категорій, що надійшли від всіх серверів протягом поточного дня.

За необхідності ви можете змінити фільтр показу повідомлень. Для цього натисніть на посилання **Змінити**. Після цього в верхній частині відкриється панель змінення фільтра.



Малюнок 35. Панель фільтра повідомлень.

В панелі фільтра ви можете задати такі параметри фільтрації повідомлень:

- **Сервери** — список серверів, повідомлення від яких показуватимуться.
- **Станції** — список станцій, повідомлення про які показуватимуться.
- **Категорії** — список категорій повідомлень, які показуватимуться.
- **Період** — період формування повідомлень, які показуватимуться (окрім вибору типового періоду зі списку, ви можете вказати конкретні моменти початку та завершення періоду формування повідомлень сервером).

Щоб застосувати змінення, внесених в фільтр, натисніть **Застосувати**. Щоб закрити панель фільтра, не зберігаючи змінень, натисніть **Скасувати**. Щоб скинути значення фільтра в значення за замовчуванням натисніть **Скинути**.

Управління правами програми

Деякі дії у вікні Dr.Web для Linux можна виконати, тільки якщо програма має підвищені права (*права адміністратора*), відповідні правам спеціального користувача системи — *суперкористувача* (користувача *root*). Зокрема, підвищені права потребують такі функції:

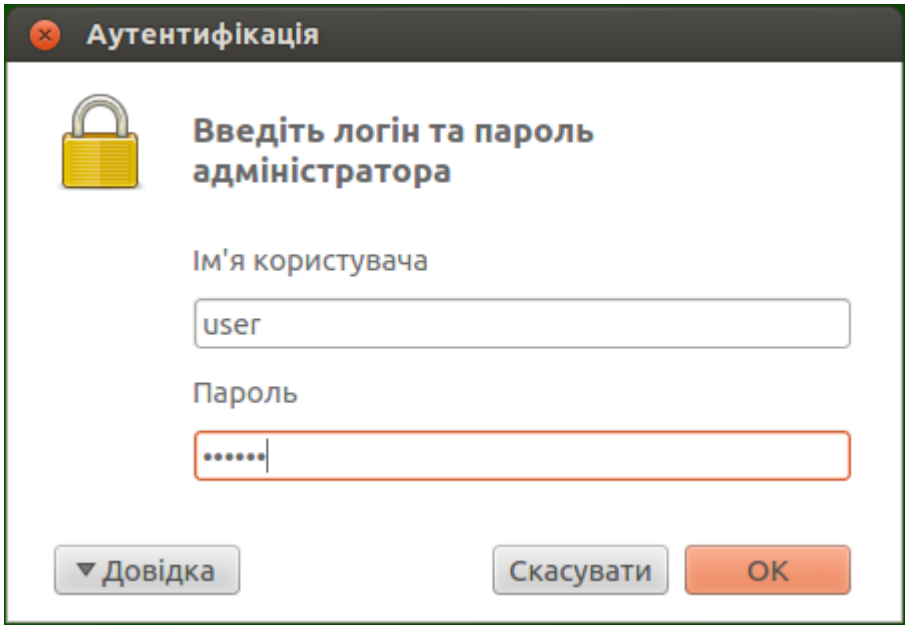
1. Управління об'єктами, поміщеними до системного карантину (тобто до каталогу карантину, що не належить користувачу, який запустив Dr.Web для Linux).
2. Перевірка файлів та каталогів, що належать іншим користувачам (зокрема — суперкористувачу).
3. Відключення монітора файлової системи SpIDer Guard.
4. Відключення монітора мережних з'єднань SpIDer Gate.
5. Видалення ліцензійного ключового файла, підключення та відключення від сервера централізованого захисту.

Навіть якщо програма була запущена від облікового запису суперкористувача (наприклад, з використанням команд **su** або **sudo**), вона за замовчуванням *не матиме* підвищені права.

На всіх сторінках вікна Dr.Web для Linux, функціональність яких залежить від наявності у програми підвищених прав, розташована спеціальна кнопка з зображенням замка. Стан замка показує, чи є в даний момент у вікна Dr.Web для Linux підвищені права:

	Програма не має підвищені права. Натиснення на замок призведе до спроби підвищення прав програми до прав суперкористувача.
	Права програми підвищені до прав суперкористувача. Натиснення на замок призведе до пониження прав програми, тобто відмови від прав суперкористувача та повернення до вихідних прав звичайного користувача.

При спробі підвищення прав, після натиснення на зображення замка з'являється вікно аутентифікації користувача.



Малюнок 36. Вікно аутентифікації.

Щоб отримати права суперкористувача, вкажіть ім'я (логін) та пароль будь-якого користувача з групи користувачів, вказаної в налаштуваннях Dr.Web для Linux як *група адміністраторів*, або логін та пароль суперкористувача (обліковий запис *root*), та натисніть **OK**. Щоб відмовитися від підвищення прав, закрийте вікно, натиснувши **Скасувати**. Щоб переглянути або приховати стислу підказку з аутентифікації, натисніть **Довідка**.

За замовчуванням при встановленні Dr.Web для Linux в якості «групи адміністраторів» в налаштуваннях автоматично фіксується ім'я системної групи користувачів, що мають можливість отримання прав суперкористувача (наприклад, група *sudo*). Якщо ім'я такої системної групи визначити не вдалося, то для підвищення прав програми у вікні аутентифікації можна використовувати логін та пароль суперкористувача (*root*).

При пониженні прав програми до прав звичайного користувача введення пароля не потребується.

Довідкові матеріали

Для доступу до довідкових матеріалів натисніть  на навігаційній панелі вікна Dr.Web для Linux.

На екрані з'явиться меню, що випадає, яке містить такі пункти:

- **Довідка** — відкрити стислий Посібник користувача Dr.Web для Linux.
- **Форум Dr.Web** — відкрити в браузері сторінку форуму користувачів продуктів компанії «Доктор Веб» (необхідне підключення до мережі Інтернет).
- **Технічна підтримка** — відкрити в браузері сторінку Служби технічної підтримки компанії «Доктор Веб» (необхідне підключення до мережі Інтернет).
- **Мій Dr.Web** — відкрити в браузері персональну сторінку користувача продуктів компанії «Доктор Веб» (необхідне підключення до мережі Інтернет).
- **Про програму** — відкрити вікно зі стислою інформацією про Dr.Web для Linux та його версії.

Окрім того, коли на будь-якій сторінці головного вікна Dr.Web для Linux відображається повідомлення про помилку, ви можете перейти за посиланням **Докладніше**, щоб отримати більш повну інформацію про помилку та вказівки щодо розв'язання проблеми, що виникла.

Налаштування роботи

Налаштування параметрів роботи програми, таких, як:

- Періодичність проведення оновлень.
- Реакції Dr.Web для Linux на виявлення загрози при перевірках на вимогу Сканером та при виявленні їх монітором файлової системи SplDer Guard.
- Список об'єктів, що виключаються Сканером та SplDer Guard з перевірки.
- Параметри контролю мережних з'єднань.
- Розклад періодичних перевірок об'єктів Сканером.
- Режим захисту (автономний, централізований).

- Використання сервісу Dr.Web Cloud.

проводиться у вікні налаштувань Dr.Web для Linux.

Для доступу до вікна налаштувань натисніть  на навігаційній панелі.

У вікні налаштувань доступні такі вкладки:

- Основні — дозволяє налаштувати використання сповіщень, а також періодичність автоматичних оновлень.
- Сканер — дозволяє налаштувати реакцію Dr.Web для Linux на загрози, що виявляються Сканером у процесі перевірки на вимогу та за розкладом.
- SpIDer Guard — дозволяє налаштувати реакцію Dr.Web для Linux на загрози, що виявляються монітором файлової системи SpIDer Guard.
- SpIDer Gate — дозволяє налаштувати параметри контролю мережних з'єднань монітором SpIDer Gate.
- Виключення — дозволяє налаштувати список об'єктів, які необхідно виключати з перевірки на вимогу та за розкладом, а також зі списку об'єктів, що перевіряються SpIDer Guard та контролюються SpIDer Gate.
- Планувальник — дозволяє налаштувати періодичний запуск перевірок за заданим розкладом.
- Мережа — дозволяє включити або відключити для SpIDer Gate режим перевірки захищених мережних з'єднань (основаних на SSL/TLS, таких як HTTPS), зберегти в файл сертифікат Dr.Web, який використовується для перехоплення захищених мережних з'єднань.
- Режим — дозволяє вибрати режим захисту (автономний, централізований), в якому працює Dr.Web для Linux.
- Dr.Web Cloud — дозволяє або забороняє Dr.Web для Linux використовувати сервіс Dr.Web Cloud.

Щоб отримати довідку, натисніть  на відповідній сторінці вікна налаштувань.

Всі змінення, що вносяться в налаштування на цих вкладках, застосовуються негайно.

Якщо Dr.Web для Linux працює в режимі централізованого захисту, то деякі налаштування можуть бути заблоковані та недоступні для змінення.

Основні налаштування

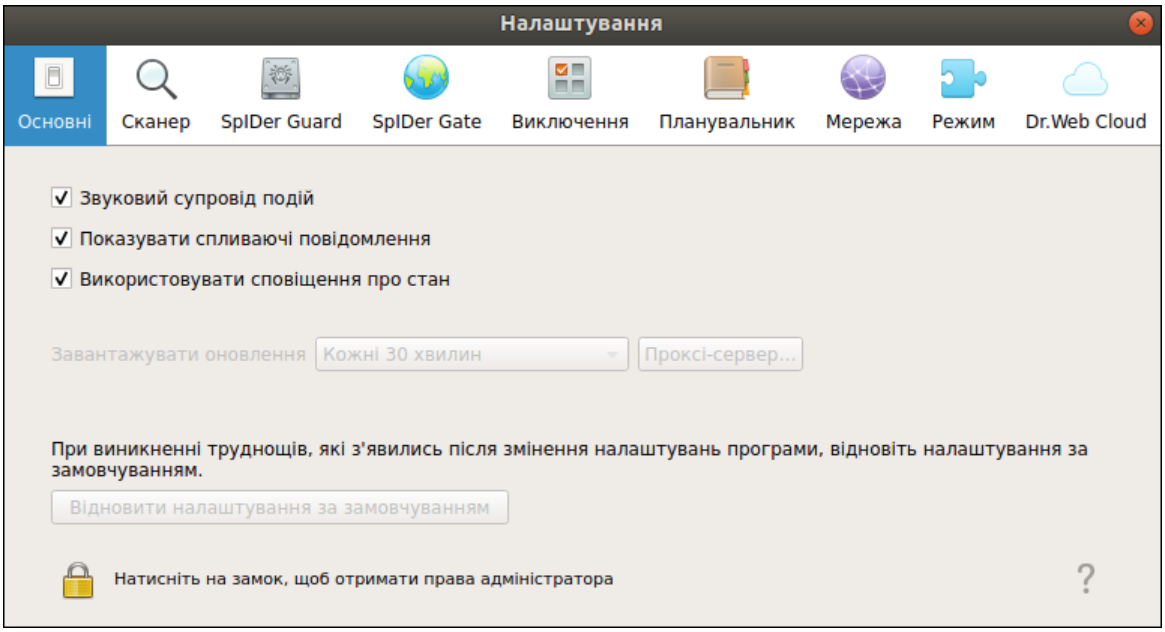
В цьому розділі:

- Загальні відомості.

- Налаштування проксі-сервера, що використовується для отримання оновлень.

Загальні відомості

На вкладці **Основні** ви можете налаштувати основні параметри роботи програми.



Малюнок 37. Вкладка основних налаштувань.

Елемент управління	Дія
Прапорець **Звуковий супровід подій**	Встановлення цього прапорця наказує Dr.Web для Linux програвати звукові сповіщення при виникненні таких подій, як: • виявлена загроза (як Сканером, так і SpIDer Guard); • помилка перевірки об'єкта; • тощо.
Прапорець **Показувати спливаючі повідомлення**	Встановлення цього прапорця наказує Dr.Web для Linux при роботі в режимі графічного робочого столу відображати на екрані спливаючі сповіщення при виникненні таких подій, як: • виявлена загроза; • помилка перевірки; • тощо.
Прапорець **Використувати сповіщення про стан**	Встановлення цього прапорця наказує Dr.Web для Linux показувати спливаючі сповіщення при зміненні стану компонентів (наприклад, при їх включенні або відключенні).
Список, що випадає **Завантажувати оновлення**	Дозволяє вибрати періодичність автоматичного оновлення вірусних баз, антивірусного ядра та баз категорій веб-ресурсів Компонентом оновлення.

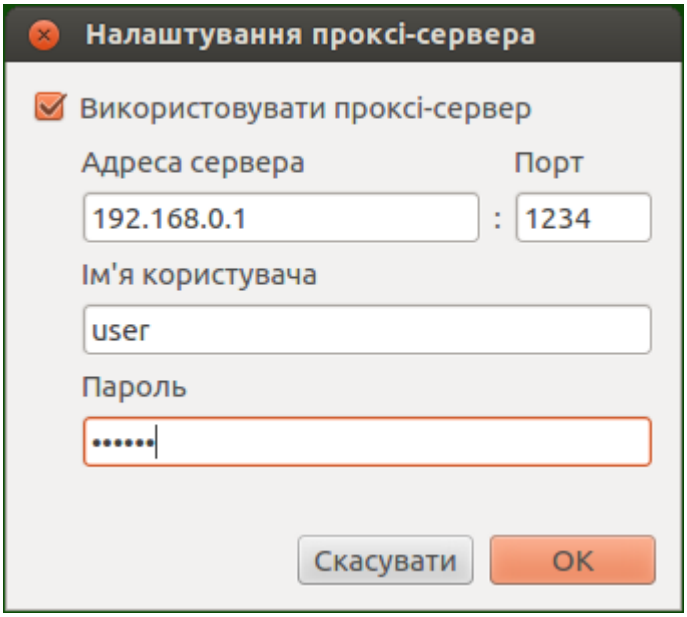
Елемент управління	Дія
Кнопка **Проксі-сервер**	Відкриває вікно налаштування використання проксі-сервера Компонентом оновлення для отримання оновлень (використання проксі-сервера може знадобитися, якщо звернення до зовнішніх сервері заборонене політиками безпеки мережі).
Кнопка **Відновити налаштування за замовчуванням**	Дозволяє скинути налаштування в значення за замовчуванням.

Для управління параметрами отримання оновлень та скидання налаштувань в значення за замовчуванням необхідно, щоб програма мала підвищені права. Див. Управління правами програми.

Налаштування проксі-сервера, що використовується для отримання оновлень

У вікні налаштування використання проксі-сервера Компонентом оновлення для отримання оновлень ви можете налаштувати такі параметри:

- Використовувати або не використовувати проксі-сервер для отримання оновлень.
- Адресу проксі-сервера, який використовуватиметься для отримання оновлень.
- Порт для підключення до проксі-сервера.
- Ім'я користувача та пароль, що використовується для аутентифікації на проксі-сервері.



Малюнок 38. Налаштування проксі-сервера.

В якості адреси можна використовувати як IP-адресу, так і FQDN вузла, на якому працює проксі-сервер. Адреса та порт необхідно вказувати обов'язково. Оскільки оновлення проводиться за протоколом HTTP, необхідно використовувати проксі-сервер HTTP. Ім'я користувача та пароль обов'язково вказувати, тільки якщо проксі-сервер HTTP потребує авторизації.

Щоб закрити вікно зі збереженням внесених змінень, натисніть **ОК**; щоб закрити вікно без збереження внесених змінень, натисніть **Скасувати**.

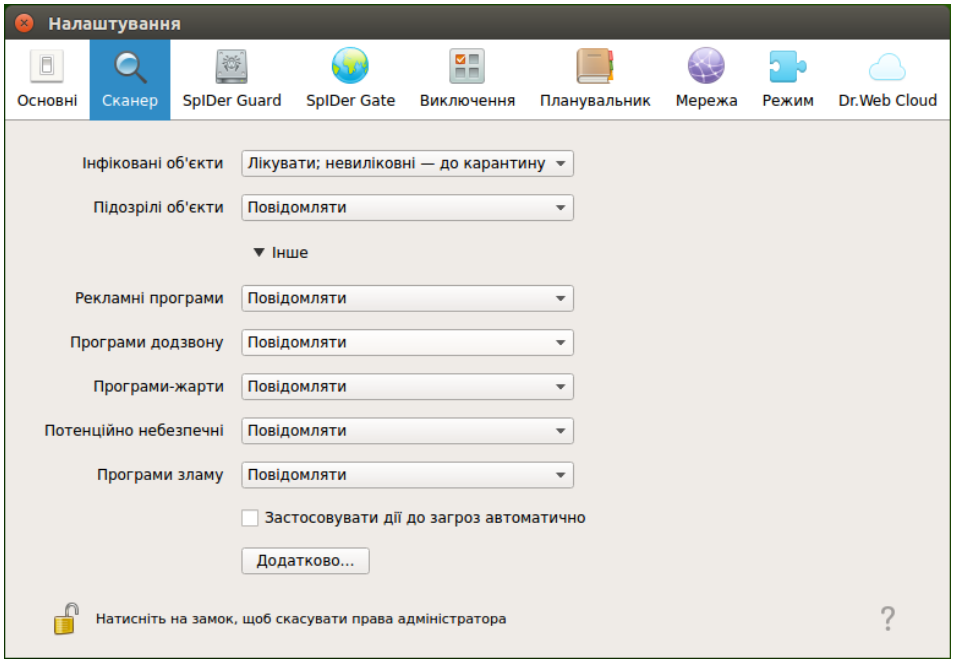
Налаштування перевірки файлів

В цьому розділі:

- Загальні відомості.
- Додаткові налаштування перевірки файлів.

Загальні відомості

На вкладці **Сканер** ви можете налаштувати дії, які Dr.Web для Linux має застосовувати до загроз при виявленні їх Сканером у процесі перевірки файлів на вимогу користувача або за розкладом.



Малюнок 39. Вкладка налаштувань перевірки файлів Сканером.

У списках, що випадають, виберіть дії, які Dr.Web для Linux застосовуватиме до об'єктів при виявленні в них будь-якої з загроз відповідного типу.

Якщо загроза виявлена в файлі, що знаходиться в контейнері (архів, поштове повідомлення тощо), замість видалення виконується переміщення контейнера до карантину.

Встановіть прапорець **Застосовувати дії до загроз автоматично**, щоб Dr.Web для Linux застосовував вказану дію до об'єкта, що містить загрозу, одразу в момент її виявлення Сканером у процесі перевірки на вимогу або за розкладом (вас буде поінформовано про нейтралізацію загрози, а інформація про неї буде доступна у списку загроз). Якщо цей прапорець скинутий, загроза, виявлена Сканером, буде тільки додана до списку виявлених загроз, й вам доведеться самостійно вибрати, яку дію застосувати до об'єкта, що містить загрозу.

Натисніть **Додаткові**, щоб відкрити вікно додаткових налаштувань перевірки файлів.

Зауваження:

- Налаштування виключення файлів та каталогів з перевірки Сканером проводиться на вкладці **Виключення**.
- Реакції на виявлення загроз, включаючи автоматичне застосування дій, задані для Сканера, не впливають на поведінку монітора SplDer Guard. Його реакції на загрози задаються на відповідній сторінці.

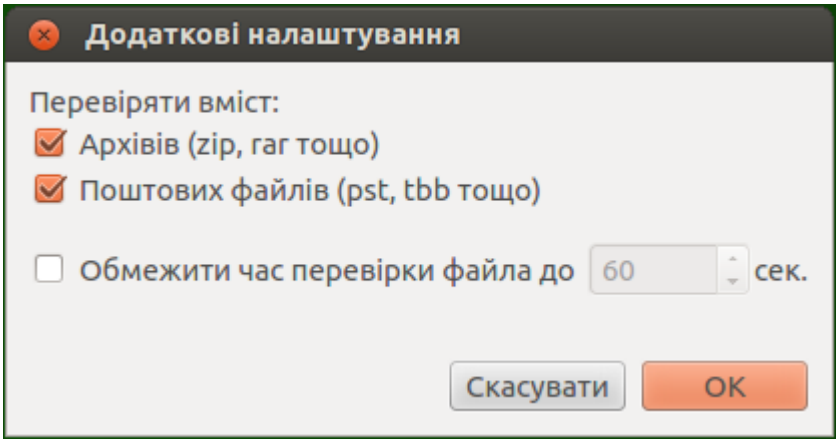
Щоб змінити реакцію Сканера на загрози та для доступу до розширених налаштувань, необхідно, щоб програма мала підвищені права. Див. Управління правами програми.

Можливість налаштування Сканера при роботі Dr.Web для Linux під управлінням сервера централізованого захисту може бути заблокована, якщо це заборонено сервером.

Додаткові налаштування перевірки файлів

У вікні додаткових налаштувань перевірки ви можете налаштувати такі параметри роботи Сканера:

- Включити або відключити перевірку вмісту контейнерів:
  - Архівів.
  - Поштових файлів.
- Задати обмеження часу перевірки одного файла.



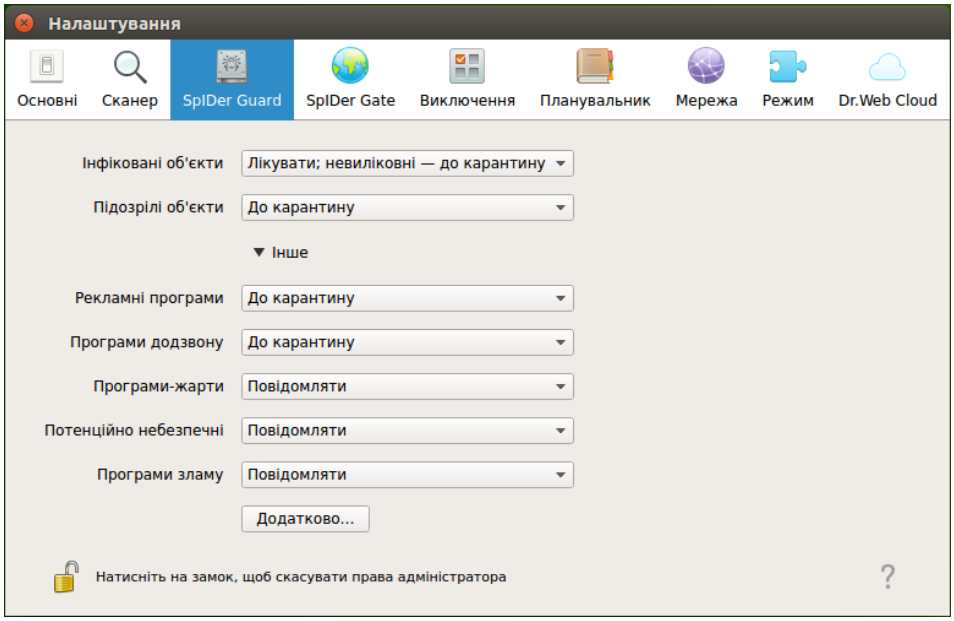
Малюнок 40. Додаткові налаштування перевірки файлів.

Якщо прапорці перевірки вмісту контейнерів не встановлені, то файли-контейнери все одно перевіряються Сканером, але без окремої перевірки вкладених в них файлів.

Щоб закрити вікно зі збереженням внесених змінень, натисніть **OK**; щоб закрити вікно без збереження внесених змінень, натисніть **Скасувати**.

Налаштування моніторингу файлової системи

На вкладці **SpIDer Guard** ви можете налаштувати дії, які Dr.Web для Linux має застосовувати до загроз при виявленні їх монітором файлової системи SpIDer Guard.



Малюнок 41. Вкладка налаштувань моніторингу файлової системи.

Ця вкладка, включаючи вікно додаткових налаштувань, аналогічна вкладці налаштування перевірки файлів (вкладка **Сканер**).

Якщо загроза виявлена в файлі, що знаходиться в контейнері (архів, поштове повідомлення тощо), замість видалення виконується переміщення контейнера до карантину.

Зауваження:

- Налаштування виключення файлів та каталогів з перевірки монітором SpIDer Guard проводиться на вкладці **Виключення**.
- Включення режиму посиленого моніторингу файлів монітором SpIDer Guard описане у розділі Режими моніторингу файлів.
- Реакції на виявлення загроз, задані для монітора SpIDer Guard, не впливають на поведінку Сканера. Його реакції на загрози задаються на відповідній сторінці.

Щоб змінити налаштування монітора файлової системи SpIDer Guard, необхідно, щоб програма мала підвищені права. Див. Управління правами програми.

Можливість налаштування SpIDer Guard при роботі Dr.Web для Linux під управлінням сервера централізованого захисту може бути заблокована, якщо це заборонено сервером.

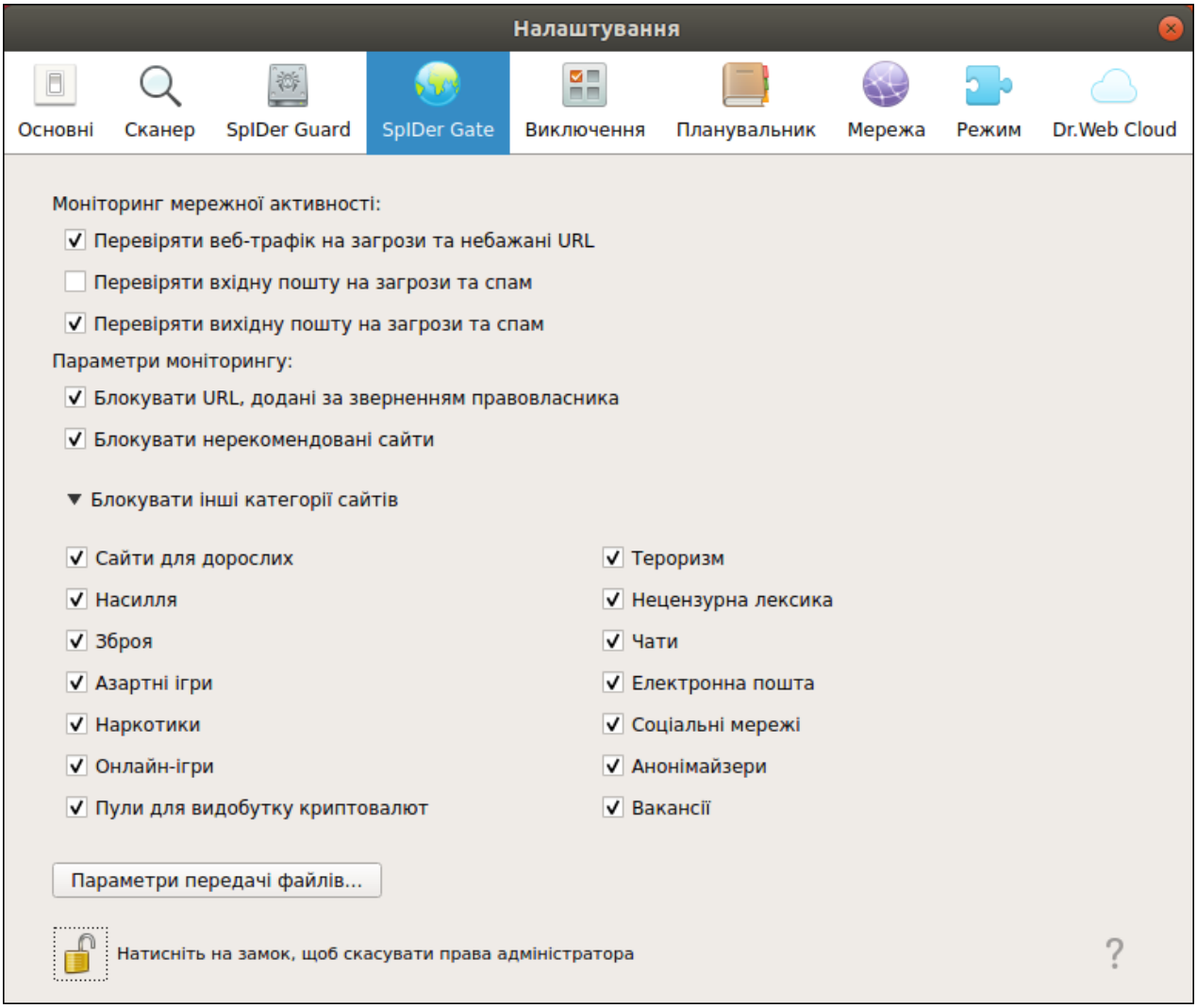
Налаштування моніторингу мережних з'єднань

В цьому розділі:

- Загальні відомості.
- Вибір категорій веб-сайтів.
- Управління параметрами перевірки файлів.

Загальні відомості

На вкладці **SpIDer Gate** ви можете налаштувати політики безпеки, які монітор мережних з'єднань SpIDer Gate використовуватиме при контролі звернень до Інтернету.



Малюнок 42. Вкладка налаштувань контролю доступу до мережі.

Встановлюючи та скидаючи перемикачі у розділі **Моніторинг мережної активності**, ви можете визначити, які типи мережної активності контролює монітор, якщо він включений.

Вибір категорій веб-сайтів

Перемикачі в розділі **Параметри моніторингу** визначають, доступ до веб-сайтів та вузлів яких категорій блокується (це стосується не тільки до спроб доступу до цих сайтів через браузер, але й до спроб звернення до FTP-серверів). Встановлюючи та скидаючи відповідні перемикачі, ви можете заборонити або дозволити доступ до веб-сайтів таких категорій:

Категорія	Опис
URL, додані за зверненням правовласника	Сайти, що містять матеріали, які порушують законодавство про авторські права (на думку правовласника розміщених на сайті матеріалів). Це різні

Категорія	Опис
	«піратські» сайти, каталоги файлових посилань, файлообмінні ресурси тощо.
Нерекомендовані сайти	Сайти, що містять сумнівний вміст, запідозрені у фішингу, викраденні паролів тощо.
Сайти для дорослих	Сайти, що містять матеріали, призначені тільки для дорослих (еротичного та порнографічного характеру)
Насилля	Сайти, що містять описи та демонстрацію сцен насилля (включаючи війни, сцени терористичних актів тощо)
Зброя	Сайти, присвячені опису та виготовленню зброї та вибухових речовин
Азартні ігри	Сайти, присвячені азартним іграм та іграм на гроші, у тому числі онлайн-казино
Наркотики	Сайти, присвячені наркотичним речовинам, у тому числі опису їх виготовлення або досвіду їх вживання
Нецензурна лексика	Сайти, що містять нецензурну лексику
Чати	Сайти чатів
Тероризм	Сайти терористичної спрямованості
Електронна пошта	Сайти безкоштовних поштових служб
Соціальні мережі	Сайти соціальних мереж
Онлайн-ігри	Сайти, на яких розміщені ігри, що використовують постійне з'єднання з мережею Інтернет.
Анонімайзери	Сайти, що дозволяють користувачу приховувати свою особисту інформацію та надають доступ до заблокованих сайтів.
Пули для видобутку криптовалют	Сайти, що надають доступ до сервісів, які об'єднують користувачів з метою видобутку («майнінгу») криптовалют.
Вакансії	Сайти для пошуку роботи

База категорій веб-ресурсів постачається у складі Dr.Web для Linux та автоматично оновлюється разом з вірусними базами. Користувач не має можливості редагувати вміст бази категорій веб-ресурсів.

Один той самий веб-сайт може бути віднесений одразу до декількох різних категорій. Монітор мережних з'єднань SplDer Gate блокуватиме доступ до веб-сайта або вузла, якщо він потрапляє хоча б до однієї з включених для заборони доступу категорій.

Натисніть на напис **Блокувати інші категорії сайтів**, щоб показати або проховати список доступних категорій.

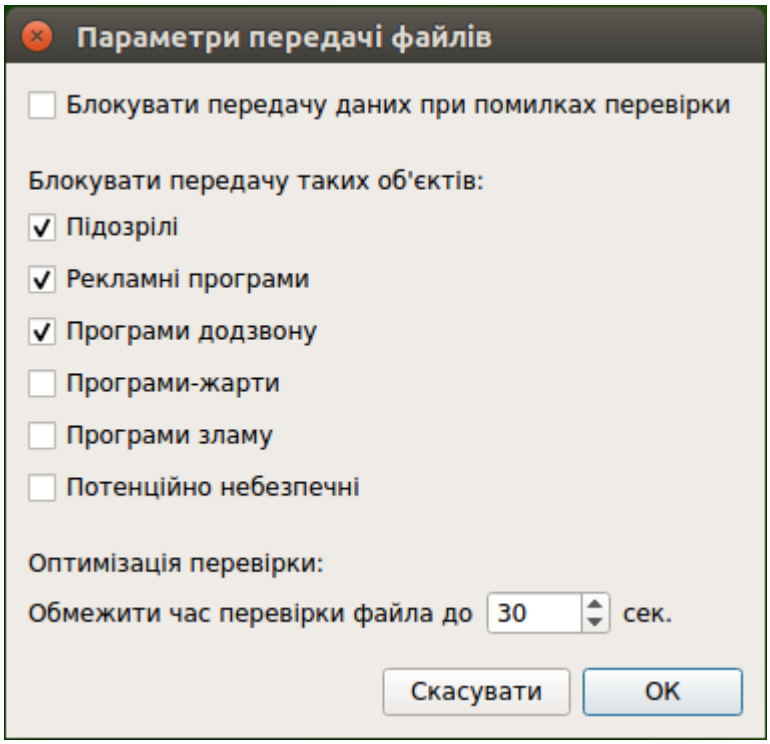
Щоб заблокувати доступ до будь-якого веб-сайта або вузла, що не відноситься до жодної з вказаних категорій, додайте його до чорного списку. Якщо навпаки, необхідно дозволити доступ до будь-якого веб-сайта або вузла, незважаючи на те, що він відноситься до будь-якої з небажаних категорій, додайте його до білого списку. Також ви можете налаштувати список програм, мережні з'єднання яких не контролюються монітором SpIDer Gate.

Налаштування чорних та білих списків веб-сайтів, а також програм, що виключаються з контролю монітором SpIDer Gate, проводиться на вкладці **Виключення**.

Існує особлива категорія веб-сайтів — *Джерела поширення вірусів*. Доступ до веб-сайтів або вузлів з цієї категорії забороняється в будь-якому випадку, навіть якщо вони додані до білого списку.

Управління параметрами перевірки файлів

Для управління параметрами, які монітор SpIDer Gate застосовуватиме при перевірці файлів, що завантажуються з Інтернету, натисніть **Параметри перевірки файлів**.



Малюнок 43. Вікно управління налаштуваннями перевірки файлів.

У вікні, що з'явилося, ви можете вказати, які категорії шкідливих об'єктів необхідно блокувати при спробі їх передачі. Якщо будь-який перемикач включений, то файли, що містять загрозу цього типу, відхилятимуться при спробі завантаження їх на комп'ютер.

Якщо перемикач відключений, то файли, що містять загрози цього типу, завантажуватимуться з Інтернету. Також ви можете також встановити максимальний інтервал часу, що відводиться на перевірку завантажуваних файлів. Якщо включений перемикач **Блокувати передачу даних при помилках перевірки**, то файли, які не вдалося перевірити через виникнення помилки, блокуватимуться при завантаженні. Щоб дозволити завантаження неперевірених файлів, перемикач можна відключити (не рекомендується).

Якщо завантажуваний файл не вдалося перевірити через те, що вичерпався час, відведений на його перевірку, то такий файл *не вважатиметься* неперевіреним та не блокуватиметься, навіть якщо прапорець **Блокувати передачу даних при помилках перевірки** встановлений.

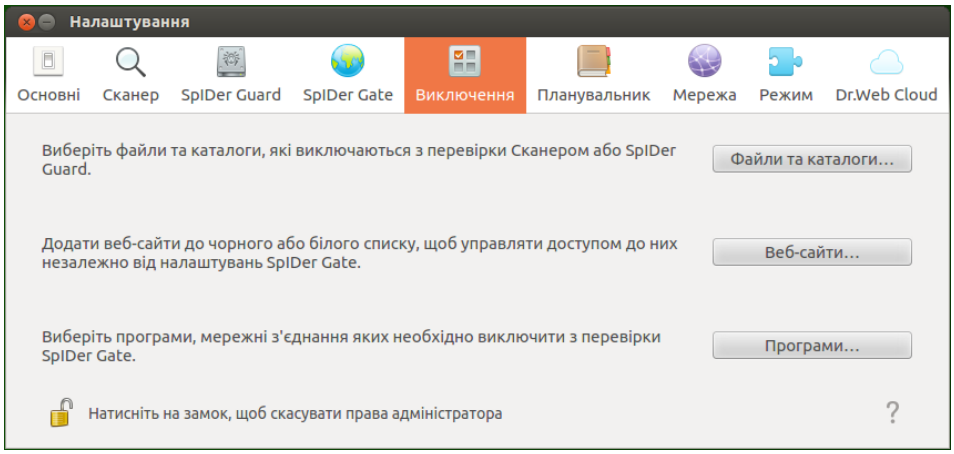
Щоб закрити вікно зі збереженням внесених змінень, натисніть **ОК**; щоб закрити вікно без збереження внесених змінень, натисніть **Скасувати**.

Щоб змінити налаштування монітора мережних з'єднань SpIDer Gate, необхідно, щоб програма мала підвищені права. Див. Управління правами програми.

Налаштування виключень

На вкладці **Виключення** доступні кнопки, що дозволяють налаштувати такі виключення:

- **Файли та каталоги** — відкриває вікно зі списком шляхів до об'єктів файлової системи, що виключаються з перевірки Сканером та монітором файлової системи SpIDer Guard.
- **Веб-сайти** — відкриває вікно управління чорними та білими списками веб-сайтів, доступ до яких регулюватиметься незалежно від політик блокування, заданих для монітора мережних з'єднань SpIDer Gate.
- **Програми** — відкриває вікно зі списком програм, мережні з'єднання яких не контролюватимуться монітором мережних з'єднань SpIDer Gate.



Малюнок 44. Вкладка налаштування виключень.

Щоб додавати та видаляти об'єкти зі списку виключень, необхідно, щоб програма мала підвищені права. Див. Управління правами програми.

Виключення файлів та каталогів

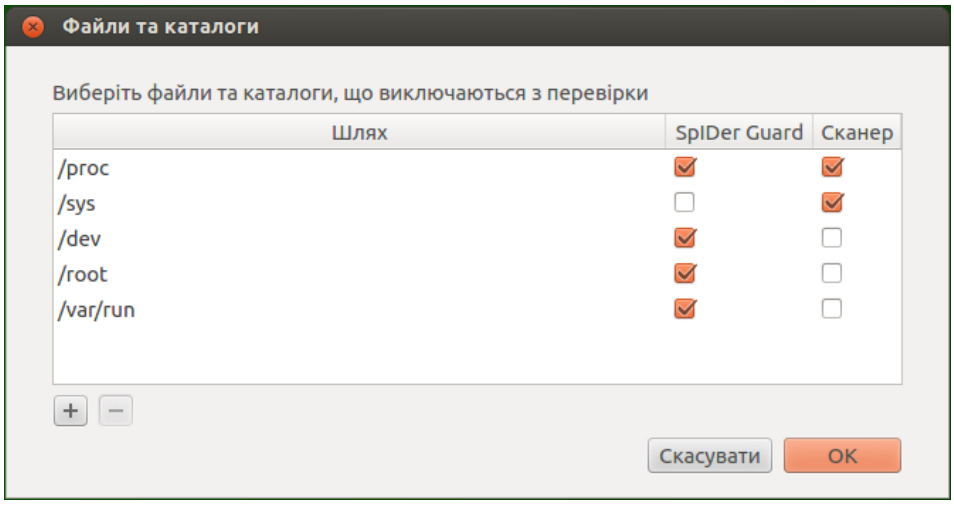
В цьому розділі:

- Загальні відомості.
- Додавання та видалення об'єктів зі списків виключень.

Загальні відомості

Управління виключенням файлів та каталогів з перевірки проводиться у вікні **Файли та каталоги**. Щоб відкрити вікно, натисніть **Файли та каталоги** на вкладці **Виключення**.

Тут ви можете вказати список шляхів до об'єктів, які необхідно виключати з перевірки Сканером на вимогу користувача та/або за розкладом, та від перевірки їх монітором файлової системи SpIDer Guard.



Малюнок 45. Налаштування виключень файлів та каталогів.

Один той самий об'єкт ви можете додати до списку виключень перевірки як Сканером (за запитом та/або за розкладом), так і монітором файлової системи SpIDer Guard. Позначка, для якого компонента об'єкт зі списку доданий до виключень, зображається прапорцем у відповідній колонці таблиці.

Додавання та видалення об'єктів зі списків виключень

- Щоб додати об'єкт до списку об'єктів, що виключаються з перевірки Сканером або для SpIDer Guard, встановіть відповідний прапорець в рядку об'єкта. Щоб видалити об'єкт зі списку об'єктів, що виключаються з перевірки Сканером або SpIDer Guard, скиньте відповідний прапорець в рядку об'єкта.

- Щоб додати до списку новий об'єкт, натисніть + під списком об'єктів, та виберіть об'єкт у вікні вибору каталогів та файлів, що з'явилося. Також ви можете додати об'єкти до цього списку, перетягнувши їх мишею з вікна файлового менеджера.
- Щоб видалити об'єкт зі списку, виділіть його рядок у списку та натисніть – під списком.

Щоб закрити вікно зі збереженням внесених змінень, натисніть **ОК**; щоб закрити вікно без збереження внесених змінень, натисніть **Скасувати**.

Виключення мережних з'єднань програм

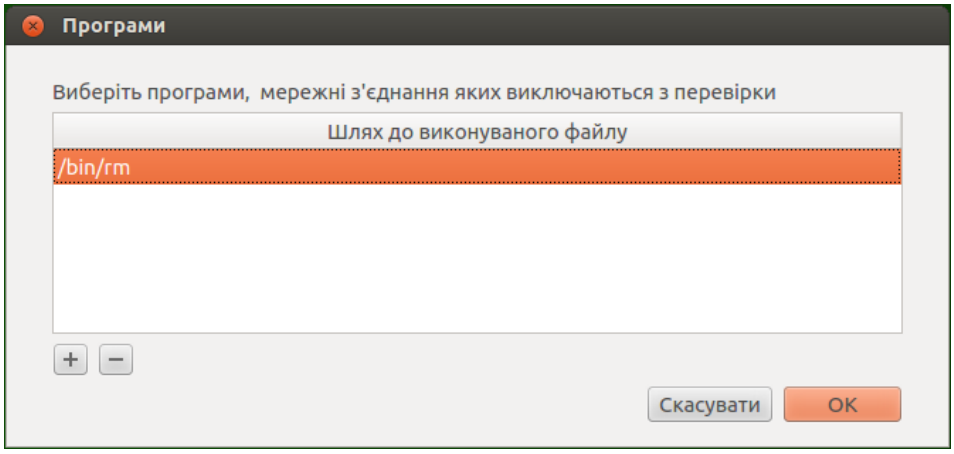
В цьому розділі:

- Загальні відомості.
- Додавання та видалення програм зі списку виключень.

Загальні відомості

Управління виключенням мережних з'єднань програм з перевірки монітором мережних з'єднань SpIDer Gate проводиться у вікні **Програми**. Щоб відкрити вікно, натисніть **Програми** на вкладці **Виключення**.

Тут ви можете вказати список шляхів до виконуваних файлів програм, мережні з'єднання яких не мають контролюватися монітором мережних з'єднань SpIDer Gate.



Малюнок 46. Налаштування виключень мережних з'єднань програм.

Додавання та видалення програм зі списку виключень

- Щоб додати до списку нову програму, натисніть + під списком програм та виберіть виконуваний файл програми у вікні вибору каталогів та файлів, що з'явилося. Окрім того, ви можете додати програму до цього списку, перетягнувши її виконуваний файл мишею з вікна файлового менеджера.
- Щоб видалити програму зі списку, виділіть її рядок у списку та натисніть – під списком.

Щоб закрити вікно зі збереженням внесених змінень, натисніть **ОК**; щоб закрити вікно без збереження внесених змінень, натисніть **Скасувати**.

Чорний та білий списки веб-сайтів

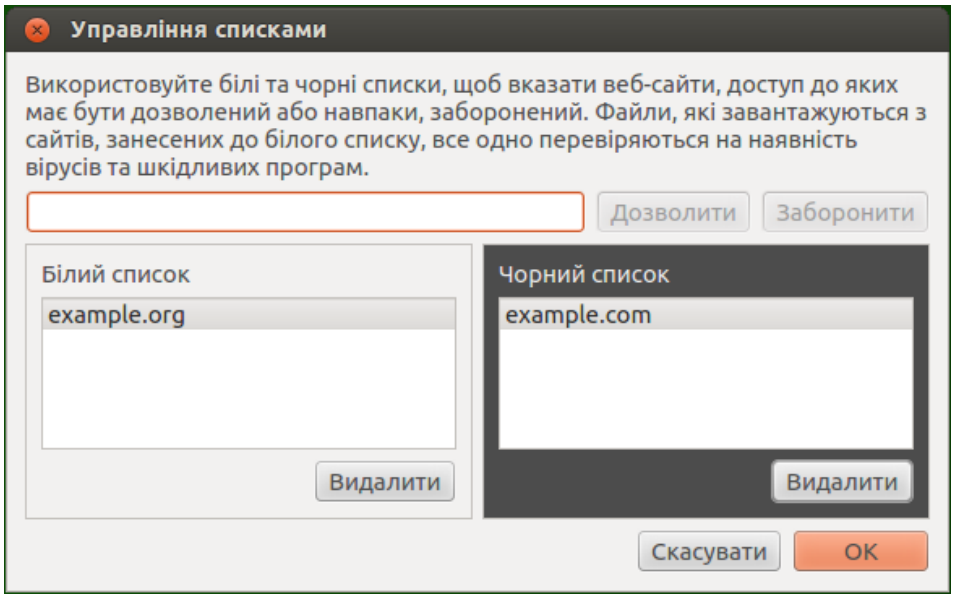
В цьому розділі:

- Загальні відомості.
- Додавання та видалення веб-сайтів з чорного та білого списку.

Загальні відомості

Управління чорними та білими списками веб-сайтів проводиться у вікні **Управління списками**. Щоб відкрити вікно, натисніть **Веб-сайти** на вкладці **Виключення**.

Тут ви можете вказати список веб-сайтів, доступ до яких буде завжди дозволений або завжди заборонений монітором мережних з'єднань SpIDer Gate.



Малюнок 47. Вікно управління чорними та білими списками.

Існує особлива категорія веб-сайтів — *Джерела поширення вірусів*. Доступ до сайтів цієї категорії забороняється в будь-якому випадку, навіть якщо вони додані до білого списку користувача.

Додавання та видалення веб-сайтів з чорного та білого списку

- Щоб додати веб-сайт до чорного або білого списку, введіть його домен у поле введення та натисніть відповідну кнопку:
  - **Дозволити**, щоб додати введену адресу до *білого* списку.
  - **Заборонити**, щоб додати введену адресу до *чорного* списку.

- Додавання будь-якої доменної адреси до чорного або білого списку забороняє або відповідно дозволяє доступ до всіх ресурсів, розташованих в цьому домені.
- Щоб видалити веб-сайт з чорного або білого списку, виділіть його у відповідному списку та натисніть **Видалити**.

Щоб закрити вікно зі збереженням внесених змінень, натисніть **ОК**; щоб закрити вікно без збереження внесених змінень, натисніть **Скасувати**.

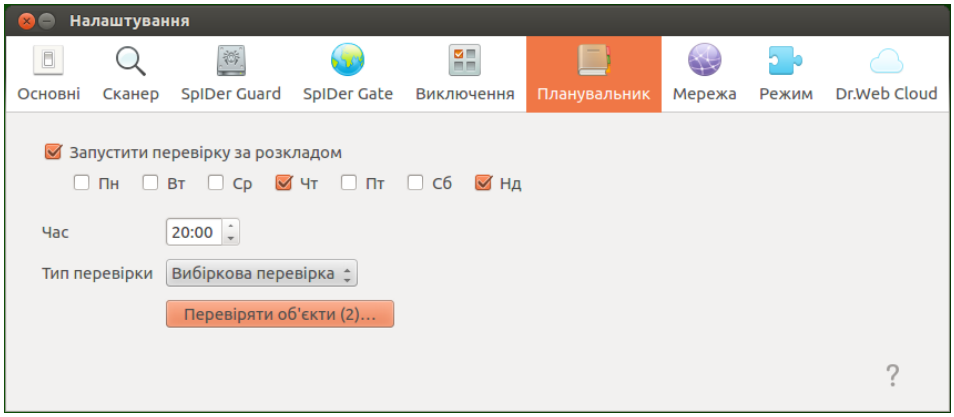
Налаштування перевірки за розкладом

В цьому розділі:

- Загальні відомості.
- Налаштування перевірки за розкладом.

Загальні відомості

На вкладці **Планувальник** ви можете включити автоматичний запуск перевірок за розкладом, задати розклад запуску та вибрати тип перевірки.



Малюнок 48. Вкладка налаштування розкладу.

Щоб включити автоматичну перевірку за розкладом, встановіть прапорець **Запустити перевірку за розкладом**. Dr.Web для Linux створить розклад періодичного запуску перевірки вибраного типу.

Перевірки за заданим розкладом запускатимуться з указаною періодичністю агентом сповіщень або безпосередньо графічним інтерфейсом управління, якщо він запущений в момент початку перевірки. Перевірки за розкладом не запускаються, якщо Dr.Web для Linux працює під управлінням сервера централізованого захисту або якщо відсутня діюча ліцензія.

Для перевірок, що запускаються за розкладом, як і для перевірок на вимогу, діють налаштування перевірки, задані на вкладці **Сканер**.

Налаштування перевірки за розкладом

Включивши перевірку за розкладом, ви можете налаштувати такі параметри:

- Вибрати дні тижня для запуску перевірки (для цього встановіть відповідні прапорці).
- Задати час (години та хвилини) початку перевірки.
- Вибрати тип перевірки (*Швидка перевірка, Повна перевірка* або *Вибіркова перевірка*).
- Якщо ви вибрали тип перевірки *Вибіркова перевірка*, то вам також необхідно задати список об'єктів для перевірки. Для цього натисніть **Перевіряти об'єкти** (в дужках вказується кількість об'єктів, вибраних для перевірки за розкладом).

  Після цього на екрані відкриється вікно вибору об'єктів для вибіркової перевірки об'єктів за розкладом, аналогічне вікну вибору об'єктів для вибіркової перевірки на вимогу. Ви можете додавати об'єкти до списку, натискаючи `+` або перетягуючи їх до списку мишею з вікна файлового менеджера.

Щоб відключити автоматичну перевірку об'єктів за розкладом, скиньте прапорець **Запустити перевірку за розкладом**. Відповідна задача для агента сповіщень буде автоматично видалена.

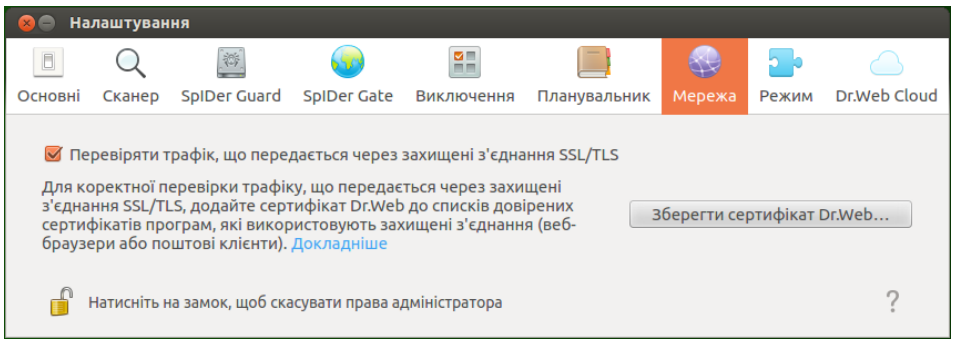
Налаштування захисту від загроз, що передаються через мережу

В цьому розділі:

- Загальні відомості.
- Налаштування перевірки захищених мережних з'єднань.
- Додавання сертифікату Dr.Web до списку довірених сертифікатів програм.

Загальні відомості

На вкладці **Мережа** ви можете включити в моніторі мережних з'єднань SpIDer Gate режим перевірки трафіку, що передається через захищені мережні з'єднання, які використовують протоколи на основі SSL та TLS.



Малюнок 49. Вкладка налаштування захисту від загроз, що передаються через мережу.

Налаштування перевірки захищених мережних з'єднань

Щоб дозволити монітору SpIDer Gate перевіряти трафік, що передається через захищені мережні з'єднання, які використовують протоколи на основі SSL та TLS, встановіть прапорець **Перевіряти трафік, що передається через захищені з'єднання SSL/TLS**. Щоб відключити перевірку захищеного трафіку, скиньте прапорець.

Для управління перевіркою захищеного трафіку необхідно, щоб програма мала підвищені права. Див. Управління правами програми.

Якщо в системі запущений поштовий клієнт (такий, як **Mozilla Thunderbird**), його необхідно перезапустити після включення режиму **Перевіряти трафік, що передається через захищені з'єднання SSL/TLS**.

Щоб забезпечити правильну роботу механізму перевірки трафіку, що передається через захищенні мережні з'єднання, експортуйте в файл спеціальний сертифікат Dr.Web. У подальшому експортований сертифікат необхідно вручну додати до списків довірених сертифікатів програм, що використовують захищенні з'єднання. В першу чергу це веб-браузери та поштові клієнти. Якщо сертифікат Dr.Web не додати до списку довірених сертифікатів веб-браузера, буде порушена коректність відображення даних, отримуваних з сайтів, доступ до яких проводиться за безпечним протоколу HTTPS (наприклад — сайтів систем онлайн-банкінгу, а також веб-інтерфейсів поштових сервісів). Якщо сертифікат Dr.Web не додати до списку довірених сертифікатів поштового клієнта, унеможливиться авторизація на поштових серверах, що використовують для передачі пошти захищені протоколи (такі, як SMTPS).

Щоб експортувати сертифікат Dr.Web в файл, натисніть **Зберегти сертифікат Dr.Web**, а далі у вікні збереження файла, що з'явилося, вкажіть місце для його збереження. За замовчуванням файл отримує ім'я `SpIDer Gate Trusted Root Certificate.pem`, яке ви можете змінити за необхідності.

Далі збережений файл сертифікату Dr.Web додайте вручну до списків довірених сертифікатів тих програм, в роботі яких будуть помічені помилки при встановленні захищених з'єднань. Додавання сертифікату до списку для будь-якої програми достатньо виконати тільки один раз. У подальшому при скиданні та повторному встановленні прапорця **Перевіряти трафік, що передається через захищені з'єднання SSL/TLS** на сторінці налаштувань **Мережа** вам не доведеться знову зберігати та встановлювати сертифікат Dr.Web до списку довірених сертифікатів.

Додавання сертифікату Dr.Web до списку довірених сертифікатів програм

Веб-браузер Mozilla Firefox

1) Виберіть пункт **Налаштування** в головному меню, потім на сторінці налаштувань, що з'явилася, виберіть пункт **Додадткові**, а на сторінці, що відкрилася, — розділ **Сертифікати**.
2) Натисніть **Перегляд сертифікатів**, у вікні, що з'явилося, виберіть вкладку **Центри сертифікації** та натисніть **Імпорт**.
3) У вікні вибору файлів, що з'явилося, вкажіть шлях до файла сертифікату Dr.Web (за замовчуванням це файл `SpIDer Gate Trusted Root Certificate.pem`) та натисніть **Відкрити**.
4) Далі у вікні, що з'явилося, за допомогою прапорців вкажіть необхідну ступінь довіри до сертифікату. Рекомендується встановить всі три прапорці (для ідентифікації веб-сайтів, для ідентифікації користувачів електронної почти, для ідентифікації програмного забезпечення). Після цього натисніть **ОК**.
5) У списку довірених сертифікатів з'явиться розділ *DrWeb,* що містить в якості сертифікату доданий сертифікат (*SpIDer Gate Trusted Root Certificate* за замовчуванням).
6) Закрийте вікно перегляду списку сертифікатів, натиснувши **ОК**, після чого закрийте сторінку налаштувань браузера (закривши відповідну вкладку на панелі вкладок браузера).

Поштовий клієнт Mozilla Thunderbird

1) Виберіть пункт **Налаштування** в головному меню, потім у вікні налаштувань, що з'явилося, виберіть розділ **Додадткові**, а на сторінці, що відкрилася, — вкладку **Сертифікати**.
2) Натисніть **Перегляд сертифікатів**, у вікні, що з'явилося, виберіть вкладку **Центри сертифікації** та натисніть **Імпорт**.
3) У вікні вибору файлів, що з'явилося, вкажіть шлях до файла сертифікату Dr.Web (за замовчуванням це файл `SpIDer Gate Trusted Root Certificate.pem`) та натисніть **Відкрити**.
4) Далі у вікні, що з'явилося, за допомогою прапорців вкажіть необхідну ступінь довіри до сертифікату. Рекомендується встановить всі три прапорці (для ідентифікації веб-сайтів, для ідентифікації користувачів електронної почти, для ідентифікації програмного забезпечення). Після цього натисніть **ОК**.
5) У списку довірених сертифікатів з'явиться розділ *DrWeb,* що містить в якості сертифікату доданий сертифікат (*SpIDer Gate Trusted Root Certificate* за замовчуванням).
6) Закрийте вікно перегляду списку сертифікатів, натиснувши **ОК**, після чого закрийте вікно налаштувань поштового клієнта, **Закрити**.
7) Перезапустіть поштовий клієнт.

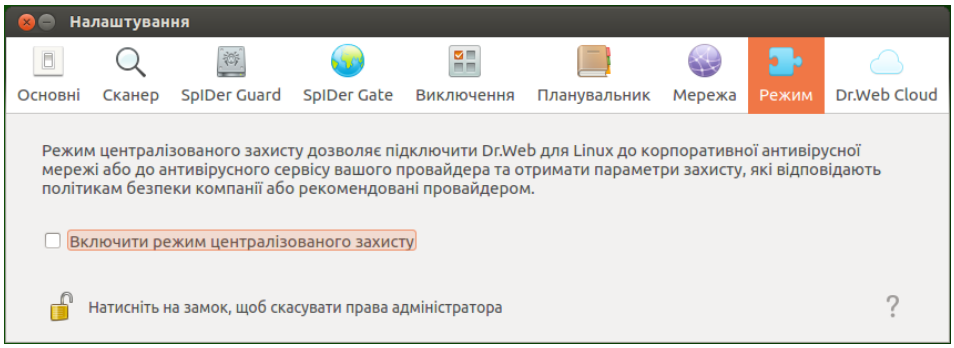
Налаштування режиму захисту

В цьому розділі:

- Загальні відомості.
- Підключення до сервера централізованого захисту.
- Додаткові налаштування.

Загальні відомості

На вкладці **Режим** ви можете підключити Dr.Web для Linux до сервера централізованого захисту (перевівши його в режим централізованого захисту) або відключитися від сервера централізованого захисту (в цьому випадку Dr.Web для Linux працюватиме в одиночному режимі).



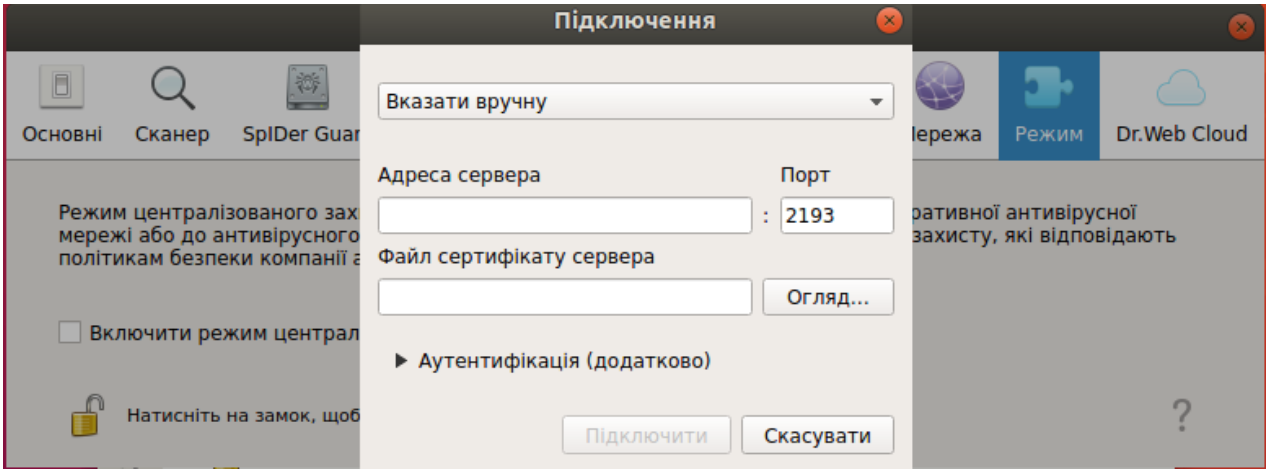
Малюнок 50. Вкладка управління режимом роботи.

Щоб підключити Dr.Web для Linux до сервера централізованого захисту або відключитися від нього, встановіть або скиньте відповідний прапорець.

Щоб підключати Dr.Web для Linux до сервера централізованого захисту або відключатися від нього, необхідно, щоб програма мала підвищені права. Див. Управління правами програми.

Підключення до сервера централізованого захисту

При спробі підключення до сервера централізованого захисту на екрані з'явиться вікно, в якому необхідно вказати параметри підключення до сервера:



Малюнок 51. Вікно підключення до сервера централізованого захисту.

У списку, що випадає, розташованому в верхній частині вікна, виберіть спосіб підключення до сервера. Доступні три способи:

- *Завантажити з файла.*
- *Вказати вручну.*
- *Визначити автоматично.*

При виборі варіанту *Завантажити з файла* достатньо вказати у відповідному полі вікна шлях до файла налаштувань підключення до сервера, який надав вам адміністратор антивірусної мережі. При виборі варіантів *Вказати вручну* та *Визначити автоматично* вкажіть адресу та порт для підключення до сервера централізованого захисту, а також шлях до файла сертифікату сервера, якщо він у вас є (зазвичай цей файл надається адміністратором антивірусної мережі або провайдером).

Додатково в розділі **Аутентифікація** ви можете вказати ідентифікатор робочої станції та пароль для аутентифікації на сервері, якщо вони вам відомі. Якщо ці поля заповнені, то підключення до сервера буде успішним, тільки якщо вказати правильну пару ідентифікатор/пароль. Якщо ці поля залишити порожніми, то підключення до сервера буде успішним тільки в разі його схвалення на сервері (автоматично або адміністратором антивірусної мережі, залежно від налаштувань сервера).

Окрім того, ви можете встановити прапорець **Підключитися як «новачок»**. Якщо опція «новачок» дозволена на сервері, то після схвалення підключення він автоматично згенерує унікальну пару ідентифікатор/пароль, яка у подальшому використовуватиметься для підключення вашого комп'ютера до цього сервера. Зверніть увагу, що при підключенні як «новачок», новий обліковий запис для вашого комп'ютера буде згенерований сервером централізованого захисту, навіть якщо раніше він вже мав обліковий запис на цьому сервері.

Параметри підключення задавайте в чіткій відповідності з інструкціями, наданими адміністратором антивірусної мережі або провайдером.

Для підключення до сервера, після зазначення всіх параметрів, натисніть **Підключити** та дочекайтеся завершення процесу підключення. Щоб закрити вікно без підключення до сервера, натисніть **Скасувати**.

Після того, як ви підключили Dr.Web для Linux до сервера централізованого захисту, він працюватиме під управлінням сервера доти, поки ви його не переведете в одиночний режим. Підключення до сервера проводитиметься автоматично кожного разу при запуску операційної системи. Докладніше див. розділ Режими роботи.

Якщо на сервері централізованого захисту включена заборона запуску перевірки файлів користувачем, то сторінка запуску сканування та кнопка **Сканер** у вікні Dr.Web для Linux будуть недоступні. Окрім того, Сканер не проводитиме перевірку файлів за заданим розкладом.

Додаткові налаштування

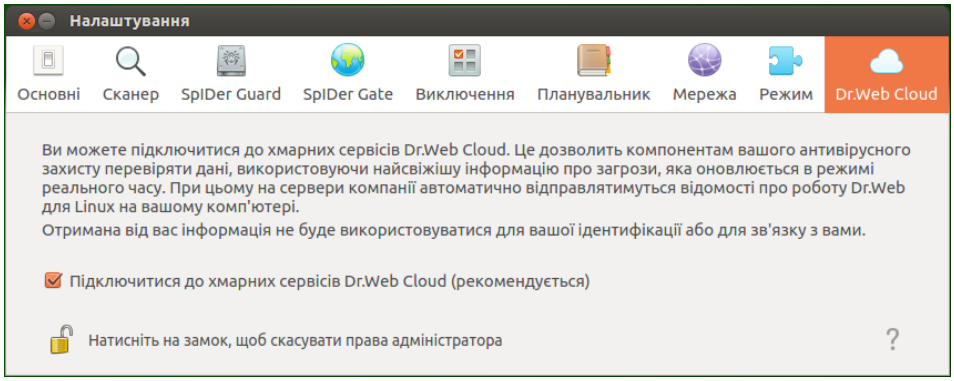
У списку, що випадає, **Максимальний час зберігання повідомлень від сервера** ви можете вказати граничний термін зберігання повідомлень про стан та події антивірусної мережі, що надходять на цю робочу станцію з сервера централізованого захисту, до якого підключений Dr.Web для Linux. Після завершення вказаного терміну повідомлення будуть видалятися автоматично, навть якщо вони не були прочитані.

Повідомлення про стан та події антивірусної мережі надходитимуть, тільки якщо адміністратор антивірусної мережі на налаштував відправлення повідомлень на вашу робочу станцію на тому сервері централізованого захисту, до якого підключений Dr.Web для Linux. В іншому випадку перегляд повідомлень недоступний та список, що випадає, **Максимальний час зберігання повідомлень від сервера** не відображається на сторінці налаштувань режиму захисту.

Налаштування використання Dr.Web Cloud

На вкладці **Dr.Web Cloud** ви можете дозволити або заборонити Dr.Web для Linux використовувати сервіс Dr.Web Cloud.

Підключення до Dr.Web Cloud дозволяє Dr.Web для Linux використовувати свіжу інформацію про загрози, яка оновлюється на серверах компанії «Доктор Веб» в режимі реального часу. Залежно від налаштувань оновлення, інформація про загрози, що використовується компонентами антивірусного захисту, може застарівати. Використання хмарних сервісів дозволяє гарантовано убезпечити користувачів вашого комп'ютера від сайтів з небажаним вмістом, а також від інфікованих файлів.



Малюнок 52. Вкладка управління використанням Dr.Web Cloud.

Щоб дозволити або заборонити Dr.Web для Linux використовувати сервіс Dr.Web Cloud, встановіть або скиньте відповідний прапорець.

Для звернення до сервісу Dr.Web Cloud необхідна наявність з'єднання з мережею Інтернет.

Щоб дозволити або заборонити Dr.Web для Linux використовувати сервіс Dr.Web Cloud, необхідно, щоб програма мала підвищені права. Див. Управління правами програми.

Додатково

Аргументи командного рядка

Для запуску графічного інтерфейсу управління Dr.Web для Linux з командного рядка операційної системи використовується така команда:

```
$ drweb-gui [<шлях>[ <шлях> …] | <параметри>]
```

де *<шлях>* — шлях, який необхідно перевірити. Може бути вказаний список шляхів, розділених пробілами.

Команда допускає також використання таких параметрів (*<параметри>*):

- `--help (-h)` — Вивести на екран стислу довідку з наявними параметрами командного рядка та завершити роботу графічного інтерфейсу управління.
- `--version (-v)` — Вивести на екран інформацію про версію графічного інтерфейсу управління.
- `--Autonomous (-a)` — Запустити графічний інтерфейс управління Dr.Web для Linux в режимі автономної копії.
- `--FullScan` — Запустити повну перевірку при старті графічного інтерфейсу управління Dr.Web для Linux.

- `--ExpressScan` — Запустити швидку перевірку при старті графічного інтерфейсу управління Dr.Web для Linux.
- `--CustomScan` — Запустити вибіркову перевірку при старті графічного інтерфейсу управління Dr.Web для Linux (відкрити сторінку вибору об'єктів, які необхідно перевірити).

Приклад:

```
$ drweb-gui /home/user/
```

Дана команда запустить графічний інтерфейс управління Dr.Web для Linux, після чого Сканер почне перевіряти файли за вказаним шляхом (відповідна задача перевірки відображатиметься у списку поточних перевірок).

Запуск автономної копії

Dr.Web для Linux підтримує роботу в особливому режимі — режимі *автономної копії*.

Якщо запустити графічний інтерфейс управління Dr.Web для Linux в режимі автономної копії, то він працюватиме з окремим комплектом сервісних компонентів (*демоном управління конфігурацією Dr.Web для Linux* (**drweb-configd**), що працює у фоновому режимі, Сканером та антивірусним ядром, яке використовується ними), запущеним спеціально для підтримки працездатності запущеного екземпляра програми.

Особливості функціонування графічного інтерфейсу управління Dr.Web для Linux в режимі автономної копії:

- Для запуску графічного інтерфейсу управління Dr.Web для Linux в режимі автономної копії необхідна наявність діючого ключового файла, робота під управлінням сервера централізованого захисту не підтримується (існує можливість встановити ключовий файл, експортований з сервера централізованого захисту). При цьому, навіть якщо Dr.Web для Linux підключений до сервера централізованого захисту, автономна копія *не повідомляє* серверу централізованого захисту про загрози, виявлені при запуску в режимі автономної копії.
- Всі допоміжні компоненти, що обслуговують роботу автономної копії графічного інтерфейсу, будуть запущені від імені поточного користувача та працюватимуть зі спеціально сформованим файлом конфігурації.
- Всі тимчасові файли та сокети UNIX, що використовуються для взаємодії компонентів між собою, створюватимуться тільки в каталозі з унікальним іменем, створеним запущеною автономною копією в каталозі тимчасових файлів (вказаному в системній перемінній оточення `TMPDIR`).
- Автономно запущена копія графічного інтерфейсу управління *не запускає* монітори SpIDer Guard та SpIDer Gate, працюють тільки функції перевірки файлів та управління карантином, які підтримуються Сканером.

- Шляхи до файлів вірусних баз, антивірусного ядра та виконуваних файлів сервісних компонентів задані за замовчуванням або беруться зі спеціальних перемінних оточення.
- Кількість одночасно працюючих автономних копій графічного інтерфейсу управління не обмежена.
- При завершенні роботи автономно запущеної копії графічного інтерфейсу також завершує роботу і комплект обслуговуючих її сервісних компонентів.

Робота з командного рядка

В цьому розділі:

- Загальні відомості.
- Віддалена перевірка вузлів.

Загальні відомості

Існує можливість управляти роботою Dr.Web для Linux з командного рядка операційної системи. Для цього до його складу входить спеціальна утиліта Dr.Web Ctl (**drweb-ctl**). З її допомогою ви можете виконувати з командного рядка такі дії:

- Запуск перевірки файлів, завантажувальних записів дисків та виконуваних файлів активних процесів.
- Запуск перевірки файлів на віддалених вузлах мережі (див. зауваження нижче).
- Запуск оновлення антивірусних компонентів (вірусних баз, антивірусного ядра та інших, залежно від поставки).
- Перегляд та змінення параметрів конфігурації Dr.Web для Linux.
- Перегляд стану компонентів Dr.Web для Linux та статистики виявлених загроз.
- Перегляд карантину та управління його вмістом.
- Підключення до сервера централізованого захисту та відключення від нього.

Щоб команди управління Dr.Web для Linux, які вводяться користувачем, мали ефект, мають бути запущені сервісні компоненти Dr.Web для Linux (за замовчуванням вони автоматично запускаються при старті операційної системи).

Зверніть увагу, що для виконання деяких управляючих команд необхідні повноваження суперкористувача.

Щоб отримати повноваження суперкористувача, скористайтеся командою зміни користувача **su** або командою виконання від імені іншого користувача **sudo**.

Утиліта **drweb-ctl** підтримує стандартне автодоповнення команд управління Dr.Web для Linux, якщо функція автодоповнення включена в використовуваній вами командній оболонці. Якщо командна оболонка не підтримує автодоповнення, ви можете

налаштувати її за необхідності. Для цього зверніться до довідкового посібника з використовуваного вами дистрибутиву операційної системи.

При завершенні роботи утиліта повертає код виходу відповідно до угоди для POSIX-сумісних систем: 0 (нуль) — якщо операція виконана успішно, та не нуль — в іншому випадку.

Зверніть увагу, що, ненульовий код виходу утиліта повертає, тільки коли сталася внутрішня помилка (наприклад, утиліта не змогла підключитися до якогось компонента, запитана операція не може бути виконана тощо). Якщо утиліта виявляє (та, можливо) нейтралізує якусь загрозу, вона повертає код виходу 0, тому що запитана операція (така, як `scan` тощо) виконана успішно. Якщо необхідно встановити перелік виявлених загроз та застосованих до них дій, то проаналізуйте повідомлення, яке утиліта виводить на консоль.

Коди всіх наявних помилок наведені в розділі Додаток Г. Опис відомих помилок.

Віддалена перевірка вузлів

Dr.Web для Linux дозволяє перевіряти на наявність загроз файлів, що знаходяться на віддалених вузлах мережі. Такими вузлами можуть бути не тільки повноцінні обчислювальні машини (робочі станції та сервери), але й роутери, ТБ-приставки та інші «розумні» пристрої, що утворюють так званий «Інтернет речей». Для проведення віддаленої перевірки необхідно, щоб віддалений вузол надав можливість віддаленого доступу через *SSH* (*Secure Shell*) або *Telnet*. Для доступу до пристрою необхідно знати його IP-адресу або доменне ім'я, ім'я та пароль користувача, який може віддалено підключитися до системи через *SSH* або *Telnet*. У вказаного користувача мають бути права доступу до перевірюваних файлів (як мінімум — право на читання).

Дана функція може бути використана тільки для виявлення шкідливих або підозрілих файлів на віддаленому вузлі. Усунення загроз (тобто ізоляція їх до карантину, видалення або лікування шкідливих об'єктів) засобами віддаленої перевірки неможливе. Щоб усунути виявлені загрози на віддаленому вузлі, скористайтеся засобами управління, які надаються безпосередньо цим вузлом. Наприклад, для роутерів та інших «розумних» пристроїв ви можете оновити прошивку, а для обчислювальних машин — підключитися до них (у тому числі — у віддаленому термінальному режимі) та виконати відповідні операції в їх файловій системі (видалення або переміщення файлів тощо) або запустити антивірусне ПЗ, встановлене на них.

Віддалена перевірка реалізується тільки через утиліту управління з командного рядка **drweb-ctl** (використовується команда `remotescan`).

Формат виклику

1. Формат виклику утиліти управління з командного рядка

Утиліта управління роботою Dr.Web для Linux має такий формат виклику:

```
$ drweb-ctl [загальні опції] | <команда> [<аргумент>] [<опції команди>]]
```

Де:

- *<загальні опції>* — опції, які можуть бути використані при запуску без зазначення команди або для будь-якої з команд. Не є обов'язковими для запуску.
- *<команда>* — команда, яка має бути виконана Dr.Web для Linux (наприклад, запустити перевірку файлів, вивести вміст карантину тощо).
- *<аргумент>* — аргумент команди. Залежить від вказаної команди. У деяких команд аргументи відсутні.
- *<опції команди>* — опції, що управляють роботою вказаної команди. Залежить від команди. У деяких команд аргументи відсутні.

2. Загальні опції

Доступні такі загальні опції:

Опція	Опис
`-h, --help`	Вивести на екран стислу загальну довідку та завершити роботу. Для виведення довідки з будь-якої команди використовуйте виклик: `$ drweb-ctl <команда> -h`
`-v, --version`	Вивести на екран версію модуля та завершити роботу
`-d, --debug`	Наказує виводити на екран розширені діагностичні повідомлення під час виконання вказаної команди. Не має сенсу без зазначення команди. Використовуйте виклик: `$ drweb-ctl <команда> -d`

3. Команди

Команди управління Dr.Web для Linux розділені на такі групи:

- Команди антивірусної перевірки.
- Команди управління оновленням та роботою в режимі централізованого захисту.

- Команди управління конфігурацією.
- Команди управління загрозами та карантином.
- Інформаційні команди.

> Щоб отримати довідку про компонент з командного рядка, скористайтеся командою **man** `1 drweb-ctl`

3.1. Команди антивірусної перевірки

Доступні такі команди антивірусної перевірки файлової системи:

Команда	Опис
`scan <шлях>`	**Призначення:** Ініціювати перевірку Сканером вказаного файла або каталогу. **Аргументи:** *<шлях>* — шлях до файла або каталогу, який необхідно перевірити (може бути відносним). *Цей аргумент може бути опущений при використанні опції* `--stdin` *або* `--stdin0`. *Для перевірки списку файлів, які вибираються за деякими умовами, рекомендується використовувати утиліту* **find** *(див.* Приклади використання*) та опції* `--stdin` *або* `--stdin0`. **Опції:** `-a [--Autonomous]` — запустити окрему копію антивірусного ядра та Сканера для проведення заданої перевірки, завершити їх роботу після завершення перевірки. Зверніть увагу, що загрози, виявлені при автономному скануванні, не будуть додані до загального списку виявлених загроз, що виводяться командою `threats` (див. нижче), також про них не буде повідомлено серверу централізованого захисту, якщо Dr.Web для Linux працює під його управлінням. `--stdin` — отримати список шляхів для перевірки зі стандартного потоку введення (*stdin*). Шляхи у списку мають бути розділені символом нового рядка ('`\n`'). `--stdin0` — отримати список шляхів для перевірки з стандартного потоку введення (*stdin*). Шляхи у списку мають бути розділені нульовим символом NUL ('`\0`'). При використанні опції `--stdin` та `--stdin0` шляхи у списку не мають містити шаблонів. Переважне використання опції `--stdin` та `--stdin0` — обробка в команді `scan` списку шляхів, що сформований зовнішньою програмою, наприклад, **find** (див. Приклади використання).

Команда	Опис
	`--Exclude` <*шлях*> — шлях, який необхідно виключити з перевірки. Може бути відносним та містити файлову маску (з символами '`?`' та '`*`', а також символьні класи '`[ ]`', '`[! ]`', '`[^ ]`'). *Необов'язкова опція; може бути вказана більш ніж один раз.* `--Report` <*тип*> — встановити тип звіту про перевірку. **Можливі значення:** • `BRIEF` — стислий звіт. • `DEBUG` — докладний звіт. • `JSON` — серіалізований звіт у форматі JSON. **Значення за замовчуванням:** *BRIEF* `--ScanTimeout` <*число*> — встановити тайм-аут на перевірку одного файла в мс. Значення *0* вказує, що час перевірки не обмежений. **Значення за замовчуванням:** *0* `--PackerMaxLevel` <*число*> — встановити максимальний рівень вкладеності об'єктів при перевірці упакованих об'єктів. Значення *0* вказує, що вкладені об'єкти будуть пропущені. **Значення за замовчуванням:** *8* `--ArchiveMaxLevel` <*число*> — встановити максимальний рівень вкладеності об'єктів при перевірці архівів (zip, rar тощо). Значення *0* вказує, що вкладені об'єкти будуть пропущені. **Значення за замовчуванням:** *8* `--MailMaxLevel` <*число*> — встановити максимальний рівень вкладеності об'єктів при перевірці поштових файлів (pst, tbb тощо). Значення *0* вказує, що вкладені об'єкти будуть пропущені. **Значення за замовчуванням:** *8* `--ContainerMaxLevel` <*число*> — встановити максимальний рівень вкладеності об'єктів при перевірці інших контейнерів (HTML тощо). Значення *0* вказує, що вкладені об'єкти будуть пропущені. **Значення за замовчуванням:** *8* `--MaxCompressionRatio` <*ступінь*> — встановити максимально допустиму ступінь стиснення перевірюваних об'єктів. Має бути не менше *2*. **Значення за замовчуванням:** *3000* `--HeuristicAnalysis` <*On*|*Off*> — чи використовувати евристичний аналіз при перевірці. **Значення за замовчуванням:** *On* `--OnKnownVirus` <*дія*> — дія, яку необхідно виконати, якщо методами сигнатурного аналізу виявлена відома загроза. **Можливі дії:** *Report, Cure, Quarantine, Delete*.

Команда	Опис
	Значення за замовчуванням: *Report* `--OnIncurable` <*дія*> — дія, яку необхідно виконати, якщо лікування (`CURE`) виявленої загрози завершилося невдало або воно неможливе. **Можливі дії:** *Report, Quarantine, Delete*. **Значення за замовчуванням:** *Report* `--OnSuspicious` <*дія*> — дія, яку необхідно виконати, якщо евристичний аналіз виявив підозрілий об'єкт. **Можливі дії:** *Report, Quarantine, Delete*. **Значення за замовчуванням:** *Report* `--OnAdware` <*дія*> — дія, яку необхідно виконати, якщо виявлена рекламна програма. **Можливі дії:** *Report, Quarantine, Delete*. **Значення за замовчуванням:** *Report* `--OnDialers` <*дія*> — дія, яку необхідно виконати, якщо виявлена програма додзвону. **Можливі дії:** *Report, Quarantine, Delete*. **Значення за замовчуванням:** *Report* `--OnJokes` <*дія*> — дія, яку необхідно виконати, якщо виявлена програма-жарт. **Можливі дії:** *Report, Quarantine, Delete*. **Значення за замовчуванням:** *Report* `--OnRiskware` <*дія*> — дія, яку необхідно виконати, якщо виявлена потенційно небезпечна програма. **Можливі дії:** *Report, Quarantine, Delete*. **Значення за замовчуванням:** *Report* `--OnHacktools` <*дія*> — дія, яку необхідно виконати, якщо виявлена програма зламу. **Можливі дії:** *Report, Quarantine, Delete*. **Значення за замовчуванням:** *Report*  Якщо загроза виявлена в файлі, що знаходиться в контейнері (архів, поштове повідомлення тощо), замість видалення (*Delete*) виконується переміщення контейнера до карантину (*Quarantine*).
`bootscan` <*пристрій*> | `ALL`	**Призначення:** Ініціювати перевірку Сканером завантажувальних записів на вказаних дискових пристроях. Перевіряються як записи MBR, так і записи VBR. **Аргументи:** <*пристрій*> — шлях до блочного файла дискового пристрою, завантажувальний запис на якому необхідно перевірити. Може бути

Команда	Опис
	вказано декілька дискових пристроїв через пробіл. Обов'язковий аргумент. Якщо замість файла пристрою вказано `ALL`, будуть перевірені всі завантажувальні записи на всіх доступних дискових пристроях. **Опції:** `-a [--Autonomous]` — запустити окрему копію антивірусного ядра та Сканера для проведення заданої перевірки, завершити їх роботу після завершення перевірки. Зверніть увагу, що загрози, виявлені при автономному скануванні, не будуть додані до загального списку виявлених загроз, що виводяться командою `threats` (див. нижче), також про них не буде повідомлено серверу централізованого захисту, якщо Dr.Web для Linux працює під його управлінням. `--Report` <*тип*> — встановити тип звіту про перевірку. **Можливі значення:** • `BRIEF` — стислий звіт. • `DEBUG` — докладний звіт. • `JSON` — серіалізований звіт у форматі JSON. **Значення за замовчуванням:** *BRIEF* `--ScanTimeout` <*число*> – встановити тайм-аут на перевірку одного файла в мс. Значення *0* вказує, що час перевірки не обмежений. **Значення за замовчуванням:** *0* `--HeuristicAnalysis` <*On*|*Off*> — чи використовувати евристичний аналіз при перевірці. **Значення за замовчуванням:** *On* `--Cure` <*Yes*|*No*> — чи необхідно робити спроби лікування виявлених загроз. Якщо вказано *No*, то проводиться тільки інформування про виявлену загрозу. **Значення за замовчуванням:** *No* `--ShellTrace` — виводити додаткову відлагоджувальну інформацію при перевірці завантажувального запису.
`procscan`	**Призначення:** Ініціювати перевірку Сканером вмісту виконуваних файлів, що містять код процесів, запущених в системі. При виявленні загрози виконується не тільки знешкодження шкідливого виконуваного файла, але й примусове завершення роботи всіх процесів, запущених з нього. **Аргументи:** Немає. **Опції:** `-a [--Autonomous]` — запустити окрему копію антивірусного ядра та Сканера для проведення заданої перевірки, завершити їх роботу після

Команда	Опис
	завершення перевірки. Зверніть увагу, що загрози, виявлені при автономному скануванні, не будуть додані до загального списку виявлених загроз, що виводяться командою `threats` (див. нижче), також про них не буде повідомлено серверу централізованого захисту, якщо Dr.Web для Linux працює під його управлінням. `--Report` <*тип*> — встановити тип звіту про перевірку. **Можливі значення:** • `BRIEF` — стислий звіт. • `DEBUG` — докладний звіт. • `JSON` — серіалізований звіт у форматі JSON. **Значення за замовчуванням:** *BRIEF* `--ScanTimeout` <*число*> – встановити тайм-аут на перевірку одного файла в мс. Значення *0* вказує, що час перевірки не обмежений. **Значення за замовчуванням:** *0* `--HeuristicAnalysis` <*On*|*Off*> — чи використовувати евристичний аналіз при перевірці. **Значення за замовчуванням:** *On* `--PackerMaxLevel` <*число*> — встановити максимальний рівень вкладеності об'єктів при перевірці упакованих об'єктів. Значення *0* вказує, що вкладені об'єкти будуть пропущені. **Значення за замовчуванням:** *8* `--OnKnownVirus` <*дія*> — дія, яку необхідно виконати, якщо методами сигнатурного аналізу виявлена відома загроза. **Можливі дії:** *Report, Cure, Quarantine, Delete*. **Значення за замовчуванням:** *Report* `--OnIncurable` <*дія*> — дія, яку необхідно виконати, якщо лікування (`CURE`) виявленої загрози завершилося невдало або воно неможливе. **Можливі дії:** *Report, Quarantine, Delete*. **Значення за замовчуванням:** *Report* `--OnSuspicious` <*дія*> — дія, яку необхідно виконати, якщо евристичний аналіз виявив підозрілий об'єкт. **Можливі дії:** *Report, Quarantine, Delete*. **Значення за замовчуванням:** *Report* `--OnAdware` <*дія*> — дія, яку необхідно виконати, якщо виявлена рекламна програма. **Можливі дії:** *Report, Quarantine, Delete*. **Значення за замовчуванням:** *Report* `--OnDialers` <дія> — дія, яку необхідно виконати, якщо виявлена програма додзвону. **Можливі дії:** *Report, Quarantine, Delete*.

Команда	Опис
	Значення за замовчуванням: *Report* `--OnJokes` <*дія*> — дія, яку необхідно виконати, якщо виявлена програма-жарт. **Можливі дії:** *Report, Quarantine, Delete.* **Значення за замовчуванням:** *Report* `--OnRiskware` <*дія*> — дія, яку необхідно виконати, якщо виявлена потенційно небезпечна програма. **Можливі дії:** *Report, Quarantine, Delete.* **Значення за замовчуванням:** *Report* `--OnHacktools` <*дія*> — дія, яку необхідно виконати, якщо виявлена програма зламу. **Можливі дії:** *Report, Quarantine, Delete.* **Значення за замовчуванням:** *Report* При виявленні загроз у виконуваному файлі всі запущені з нього процеси примусово завершуються Dr.Web для Linux.
`remotescan` <*вузол*> <*шлях*>	**Призначення:** Ініціювати перевірку вказаного файла або каталогу на вказаному віддаленому вузлі, підключившись до нього через *SSH* або *Telnet*. Зверніть увагу, що загрози, виявлені при віддаленому скануванні, не будуть нейтралізовані, а також вони не будуть додані до загального списку виявлених загроз, що виводяться командою `threats` (див. нижче). Ви можете використовувати цю команду тільки для виявлення шкідливих або підозрілих файлів на віддаленому вузлі. Для усунення виявлених загроз на віддаленому вузлі необхідно скористатися засобами управління, які надаються безпосередньо цим вузлом. Наприклад, для роутерів, ТБ-приставок та інших «розумних» пристроїв ви можете скористатися механізмом оновлення прошивки, а для обчислювальних машин — підключившись до них (у тому числі — у віддаленому термінальному режимі) та виконавши відповідні операції в їхній файловій системі (видалення або переміщення файлів тощо) або запустивши антивірусне ПЗ, встановлене на них. **Аргументи:** <*вузол*> — IP-адреса або доменне ім'я вузла, до якого необхідно підключитися для перевірки.

Команда	Опис
	<*шлях*> — шлях до файла або каталогу, який необхідно перевірити (має бути абсолютним). **Опції:** `-m [--Method]` <*SSH*|*Telnet*> — метод (протокол) підключення до віддаленого вузла. *Якщо метод не вказаний, використовуватиметься SSH.* `-l [--Login]` <*ім'я*> — логін (ім'я користувача) для авторизації на віддаленому вузлі через вибраний протокол. *Якщо ім'я користувача не вказане, буде проведена спроба підключитися до віддаленого вузла від імені користувача, що запустив команду.* `-i [--Identity]` <*шлях до файла*> — файл закритого ключа для аутентифікації вказаного користувача через вибраний протокол. `-p [--Port]` <*число*> — номер порту на віддаленому вузлі для підключення через вибраний протокол. **Значення за замовчуванням:** *порт за замовчуванням для вибраного протоколу (22 — для SSH, 23 — для Telnet).* `--ForceInteractive` — Використовувати інтерактивну сесію SSH (тільки для методу підключення *SSH*). *Необов'язкова опція.* `--TransferListenAddress` <*адреса*> — Адреса, що прослуховується для прийому файлів, які передаються на перевірку віддаленим пристроєм. *Необов'язкова опція. Якщо не вказана, використовується довільна адреса.* `--TransferListenPort` <*порт*> — Порт, що прослуховується для прийому файлів, які передаються на перевірку віддаленим пристроєм. *Необов'язкова опція. Якщо не вказана, використовується довільний порт.* `--TransferExternalAddress` <*адреса*> — Адреса для передачі файлів на перевірку, яка повідомляється віддаленому пристрою. *Необов'язкова опція. Якщо не вказана, використовується значення опції* `--TransferListenAddress`*, або вихідна адреса вже встановленої сесії.* `--TransferExternalPort` <*порт*> — Порт для передачі файлів на перевірку, який повідомляється віддаленому пристрою. *Необов'язкова опція. Якщо не вказана, використовується порт, визначений автоматично.* `--Password` <*пароль*> — пароль для аутентифікації вказаного користувача через вибраний протокол. *Зверніть увагу, що пароль передається у відкритому виді.* `--Exclude` <*шлях*> — шлях, який необхідно виключити з перевірки. Може містити файлову маску (з символами '`?`' та '`*`', а також символьні

Команда	Опис
	класи '[ ]', '[!]', '[^]'). Шлях (у тому числі той, що містить маску) має бути абсолютним. *Необов'язкова опція; може бути вказана більш ніж один раз.* `--Report` <*тип*> — встановити тип звіту про перевірку. **Можливі значення:** • `BRIEF` — стислий звіт. • `DEBUG` — докладний звіт. • `JSON` — серіалізований звіт у форматі JSON. **Значення за замовчуванням:** *BRIEF* `--ScanTimeout` <*число*> – встановити тайм-аут на перевірку одного файла в мс. Значення *0* вказує, що час перевірки не обмежений. **Значення за замовчуванням:** *0* `--PackerMaxLevel` <*число*> — встановити максимальний рівень вкладеності об'єктів при перевірці упакованих об'єктів. Значення *0* вказує, що вкладені об'єкти будуть пропущені. **Значення за замовчуванням:** *8* `--ArchiveMaxLevel` <*число*> — встановити максимальний рівень вкладеності об'єктів при перевірці архівів (zip, rar тощо). Значення *0* вказує, що вкладені об'єкти будуть пропущені. **Значення за замовчуванням:** *8* `--MailMaxLevel` <*число*> — встановити максимальний рівень вкладеності об'єктів при перевірці поштових файлів (pst, tbb тощо). Значення *0* вказує, що вкладені об'єкти будуть пропущені. **Значення за замовчуванням:** *8* `--ContainerMaxLevel` <*число*> — встановити максимальний рівень вкладеності об'єктів при перевірці інших контейнерів (HTML тощо). Значення *0* вказує, що вкладені об'єкти будуть пропущені. **Значення за замовчуванням:** *8* `--MaxCompressionRatio` <*ступінь*> — встановити максимально допустиму ступінь стиснення перевірюваних об'єктів. Має бути не менше *2*. **Значення за замовчуванням:** *3000* `--HeuristicAnalysis` <*On*|*Off*> — чи використовувати евристичний аналіз при перевірці. **Значення за замовчуванням:** `On`
`checkmail` <*шлях до файла*>	**Призначення:** Провести компонентом перевірки листів перевірку збереженого в файл поштового повідомлення на наявність загроз, ознак спаму або невідповідності правилам обробки листів. В потік виведення консолі (*stdout*) будуть повернені результати перевірки листа,

Команда	Опис

	а також - яка дія була б застосована до даного листа при його перевірці компонентом перевірки листів.
	
	Аргументи:
	
	<*шлях до файла*> — шлях до файла повідомлення електронної пошти, яке необхідно перевірити. Обов'язковий аргумент.
	
	Опції:
	
	`--Report` <*тип*> — встановити тип звіту про перевірку.
	
	Можливі значення:
	
	• *BRIEF* — стислий звіт.
	• *DEBUG* — докладний звіт.
	• *JSON* — серіалізований звіт у форматі JSON.
	
	Значення за замовчуванням: *BRIEF*
	
	`-r [--Rules]` <*список правил*> — вказати набір правил, які необхідно застосувати до листа при його перевірці.
	
	Якщо правила не вказані, використовуватиметься набір правил за замовчуванням, а саме:
	
	`threat_category in (KnownVirus, VirusModification, UnknownVirus, Adware, Dialer) : REJECT`
	`total_spam_score gt 0.80 : REJECT`
	`url_category in (InfectionSource, NotRecommended, CopyrightNotice) : REJECT`
	
	При цьому, якщо компонент Dr.Web Anti-Spam не встановлений, то правило перевірки на спам (другий рядок) буде автоматично виключений з набору.
	
	`-c [--Connect]` <*IP*>:<*port*> — вказати мережний сокет, що використовуватиметься як адреса, з якої підключився відправник повідомлення, яке перевіряється.
	
	`-e [--Helo]` <*ім'я*> — вказати ідентифікатор клієнта, який відправив повідомлення (IP-адреса або FQDN вузла, як для SMTP-команди HELO/EHLO).
	
	`-f [--From]` <*email*> — вказати адресу електронної пошти відправника (як для SMTP-команди MAIL FROM).
	
	Якщо адреса не вказана, використовуватиметься відповідна адреса з листа.
	
	`-t [--Rcpt]` <*email*> — вказати адресу електронної пошти отримувача (як для SMTP-команди RCPT TO).
	
	Якщо адреса не вказана, використовуватиметься відповідна адреса з листа.

Команда	Опис
	Якщо компонент перевірки листів не встановлений, виклик даної команди поверне помилку.

Окрім команд, наведених в таблиці вище, утиліта **drweb-ctl** підтримує додаткові команди перевірки. З їхнім описом ви можете ознайомитися, звернувшись до документації **man** `1 drweb-ctl`.

3.2. Команди управління оновленням та роботою в режимі централізованого захисту

Доступні такі команди управління оновленням та роботою в режимі централізованого захисту:

Команда	Опис
`update`	**Призначення:** Ініціювати процес оновлення антивірусних компонентів (вірусних баз, антивірусного ядра та інших залежно від поставки) з серверів оновлень компанії «Доктор Веб» або з локальної хмари, перервати вже запущений процес оновлення або відкатити результати останнього оновлення, відновивши попередні версії оновлених файлів. Команда не має ефекту, якщо Dr.Web для Linux працює під управлінням сервера централізованого захисту. **Аргументи:** Немає. **Опції:** `-l [--local-cloud]` — використовувати для завантаження оновлень локальну хмару, до якої підключений Dr.Web для Linux. Якщо опція не вказана, оновлення завантажуються з серверів оновлень компанії «Доктор Веб» (поведінка за замовчуванням). `--Rollback` — відкатити останнє оновлення та відновити останні збережені копії оновлених файлів. `--Stop` — перервати вже запущений процес оновлення.
`esconnect` *<сервер>*`[:`*<порт>*`]`	**Призначення:** Підключити Dr.Web для Linux до вказаного сервера централізованого захисту (наприклад, Dr.Web Enterprise Server). Про

Команда	Опис
	режими роботи див. у розділі Режими роботи. **Аргументи:** • *<сервер>* — IP-адреса або ім'я вузла в мережі, на якому розташовується сервер централізованого захисту. Обов'язковий аргумент. • *<порт>* — номер порту, що використовується сервером централізованого захисту. Необов'язковий аргумент, вказується, якщо сервер централізованого захисту використовує нестандартний порт. **Опції:** `--Certificate` *<шлях>* — шлях до файла сертифікату сервера централізованого захисту, до якого проводиться підключення. `--Login` *<ID>* — логін (ідентифікатор робочої станції) для підключення до сервера централізованого захисту. `--Password` *<пароль>* — пароль для підключення до сервера централізованого захисту. `--Group` *<ID>* — ідентифікатор групи на сервері, до якої необхідно помістити робочу станцію після підключення. `--Rate` *<ID>* — ідентифікатор тарифної групи, яку необхідно застосувати до робочої станції при її включенні до групи на сервері централізованого захисту (може бути вказана тільки сумісно з опцією `--Group`). `--Compress` *<On|Off>* — примусово ініціювати стиснення даних, що передаються (*On*) або заборонити стиснення (*Off*). Якщо опція не вказана, використання стиснення визначається сервером. `--Encrypt` *<On|Off>* — примусово ініціювати шифрування даних, що передаються (*On*) або заборонити шифрування (*Off*). Якщо опція не вказана, використання шифрування визначається сервером. `--Newbie` — підключиться як «новачок» (отримати новий обліковий запис на сервері). Для виконання цієї команди необхідно, щоб **drweb-ctl** була запущена від імені суперкористувача (користувача *root*). За необхідності скористайтеся командами **su** або **sudo**.
`esdisconnect`	**Призначення:** Відключити Dr.Web для Linux від сервера централізованого захисту та перевести його в одиночний режим роботи.

Команда	Опис
	Команда не має ефекту, якщо Dr.Web для Linux вже працює в одиночному режимі (standalone mode). **Аргументи:** Немає. **Опції:** Немає. Для виконання цієї команди необхідно, щоб **drweb-ctl** була запущена від імені суперкористувача (користувача *root*). За необхідності скористайтеся командами **su** або **sudo**.

3.3. Команди управління конфігурацією

Доступні такі команди управління конфігурацією:

Команда	Опис
`cfset` *<секція>*`.`*<параметр>* *<значення>*	**Призначення:** Змінити активне значення вказаного параметра поточної конфігурації Dr.Web для Linux. **Аргументи:** • *<секція>* — ім'я секції конфігураційного файла, в якій знаходиться змінюваний параметр. Обов'язковий аргумент. • *<параметр>* — ім'я змінюваного параметра. Обов'язковий аргумент. • *<значення>* — нове значення параметра. Обов'язковий аргумент.

Команда	Опис
	 Для завдання значення параметрів завжди використовується формат <*секція*>.<*параметр*> <*значення*>, знак '=' не використовується. Якщо ви хочете задати декілька значень параметра, то необхідно повторити виклик команди `cfset` стільки разів, скільки значень параметра ви хочете додати. Щоб додати нове значення до списку значень параметра, необхідно використовувати опцію `-a` (див. нижче). Не можна вказувати як аргумент послідовність <*параметр*> <*значення 1*>, <*значення 2*>, тому що рядок <*значення 1*>, <*значення 2*> вважатиметься єдиним значенням параметра <*параметр*>. Опис конфігураційного файла доступний в документації **man** `5 drweb.ini`. **Опції:** `-a [--Add]` — не замінювати поточне значення параметра, а додати вказане значення до списку значень параметра (допустимо тільки для параметрів, які можуть мати список значень). Також цю опцію необхідно використовувати, щоб додавати нові груп параметрів з тегом. `-e [--Erase]` — не замінювати поточне значення параметра, а видалити вказане значення з його списку (допустимо тільки для параметрів, які можуть мати список значень). `-r [--Reset]` — скинути параметр в значення за замовчуванням. <*значення*> в цьому випадку в команді не вказується, а якщо вказане – ігнорується. Опції не є обов'язковими. Якщо вони не вказані, то поточне значення параметра (у тому числі — список значень) замінюється на вказане значення.  Для виконання цієї команди необхідно, щоб **drweb-ctl** була запущена від імені суперкористувача. За необхідності скористайтеся командами **su** або **sudo**.
`cfshow [<`*секція*`>[.<`*параметр*`>]]`	**Призначення:** Вивести на екран параметри поточної конфігурації Dr.Web для Linux. Для виведення параметрів за замовчуванням використвується формат <*секція*>.<*параметр*> = <*значення*>. Секції та параметри не встановлених компонентів за замовчуванням не виводяться.

Команда	Опис
	Аргументи: • *<секція>* — ім'я секції конфігураційного файла, параметри якої необхідно вивести на екран. Необов'язковий аргумент. Якщо не вказаний, то на екран виводяться параметри всіх секцій конфігураційного файла. • *<параметр>* — ім'я параметра, що виводиться. Необов'язковий аргумент. Якщо не вказаний, виводяться всі параметри вказаної секції, в іншому випадку виводиться тільки цей параметр. Якщо вказаний без імені секції, то виводяться всі входження цього параметра в усі секції конфігураційного файла. **Опції:** `--Uncut` — вивести на екран всі параметри конфігурації, а не тільки ті, які використовуються поточним встановленим набором компонентів. В іншому випадку виводяться тільки ті параметри, які використовуються встановленими компонентами. `--Changed` — вивести тільки ті параметри, значення яких відрізняються від значень за замовчуванням. `--Ini` — вивести значення параметрів у форматі INI-файла: спочатку в окремому рядку виводиться ім'я секції, укладене в квадратні дужки, після чого параметри, що містяться в секції, виводяться в виді пар *<параметр>* = *<значення>* (по одній в рядку). `--Value` — вивести тільки значення вказаного параметра. В цьому випадку аргумент *<параметр>* обов'язковий.
`reload`	**Призначення:** Перезапустити сервісні компоненти Dr.Web для Linux. При цьому заново відкриваються журнали, перечитується файл конфігурації та проводиться спроба перезапустити аварійно завершені компоненти. **Аргументи:** Немає. **Опції:** Немає.

3.4. Команди управління загрозами та карантином

Доступні такі команди управління загрозами та карантином:

Команда	Опис
`threats [`*`<дія>`* *`<об'єкт>`*`]`	**Призначення:** Застосувати вказану дію до виявлених раніше загроз за їхніми ідентифікаторам. Тип дії визначається вказаною опцією команди. Якщо дія не вказана, то вивести на екран інформацію про виявлені, але не знешкоджені загрози. Інформація про загрози виводиться відповідно до формату, заданого необов'язковою опцією `--Format`. Якщо опція `--Format` не вказана, то для кожної загрози виводиться така інформація:

Команда	Опис
	• Ідентифікатор, присвоєний загрозі (порядковий номер). • Повний шлях до інфікованого файла. • Інформація про загрозу (ім'я, тип за класифікацією компанії «Доктор Веб»). • Інформація про файл: розмір, користувач-власник, дата останнього змінення. • Історія дій з інфікованим файлом: виявлення, застосована дія тощо. **Аргументи:** Немає. **Опції:** `--Format "`*<рядок формату>*`"` — виводити інформацію про загрози у вказаному форматі. Опис рядка формату наведений нижче. *Якщо ця опція вказана разом з будь-якою з опцій-дій, вона ігнорується.* `-f [--Follow]` — очікувати надходження нових повідомлень про загрози та виводити їх одразу, щойно вони надходитимуть (CTRL+C перериває очікування). *Якщо ця опція вказана разом з будь-якою з опцій-дій, вона ігнорується.* `--Directory` *<список каталогів>* — виводити тільки ті загрози, які були виявлені в файлах в каталогах зі *<списку каталогів>*. *Якщо ця опція вказана разом з будь-якою з опцій, вказаних нижче, вона ігнорується.* `--Cure` *<список загроз>* — виконати спробу лікування вказаних загроз (ідентифікатори загроз наводяться через кому). `--Quarantine` *<список загроз>* — виконати переміщення до карантину вказаних загроз (ідентифікатори загроз наводяться через кому). `--Delete` *<список загроз>* — виконати видалення вказаних загроз (ідентифікатори загроз наводяться через кому). `--Ignore` *<список загроз>* — ігнорувати вказані загрози (ідентифікатори загроз наводяться через кому). Якщо необхідно застосувати дію до всіх виявлених загроз, замість *<список загроз>* необхідно вказати `All`. Наприклад, команда: `$ drweb-ctl threats --Quarantine All` переміщує до карантину всі виявлені об'єкти з загрозами.
`quarantine [`*<дія>* *<об'єкт>*`]`	**Призначення:** Застосувати дію до вказаного об'єкта, що знаходиться в карантині. Якщо дія не вказана, то вивести на екран інформацію про об'єкти, що знаходяться в карантині, із зазначенням їхніх ідентифікаторів та стислої інформації про вихідні файли, переміщені до карантину. Інформація про

Команда	Опис
	ізольовані об'єкти виводиться відповідно до формату, заданого необов'язковою опцією `--Format`. Якщо опція `--Format` не вказана, то для кожної загрози виводиться така інформація: • Ідентифікатор, присвоєний ізольованому об'єкту в карантині. • Вихідний шлях до файла, переміщеного в карантину. • Дата переміщення файла до карантину. • Інформація про файл: розмір, користувач-власник, дата останнього змінення. • Інформація про загрозу (ім'я, тип за класифікацією компанії «Доктор Веб»). **Аргументи:** Немає. **Опції:** `-a [--Autonomous]` — запустити окрему копію Сканера для виконання заданої дії з карантином, завершити її роботу після завершення дії. *Ця опція може бути застосована разом з будь-якою з опцій, вказаних нижче.* `--Format "<`*рядок формату*`>"` — виводити інформацію про об'єкти, що знаходяться в карантині, у вказаному форматі. Опис рядка формату наведений нижче. *Якщо ця опція вказана разом з будь-якою з опцій-дій, вона ігнорується.* `-f [--Follow]` — очікувати надходження нових повідомлень про загрози та виводити їх одразу, щойно вони надходитимуть (CTRL+C перериває очікування). *Якщо ця опція вказана разом з будь-якою з опцій-дій, вона ігнорується.* `--Discovery [<`*список каталогів*`>,]` — провести пошук каталогів карантину у вказаному списку каталогів та додати їх до консолідованого карантину при виявленні. Якщо `<`*список каталогів*`>` не вказаний, то провести пошук каталогів карантину в стандартних місцях файлової системи (точки монтування томів та домашні каталоги користувачів). *Ця опція може бути вказана разом не тільки з опцією `-a` (`--Autonomous`) (див. вище), але й з будь-якою з опцій-дій, наведених нижче. Більш того, якщо команда `quarantine` запускається в режимі автономної копії, тобто з опцією `-a` (`--Autonomous`), але без опції `--Discovery`, то це аналогічно виклику:* `quarantine --Autonomous --Discovery` `--Delete <`*об'єкт*`>` — видалити вказаний об'єкт з карантину. *Зверніть увагу, що видалення з карантину — безповоротна операція.*

Команда	Опис
	`--Cure` *<об'єкт>* — спробувати вилікувати вказаний об'єкт в карантині. *Зверніть увагу, що навіть якщо об'єкт був успішно зцілений, то він все одно залишиться в карантині. Щоб витягнути об'єкт з карантину необхідно скористатися опцією відновлення* `--Restore`. `--Restore` *<об'єкт>* — відновити вказаний об'єкт з карантину у вихідне місце. *Зверніть увагу, що для виконання цієї дії може бути необхідно, щоб* **drweb-ctl** *була запущена від імені суперкористувача. Відновити файл з карантину можна, навіть якщо він інфікований.* `--TargetPath` *<шлях>* — відновити об'єкт з карантину в указане місце: як файл з указаним іменем, якщо *<шлях>* — це шлях до файла, або у вказаний каталог, якщо *<шлях>* — це шлях до каталогу. Може бути вказаний як абсолютний, так і відносний (відносно поточного каталогу) шлях. *Зверніть увагу, що опція застосовується тільки сумісно з опцією відновлення* `--Restore`. В якості *<об'єкт>* використовується ідентифікатор об'єкта в карантині. Якщо необхідно застосувати дію до всіх об'єктів, що знаходяться в карантині, замість *<об'єкт>* вкажіть `All`. Наприклад, команда: `$ drweb-ctl quarantine --Restore All --TargetPath test` відновлює з карантину всі наявні в ньому об'єкти, поміщуючи їх до підкаталогу `test`, що знаходиться в поточному каталозі, з якого запущена команда **drweb-ctl**. *Зверніть увагу, що для варіанта* `--Restore All` *додаткова опція* `--TargetPath`*, якщо вказана, має задавати шлях до каталогу, а не до файла.*

Форматоване виведення даних для команд threats та quarantine

Формат виведення задається рядком формату, вказаним як аргумент необов'язкової опції `--Format`. Рядок формату обов'язково укладається в лапки. Рядок формату може містити як звичайні символи (виводитимуться на екран «як є»), так і спеціалізовані маркери, які при виведенні замінятимуться на відповідну інформацію. Доступні такі маркери:

1. Спільні для команд `threats` та `quarantine`:

Маркер	Опис
`%{n}`	Переведення рядка
`%{t}`	Табуляція

Маркер	Опис
`%{threat_name}`	Ім'я виявленої загрозаи (вірусу) за класифікацією компанії «Доктор Веб»
`%{threat_type}`	Тип загрози («known virus» тощо) за класифікацією компанії «Доктор Веб»
`%{size}`	Розмір вихідного файла
`%{origin}`	Повне ім'я вихідного файла зі шляхом
`%{path}`	Синонім для `%{origin}`
`%{ctime}`	Дата/час модифікації вихідного файла у форматі *"%Y-%b-%d %H:%M:%S"* (наприклад, `"2018-Jul-20 15:58:01"`)
`%{timestamp}`	Те саме, що й `%{ctime}`, але у форматі часу *UNIX timestamp*
`%{owner}`	Користувач-власник виіхідного файла
`%{rowner}`	Віддалений користувач-власник виіхідного файла (якщо незастосовне або значення невідоме — замінюється на `?`)

2. Специфічні для команди `threats`:

Маркер	Опис
`%{hid}`	Ідентифікатор запису про загрозу в реєстрі історії подій, пов'язаних з загрозою
`%{tid}`	Ідентифікатор загрози
`%{htime}`	Дата/час події, пов'язаної з загрозою
`%{app}`	Ідентифікатор компонента Dr.Web для Linux, який обробив загрозу
`%{event}`	Остання подія, пов'язана з загрозою: • `FOUND` — загроза була виявлена; • `Cure` — загроза була зцілена; • `Quarantine` — файл з загрозою був переміщений до карантину; • `Delete` — файл з загрозою був видалений; • `Ignore` — загроза була проігнорована; • `RECAPTURED` — загроза була виявлена повторно іншим компонентом.
`%{err}`	Текст повідомлення про помилку (якщо помилки немає — замінюється на порожній рядок)

3. Специфічні для команди `quarantine`:

Маркер	Опис
`%{qid}`	Ідентифікатор об'єкта в карантині

Маркер	Опис
`%{qtime}`	Дата/час переміщення об'єкта до карантину
`%{curetime}`	Дата/час спроби лікування об'єкта, переміщеного до карантину (якщо незастосовне або значення невідоме — замінюється на `?`)
`%{cureres}`	Результат спроби лікування об'єкта, переміщеного до карантину: • `cured` — загроза зцілена; • `not cured` — загроза не зцілена або спроби лікування не проводилися.

Приклад

```
$ drweb-ctl quarantine --Format "{%{n} %{origin}: %{threat_name} - %{qtime}%{n}}"
```

Дана команда виведе вміст карантину в виді записів такого виду:

```
{
 <шлях до файла>: <ім'я загрози - <дата переміщення до карантину
}
...
```

3.5. Інформаційні команди

Доступні такі інформаційні команди:

Команда	Опис
`appinfo`	**Призначення:** Вивести на екран інформацію про працюючі модулі Dr.Web для Linux. Для кожного запущеного компонента виводиться така інформація: • Внутрішнє ім'я. • Ідентифікатор процесу **GNU/Linux** (PID). • Стан (запущений, зупинений тощо). • Код помилки, якщо робота компонента завершена через помилку. • Додаткова інформація (опціонально). Для демона управління конфігурацією (**drweb-configd**) як додаткова інформація виводиться: • Список встановлених компонентів — *Installed*. • Список компонентів, запуск яких має забезпечуватися демоном — *Should run*. **Аргументи:** Немає.

Команда	Опис
	Опції: `-f [--Follow]` — очікувати надходження нових повідомлень про змінення стану модулів та виводити їх одразу, щойно вони надходитимуть (CTRL+C перериває очікування).
`baseinfo`	**Призначення:** Вивести на екран інформацію про поточну версію антивірусного ядра та стан вірусних баз. Виводиться така інформація: • Версія антивірусного ядра. • Дата та час випуску використовуваних вірусних баз. • Кількість доступних вірусних записів. • Час останнього успішного оновлення вірусних баз та антивірусного ядра. • Час наступного запланованого автоматичного оновлення. **Аргументи:** Немає. **Опції:** `-l [--List]` — вивести повний список завантажених файлів вірусних баз даних та кількість вірусних записів в кожному файлі.
`certificate`	**Призначення:** Вивести на екран вміст довіреного сертифікату Dr.Web, що використовується Dr.Web для Linux для доступу до захищених з'єднань з метою перевірки, якщо ця перевірка включена в налаштуваннях. Щоб зберегти сертифікат в файл `<cert_name>.pem`, ви можете використати команду: `$ drweb-ctl certificate > <cert_name>.pem` **Аргументи:** Немає. **Опції:** Немає.
`events`	**Призначення:** Переглянути події Dr.Web для Linux. Окрім цього, ця команда дозволяє управляти подіями (позначка як «прочитані», видалення). **Аргументи:** Немає. **Опції:** `--Report <mun>` — встановити тип звіту про перевірку. **Можливі значення:** • `BRIEF` — стислий звіт. • `DEBUG` — докладний звіт. • `JSON` — серіалізований звіт у форматі JSON.

Команда	Опис
	`-f [--Follow]` — очікувати надходження нових повідомлень та виводити їх на екран одразу, як тільки вони надходитимуть (CTRL+C перериває очікування). `-s [--Since]` <*дата, час*> — показувати події, що сталися не раніше вказаного моменту часу (<*дата, час*> вказується у форматі `"YYYY-MM-DD hh:mm:ss"`). `-u [--Until]` <*дата, час*> — показувати події, що сталися не пізніше вказаного моменту часу (<*дата, час*> вказується у форматі `"YYYY-MM-DD hh:mm:ss"`). `-t [--Types]` <*список типів*> — показувати події тільки зазначених типів (типи подій наводяться через кому). Доступні такі типи подій: • `Mail` — виявлена загроза в повідомленні електронної пошти; • `UnexpectedAppTermination` — аварійне завершення роботи будь-якого компонента. Щоб вивести події всіх типів, використовуйте `All`. `--ShowSeen` — показати також й вже прочитані події. `--Show` <*список подій*> — вивести на екран зазначені події (ідентифікатори подій наводяться через кому). `--Delete` <*список подій*> — видалити зазначені події (ідентифікатори подій наводяться через кому). `--MarkAsSeen` <*список подій*> — позначити зазначені події як «прочитані» (ідентифікатори подій наводяться через кому). Якщо необхідно позначити як «прочитані» або видалити всі події, замість <*список подій*> вкажіть `All`. Наприклад, команда: `$ drweb-ctl events --MarkAsSeen All` позначить як «прочитані» всі наявні події.
`report` <*тип*>	**Призначення:** Сформувати звіт про події Dr.Web для Linux в виді HTML-сторінки (тіло сторінки виводиться у вказаний файл). **Аргументи:** <*тип*> — тип подій, для яких формується звіт (вказується один тип). Можливі значення див. в описі опції `--Types` команди `events` вище. Обов'язковий аргумент. **Опції:** `-o [--Output]` <*шлях до файла*> — зберегти звіт у вказаний файл. Обов'язкова опція. `-s [--Since]` <*дата, час*> — включити в звіт події, що сталися не раніше вказаного моменту часу (<*дата, час*> вказується у форматі `"YYYY-MM-DD hh:mm:ss"`).

Команда	Опис
	`-u [--Until]` <*дата, час*> — включити в звіт події, що сталися не пізніше вказаного моменту часу (<*дата, час*> вказується у форматі `"YYYY-MM-DD hh:mm:ss"`). `--TemplateDir` <*шлях до каталогу*> — шлях до каталогу, в якому знаходяться файли шаблонів HTML-сторінки звіту. Опції `-s`, `-u` та `--TemplateDir` є необов'язковими. Наприклад, команда: `$ drweb-ctl report Mail -o report.html` сформує звіт за всіма наявними подіями виявлення загроз в повідомленнях електронної пошти на базі шаблону за замовчуванням та збереже результат в файл `report.html` в поточному каталозі.
`license`	**Призначення:** Вивести на екран інформацію про активну ліцензію, отримати демонстраційну ліцензію або отримати ключовий файл для вже зареєстрованої ліцензії (наприклад — на сайті компанії). Якщо не вказана жодна опція, то виводиться така інформація (якщо використовується ліцензія для одиночного режиму роботи): • Номер ліцензії. • Дата та час завершення дії ліцензії. Якщо використовується ліцензія, видана сервером централізованого захисту (для роботи в режимі централізованого захисту або в мобільному режимі), виводиться відповідна інформація. **Аргументи:** Немає. **Опції:** `--GetDemo` — запитати демонстраційний ключ терміном на місяць та отримати його, якщо не порушені умови отримання демонстраційного періоду. `--GetRegistered` <*серійний номер*> — отримати ліцензійний ключовий файл для вказаного серійного номера, якщо не порушені умови отримання нового ключового файла (наприклад, програма не знаходиться в режимі централізованого захисту, коли ліцензією управляє сервер централізованого захисту). *Якщо серійний номер не є серійним номером демонстраційного періоду, то він має бути попередньо зареєстрований на сайті компанії.* Докладніше про ліцензування продуктів Dr.Web див. у розділі Ліцензування. Для реєстрації серійного номера та для отримання демонстраційного періоду необхідна наявність підключення до мережі Інтернет.

Команда	Опис
`log`	**Призначення:** Вивести на екран консолі (в потік *stdout*) останні записи журналу Dr.Web для Linux (аналогічно команді **tail**). **Аргументи:** Немає. **Опції:** `-s [--Size]` <*число*> — кількість останніх записів журналу, які необхідно вивести на екран. `-c [--Components]` <*список компонентів*> — список ідентифікаторів компонентів, записи яких будуть виведені. Вказуються через кому. Якщо параметр не вказаний, виводяться всі доступні останні записи, внесені в журнал будь-яким з компонентів. *Актуальні ідентифікатори встановлених компонентів (тобто внутрішні імена компонентів, що записуються в журнал) ви можете дізнатися, використовуючи команду* `appinfo` *(див. вище).* `-f [--Follow]` — очікувати на нові записи в журнал та виводити їх на екран консолі одразу, як тільки вони надходитимуть (CTRL+C перериває очікування).

Приклади використання

В цьому розділі наведені приклади використання утиліти Dr.Web Ctl (**drweb-ctl**):

- Перевірка об'єктів:
  - Прості команди перевірки.
  - Перевірка файлів за критеріями.
  - Перевірка додаткових об'єктів.
- Управління конфігурацією.
- Управління загрозами.
- Приклад роботи в режимі автономної копії.

1. Перевірка об'єктів

1.1. Прості команди перевірки

1. Провести перевірку каталогу `/home` з параметрами за замовчуванням:

```
$ drweb-ctl scan /home
```

2. Провести перевірку списку шляхів, зазначених в файлі `daily_scan` (по одному шляху в рядку файла):

```
$ drweb-ctl scan --stdin < daily_scan
```

3. Провести перевірку завантажувального запису на дисковому пристрої *sda*:

```
$ drweb-ctl bootscan /dev/sda
```

4. Провести перевірку запущених процесів:

```
$ drweb-ctl procscan
```

1.2. Перевірка файлов за критеріями

В наведених нижче прикладах для формування списку файлів, які необхідно перевірити, використовується результат роботи утиліти **find**. Отриманий список файлів передається команді **drweb-ctl** `scan` з параметром `--stdin` або `--stdin0`.

1. Провести перевірку списку файлів, що повернені утилітою **find**, та розділених символом NUL ('`\0`'):

```
$ find -print0 | drweb-ctl scan --stdin0
```

2. Перевірити всі файли всіх каталогів, починаючи з кореневого, що знаходяться в одному розділі файлової системи:

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

3. Перевірити всі файли всіх каталогів, починаючи з кореневого, окрім файлів `/var/log/messages` та `/var/log/syslog`:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog |
drweb-ctl scan --stdin
```

4. Перевірити в усіх каталогах, починаючи з кореневого, файли, що належать користувачу *root*:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

5. Перевірити в усіх каталогах, починаючи з кореневого, файли, що належать користувачам *root* та *admin*:

```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

6. Перевірити в усіх каталогах, починаючи з кореневого, файли, що належать користувачам з UID з діапазону 1000–1005:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

7. Перевірити файли в усіх каталогах, починаючи з кореневого, але що знаходяться не більш ніж на п'ятому рівні вкладеності відносно кореневого каталогу:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

8. Перевірити файли в кореневому каталозі, не заходячи у вкладені каталоги:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

9. Перевірити файли в усіх каталогах, починаючи з кореневого, при цьому слідувати за символічними посиланнями, що зустрічаються:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

10. Перевірити файли в усіх каталогах, починаючи з кореневого, при цьому не слідувати за символічними посиланнями, що зустрічаються:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

11. Перевірити в усіх каталогах, починаючи з кореневого, файли, створені не пізніше 01 травня 2017 року:

```
$ find / -type f -newermt 2017-05-01 | drweb-ctl scan --stdin
```

1.3. Перевірка додаткових об'єктів

1. Перевірка об'єктів, розташованих в каталозі `/tmp` на віддаленому вузлі *192.168.0.1*, підключившись до нього через SSH як користувач *user* з паролем *passw*:

```
$ drweb-ctl remotescan 192.168.0.1 /tmp --Login user --Password passw
```

2. Перевірка повідомлення електронної пошти, збереженого в файл `email.eml`, з використанням набору правил за замовчуванням:

```
$ drweb-ctl checkmail email.eml
```

2. Управління конфігурацією

1. Вивести на екран інформацію про поточний склад Dr.Web для Linux, включаючи інформацію про запущені компоненти:

```
$ drweb-ctl appinfo
```

2. Вивести на екран всі параметри з секції `[Root]` активної конфігурації:

```
$ drweb-ctl cfshow Root
```

3. Задати значення 'No' для параметра **Start** з секції `[LinuxSpider]` активної конфігурації (це призведе до зупинення роботи SpIDer Guard):

```
# drweb-ctl cfset LinuxSpider.Start No
```

Зверніть увагу, що для цього необхідні повноваження суперкористувача. Приклад виклику цієї самої команди з використанням **sudo** для тимчасового підвищення повноважень:

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

4. Провести примусове оновлення антивірусних компонентівDr.Web для Linux:

```
$ drweb-ctl update
```

5. Перезавантажити конфігурації для компонентів Dr.Web для Linux:

```
# drweb-ctl reload
```

Зверніть увагу, що для цього необхідні повноваження суперкористувача. Приклад виклику цієї самої команди з використанням **sudo** для тимчасового підвищення повноважень:

```
$ sudo drweb-ctl reload
```

6. Підключити Dr.Web для Linux до сервера централізованого захисту, що працює на вузлі *192.168.0.1* за умови, що сертифікат сервера знаходиться в файлі `/home/user/cscert.pem`:

```
$ drweb-ctl esconnect 192.168.0.1 --Certificate /home/user/cscert.pem
```

7. Відключити Dr.Web для Linux від сервера централізованого захисту:

```
# drweb-ctl esdisconnect
```

Зверніть увагу, що для цього необхідні повноваження суперкористувача. Приклад виклику цієї самої команди з використанням **sudo** для тимчасового підвищення повноважень:

```
$ sudo drweb-ctl esdisconnect
```

8. Переглянути останні записи, внесені компонентами **drweb-update** та **drweb-configd** в журнал Dr.Web для Linux:

```
# drweb-ctl log -c Update,ConfigD
```

3. Управління загрозами

1. Вивести на екран інформацію про виявлені загрози:

```
$ drweb-ctl threats
```

2. Перемістити до карантину всі файли, що містять незнешкоджені загрози:

```
$ drweb-ctl threats --Quarantine All
```

3. Вивести на екран список файлів, переміщених до карантину:

```
$ drweb-ctl quarantine
```

4. Відновити все файли з карантину:

```
$ drweb-ctl quarantine --Restore All
```

4. Приклад роботи в режимі автономної копії

1. Перевірити файли та опрацювати карантин в режимі автономної копії:

```
$ drweb-ctl scan /home/user -a --OnKnownVirus=Quarantine
$ drweb-ctl quarantine -a --Delete All
```

Перша команда перевірить файли в каталозі `/home/user` в режимі автономної копії, та файли, що містять відомі віруси, будуть поміщені до карантину. Друга команда опрацює вміст карантину (теж в режимі автономної копії) та видалить всі об'єкти, що містяться в карантині.

Додатки

Додаток А. Види комп'ютерних загроз

Під терміном *«загроза»* в цій класифікації мається на увазі будь-який програмний засіб, який напряму або опосередковано здатен заподіяти шкоди комп'ютеру, мережі, інформації або правам користувача (тобто шкідливі та інші небажані програми). В ширшому сенсі термін «загроза» може означати будь-яку потенційну небезпеку для комп'ютера або мережі (тобто її уразливість, яка може бути використана для проведення хакерських атак).

Всі описані нижче типи програм потенційно здатні наразити на небезпеку дані користувача або їхню конфіденційність. Програми, які не приховують своєї присутності в системі (наприклад, деякі програми для розсилання спаму або аналізатори трафіку), зазвичай не зараховують до комп'ютерних загроз, хоча за визначених обставин вони також можуть заподіяти шкоди користувачу.

Комп'ютерні віруси

Даний тип комп'ютерних загроз характеризується здатністю впроваджувати свій код у виконуваний код інших програм. Таке впровадження називається *інфікуванням*. В більшості випадків інфікований файл сам стає носієм вірусу, а впроваджений код не обов'язково повністю відповідає оригіналу. Більша частина вірусів створюється для пошкодження або знищення даних.

В компанії «Доктор Веб» віруси поділяють за типом файлів, які вони інфікують:

- *Файлові віруси* інфікують файли операційної системи (зазвичай виконувані файли та динамічні бібліотеки) та активізуються при зверненні до інфікованого файла.
- *Макро-віруси* інфікують документи, з якими працюють програми з пакета **Microsoft® Office** (та інші програми, які використовують макроси, написані, наприклад, мовою **Visual Basic**). *Макроси* — це вбудовані програми, написані повноцінною мовою програмування, які можуть запускатися за визначених умов (наприклад, в **Microsoft® Word** макроси можуть запускатися при відкритті, закритті або збереженні документу).
- *Скрипт-віруси* пишуться мовами сценаріїв (скриптів) та в більшості випадків інфікують інші файли сценаріїв (наприклад, службові файли операційної системи). Вони можуть інфікувати також інші типи файлів, які підтримують виконання сценаріїв, користуючись уразливими сценаріями в веб-програмах.
- *Завантажувальні віруси* інфікують завантажувальні сектори дисків та розділів, а також головні завантажувальні сектора жорстких дисків. Вони займають дужа мало пам'яті та залишаються готовими до виконання своїх функцій доти, доки не буде проведене вивантаження, перевантаження або завершення роботи системи.

Більшість вірусів мають захисні механізми проти виявлення. Методи захисту від виявлення постійно удосконалюються, тому для антивірусних програм розробляються нові способи подолання цього захисту. Віруси можна розділити за принципом захисту від виявлення:

- *Шифровані віруси* шифрують свій код при кожному новому інфікуванні, що ускладнює його виявлення в файлі, пам'яті або завантажувальному секторі. Кожний екземпляр такого вірусу містить тільки короткий спільний фрагмент (процедуру розшифрування), який можна вибрати як сигнатуру.
- *Поліморфні віруси* використовують, окрім шифрування коду, спеціальну процедуру розшифрування, що змінює саму себе в кожному новому екземплярі вірусу, що призводить до відсутності у такого вірусу байтових сигнатур.
- *Стелс-віруси* (віруси-невидимки) застосовують спеціальні дії для маскування своєї діяльності з метою приховування своєї присутності в інфікованих об'єктах. Такий вірус знімає характеристики об'єкта перед його інфікуванням, а потім передає старі данні при запиті операційної системи або програми, що шукає змінені файли.

Віруси також можна класифікувати за мовою, якою вони написані (більшість пишуться мовою асемблера, але є також і віруси, написані високорівневими мовами програмування, мовами сценаріїв тощо) та за операційними системами, що ними інфікуються.

Комп'ютерні хробаки

Останнім часом шкідливі програми типу «комп'ютерний хробак» стали набагато поширенішими, ніж віруси та інші шкідливі програми. Як і віруси, такі програми здатні створювати свої копії, але при цьому вони не інфікують інші об'єкти. Хробак проникає на комп'ютер з мережі (найчастіше як вкладення у повідомлення електронної пошти або через мережу Інтернет) та розсилає свої функціональні копії на інші комп'ютери. Для початку поширення хробаки можуть використовувати як дії користувача, так і автоматичний режим вибору та атаки комп'ютера.

Хробаки не обов'язково цілком складаються з одного файла (тіла хробака). У багатьох хробаків є так звана інфекційна частина (шел-код), яка завантажується в оперативну пам'ять комп'ютера та «довантажує» з мережі безпосередньо саме тіло хробака в виді виконуваного файла. Поки в системі немає тіла хробака, від нього можна позбавитися перезавантаженням комп'ютера (при якій скидається оперативна пам'ять). Якщо ж системі виявляється тіло хробака, то впоратися з ним може тільки антивірус.

За рахунок інтенсивного поширення хробаки здатні вивести з ладу цілі мережі, навіть якщо вони не несуть жодного корисного навантаження (не заподіюють прямої шкоди системі).

В компанії «Доктор Веб» хробаків поділяють за способом (середовищем) поширення:

- *Мережні хробаки* поширюються за допомогою різних мережних протоколів та протоколів обміну файлами.

- *Почтові хробаки* поширюються за допомогою поштових протоколів (POP3, SMTP тощо).
- *Чат-хробаки* поширюються, використовуючи популярні програми для пересилання миттєвих повідомлень (ICQ, IM, IRC тощо).

Троянські програми

Цей тип шкідливих програм не здатен до самореплікації. Троянські програми підмінюють будь-яку з програм, що запускаються найчастіше, та виконують її функції (або імітують виконання цих функцій), одночасно виконуючи якісь шкідливі дії (пошкодження та видалення даних, пересилання конфіденційної інформації тощо), або уможливлюючи несанкціоноване використання комп'ютера зловмисником, наприклад, для заподіяння шкоди третім особам.

Ці програми мають подібні до вірусів маскувальні та шкідливі функції та навіть можуть бути модулем вірусу, але, як правило, троянські програми поширюються як окремі виконувані файли (викладаються на файлових серверах, записуються на носії інформації або пересилаються в виді вкладень в повідомленнях електронної пошти), які запускаються або самим користувачем, або визначеним процесом системи.

Класифікувати троянські програми дуже важко, по-перше, тому що вони часто поширюються вірусами та хробаками, по-друге, шкідливі дії, які можуть виконувати інші типи загроз, прийнято приписувати тільки троянським програмам. Нижче наведений список деяких типів троянських програм, які в компанії «Доктор Веб» виділяють в окремі класи:

- *Бекдори* — це троянські програми, які дозволяють отримати привілейований доступ до системи, оминаючи існуючий механізм надання доступу та захисту. Бекдори не інфікують файли; вони прописують себе в реєстрі, модифікуючи ключі.
- *Руткіти* призначені для перехоплення системних функцій операційної системи з метою приховування своєї присутності в системі. Окрім того, руткіт може маскувати процеси інших програм, різні ключі реєстру, каталоги, файли. Руткіт поширюється як самостійна програма або як додатковий компонент у складі іншої шкідливої програми. За принципом своєї роботи руткіти умовно поділяють на дві групи: руткіти, що працюють в режимі користувача (перехоплення функцій бібліотек режиму користувача) (*User Mode Rootkits — UMR*), та руткіти, що працюють в режимі ядра (перехоплення функцій на рівні системного ядра, що значно ускладнює виявлення та знешкодження) (*Kernel Mode Rootkits — KMR*).
- *Клавіатурні перехоплювачі* (*кейлоггери*) використовуються для збору даних, які користувач вводить за допомогою клавіатури. Метою таких дій є викрадення особистої інформації (наприклад, мережних паролів, логінів, номерів банківських карток тощо).
- *Клікери* перевизначають посилання при натисненні на них і таким чином перенаправляють користувачів на визначені (можливо, шкідливі) сайти. Зазвичай користувач перенаправляється з метою збільшення рекламного трафіку веб-сайтів або для організації розподілених атак відмови від обслуговування (DDoS-атак).

- *Проксі-трояни* надають зловмиснику анонімний вихід в мережу Інтернет через комп'ютер жертви.

Окрім наведених вище, троянські програми можуть виконувати й інші шкідливі дії, наприклад, змінювати стартову сторінку в веб-браузері або видаляти визначені файли. Проте такі дії можуть виконуватися й загрозами інших типів (наприклад, вірусами та хробаками).

Програми зламу

Програми зламу створені з метою допомогти зламщику. Найпоширенішим видом подібних програм є сканери портів, які дозволяють виявляти уразливості в міжмережних екранах (файєрволах, брандмауерах) та інших компонентах, які забезпечують безпеку комп'ютера. Окрім хакерів, такими інструментами можуть користуватися адміністратори для перевірки надійності своїх мереж. Іноді до програм зламу відносять програми, що використовують методи соціальної інженерії (елементи соціотехніки).

Рекламні програми

Найчастіше під цим терміном мають на увазі програмний код, вбудований в різне безкоштовне програмне забезпечення, при використанні якого користувачу примусово показується реклама. Але іноді такий код може приховано поширюватися за допомогою інших шкідливих програм та демонструвати рекламу, наприклад в веб-браузерах. Часто рекламні програми працюють на основі даних, зібраних шпигунськими програмами.

Програми-жарти

Цей тип шкідливих програм, які, як і рекламні програми, не заподіюють прямої шкоди системі. Найчастіше вони генерують повідомлення про неіснуючі помилки та погрожують діями, які можуть призвести до пошкодження даних. Їхня основна функція полягає в залякуванні користувача, або нав'язливе його роздратування.

Програми додзвону

Це спеціальні комп'ютерні програми, розроблені для сканування деякого діапазону телефонних номерів для виявлення такого, на який відповідає модем. У подальшому зловмисники використовують знайдені номери для накручування сплати за телефон або для непомітного підключення користувача через модем до дорогих платних телефонних служб.

Потенційно небезпечні програми

Ці програми не створювалися для заподіяння шкоди, але через свої особливості можуть становити загрозу для безпеки системи. До таких програм відносяться не тільки ті, які

можуть випадково пошкодити або видалити дані, але й ті, які можуть використовуватися хакерами або іншими програмами для заподіяння шкоди системі. До потенційно небезпечних програм можна віднести різні програми віддаленого спілкування та адміністрування, FTP-сервери тощо.

Підозрілі об'єкти

До підозрілих об'єктів відносяться будь-які потенційні загрози, виявлені за допомогою евристичного аналізу. Такі об'єкти можуть бути будь-яким типом комп'ютерних загроз (можливо, навіть невідомим для спеціалістів з інформаційної безпеки), а можуть виявитися безпечними при помилковому спрацьовуванні. Файли, що містять підозрілі об'єкти, рекомендується поміщати до карантину, а також відправляти на аналіз спеціалістам антивірусної лабораторії «Доктор Веб».

Додаток Б. Усунення комп'ютерних загроз

Всі антивірусні продукти, розроблені компанією Dr.Web, застосовують цілий набір методів виявлення загроз, що дозволяє перевіряти підозрілі об'єкти максимально ретельно.

- Методи виявлення загроз.
- Дії з загрозами.

Методи виявлення загроз

Сигнатурний аналіз

Цей метод виявлення застосовується в першу чергу. Виявлення проводиться шляхом перевірки вмісту об'єкта, що аналізується, на наявність в ньому сигнатур вже відомих загроз. *Сигнатурою* називається неперервна кінцева послідовність байт, необхідна та достатня для однозначної ідентифікації загрози. При цьому порівнянні вмісту об'єкта, що аналізується, з сигнатурами проводиться не напряму, а за їхніми контрольними сумами, що дозволяє значно зменшити розмір записів в вірусних базах, зберігши при цьому однозначність відповідності й, отже, коректність виявлення загроз та лікування інфікованих об'єктів. Записи в вірусних базах Dr.Web складені таким чином, що завдяки одному тому самому запису можна виявляти цілі класи або сімейства загроз.

Origins Tracing™

Ця унікальна технологія Dr.Web, яка дозволяє визначити нові або модифіковані загрози, що використовує вже відомі та описані в вірусних базах механізми зараження та заподіяння шкоди. Вона проводиться після завершення сигнатурного аналізу та забезпечує захист користувачів, які використовують антивірусні рішення Dr.Web від таких загроз, як троянська програма-вимагач **Trojan.Encoder.18** (також відома під назвою **gpcode**). Окрім того, використання технології Origins Tracing™ дозволяє значно зменшити кількість помилкових спрацьовувань евристичного аналізатора. До назв загроз, виявлених за допомогою Origins Tracing™, додається постфікс `.Origin`.

Емуляція виконання

Метод емуляції виконання програмного коду використовується для виявлення поліморфних та шифрованих вірусів, коли використання пошуку за контрольними сумами сигнатур незастосовне або значно ускладнене через неможливість побудови надійних сигнатур. Метод полягає в імітації виконання коду, що аналізується, за допомогою *емулятора* — програмної моделі процесора та середовища виконання програм. Емулятор оперує захищеною областю пам'яті (буфером емуляції). При цьому інструкції не передаються на центральний процесор для реального виконання. Якщо

код, що опрацьовується емулятором, інфікований, то результатом його емуляції стане відновлення вихідного шкідливого коду, доступного для сигнатурного аналізу.

Евристичний аналіз

Робота евристичного аналізатора грунтується на наборі *евристик* (припущень, статистична значимість яких підтверджена дослідним шляхом) про характерні ознаки шкідливого та, навпаки, безпечного виконуваного коду. Кожна ознака коду має визначену *вагу* (тобто число, що показує важливість та достовірність цієї ознаки). Вага може бути як позитивною, якщо ознака вказує на наявність шкідливої поведінки коду, так і негативною, якщо ознака не властива комп'ютерним загрозам. На основі сумарної ваги, що характеризує вміст об'єкта, евристичний аналізатор обчислює вірогідність вмісту в ньому невідомого шкідливого об'єкта. Якщо ця вірогідність перевищує деяке порогове значення, то видається висновок про те, що об'єкт, який аналізується, є шкідливим.

Евристичний аналізатор також використовує технологію FLY-CODE™ — універсальний алгоритм розпакування файлів. Цей механізм дозволяє будувати евристичні припущення про наявність шкідливих об'єктів в об'єктах, стиснених програмами упаковування (пакувальниками), причому не тільки відомими розробникам продукту Dr.Web, але й новими програмами. При перевірці упакованих об'єктів також використовується технологія аналізу їхньої структурної ентропії, яка дозволяє виявляти загрози за особливостями розташування ділянок їхнього коду. Ця технологія дозволяє на основі одного запису вірусної бази провести виявлення набору різних загроз, упакованих однаковим поліморфним пакувальником.

Оскільки евристичний аналізатор є системою перевірки гіпотез в умовах невизначеності, то він може припускатися помилки як першого (пропуск невідомих загроз), так і другого роду (визнання безпечної програми шкідливою). Тому об'єктам, позначеним евристичним аналізатором як «шкідливі», присвоюється статус «підозрілі».

Під час будь-якої з перевірок всі компоненти антивірусних продуктів Dr.Web використовують найсвіжішу інформацію про всі відомі шкідливі програми. Сигнатури загроз й інформація про їхні ознаки та моделі поведінки оновлюються та додаються до вірусних баз одразу, як тільки спеціалісти антивірусної лабораторії «Доктор Веб» виявляють нові загрози, іноді — до декількох раз на годину. Навіть якщо найновіша шкідлива програма проникає на комп'ютер, оминаючи резидентний захист Dr.Web, то вона буде виявлена у списку процесів та нейтралізована після отримання оновлених вірусних баз.

Хмарні технології виявлення загроз

Хмарні методи виявлення дозволяють перевірити будь-який об'єкт (файл, програму, розширення для браузера тощо) за *хеш-сумою*. Вона є унікальна послідовність цифр та літер заданої довжини. При аналізі за хеш-сумою об'єкти перевіряються за існуючою базою та потім класифікуються за категоріями: чисті, підозрілі, шкідливі тощо.

Така технологія оптимізує час перевірки файлів та економить ресурси пристрою. Завдяки тому, що аналізується не сам об'єкт, а його унікальна хеш-сума, рішення виноситься практично моментально. За відсутності підключення до серверів Dr.Web Cloud файли перевіряються локально, а хмарна перевірка поновлюється після відновлення зв'язку.

Таким чином, хмарний сервіс Dr.Web Cloud збирає інформацію від багаточисельних користувачів та оперативно оновлює дані про раніше невідомі загрози, тим самим підвищуючи ефективність захисту пристроїв.

Дії з загрозами

В антивірусних продуктах Dr.Web реалізована можливість застосовувати визначені дії до виявлених об'єктів для знешкодження комп'ютерних загроз. Користувач може залишити задані за замовчуванням дії, що автоматично застосовуються до визначених типів загроз, змінити їх або вибирати необхідну дію для кожного виявленого об'єкта окремо. Нижче наведений список доступних дій:

- **Ignore** *(Ігнорувати)* — Пропустити виявлену загрозу, не застосовуючи жодних дій;
- **Report** *(Report)* — Сповістити про наявність загрози, але нічого не робити з інфікованим об'єктом;
- **Cure** *(Лікувати)* — Спробувати зцілити інфікований об'єкт, видаливши з нього шкідливий вміст, та залишивши цілим корисний вміст. Зверніть увагу, що ця дія застосовна не до всіх видів загроз;
- **Quarantine** *(До карантину)* — Перемістити інфікований об'єкт (якщо він допускає цю операцію) до спеціального каталогу карантину з метою його ізоляції;
- **Delete** *(Видалити)* — Безповоротно видалити інфікований об'єкт.

Якщо загроза виявлена в файлі, що знаходиться в контейнері (архів, поштове повідомлення тощо), замість видалення виконується переміщення контейнера до карантину.

Додаток В. Технічна підтримка

При виникненні проблем зі встановленням або роботою продуктів компанії, перш ніж звертатися за допомогою до Служби технічної підтримки, спробуйте знайти рішення таким чином:

- ознайомтеся з останніми версіями описів та посібників за адресою https://download.drweb.com/doc/;
- прочитайте розділ питань, що ставляться найчастіше, за адресою https://support.drweb.com/show_faq/;
- відвідайте форуми компанії «Доктор Веб» за адресою https://forum.drweb.com/.

Якщо після цього не вдалося розв'язати проблему, ви можете скористатися в один з таких способів, щоб зв'язатися зі Службою технічної підтримки компанії «Доктор Веб»:

- заповніть веб-форму у відповідній секції розділу https://support.drweb.com/;
- зателефонуйте до української Служби технічної підтримки за телефоном у Києві: +380 (44) 238-24-35 або до глобальної підтримки за телефоном +7 (495) 789-45-86.

Інформацію про регіональні представництва та офиси компанії «Доктор Веб» ви можете знайти на офіційному сайті за адресою https://company.drweb.com/contacts/offices/.

Для спрощення роботи Служби технічної підтримки з аналізу проблеми, що виникла у вас, рекомендується попередньо сформувати пакет інформації про встановлений у вас продукт, його налаштування та системне оточення. Для цього призначена спеціалізована утиліта, що входить до складу Dr.Web для Linux.

Щоб зібрати інформацію для Служби технічної підтримки, введіть таку команду:

```
# /opt/drweb.com/bin/support-report.sh
```

Для збору інформації для Служби технічної підтримки рекомендується запустити утиліту з правами суперкористувача (користувача *root*). Щоб отримати права суперкористувача, скористайтеся командою зміни користувача **su** або командою виконання від імені іншого користувача **sudo**.

У процесі роботи утиліта збирає та упаковує в архів таку інформацію:

- Інформація про ОС (назва, архітектура, виведення команди **uname** `-a`);
- Список встановлених в системі пакетів, у тому числі — пакетів «Доктор Веб»;
- Вміст журналів:
  - журнали Dr.Web для Linux (якщо налаштовані для окремих компонентів);
  - журнал, який ведеться демоном журналювання **syslog** (`/var/log/syslog`, `/var/log/messages`);

- журнал системного пакетного менеджера (**apt**, **yum** тощо);
- журнал **dmesg**;

- Результати запуску таких команд: **df**, **ip** `a` (**ifconfig** `-a`), **ldconfig** `-p`, **iptables-save**, **nft** `export xml`.
- Інформація про налаштування та конфігурації Dr.Web для Linux:
  - список завантажених вірусних баз (**drweb-ctl** `baseinfo -l`);
  - список файлів з каталогів Dr.Web для Linux та їх MD5-хеші;
  - версія та MD5-хеш файла антивірусного ядра Dr.Web Virus-Finding Engine;
  - параметри конфігурації Dr.Web для Linux (у тому числі: вміст файла `drweb.ini`, правила та файли значень, що використовуються в правилах, Lua-процедури тощо);
  - Інформація про користувача та дозволи, витягнута з ключового файла, якщо Dr.Web для Linux працює не в режимі централізованого захисту.

Сформований архів з інформацією про продукт та системне оточення буде збережений в домашній каталог користувача, який запустив утиліту, та називатиметься таким чином:

```
drweb.report.<timestamp>.tgz
```

де <*timestamp*> — повна мітка часу створення звіту, включаючи мілісекунди, наприклад: `20190618151718.23625`.

Додаток Г. Опис відомих помилок

Тут надані:

- Рекомендації з ідентифікації помилок.
- Описи помилок, що визначаються за кодом.
- Описи помилок, що не мають коду, але визначаються за симптомами прояви.

Якщо опис помилки, що сталася, тут відсутній, рекомендуємо звернутися до Технічної підтримки, повідомивши код помилки та описавши обставини її виникнення.

Рекомендації з ідентифікації помилок

- Щоб уточнити місце та причину виникнення помилки, ознайомтеся з журналом Dr.Web для Linux (за замовчуванням він знаходиться в файлі `/var/log/syslog` або `/var/log/messages`, залежно від використовуваної ОС). Також ви можете скористатися командою **drweb-ctl** `log`.
- Щоб полегшити ідентифікацію помилок, рекомендується налаштувати виведення журналу в окремий файл та дозволити виведення розширеної відлагоджувальної інформації. Для цього виконайте такі команди:

```
# drweb-ctl cfset Root.Log <шлях до файла журналу>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- Щоб повернути налаштування ведення журналу за замовчуванням, виконайте такі команди:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

Помилки, що визначаються за кодом

Повідомлення про помилку	*Помилка зв'язку з монітором*
Код помилки	`x1`
Опис	Помилка зв'язку якогось компонента з демоном управління конфігурацією Dr.Web ConfigD.

Усунення помилки:

1. Перезапустіть демон управління конфігурацією, виконавши команду

```
# service drweb-configd restart
```

2. Перевірте, що в системі встановлений, налаштований та коректно функціонує механізм аутентифікації **PAM**. Якщо це не так, встановіть та налаштуйте його (за докладною інформацією зверніться до посібників з адміністрування вашого дистрибутиву ОС).
3. Якщо перезапуск демона управління конфігурацією при коректно налаштованому **PAM** не допомагає, спробуйте скинути налаштування Dr.Web для Linux в значення за замовчуванням.

   Для цього очистіть вміст файла *<etc_dir>*`/drweb.ini` (при цьому рекомендується створити резервну копію файла конфігурації), наприклад, виконавши команди:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Після очищення файла конфігурації перезапустіть демон управління конфігурацією.
4. Якщо демон управління конфігурацією запустити не вдається, спробуйте перевстановити пакет `drweb-configd`.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Операція вже виконується*
Код помилки	`x2`
Опис	Операція, запитана користувачем, в даний момент вже виконується.

Усунення помилки:

1. Дочекайтеся завершення операції та за необхідності повторіть необхідну дію через деякий час.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Операція очікує виконання*
Код помилки	`x3`
Опис	Операція, запитана користувачем, в даний момент очікує виконання (можливо, проводиться встановлення мережного з'єднання або триває завантаження та ініціалізація будь-якого компонента Dr.Web для Linux, що потребує тривалого часу).

Усунення помилки:

1. Дочекайтеся початку виконання операції та за необхідності повторіть необхідну дію через деякий час.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Перервано користувачем*
Код помилки	x4
Опис	Дія, що виконувалася, була перервана користувачем (можливо, вона виконувалася занадто довго).
Усунення помилки: 1. Повторіть необхідну дію через деякий час.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Операція скасована*
Код помилки	x5
Опис	Дія, що виконувалася, була скасаова (можливо, вона виконувалася занадто довго).
Усунення помилки: 1. Повторіть необхідну дію через знову.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*З'єднання IPC розірване*
Код помилки	x6
Опис	IPC-з'єднання з деяким компонентом Dr.Web для Linux розірване (швидше за все, компонент завершив свою роботу через простій або за командою користувача).
Усунення помилки: 1. Якщо операція, що виконувалася, не була завершена, то повторіть її запуск знову. В іншому випадку розрив з'єднання не є помилкою.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Недопустимий розмір повідомлення IPC*
Код помилки	x7
Опис	У процесі обміну даними між компонентами отримано повідомлення недопустимого розміру.

Усунення помилки:

1. Перезапустіть Dr.Web для Linux, виконавши команду:

```
# service drweb-configd restart
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустимий формат повідомлення IPC*
Код помилки	x8
Опис	У процесі обміну даними між компонентами отримано повідомлення недопустимого формату.

Усунення помилки:

1. Перезапустіть Dr.Web для Linux, виконавши команду:

```
# service drweb-configd restart
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Не готовий*
Код помилки	x9
Опис	Необхідна дія не може бути виконана, тому що запитаний компонент або пристрій ще не ініціалізовані.

Усунення помилки:

1. Повторіть необхідну дію через деякий час.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Компонент не встановлений*
Код помилки	x10
Опис	Деяка функція Dr.Web для Linux недоступна, оскільки компонент, що реалізує її, не встановлений.

Усунення помилки:

1. Виконайте окреме встановлення або перевстановлення пакета, що містить необхідний компонент:

- `drweb-filecheck`, якщо не встановлений Сканер.
- `drweb-spider`, якщо не встановлений SplDer Guard.
- `drweb-gated`, якщо не встановлений SplDer Gate.
- `drweb-update`, якщо не встановлений Компонент оновлення.

2. Якщо помилка повториться або якщо ви не можете визначити, який компонент відсутній, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Неочікуване повідомлення IPC*
Код помилки	`x11`
Опис	У процесі обміну даними між компонентами отримано недопустиме повідомлення.

Усунення помилки:

1. Перезапустіть Dr.Web для Linux, виконавши команду:

```
# service drweb-configd restart
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Порушення протоколу IPC*
Код помилки	`x12`
Опис	У процесі обміну даними між компонентами сталося порушення протоколу обміну даними.

Усунення помилки:

1. Перезапустіть Dr.Web для Linux, виконавши команду:

```
# service drweb-configd restart
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Невідомий стан підсистеми*
Код помилки	`x13`

Опис	Виявлено, що якась підсистема Dr.Web для Linux, необхідна для виконання операції, знаходиться в невідомому стані.

Усунення помилки:

1. Повторіть операцію.
2. При повторенні помилки перезапустіть Dr.Web для Linux, виконавши команду:

   ```
   # service drweb-configd restart
   ```

   після чого повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Шлях має бути абсолютним*
Код помилки	x20
Опис	Необхідний абсолютний (тобто такий, що починається від кореня файлової системи) шлях до файла або каталогу, а вказаний відносний шлях.

Усунення помилки:

1. Змініть шлях до файла або каталогу таким чином, щоб він був абсолютним, та повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недостатньо пам'яті для завершення операції*
Код помилки	x21
Опис	Для виконання необхідної операції не вистачає пам'яті (наприклад, спроба розпакувати занадто великий файл).

Усунення помилки:

1. Спробуйте збільшити об'єм пам'яті, доступної процесам Dr.Web для Linux (наприклад, змінивши ліміти за допомогою команди **ulimit**), перезапустіть його та повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Помилка введення-виведення*
Код помилки	x22

Опис	Сталася помилка введення-виведення (наприклад, дисковий пристрій ще не ініціалізований або розділ файлової системи більше недоступний).
Усунення помилки: 1. Перевірте доступність необхідного пристрою введення/виведення або розділу файлової системи. За необхідності змонтуйте його та повторіть операцію.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Немає такого файла або каталогу*
Код помилки	`x23`
Опис	Вказаний об'єкт файлової системи (файл або каталог) відсутній. Можливо, він був видалений.
Усунення помилки: 1. Перевірте правильність вказаного шляху. За необхідності виправте шлях та повторіть операцію.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Доступ заборонений*
Код помилки	`x24`
Опис	Недостатньо прав для доступу до вказаного об'єкта файлової системи (файла або каталогу).
Усунення помилки: 1. Перевірте правильність вказаного шляху та наявність необхідних прав у компонента. За необхідності змініть права доступу до нього або підвищіть права компонента та повторіть операцію.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Не каталог*
Код помилки	`x25`
Опис	Очікувався шлях до каталогу, проте вказаний об'єкт файлової системи не є каталогом.
Усунення помилки:	

1. Перевірте правильність вказаного шляху. Виправте шлях та повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Файл даних пошкоджений*
Код помилки	`x26`
Опис	Дані, до яких проводиться звернення, пошкоджені.

Усунення помилки:

1. Повторіть операцію.
2. При повторенні помилки перезапустіть Dr.Web для Linux, виконавши команду

   ```
   # service drweb-configd restart
   ```

   після чого повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Файл вже існує*
Код помилки	`x27`
Опис	При спробі створити файл було виявлено, що файл з таким іменем вже існує.

Усунення помилки:

1. Перевірте правильність вказаного шляху. Виправте шлях та повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Файлова система тільки для читання*
Код помилки	`x28`
Опис	При спробі створити або змінити об'єкт файлової системи (каталог, файл або сокет) було виявлено, що файлова система доступна тільки для читання.

Усунення помилки:

1. Перевірте правильність вказаного шляху. Виправте шлях так, щоб він вів на розділ файлової системи, доступної для запису, та повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Помилка мережі*
Код помилки	x29
Опис	Сталася мережна помилка (можливо, несподівано перестав відповідати віддалений вузол або не вдається встановити необхідне з'єднання).
Усунення помилки: 1. Перевірте доступність мережі та правильність мережних налаштувань. За необхідності виправте мережні налаштування та повторіть операцію.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Не дисковий пристрій*
Код помилки	x30
Опис	Спроба звернення до пристрою введення/виведення, що не є дисковим пристроєм.
Усунення помилки: 1. Перевірте правильність вказаного імені пристрою. Виправте шлях так, щоб він вів до дискового пристрою, та повторіть операцію.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Неочікуваний кінець файла*
Код помилки	x31
Опис	При читанні даних несподівано був досягнутий кінець файла.
Усунення помилки: 1. Перевірте правильність вказаного імені файла. Виправте шлях так, щоб він вів до правильного файла, та повторіть операцію.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Файл був змінений*
Код помилки	x32
Опис	При скануванні файла було виявлено, що він був змінений.

Усунення помилки:

1. Повторіть операцію сканування.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Спеціальний файл*
Код помилки	x33
Опис	При доступі до об'єкта файлової системи було виявлено, що це не регулярний файл (це каталог, сокет або інший об'єкт файлової системи).

Усунення помилки:

1. Перевірте правильність вказаного імені файла. Виправте шлях так, щоб він вів до регулярного файла, та повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Ім'я вже використовується*
Код помилки	x34
Опис	При спробі створити об'єкт файлової системи (каталог, файл або сокет) було виявлено, що об'єкт з таким іменем вже існує.

Усунення помилки:

1. Перевірте правильність вказаного шляху. Виправте шлях та повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Хост відключений*
Код помилки	x35
Опис	Виявлено, що віддалений вузол недоступний по мережі.

Усунення помилки:

1. Перевірте доступність необхідного вузла мережі. За необхідності виправте адресу вузла та повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Досягнуто межі використання ресурсу*
Код помилки	x36
Опис	Досягнуто межі використання якогось ресурсу.
Усунення помилки: 1. Перевірте доступність необхідного ресурсу. За необхідності збільшіть ліміт на використання ресурсу та повторіть операцію.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Різні точки монтування*
Код помилки	x37
Опис	Проводиться спроба відновлення файла, що потребує його переміщення між каталогами файлової системи з різними точкам монтування.
Усунення помилки: 1. Виберіть інший шлях для відновлення файла та повторіть операцію.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Помилка розпакування*
Код помилки	x38
Опис	Не вдалося розпакувати архів (можливо, він захищений паролем або пошкоджений)
Усунення помилки: 1. Переконайтеся, що файл не пошкоджений. Якщо архів захищений паролем, зніміть захист, вказавши правильний пароль, та повторіть операцію.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Вірусна база пошкоджена*
Код помилки	x40
Опис	Пошкоджені вірусні бази.

Усунення помилки:

1. Перевірте правильність шляху до каталогу вірусних баз та за необхідності виправте його (параметр **`VirusBaseDir`** в секції `[Root]` файла конфігурації).

   Для перегляду та виправлення шляху скористайтеся командами утиліти управління з командного рядка:

   - Щоб переглянути поточне значення параметра, введіть команду:

     ```
     $ drweb-ctl cfshow Root.VirusBaseDir
     ```

   - Щоб встановити нове значення параметра, введіть команду:

     ```
     # drweb-ctl cfset Root.VirusBaseDir <новий шлях>
     ```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

     ```
     # drweb-ctl cfset Root.VirusBaseDir -r
     ```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

     ```
     $ drweb-ctl update
     ```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Непідтримувана версія вірусних баз*
Код помилки	`x41`
Опис	Наявні вірусні бази призначені для старої версії програми.

Усунення помилки:

1. Перевірте правильність шляху до каталогу вірусних баз та за необхідності виправте його (параметр **`VirusBaseDir`** в секції `[Root]` файла конфігурації).

   Для перегляду та виправлення шляху скористайтеся командами утиліти управління з командного рядка:

   - Щоб переглянути поточне значення параметра, введіть команду:

     ```
     $ drweb-ctl cfshow Root.VirusBaseDir
     ```

   - Щоб встановити нове значення параметра, введіть команду:

     ```
     # drweb-ctl cfset Root.VirusBaseDir <новий шлях>
     ```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Вірусна база порожня*
Код помилки	x42
Опис	Порожні вірусні бази.

Усунення помилки:

1. Перевірте правильність шляху до каталогу вірусних баз та за необхідності виправте його (параметр **VirusBaseDir** в секції [Root] файла конфігурації).

   Для перегляду та виправлення шляху скористайтеся командами утиліти управління з командного рядка:
   - Щоб переглянути поточне значення параметра, введіть команду:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

   - Щоб встановити нове значення параметра, введіть команду:

```
# drweb-ctl cfset Root.VirusBaseDir <новий шлях>
```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Об'єкт не може бути зцілений*
Код помилки	`x43`
Опис	Спроба застосувати дію «Лікувати» до невиліковного об'єкта при нейтралізації загрози.

Усунення помилки:

1. Виберіть дію, допустиму для даного об'єкта, та повторіть операцію.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Непідтримувана комбінація вірусних баз*
Код помилки	`x44`
Опис	Наявний набір вірусних баз несумісний.

Усунення помилки:

1. Перевірте правильність шляху до каталогу вірусних баз та за необхідності виправте його (параметр **`VirusBaseDir`** в секції `[Root]` файла конфігурації).

   Для перегляду та виправлення шляху скористайтеся командами утиліти управління з командного рядка:

   - Щоб переглянути поточне значення параметра, введіть команду:

     ```
     $ drweb-ctl cfshow Root.VirusBaseDir
     ```

   - Щоб встановити нове значення параметра, введіть команду:

     ```
     # drweb-ctl cfset Root.VirusBaseDir <новий шлях>
     ```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

     ```
     # drweb-ctl cfset Root.VirusBaseDir -r
     ```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

     ```
     $ drweb-ctl update
     ```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Досягнуто межі перевірки*
Код помилки	`x45`
Опис	При скануванні об'єкта перевищені задані обмеження (наприклад, на розмір розпакованого файла, на глибину рівнів вкладень тощо).
Усунення помилки: 1. Змініть обмеження для сканування об'єктів (в налаштуваннях відповідного компонента) в будь-який спосіб: • За допомогою сторінки налаштувань цього компонента у вікні управління налаштуваннями програми. • За допомогою команд **drweb-ctl** `cfshow` та **drweb-ctl** `cfset`. 2. Після змінення налаштувань повторіть операцію.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Невірні облікові дані користувача*
Код помилки	`x47`
Опис	Спроба пройти аутентифікацію з невірними обліковими даними користувача.
Усунення помилки: 1. Повторіть спробу аутентифікації, вказавши правильні облікові дані користувача з необхідними повноваженнями.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Користувач не має необхідних прав*
Код помилки	`x48`
Опис	Спроба пройти аутентифікацію з обліковими даними користувача, який не має необхідних прав.
Усунення помилки: 1. Повторіть спробу аутентифікації, вказавши правильні облікові дані користувача з необхідними повноваженнями.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Недопустимий токен доступу*
Код помилки	`x49`
Опис	Компонент Dr.Web для Linux надав некоректний токен авторизації при спробі отримання доступу до операції, що потребує підвищені права.
Усунення помилки: 1. Пройдіть аутентифікацію, вказавши правильні облікові дані користувача з необхідними повноваженнями.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Недопустимий аргумент*
Код помилки	`x60`
Опис	При спробі виконати команду був вказаний недопустимий аргумент.
Усунення помилки: 1. Повторіть потрібну дію знову, вказавши допустимий аргумент.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Недопустима операція*
Код помилки	`x61`
Опис	Спроба виконати недопустиму команду.
Усунення помилки: 1. Повторіть потрібну дію знову, вказавши допустиму команду.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Необхідні повноваження суперкористувача*
Код помилки	`x62`
Опис	Необхідна дія може бути виконана тільки користувачем з повноваженнями суперкористувача.
Усунення помилки:	

1. Підвищіть свої права до суперкористувача та повторіть необхідну дію знову. Для підвищення прав ви можете скористатися командами **su** та **sudo**.
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Не дозволено в режимі централізованого захисту*
Код помилки	`x63`
Опис	Необхідна дія може бути виконана тільки при роботі Dr.Web для Linux в одиночному (standalone) режимі.
Усунення помилки: 1. Переведіть Dr.Web для Linux в одиночний режим та повторіть операцію знову. 2. Для цього: • Скиньте прапорець **Включити режим централізованого захисту** на сторінці налаштувань **Режим**. • Або виконайте команду: `# drweb-ctl esdisconnect`	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Непідтримувана ОС*
Код помилки	`x64`
Опис	Операційна система, встановлена на вузлі, не підтримується Dr.Web для Linux.
Усунення помилки: 1. Встановіть операційну систему зі списку, вказаного в системних вимогах.	
Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.	

Повідомлення про помилку	*Функція не реалізована*
Код помилки	`x65`
Опис	Спроби використання функцій якогось компонента, що не реалізовані в поточній версії.
Усунення помилки:	

1. Скиньте налаштування Dr.Web для Linux в значення за замовчуванням, очистивши вміст файла конфігурації `/etc/opt/drweb.com/drweb.ini`. Рекомендується попередньо створити резервну копію файла. Наприклад:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

2. Після очищення файла конфігурації Dr.Web для Linux, виконавши команду:

```
# service drweb-configd restart
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Невідомий параметр*
Код помилки	`x66`
Опис	Файл конфігурації містить параметри, невідомі або непідтримувані в поточній версії Dr.Web для Linux.

Усунення помилки:

1. Відкрийте файл `/etc/opt/drweb.com/drweb.ini` в будь-якому текстовому редакторі, видаліть рядок, що містить недопустимий параметр, збережіть файл та перезапустіть Dr.Web для Linux, виконавши команду:

```
# service drweb-configd restart
```

2. Якщо це не допоможе, спробуйте скинути налаштування Dr.Web для Linux в значення за замовчуванням.

   Для цього очистіть вміст файла `/etc/opt/drweb.com/drweb.ini` (при цьому рекомендується створити резервну копію файла конфігурації), наприклад, виконавши команди:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   Після очищення файла конфігурації перезапустіть Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Невідома секція*
Код помилки	`x67`
Опис	Файл конфігурації містить секції, невідомі або непідтримувані в поточній версії Dr.Web для Linux.

Усунення помилки:

1. Відкрийте файл `/etc/opt/drweb.com/drweb.ini` в будь-якому текстовому редакторі та видаліть невідому секцію, після чого збережіть файл та перезапустіть Dr.Web для Linux, виконавши команду:

   ```
   # service drweb-configd restart
   ```

2. Якщо це не допоможе, спробуйте скинути налаштування Dr.Web для Linux в значення за замовчуванням.

   Для цього очистіть вміст файла `/etc/opt/drweb.com/drweb.ini` (при цьому рекомендується створити резервну копію файла конфігурації), наприклад, виконавши команди:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Після очищення файла конфігурації перезапустіть Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустиме значення параметра*
Код помилки	`x68`
Опис	Якийсь параметр в файлі конфігурації має недопустиме для цього параметра значення.

Усунення помилки:

1. Змініть значення параметра в будь-який спосіб:
   - За допомогою сторінки налаштувань цього компонента у вікні управління налаштуваннями програми.
   - За допомогою команд **drweb-ctl** `cfshow` та **drweb-ctl** `cfset`.

   Якщо ви не знаєте, яке саме значення параметра допустиме, зверніться до довідки компонента, що використовує даний параметр, або спробуйте скинути значення цього параметра в значення за замовчуванням.
2. Також ви можете відредагувати безпосередньо файл конфігурації `/etc/opt/drweb.com/drweb.ini`. Для цього відкрийте його в будь-якому текстовому редакторі, знайдіть рядок, що містить недопустиме значення параметра, задайте допустиме значення, збережіть файл та перезапустіть Dr.Web для Linux, виконавши команду:

   ```
   # service drweb-configd restart
   ```

3. Якщо попередні кроки не допомогли, спробуйте скинути налаштування Dr.Web для Linux в значення за замовчуванням.

   Для цього очистіть вміст файла `/etc/opt/drweb.com/drweb.ini` (при цьому рекомендується створити резервну копію файла конфігурації), наприклад, виконавши команди:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Після очищення файла конфігурації перезапустіть Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустимий стан*
Код помилки	`x69`
Опис	Якийсь компонент або весь Dr.Web для Linux знаходяться в недопустимому стані для виконання запитаної операції.

Усунення помилки:

1. Повторіть необхідну дію через деякий час.
2. При повторенні помилки перезапустіть Dr.Web для Linux, виконавши команду:

```
# service drweb-configd restart
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Дозволене тільки одне значення*
Код помилки	`x70`
Опис	Якийсь параметр в файлі конфігурації має список значень, що недопустимо для цього параметра.

Усунення помилки:

1. Змініть значення параметра в будь-який спосіб:
   - За допомогою сторінки налаштувань цього компонента у вікні управління налаштуваннями програми.
   - За допомогою команд **drweb-ctl** `cfshow` та **drweb-ctl** `cfset`.

   Якщо ви не знаєте, яке саме значення параметра допустиме, зверніться до довідки компонента, що використовує даний параметр, або спробуйте скинути значення цього параметра в значення за замовчуванням.
2. Також ви можете відредагувати безпосередньо файл конфігурації `/etc/opt/drweb.com/drweb.ini`. Для цього відкрийте його в будь-якому текстовому редакторі, знайдіть рядок, що містить недопустиме значення параметра, задайте допустиме значення, збережіть файл та перезапустіть Dr.Web для Linux, виконавши команду:

```
# service drweb-configd restart
```

3. Якщо попередні кроки не допомогли, спробуйте скинути налаштування Dr.Web для Linux в значення за замовчуванням.

   Для цього очистіть вміст файла `/etc/opt/drweb.com/drweb.ini` (при цьому рекомендується створити резервну копію файла конфігурації), наприклад, виконавши команди:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

Після очищення файла конфігурації перезапустіть Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустиме ім'я тегу*
Код помилки	x71
Опис	Якась секція в файлі конфігурації, ім'я якої містить унікальний ідентифікатор-тег, має недопустиме значення тегу.

Усунення помилки:

1. Якщо помилка сталася при використанні команди

   ```
   # drweb-ctl cfset <секція>.<параметр> <нове значення>
   ```

   то повторіть збереження, задавши для тегу допустиме значення.
2. Якщо секція збережена безпосередньо файл конфігурації `/etc/opt/drweb.com/drweb.ini`, то відредагуйте його. Для цього відкрийте його в будь-якому текстовому редакторі, знайдіть заголовок секції, що містить недопустиме значення тегу, задайте допустиме значення, збережіть файл та перезапустіть Dr.Web для Linux, виконавши команду:

   ```
   # service drweb-configd restart
   ```
3. Якщо попередні кроки не допомогли, спробуйте скинути налаштування Dr.Web для Linux в значення за замовчуванням.

   Для цього очистіть вміст файла `/etc/opt/drweb.com/drweb.ini` (при цьому рекомендується створити резервну копію файла конфігурації), наприклад, виконавши команди:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Після очищення файла конфігурації перезапустіть Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Запис не знайдений*
Код помилки	x80
Опис	При спробі звернутися до інформації про виявлену загрозу було виявлено, що інформація про неї відсутня (можливо, загроза вже була опрацьована іншим компонентом Dr.Web для Linux).

Усунення помилки:

1. Оновіть список загроз через деякий час.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Запис опрацьовується в даний момент*
Код помилки	`x81`
Опис	При спробі звернутися до інформації про виявлену загрозу було виявлено, що даний момент часу загроза опрацьовується іншим компонентом Dr.Web для Linux.

Усунення помилки:

1. Оновіть список загроз через деякий час.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Файл вже знаходиться в карантині*
Код помилки	`x82`
Опис	При спробі переміщення файла з виявленою загрозою до карантину було виявлено, що він вже в карантині (швидше за все, загроза вже була опрацьована іншим компонентом Dr.Web для Linux).

Усунення помилки:

1. Оновіть список загроз через деякий час.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Не вдалося зберегти резервну копію перед оновленням*
Код помилки	`x89`
Опис	Перед початком завантаження оновлень з сервера оновлень не вдалося зберегти резервну копію оновлюваних файлів.

Усунення помилки:

1. Перевірте правильність шляху до каталогу, що містить резервні копії оновлюваних файлів та за необхідності виправте його (параметр **`BackupDir`** в секції `[Update]` файла конфігурації).

   Для перегляду та виправлення шляху скористайтеся командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду:

```
$ drweb-ctl cfshow Update.BackupDir
```

- Щоб встановити нове значення параметра, введіть команду:

```
# drweb-ctl cfset Update.BackupDir <новий шлях>
```

- Щоб скинути параметри в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset Update.BackupDir -r
```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

3. Якщо помилка повториться, перевірте, що користувач, від імені якого запущений Компонент оновлення, має права на запис до каталогу, вказаного в параметрі **BackupDir**. Ім'я користувача вказане в параметрі **RunAsUser**. За необхідності змініть ім'я користувача, змінивши значення параметра **RunAsUser**, або надайте відсутні права у властивостях каталогу.
4. Якщо помилка повториться, спробуйте перевстановити пакет `drweb-update`.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустимий DRL-файл*
Код помилки	x90
Опис	Порушена структура одного з файлів списків серверів оновлень.

Усунення помилки:

1. Перевірте правильність шляху до файла списку серверів та за необхідності виправте його (параметри з іменем виду ***DrlDir** в секції `[Update]` файла конфігурації. Для цього скористайтеся командами утиліти управління з командного рядка).
   - Щоб переглянути поточне значення параметра, введіть команду (<**DrlDir*> необхідно замінити на ім'я конкретного параметра. Якщо ім'я параметра невідоме, перегляньте значення всіх параметрів в секції, опустивши частину команди, укладену в квадратні дужки):

```
$ drweb-ctl cfshow Update[.<*DrlDir>]
```

   - Щоб встановити нове значення параметра, введіть команду (<**DrlDir*> необхідно замінити на ім'я конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> <новий шлях>
```

- Щоб скинути значення параметра в значення за замовчуванням, введіть команду (<*DrlDir> необхідно замінити на ім'я конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> -r
```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

3. Якщо помилка повториться, встановіть або перевстановіть пакети `drweb-bases` та `drweb-dws`, після чого проведіть оновлення.
4. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустимий LST-файл*
Код помилки	`x91`
Опис	Порушена структура файла, що містить список оновлюваних вірусних баз.

Усунення помилки:

1. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

2. Якщо помилка повториться, спробуйте перевстановити пакет `drweb-update`.
3. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустимий стиснений файл*
Код помилки	x92
Опис	Порушена структура файла, що містить список оновлюваних вірусних баз.

Усунення помилки:

1. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Помилка аутентифікації на проксі-сервері*
Код помилки	x93
Опис	Не вдалося підключитися до серверів оновлень через прокси-сервер, заданий в налаштуваннях.

Усунення помилки:

1. Перевірте правильність параметрів підключення до проксі-сервера (задаються в параметрі з іменем **Proxy** в секції [Update] файла конфігурації). За необхідності змініть використовуваний проксі-сервер або відомовтеся від використання проксі-сервера.

   Щоб переглянути та задати параметри підключення, перейдіть на сторінку основних налаштувань.

   Також ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду:

```
$ drweb-ctl cfshow Update.Proxy
```

   - Щоб встановити нове значення параметра, введіть команду:

```
# drweb-ctl cfset Update.Proxy <нові параметри>
```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset Update.Proxy -r
```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Немає доступних серверів оновлень*
Код помилки	x94
Опис	Не вдалося підключитися до жодного сервера оновлень.

Усунення помилки:

1. Перевірте доступність мережі та за необхідності виправте мережні налаштування.
2. Якщо доступ до мережі можливий тільки через проксі-сервер, задайте параметри підключення до проксі-сервера (визначаються в параметрі з іменем **Proxy** в секції [Update] файла конфігурації). За необхідності змініть використовуваний проксі-сервер або відомовтеся від використання проксі-сервера.

   Щоб переглянути та задати параметри підключення, перейдіть на сторінку основних налаштувань.

   Також ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду:

```
$ drweb-ctl cfshow Update.Proxy
```

   - Щоб встановити нове значення параметра, введіть команду:

```
# drweb-ctl cfset Update.Proxy <нові параметри>
```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset Update.Proxy -r
```

3. Якщо параметри мережного підключення (у тому числі — використовуваного проксі-сервера) правильні, а помилка виникає, переконайтеся у тому, що ви використовуєте доступний список серверів оновлення. Список використовуваних серверів оновлення вказується в параметрах виду ***DrlDir** в секції [Update] файла конфігурації. Зверніть увагу, що якщо параметри виду ***CustomDrlDir** вказують на існуючий коректний файл списку серверів, то вказані там сервери використовуватимуться замість серверів стандартної зони оновлення (значення, вказане у відповідному параметрі ***DrlDir**, ігнорується).

Щоб переглянути та задати параметри підключення, ви можете скористатися командами утиліти управління з командного рядка.

Щоб переглянути поточне значення параметра, введіть команду (<*DrlDir> необхідно замінити на ім'я конкретного параметра. Якщо ім'я параметра невідоме, перегляньте значення всіх параметрів в секції, опустивши частину команди, укладену в квадратні дужки):

```
$ drweb-ctl cfshow Update[.<*DrlDir>]
```

Щоб встановити нове значення параметра, введіть команду (<*DrlDir> необхідно замінити на ім'я конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> <новий шлях>
```

Щоб скинути значення параметра в значення за замовчуванням, введіть команду (<*DrlDir> необхідно замінити на ім'я конкретного параметра):

```
# drweb-ctl cfset Update.<*DrlDir> -r
```

4. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустимий формат ключового файла*
Код помилки	x95
Опис	Порушений формат ключевого файла.

Усунення помилки:

1. Перевірте наявність ключового файла та правильність шляху до нього. Шлях до ключового файла задається в параметрі **KeyPath** в секції [Root] файла конфігурації.

   Щоб переглянути параметри ліцензії та задати шлях до ключового файла, перейдіть на сторінку Менеджера ліцензій головного вікна програми.

   Також ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду:

```
$ drweb-ctl cfshow Root.KeyPath
```

   - Щоб встановити нове значення параметра, введіть команду:

```
# drweb-ctl cfset Root.KeyPath <шлях до файла>
```

- Щоб скинути параметри в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset Root.KeyPath -r
```

2. Якщо у вас відсутній ключовий файл або використовуваний ключовий файл пошкоджений, придбайте та встановіть його. Опис ключового файла, способи придбання та встановлення наведені у розділі Ліцензування.
3. Щоб встановити наявний у вас ключовий файл, ви можете скористатися Менеджером ліцензій.
4. Параметри поточної ліцензії ви також можете переглянути в особистому кабінеті **Мій Dr.Web** за посиланням https://support.drweb.com/get+cabinet+link/.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Термін дії ліцензії завершився*
Код помилки	x96
Опис	Термін дії наявної у вас ліцензії завершився.

Усунення помилки:

1. Придбайте нову ліцензію та встановіть отриманий ключовий файл. Способи придбання ліцензії та встановлення ключового файла описані у розділі Ліцензування.
2. Щоб встановити придбаний ключовий файл, ви можете скористатися Менеджером ліцензій.
3. Параметри поточної ліцензії ви також можете переглянути в особистому кабінеті **Мій Dr.Web** за посиланням https://support.drweb.com/get+cabinet+link/.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Минув тайм-аут мережної операції*
Код помилки	x97
Опис	

Усунення помилки:

1. Перевірте доступність мережі та правильність мережних налаштувань. За необхідності виправте мережні налаштування та повторіть операцію.
2. Якщо помилка виникає при отриманні оновлень, то додатково перевірте параметри використання проксі-сервера, за необхідності змініть використовуваний проксі-сервер або відмовтеся від його використання.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустима контрольна сума*

Код помилки	`x98`
Опис	Порушена контрольна сума завантаженого файла, що містить оновлення.

Усунення помилки:

1. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустимий демонстраційний ключовий файл*
Код помилки	`x99`
Опис	Використовуваний демонстраційний ключовий файл недійсний (наприклад, він був отриманий для іншого комп'ютера).

Усунення помилки:

1. Запитайте новий демонстраційний період для даного комп'ютера або придбайте нову ліцензію та встановіть отриманий ключовий файл. Способи придбання ліцензії та встановлення ключового файла описані у розділі Ліцензування.
2. Щоб встановити придбаний ключовий файл, ви можете скористатися Менеджером ліцензій.
3. Параметри поточної ліцензії ви також можете переглянути в особистому кабінеті **Мій Dr.Web** за посиланням https://support.drweb.com/get+cabinet+link/.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Ліцензійний ключовий файл заблокований*
Код помилки	`x100`
Опис	Використовувана вами ліцензія була заблокована (можливо, порушені умови ліцензійної угоди на використання Dr.Web для Linux).

Усунення помилки:

1. Придбайте нову ліцензію та встановіть отриманий ключовий файл. Способи придбання ліцензії та встановлення ключового файла описані у розділі Ліцензування.
2. Щоб встановити придбаний ключовий файл, ви можете скористатися Менеджером ліцензій.

3. Параметри поточної ліцензії ви також можете переглянути в особистому кабінеті **Мій Dr.Web** за посиланням https://support.drweb.com/get+cabinet+link/.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустима ліцензія*
Код помилки	`x101`
Опис	Використовувана вами ліцензія призначена для іншого продукту Dr.Web або не містить необхідних дозволів для роботи компонентів Dr.Web для Linux.

Усунення помилки:

1. Придбайте нову ліцензію та встановіть отриманий ключовий файл. Способи придбання ліцензії та встановлення ключового файла описані у розділі Ліцензування.
2. Щоб встановити придбаний ключовий файл, ви можете скористатися Менеджером ліцензій.
3. Параметри поточної ліцензії ви також можете переглянути в особистому кабінеті **Мій Dr.Web** за посиланням https://support.drweb.com/get+cabinet+link/.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустима конфігурація*
Код помилки	`x102`
Опис	Деякий компонент Dr.Web для Linux не може функціонувати через неправильні налаштування конфігурації.

Усунення помилки:

1. Якщо ім'я компонента, що спричинив помилку, невідоме, спробуйте його визначити, ознайомившись з журналом.
2. Якщо помилка викликана компонентом SplDer Guard, то, швидше за все, заданий спосіб роботи компонента, що не підтримується операційною системою. Перевірте встановлений режим роботи компонента та за необхідності виправте його, вказавши значення `AUTO` (параметр **Mode** в секції `[LinuxSpider]` файла конфігурації).

   Щоб переглянути та виправити режим роботи, ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб встановити значення `AUTO`, введіть команду

   ```
   # drweb-ctl cfset LinuxSpider.Mode AUTO
   ```

   - Щоб скинути значення параметра в значення за замовчуванням, введіть команду:

   ```
   # drweb-ctl cfset LinuxSpider.Mode -r
   ```

Якщо помилка повториться, виконайте ручну збірку та встановлення завантажуваного модуля ядра для компонента SpIDer Guard.

Зверніть увагу, що робота компонента SpIDer Guard та завантажуваного модуля ядра гарантується, якщо використовувана вами ОС входить до списку протестованих дистрибутивів **Linux** (див. розділ Системні вимоги та сумісність).

3. Якщо помилка викликана компонентомSpIDer Gate, то, швидше за все, є конфлікт з іншим міжмережним екраном. Наприклад, відомо, що SpIDer Gate конфліктує з міжмережним екраном **FirewallD** в ОС **Fedora**, **CentOS**, **Red Hat Enterprise Linux** (при кожному перезапуску **FirewallD** пошкоджує правила маршрутизації трафіку, задані SpIDer Gate). Щоб усунути помилки, перезавантажте Dr.Web для Linux, виконавши команду

   ```
   # service drweb-configd restart
   ```

   або

   ```
   # drweb-ctl reload
   ```

   Зверніть увагу, що якщо не заборонити роботу **FirewallD**, вказана помилка SpIDer Gate може повторюватися при кожному перезапуску **FirewallD**, у тому числі — при перезапуску ОС. Ви можете усунути дану помилку, відключивши **FirewallD** (зверніться до посібника **FirewallD** у складі посібника з вашої ОС).

4. Якщо помилка спричинена іншим компонентом, то спробуйте скинути налаштування компонента в значення за замовчування в будь-який спосіб:
   - За допомогою команд **drweb-ctl** `cfshow` та **drweb-ctl** `cfset`.
   - Відредагувавши вручну файл конфігурації, видаливши всі параметри з секції компонента.
5. Якщо попередні кроки не допомогли, спробуйте скинути налаштування Dr.Web для Linux в значення за замовчуванням.

   Для цього очистіть вміст файла `/etc/opt/drweb.com/drweb.ini` (при цьому рекомендується створити резервну копію файла конфігурації), наприклад, виконавши команди:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Після очищення файла конфігурації перезапустіть Dr.Web для Linux, виконавши команду:

   ```
   # service drweb-configd restart
   ```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустимий виконуваний файл*
Код помилки	x104

Опис	Не запускається якийсь компонент Dr.Web для Linux, через те, що невірно вказаний шлях до його виконуваного файла або вміст файла пошкоджений.

Усунення помилки:

1. Якщо ім'я компонента, що спричинив помилку, невідоме, спробуйте його визначити, ознайомившись з журналом.
2. Перевірте значення шляху до виконуваного файла компонента в конфігурації Dr.Web для Linux (параметр **ExePath** в секції компонента), виконавши команду (замініть *<секція компонента>* на назву відповідної секції файла конфігурації)

   ```
   $ drweb-ctl cfshow <секція компонента>.ExePath
   ```

3. Спробуйте скинути шлях в значення за замовчуванням, виконавши команду (замініть *<секція компонента>* на назву відповідної секції файла конфігурації)

   ```
   # drweb-ctl cfset <секція компонента>.ExePath -r
   ```

4. Якщо попередні кроки не допомогли, спробуйте встановити пакет відповідного компонента.
   - `drweb-filecheck`, якщо пошкоджений виконуваний файл компонента Сканер.
   - `drweb-spider`, якщо пошкоджений виконуваний файл SpIDer Guard.
   - `drweb-spider`, якщо пошкоджений виконуваний файл SpIDer Gate.
   - `drweb-spider`, якщо пошкоджений виконуваний файл Компонента оновлення.
5. Якщо помилка повториться, або якщо ви не можете визначити, виконуваний файл якого компонента пошкоджений, видаліть продукт Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Ядро Virus-Finding Engine недоступне*
Код помилки	`x105`
Опис	Відсутній або недоступний файл антивірусного ядра Dr.Web Virus-Finding Engine (необхідний для пошуку загроз).

Усунення помилки:

1. Перевірте правильність шляху до файлу антивірусного ядра **drweb32.dll** та за необхідності виправте його (параметр **CoreEnginePath** в секції `[Root]` файла конфігурації).

   Для перегляду та виправлення шляху скористайтеся командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду

```
$ drweb-ctl cfshow Root.CoreEnginePath
```

- Щоб встановити нове значення параметра, введіть команду

```
# drweb-ctl cfset Root.CoreEnginePath <новий шлях>
```

- Щоб скинути значення параметра в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset Root.CoreEnginePath -r
```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

3. Якщо шлях правильний та помилка повториться після оновлення вірусних баз, перевстановіть пакет `drweb-bases`.
4. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Вірусні бази відсутні*
Код помилки	`x106`
Опис	Вірусні бази відсутні.

Усунення помилки:

1. Перевірте правильність шляху до каталогу вірусних баз та за необхідності виправте його (параметр **`VirusBaseDir`** в секції `[Root]` файла конфігурації).

   Для перегляду та виправлення шляху скористайтеся командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

   - Щоб встановити нове значення параметра, введіть команду

```
# drweb-ctl cfset Root.VirusBaseDir <новий шлях>
```

   - Щоб скинути значення параметра в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

3. Якщо помилка повториться, проведіть окреме встановлення або перевстановлення пакета `drweb-bases`, що містить антивірусне ядро та вірусні бази.
4. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Процес завершений за сигналом*
Код помилки	`x107`
Опис	Компонент завершив свою роботу (можливо, через простій або внаслідок команди користувача).

Усунення помилки:

1. Якщо операція, що виконувалася, не була завершена, то повторіть її запуск знову. В іншому випадку завершення роботи не є помилкою.
2. Якщо компонент постійно завершує свою роботу, спробуйте скинути налаштування компонента в значення за замовчування в будь-який спосіб:
   - За допомогою команд **drweb-ctl** `cfshow` та **drweb-ctl** `cfset`.
   - Відредагувавши вручну файл конфігурації, видаливши всі параметри з секції компонента.
3. Якщо це не допомогло, спробуйте скинути налаштування Dr.Web для Linux в значення за замовчуванням.

   Для цього очистіть вміст файла `/etc/opt/drweb.com/drweb.ini` (при цьому рекомендується створити резервну копію файла конфігурації), наприклад, виконавши команди:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

   Після очищення файла конфігурації Dr.Web для Linux, виконавши команду:

```
# service drweb-configd restart
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Непередбачуване завершення процесу*
Код помилки	`x108`
Опис	Компонент неочікувано завершив свою роботу через збій.

Усунення помилки:

1. Спробуйте повторити операцію, що виконувалася.
2. Якщо компонент постійно аварійно завершує свою роботу, спробуйте скинути налаштування компонента в значення за замовчування в будь-який спосіб:
   - За допомогою команд **drweb-ctl** `cfshow` та **drweb-ctl** `cfset`.
   - Відредагувавши вручну файл конфігурації, видаливши всі параметри з секції компонента.
3. Якщо це не допомогло, спробуйте скинути налаштування Dr.Web для Linux в значення за замовчуванням.

   Для цього очистіть вміст файла `/etc/opt/drweb.com/drweb.ini` (при цьому рекомендується створити резервну копію файла конфігурації), наприклад, виконавши команди:

   ```
   # cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
   # echo "" > /etc/opt/drweb.com/drweb.ini
   ```

   Після очищення файла конфігурації Dr.Web для Linux, виконавши команду:

   ```
   # service drweb-configd restart
   ```
4. Якщо помилка повториться після скидання налаштувань Dr.Web для Linux, спробуйте перевстановити пакет компонента.
5. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Виявлене несумісне ПЗ*
Код помилки	`x109`
Опис	Компонент Dr.Web для Linux не може функціонувати, оскільки виявлено програмне забезпечення, що перешкоджає його коректній роботі.

Усунення помилки:

1. Якщо помилка спричинена компонентом SpIDer Gate, то, швидше за все, проблема в тому, що в системі наявне програмне забезпечення, яке формує для системного міжмережного екрана **NetFilter** правила, що перешкоджають коректній роботі SpIDer Gate. Наприклад, це може бути **Shorewall** або **SuseFirewall2** (в ОС **SUSE Linux**). Основна причина конфлікту SpIDer Gate з іншими програмами, що налаштовують системний міжмережний екран **NetFilter**, в тому, що

вони періодично проводять перевірку цілісності заданої ними системи правил та перезаписують її.

Налаштуйте конфліктуюче програмне забезпечення таким чином, щоб воно не заважало роботі SpIDer Gate. Якщо не вдається налаштувати конфліктну програму таким чином, щоб воно не заважало роботі SpIDer Gate, відключіть цю програму з забороною її запуску при подальших завантаженнях ОС. Програму **SuseFirewall2** (в ОС **SUSE Linux**) можна спробувати налаштувати в такий спосіб:

1) Відкрийте файл конфігурації **SuseFirewall2** (за замовчуванням це файл `/etc/sysconfig/SuSEfirewall2`).
2) Знайдіть в файлі блок тексту:

```
# Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

3) Встановіть значення параметра в `"no"`:

```
FW_LO_NOTRACK="no"
```

4) Перезапустіть **SuseFirewall2**, виконавши команду:

```
# rcSuSEfirewall2 restart
```

> Зверніть увагу, що якщо в налаштуваннях **SuseFirewall2** параметр `FW_LO_NOTRACK` відсутній, то для усунення конфлікту необхідно відключити програму з забороною її запуска при подальших завантаженнях ОС (наприклад, це необхідно зробити в ОС **SUSE Linux Enterprise Server** 11).

5) Після змінення налаштувань або відключення конфліктної програми перезапустіть SpIDer Gate (відключіть, а потім включіть його на відповідній сторінці).

2. Якщо помилка спричинена іншим компонентом, то відключіть або переналаштуйте конфліктне програмне забезпечення таким чином, щоб воно не заважало роботі Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недопустима бібліотека VadeRetro*
Код помилки	`x110`
Опис	Відсутній, недоступний або пошкоджений файл антиспам-бібліотеки **VadeRetro** (необхідний при перевірці електронної пошти).

Усунення помилки:

1. Перевірте правильність шляху до файла библиотеки **vaderetro.so** та за необхідності виправте його (параметр **`VaderetroLibPath`** в секції `[Root]` файла конфігурації).

   Для перегляду та виправлення шляху скористайтеся командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду

   ```
   $ drweb-ctl cfshow Root.VaderetroLibPath
   ```

   - Щоб встановити нове значення параметра, введіть команду

   ```
   # drweb-ctl cfset Root.VaderetroLibPath <новий шлях>
   ```

   - Щоб скинути значення параметра в значення за замовчуванням, введіть команду:

   ```
   # drweb-ctl cfset Root.VaderetroLibPath -r
   ```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

   ```
   $ drweb-ctl update
   ```

3. Якщо шлях правильний та помилка повториться після оновлення вірусних баз, перевстановіть пакет `drweb-maild`.
4. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Бази категорій веб-ресурсів відсутні*
Код помилки	`x112`
Опис	Бази категорій веб-ресурсів відсутні.

Усунення помилки:

1. Перевірте правильність шляху до каталогу баз даних категорій веб-ресурсів та за необхідності виправте його (параметр **`DwsDir`** в секції `[Root]` файла конфігурації).
   - Для перегляду та виправлення шляху скористайтеся командами утиліти управління з командного рядка.

   Щоб переглянути поточне значення параметра, введіть команду

```
$ drweb-ctl cfshow Root.DwsDir
```

Щоб встановити нове значення параметра, введіть команду

```
# drweb-ctl cfset Root.DwsDir <новий шлях>
```

Щоб скинути значення параметра в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset Root.DwsDir -r
```

2. Оновіть вірусні бази в будь-який указаний нижче спосіб:
   - Натисніть **Оновити** на сторінці управління оновленнями головного вікна програми.
   - Виберіть пункт **Оновити** в контекстному меню індикатор програми в області сповіщень робочого столу.
   - Виконайте команду:

```
$ drweb-ctl update
```

3. Якщо помилка повториться, проведіть окреме встановлення або перевстановлення пакета `drweb-dws`, що містить бази категорій веб-ресурсів.
4. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Недоступний модуль ядра Linux для SplDer Guard*
Код помилки	`x113`
Опис	SplDer Guard для роботи необхідний модуль ядра **Linux**, який відсутній.

Усунення помилки:

1. Перевірте встановлений режим роботи компонента та за необхідності виправте його, вказавши значення `AUTO` (параметр **Mode** в секції `[LinuxSpider]` файла конфігурації).

   Щоб переглянути та виправити режим роботи, ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб встановити значення `AUTO`, введіть команду

```
# drweb-ctl cfset LinuxSpider.Mode AUTO
```

   - Щоб скинути значення параметра в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset LinuxSpider.Mode -r
```

2. Якщо помилка повториться, виконайте ручну збірку та встановлення завантажуваного модуля ядра для компонента SpIDer Guard.

   Зверніть увагу, що робота компонента SpIDer Guard та завантажуваного модуля ядра гарантується, якщо використовувана вами ОС входить до списку протестованих дистрибутивів **Linux** (див. розділ Системні вимоги та сумісність).

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*SpIDer Gate недоступний*
Код помилки	`x117`
Опис	Відсутній компонент SpIDer Gate (необхідний для перевірки мережних з'єднань).

Усунення помилки:

1. Перевірте правильність шляху до виконуваного файла **drweb-gated** та за необхідності виправте його (параметр **`ExePath`** в секції `[GateD]` файла конфігурації).

   Також ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду:

     ```
     $ drweb-ctl cfshow GateD.ExePath
     ```

   - Щоб встановити нове значення параметра, введіть команду:

     ```
     # drweb-ctl cfset GateD.ExePath <новий шлях>
     ```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

     ```
     # drweb-ctl cfset GateD.ExePath -r
     ```

2. За відсутності налаштувань компонента SpIDer Gate в конфігурації або якщо помилка виникає при вказанні правильного шляху, встановіть або перевстановіть пакет `drweb-gated`.
3. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Компонент MailD недоступний*
Код помилки	`x118`

Опис	Відсутній компонент Dr.Web MailD (необхідний для перевірки електронної пошти).

Усунення помилки:

1. Перевірте правильність шляху до виконуваного файла **drweb-maild** та за необхідності виправте його (параметр **ExePath** в секції `[MailD]` файла конфігурації).

   Також ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду:

   ```
   $ drweb-ctl cfshow MailD.ExePath
   ```

   - Щоб встановити нове значення параметра, введіть команду:

   ```
   # drweb-ctl cfset MailD.ExePath <новий шлях>
   ```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

   ```
   # drweb-ctl cfset MailD.ExePath -r
   ```

2. За відсутності налаштувань компонента Dr.Web MailD в конфігурації або якщо помилка виникає при вказанні правильного шляху, встановіть або перевстановіть пакет `drweb-maild`.
3. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Scanning Engine недоступний*
Код помилки	`x119`
Опис	Неможливо перевіряти файли, оскільки відсутній або не запускається компонент Dr.Web Scanning Engine (**drweb-se**), що використовується для перевірки файлів. Неможлива робота компонентів: Сканер, SpIDer Guard, SpIDer Gate (частково).

Усунення помилки:

1. Перевірте правильність шляху до виконуваного файла **drweb-se** та за необхідності виправте його (параметр **ExePath** в секції `[ScanEngine]` файла конфігурації).

   Також ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду:

   ```
   $ drweb-ctl cfshow ScanEngine.ExePath
   ```

   - Щоб встановити нове значення параметра, введіть команду:

```
# drweb-ctl cfset ScanEngine.ExePath <новий шлях>
```

- Щоб скинути параметри в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset ScanEngine.ExePath -r
```

2. При виникненні помилки при вказанні правильного шляху:
   - Виконайте команду

```
$ drweb-ctl rawscan /
```

   якщо у виведенні на екран наявний рядок `Error: No valid license provided`, то це означає, що відсутній діючий ключовий файл. Зареєструйте Dr.Web для Linux та отримайте ліцензію. Якщо ліцензія вами отримана, то перевірте наявність ключового файла та встановіть його за необхідності.
   - Якщо ваша ОС використовує підсистему безпеки **SELinux**, налаштуйте політику безпеки для модуля **drweb-se** (див. розділ Налаштування політик безпеки для SELinux).
3. За відсутності налаштувань компонента в конфігурації або якщо попередні кроки не допомогли, встановіть або перевстановіть пакет `drweb-se`.
4. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Сканер недоступний*
Код помилки	`x120`
Опис	Неможливо перевіряти файли, оскільки відсутній компонент **drweb-filecheck**, що використовується для перевірки файлів. Неможлива робота компонентів: Сканер, SpIDer Guard.

Усунення помилки:

1. Перевірте правильність шляху до виконуваного файла **drweb-filecheck** та за необхідності виправте його (параметр **`ExePath`** в секції `[FileCheck]` файла конфігурації).

   Також ви можете скористатися командами утиліти управління з командного рядка.

   Щоб переглянути поточне значення параметра, введіть команду:

```
$ drweb-ctl cfshow FileCheck.ExePath
```

   Щоб встановити нове значення параметра, введіть команду:

```
# drweb-ctl cfset FileCheck.ExePath <новий шлях>
```

   Щоб скинути параметри в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset FileCheck.ExePath -r
```

2. При виникненні помилки при вказанні правильного шляху:
   - Якщо ваша ОС використовує підсистему безпеки **SELinux**, налаштуйте політику безпеки для модуля **drweb-filecheck** (див. розділ Налаштування політик безпеки для SELinux).
3. За відсутності налаштувань компонента в конфігурації або якщо попередні кроки не допомогли, встановіть або перевстановіть пакет `drweb-filecheck`.
4. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*ES Agent недоступний*
Код помилки	`x121`
Опис	Відсутній компонент Dr.Web ES Agent (необхідний для підключення до сервера централізованого захисту).

Усунення помилки:

1. Перевірте правильність шляху до виконуваного файла **drweb-esagent** та за необхідності виправте його (параметр **`ExePath`** в секції `[ESAgent]` файла конфігурації).

   Також ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду:

   ```
   $ drweb-ctl cfshow ESAgent.ExePath
   ```

   - Щоб встановити нове значення параметра, введіть команду:

   ```
   # drweb-ctl cfset ESAgent.ExePath <новий шлях>
   ```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

   ```
   # drweb-ctl cfset ESAgent.ExePath -r
   ```

2. За відсутності налаштувань компонента в конфігурації або якщо помилка виникає при вказанні правильного шляху, встановіть або перевстановіть пакет `drweb-esagent`.
3. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Компонент Firewall для Linux недоступний*
Код помилки	`x122`
Опис	Неможливо контролювати мережні з'єднання, оскільки відсутній або не запускається допоміжний модуль **drweb-firewall**, призначений для перенаправлення з'єднань. Неможлива робота компонентів: SplDer Gate.

Усунення помилки:

1. Перевірте правильність шляху до виконуваного файла **drweb-firewall** та за необхідності виправте його (параметр **`ExePath`** в секції `[LinuxFirewall]` файла конфігурації).

   Також ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду:

     ```
     $ drweb-ctl cfshow LinuxFirewall.ExePath
     ```

   - Щоб встановити нове значення параметра, введіть команду:

     ```
     # drweb-ctl cfset LinuxFirewall.ExePath <новий шлях>
     ```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

     ```
     # drweb-ctl cfset LinuxFirewall.ExePath -r
     ```

2. За відсутності налаштувань компонента Dr.Web Firewall для Linux в конфігурації або якщо помилка виникає при вказанні правильного шляху, встановіть або перевстановіть пакет `drweb-firewall`.
3. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Network Checker недоступний*
Код помилки	`x123`
Опис	Неможливо контролювати мережні з'єднання, оскільки відсутній або не запускається допоміжний модуль **drweb-netcheck**, призначений для перевірки файлів, що завантажуються по мережі. Неможлива робота компонентів: SplDer Gate (частково).

Усунення помилки:

1. Перевірте правильність шляху до виконуваного файла **drweb-netcheck** та за необхідності виправте його (параметр **`ExePath`** в секції `[NetCheck]` файла конфігурації).

Також ви можете скористатися командами утиліти управління з командного рядка.

- Щоб переглянути поточне значення параметра, введіть команду:

```
$ drweb-ctl cfshow NetCheck.ExePath
```

- Щоб встановити нове значення параметра, введіть команду:

```
# drweb-ctl cfset NetCheck.ExePath <новий шлях>
```

- Щоб скинути параметри в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset NetCheck.ExePath -r
```

2. За відсутності налаштувань компонента в конфігурації або якщо помилка виникає при вказанні правильного шляху, встановіть або перевстановіть пакет `drweb-netcheck`.
3. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Компонент CloudD недоступний*
Код помилки	`x124`
Опис	Відсутній компонент Dr.Web CloudD (необхідний для звернення до хмари Dr.Web Cloud).

Усунення помилки:

1. Перевірте правильність шляху до виконуваного файла **drweb-cloudd** та за необхідності виправте його (параметр **`ExePath`** в секції `[CloudD]` файла конфігурації).

   Також ви можете скористатися командами утиліти управління з командного рядка.

   - Щоб переглянути поточне значення параметра, введіть команду:

```
$ drweb-ctl cfshow CloudD.ExePath
```

   - Щоб встановити нове значення параметра, введіть команду:

```
# drweb-ctl cfset CloudD.ExePath <новий шлях>
```

   - Щоб скинути параметри в значення за замовчуванням, введіть команду:

```
# drweb-ctl cfset CloudD.ExePath -r
```

2. За відсутності налаштувань компонента в конфігурації або якщо помилка виникає при вказанні правильного шляху, встановіть або перевстановіть пакет `drweb-cloudd`.

3. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Повідомлення про помилку	*Непередбачувана помилка*
Код помилки	`x125`
Опис	Сталася непередбачувана помилка в роботі якогось компонента.

Усунення помилки:

1. Спробуйте перезапустити Dr.Web для Linux, виконавши команду:

```
# service drweb-configd restart
```

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки, повідомивши код помилки.

Помилки, що не мають кодів

Симптоми	Після встановлення модуля ядра SpIDer Guard робота операційної системи аварійно завершується з помилкою ядра «*Kernel panic*»
Опис	Робота модуля ядра SpIDer Guard неможлива в середовищі виконання ядра ОС (наприклад, ОС працює в середовищі гіпервізора **Xen**).

Усунення помилки:

1. Скасуйте завантаження модуля ядра SpIDer Guard (модуль ядра має ім'я `drweb`), додавши в завантажувачі **grub** рядок

```
drweb.blacklist=yes
```

   в рядок параметрів завантаження ядра ОС.

2. Після завантаження ОС видаліть модуль ядра `drweb.ko` з каталогу додаткових модулів ядра `/lib/modules/`uname -r`/extra`.
3. Встановіть для SpIDer Guard режим роботи *AUTO*, виконавши команди:

```
# drweb-ctl cfset LinuxSpider.Mode Auto
# drweb-ctl reload
```

4. Якщо встановлена ОС не підтримує механізм **fanotify**, або цей режим не дозволяє використовувати SpIDer Guard для повноцінного контролю файлової системи (актуально для систем **GNU/Linux** з мандатними моделями доступу, наприклад — **Astra Linux SE**), й, таким

чином, використання режиму *LKM* є обов'язковим для контролю файлової системи, то відмовтеся від гіпервізора **Xen**.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки.

Симптоми	Головне вікно Dr.Web для Linux неактивне, індикатор в області сповіщень робочого столу відображається з символом критичної помилки, а меню індикатора, що випадає, містить тільки один неактивний пункт **Завантаження**
Опис	Dr.Web для Linux не може запуститися, оскільки основний сервісний компонент **drweb-configd** недоступний.

Усунення помилки:

1. Перезапустіть Dr.Web для Linux, виконавши команду:

   ```
   # service drweb-configd restart
   ```

2. Якщо ця команда поверне помилку або не принесе жодного ефекту, виконайте окреме встановлення або перевстановлення пакета `drweb-configd`.
3. Зверніть увагу, що це також може означати, що в системі для аутентифікації користувачів не використовується **PAM**. Якщо це так, що встановіть та налаштуйте його.
4. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки.

Симптоми	1. Індикатор в області сповіщень робочого столу не відображається після входу в систему. 2. Спроба виконати команду запуску графічного інтерфейсу `$ drweb-gui` призводить до запуску головного вікна Dr.Web для Linux.
Опис	Можливо, дана помилка пов'язана з відсутністю в вашій системі додаткової бібліотеки **libappindicator1**.

Усунення помилки:

1. Перевірте наявність в вашій системі пакета `libappindicator1`, виконавши команду:

   ```
   # dpkg -l | grep libappindicator1
   ```

2. Якщо команда не виведе жодного результату, то встановіть цей пакет, використовуючи будь-який з наявних в системі менеджер пакетів. Після цього виконайте повторний вхід в систему (*log in*).

3. Зверніть увагу, що це також може означати, що в системі для аутентифікації користувачів не використовується **PAM**. Якщо це так, що встановіть та налаштуйте його.
4. Якщо попередні дії не допомогли, видаліть Dr.Web для Linux цілком, після чого встановіть його повторно.

   Інструкції зі встановлення та видалення Dr.Web для Linux та його компонентів див. у розділах Встановлення Dr.Web для Linux та Видалення Dr.Web для Linux.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки.

Симптоми	1. Після відключення SpIDer Gate припиняють працювати мережні з'єднання (як вихідні, так і, можливо, вхідні — по протоколам SSH, FTP). 2. Пошук в правилах **NetFilter** (**iptables**) з використанням команди `# iptables-save | grep "comment --comment --comment"` видає непорожній результат.
Опис	Дана помилка пов'язана з некоректною роботою **NetFilter** (**iptables**) версії нижче 1.4.15, яка полягає в тому, що правила з унікальною міткою (коментарем) додаються некоректно, внаслідок чого SpIDer Gate при завершенні своєї роботи не може видалити додані ним правила перенаправлення мережних з'єднань.

Усунення помилки:

1. Повторно включіть SpIDer Gate, щоб він проводив перевірку.
2. Якщо SpIDer Gate необхідно залишити відключеним, видаліть некоректні правила **NetFilter** (**iptables**), виконавши команду:

   ```
   # iptables-save | grep -v "comment --comment --comment" | iptables-restore
   ```

   Зверніть увагу, що виклик команд **iptables-save** та **iptables-restore** потребує прав суперкористувача. Щоб отримати права суперкористувача, ви можете скористатися командами **su** та **sudo**. Також зверніть увагу, що вказана команда видалить зі списку правил всі правила з некоректно доданим коментарем, наприклад, додані іншими програмами, що виконують коректування маршрутизації з'єднань.

Додаткова інформація:

- Щоб попередити виникнення даної помилки у подальшому, рекомендується оновити операційну систему (або, як мінімум, **NetFilter** до версії 1.4.15 або вище).
- Окрім цього, ви можете включити ручний режим перенаправлення з'єднань для SpIDer Gate, задаючи необхідні правила вручну за допомогою утиліти **iptables** (не рекомендується).
- Додаткові відомості див. в документації **man**: `drweb-firewall(1)`, `drweb-gated(1)`, `iptables(8)`.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки.

Симптоми	Подвійне натиснення на значок файла або каталогу в графічному файловому менеджері замість його відкриття запускає перевірку в **Dr.Web**

	для Linux.
Опис	Графічна оболонка виконала автоматичну асоціацію файлів якогось типу та/або каталогів з дією **Відкрити за допомогою Dr.Web для Linux**.

Усунення помилки:

1. Скасуйте асоціацію між файлами даного типу та програмою **Dr.Web для Linux**. Налаштовані асоціації фіксуються в файлі `mimeapps.list` або `defaults.list`. Файли, що визначають локальні налаштування, змінені в профілі користувача, зберігаються в каталозі `~/.local/share/applications/` або `~/.config/` (зазвичай ці каталоги мають атрибут «прихований»).
2. Відкрийте файл `mimeapps.list` або `defaults.list` в будь-якому текстовому редакторі (зверніть увагу, що для редагування системного файла асіоциацій вам необхідні повноваження суперкористувача, за необхідності скористайтеся командами **su** або **sudo**).
3. Знайдіть в файлі секцію `[Default Applications]`, а в ній рядки асоціацій виду <*MIME-тип*>`=drweb-gui.desktop`, наприклад:

   ```
   [Default Applications]
   inode/directory=drweb-gui.desktop
   text/plain=drweb-gui.desktop;gedit.desktop
   ```

4. Якщо в правій частині (після знаку рівності) рядки асоціації, окрім `drweb-gui.desktop` містяться також посилання на інші прпрограми, видаліть з рядка тільки посилання на програму **drweb-gui** (`drweb-gui.desktop`). Якщо асоціація містить посилання тільки на програму **drweb-gui**, видаліть рядок асоціації повністю.
5. Збережіть змінений файл.

Додаткова інформація:

- Для перевірки поточних асоціацій ви можете скористатися утилітами **xdg-mime**, **xdg-open** та **xdg-settings** (входять до складу пакета `xdg-utils`).
- Відомості про роботу утиліт **xdg** див. в документації **man**: `xdg-mime(1)`, `xdg-open(1)`, `xdg-settings(1)`.

Якщо усунути помилку не вдасться, зверніться до Технічної підтримки.

Додаток Д. Збірка модуля ядра для SpIDer Guard

В цьому розділі:

Загальні відомості

Якщо операційна система не надає механізм **fanotify**, що використовується SpIDer Guard для моніторингу дій з об'єктами файлової системи, він може використовувати спеціальний завантажуваний модуль, який працює в просторі ядра (LKM-модуль).

За замовчуванням у складі SpIDer Guardпостачається скомпільований модуль ядра для ОС, що не надають сервіс **fanotify**. Також сумісно з SpIDer Guard постачається архів у форматі `tar.bz2`, що містить вихідні файли завантажуваного модуля ядра, щоб його можна було зібрати вручну.

LKM-модуль, що використовується SpIDer Guard, призначений для роботи з ядрами GNU/Linux версій 2.6.* та вище.

Для архітектури ARM64 модуль ядра LKM не підтримується.

Архів з вихідними кодами завантажуваного модуля ядра розташовується в каталозі основних файлів Dr.Web для Linux (за замовчуванням — `/opt/drweb.com`) в підкаталозі `share/drweb-spider-kmod/src` та має ім'я виду `drweb-spider-kmod-`*<версія>*`-`*<дата>*`.tar.bz2`. Також в каталозі `drweb-spider-kmod` є сценарій перевірки `check-kmod-install.sh`, запустивши який, ви отримаєте інформацію, чи підтримує встановлена операційна система попередньо скомпільовані версії ядра, вже включені до складу Dr.Web для Linux. Якщо не підтримує, на екран буде виведена рекомендація виконати ручну збірку.

Якщо вказаний каталог `drweb-spider-kmod` відсутній, встановіть пакет `drweb-spider-kmod`.

Щоб виконанти ручну збірку завантажуваного модуля ядра з вихідних кодів, необхідні права суперкористувача. Щоб отримати права суперкористувача, при збірці скористайтеся командою змінення користувача **su** або командою виконання від імені іншого користувача **sudo**.

Інструкція зі збірки модуля ядра

1. Розпакуйте архів з вихідними кодами в будь-який каталог. Наприклад, команда

   ```
   # tar -xf drweb-spider-kmod-<версія>-<дата>.tar.bz2
   ```

   розпакує архів безпосередньо до каталогу, в якому міститься сам архів, створивши в ньому підкаталог з іменем файла архіву (зверніть увагу, що для запису в каталог, що містить архів, необхідні права суперкористувача).

2. Перейдіть у створений каталог з вихідними кодами та виконайте команду:

   ```
   # make
   ```

   При виникненні помилок на етапі *make* усуньте їх (див. нижче) та виконайте компіляцію повторно.

3. Після успішного завершення етапу *make* виконайте такі команди:

   ```
   # make install
   # depmod
   ```

4. Після успішної збірки модуля ядра та його реєстрації в системі додатково налаштуйте SplDer Guard, вказавши йому режим роботи з модулем ядра, виконавши команду

   ```
   # drweb-ctl cfset LinuxSpider.Mode LKM
   ```

   Також допускається встановлення значення `AUTO` замість значення `LKM`. В цьому випадку SplDer Guard пробуватиме використовувати не тільки модуль ядра, але й системний механізм **fanotify**. Щоб отримати додаткову інформацію, використовуйте документацію **man**: `drweb-spider(1)`.

Можливі помилки збірки

На етапі виконання збірки *make* можуть виникати помилки. При виникненні помилок перевірте таке:

- Для успішної збірки необхідна наявність **Perl** та компілятора **GCC**. Якщо вони відсутні, встановіть їх.
- В деяких ОС може знадобитися попереднє встановлення пакета `kernel-devel`.
- В деяких ОС збірка може завершитися з помилкою через невірно визначений шлях до каталогу вихідних кодів ядра. В цьому випадку використовуйте команду **make** з параметром `KDIR=`*<шлях до вихідних кодів ядра>*. Зазвичай вони розміщуються в каталозі `/usr/src/kernels/`*<версія ядра>*.

Зверніть увагу, що версія ядра, яка видається командою **uname** `-r`, може не збігатися з іменем каталогу *<версія ядра>*.

Предметний покажчик

Предметний покажчик

Предметний покажчик