

ESET NOD32 Antivirus

Посібник користувача

[Натисніть тут щоб відкрити версію цього документа](#)

© ESET, spol. s r.o., 2024.

ESET NOD32 Antivirus розроблено компанією ESET, spol. s r.o.

Докладніше див. на сайті <https://www.eset.com>.

Усі права захищено. Без письмового дозволу автора жодну частину цього документа не можна відтворювати, зберігати в системі автоматичного пошуку або передавати в будь-якій формі чи будь-яким способом (електронним, механічним, фотокопіюванням, записуванням, скануванням тощо).

ESET, spol. s r.o. зберігає право вносити зміни до будь-якого описаного програмного забезпечення без попередження.

Служба технічної підтримки: <https://support.eset.com>

REV. 12.04.2024

1 ESET NOD32 Antivirus	1
1.1 Нові функції та можливості	2
1.2 Визначення продукту	2
1.3 Системні вимоги	3
1.3 Ваша версія Windows 7 застаріла	4
1.3 Windows 7 більше не підтримується Microsoft	4
1.3 Windows Vista більше не підтримується	5
1.4 Запобігання зараженню комп'ютера	6
1.5 Довідкові сторінки	7
2 Інсталяція	8
2.1 Інсталятор Live installer	8
2.2 Інсталяція в автономному режимі	10
2.3 Активація продукту	12
2.3 Введення ліцензійного ключа під час активації	13
2.3 Використовувати обліковий запис ESET HOME	13
2.3 Активація ліцензії для ознайомлювальної версії	14
2.3 Безкоштовний ліцензійний ключ ESET	15
2.3 Помилка активації: поширені сценарії	16
2.3 Не вдалося виконати активацію через перевикористану ліцензію	16
2.3 Оновлення ліцензії	17
2.3 Оновлення продукту	18
2.3 Пониження рівня ліцензії	19
2.3 Пониження версії продукту	20
2.4 Засіб виправлення неполадок під час інсталяції	21
2.5 Перше сканування після інсталяції	21
2.6 Оновлення до останньої версії	21
2.6 Автоматичне оновлення застарілих версій продуктів	22
2.7 Рекомендація продукту ESET другу або подрузі	23
2.7 ESET NOD32 Antivirus буде інстальовано	23
2.7 Змінити на іншу продуктову лінійку	24
2.7 Реєстрація	24
2.7 Хід активації	24
2.7 Успішне завершення активації	24
3 Посібник для початківців	24
3.1 Підключіться до ESET HOME	24
3.1 Вхід у ESET HOME	26
3.1 Не вдалося виконати вхід: поширені помилки	27
3.1 Додавання пристрою в ESET HOME	27
3.2 Головне вікно програми	28
3.3 Оновлення	31
4 Робота з ESET NOD32 Antivirus	33
4.1 Захист комп'ютера	35
4.1 Ядро виявлення	36
4.1 Розширені параметри ядра виявлення	41
4.1 Дії в разі виявлення загрози	41
4.1 Захист файлової системи в режимі реального часу	44
4.1 Рівні очистки	46
4.1 Можливі причини для змінення конфігурації захисту в режимі реального часу	46
4.1 Перевірка захисту в режимі реального часу	47
4.1 Необхідні дії, коли не працює захист у режимі реального часу	47

4.1 Виключення процесів	48
4.1 Додавання або зміна виключень процесів	49
4.1 Захист із використанням хмари	49
4.1 Фільтр виключень для хмарного захисту	52
4.1 Сканування комп'ютера	52
4.1 Модуль запуску вибіркового сканування	55
4.1 Хід сканування	57
4.1 Журнал сканування комп'ютера	59
4.1 Сканування шкідливого програмного забезпечення	61
4.1 Сканування в неактивному стані	61
4.1 Профілі сканування	62
4.1 Об'єкти сканування	63
4.1 Контроль пристроїв	63
4.1 Редактор правил контролю пристроїв	64
4.1 Виявлені пристрої	65
4.1 Групи пристроїв	66
4.1 Додавання правил контролю пристроїв	67
4.1 Систему запобігання вторгненням (HIPS)	69
4.1 Інтерактивне вікно HIPS	72
4.1 Виявлено потенційно зловмисну програму, яка вимагає викуп	73
4.1 Керування правилами HIPS	74
4.1 Параметри правила HIPS	75
4.1 Додавання шляху до програми/реєстру для HIPS	78
4.1 Додаткові параметри HIPS	78
4.1 Драйвери, які дозволено завантажувати завжди	79
4.1 Ігровий режим	79
4.1 Сканування під час запуску	80
4.1 Автоматична перевірка файлів під час запуску системи	80
4.1 Захист документів	81
4.1 Виключення	81
4.1 Виключення в роботі	82
4.1 Додавання або зміна виключення в роботі	83
4.1 Формат виключення шляху	84
4.1 Виключення об'єктів виявлення	85
4.1 Додавання або зміна виключення об'єкта виявлення	87
4.1 Майстер створення виключень виявлених об'єктів	88
4.1 Виключення HIPS	89
4.1 Параметри ThreatSense	89
4.1 Список розширень файлів, виключених із перевірки	93
4.1 Додаткові параметри ThreatSense	94
4.2 Безпечна робота в Інтернеті	95
4.2 Фільтрація протоколів	96
4.2 Виключені програми	96
4.2 Виключені IP-адреси	97
4.2 Додати адресу IPv4	98
4.2 Додати адресу IPv6	98
4.2 SSL/TLS	99
4.2 Сертифікати	100
4.2 Зашифрований мережевий трафік	101
4.2 Список відомих сертифікатів	101
4.2 Список програм, до яких застосовуються фільтри SSL/TLS	102

4.2	Захист поштового клієнта	103
4.2	Інтеграція з поштовими клієнтами	104
4.2	Панель інструментів Microsoft Outlook	104
4.2	Панель інструментів Outlook Express і Windows Mail	105
4.2	Діалогове вікно підтвердження	105
4.2	Повторне сканування повідомлень	105
4.2	Протоколи електронної пошти	106
4.2	Фільтр POP3, POP3S	107
4.2	Теги електронної пошти	108
4.2	Захист доступу до Інтернету	108
4.2	Розширене налаштування функції захисту доступу до Інтернету	111
4.2	Веб-протоколи	111
4.2	Управління URL-адресами	112
4.2	Список URL-адрес	113
4.2	Створити новий список URL-адрес	114
4.2	Додавання маски URL-адреси	115
4.2	Захист від фішинг-атак	116
4.3	Оновлення програми	118
4.3	Параметри оновлення	121
4.3	Відкочування оновлення	123
4.3	Інтервал часу відкочування	124
4.3	Оновлення продукту	125
4.3	Параметри підключення	125
4.3	Створення завдань оновлення	126
4.3	Діалогове вікно	126
4.4	Інструменти	127
4.4	Інструменти ESET NOD32 Antivirus	127
4.4	Журнали	128
4.4	Фільтрація журналу	131
4.4	Налаштування ведення журналу	132
4.4	Запущені процеси	133
4.4	Звіт про безпеку	135
4.4	ESET SysInspector	136
4.4	Планувальник	137
4.4	Параметри сканування за розкладом	141
4.4	Огляд запланованого завдання	142
4.4	Відомості про завдання	142
4.4	Часовий параметр завдання	142
4.4	Часовий параметр завдання: одноразово	143
4.4	Часовий параметр завдання: щодня	143
4.4	Часовий параметр завдання: щотижня	143
4.4	Часовий параметр завдання: за умови виникнення події	143
4.4	Невиконане завдання	143
4.4	Відомості про завдання: оновлення	144
4.4	Відомості про завдання: запуск програми	144
4.4	Засіб очищення системи	145
4.4	ESET SysRescue Live	146
4.4	Карантин	146
4.4	Проксі-сервер	149
4.4	Вибір зразка для аналізу	150
4.4	Вибір зразка для аналізу: підозрілий файл	152

4.4 Вибір зразка для аналізу: підозрілий сайт	152
4.4 Вибір зразка для аналізу: помилково розпізнаний файл	152
4.4 Вибір зразка для аналізу: помилково розпізнаний сайт	153
4.4 Вибір зразка для аналізу: інше	153
4.4 Оновлення Microsoft Windows®	153
4.4 Діалогове вікно	154
4.4 Інформація про оновлення	154
4.5 Інтерфейс користувача	154
4.5 Елементи інтерфейсу користувача	154
4.5 Параметри доступу	155
4.5 Пароль для розділу	156
4.5 Піктограма в системному треї	157
4.5 Підтримка програм для читання екрана	158
4.5 Довідка та підтримка	158
4.5 Про продукт ESET NOD32 Antivirus	159
4.5 Новини ESET	159
4.5 Надсилання даних про конфігурацію системи	160
4.5 Технічна підтримка	161
4.6 Сповіщення	161
4.6 Діалогове вікно: статуси програми	162
4.6 Сповіщення на робочому столі	163
4.6 Список сповіщень на робочому столі	164
4.6 Інтерактивні сповіщення	166
4.6 Повідомлення про підтвердження	167
4.6 Знімні носії	168
4.6 Пересилання	169
4.7 Параметри конфіденційності	172
4.8 Профілі	173
4.9 Сполучення клавіш	174
4.10 Діагностичні дані	175
4.10 Технічна підтримка	176
4.10 Параметри імпорту та експорту	176
4.10 Відновлення всіх параметрів у поточному розділі	177
4.10 Відновити налаштування за замовчуванням	178
4.10 Помилка під час збереження конфігурації	178
4.11 Сканер командного рядку	178
4.12 ESET CMD	181
4.13 Виявлення неактивного стану	182
5 Поширені запитання	183
5.1 Оновлення ESET NOD32 Antivirus	184
5.2 Видалення вірусу з ПК	184
5.3 Створення нового запланованого завдання	184
5.4 Додавання до розкладу завдання щотижневого сканування комп'ютера	185
5.5 Як розблокувати додаткові параметри	186
5.6 Як вирішити проблему з деактивацією продукту на порталі ESET HOME	186
5.6 Продукт деактивовано, пристрій відключено	187
5.6 Продукт не активовано	187
6 Програма підвищення якості програмного забезпечення	188
7 Ліцензійна угода з кінцевим користувачем	189
8 Політика конфіденційності	202

ESET NOD32 Antivirus

ESET NOD32 Antivirus – це новий підхід до розробки повністю інтегрованої системи безпеки комп'ютера. Робота останньої версії підсистеми сканування ESET LiveGrid® ґрунтується на принципах швидкості й точності для захисту вашого комп'ютера. У результаті ви отримуєте інтелектуальну систему, що безперервно захищає комп'ютер від атак і шкідливого програмного забезпечення, яке може становити загрозу.

ESET NOD32 Antivirus – це комплексне рішення безпеки, яке забезпечує максимальний рівень захисту та використовує мінімум системних ресурсів. Передові технології на базі штучного інтелекту блокують проникнення вірусів, шпигунських і троянських програм, черв'яків, нав'язливої реклами, руткітів та інших загроз, не знижуючи продуктивність системи й не заважаючи роботі комп'ютера.

Функції та переваги

Удосконалений інтерфейс користувача	У цій версії інтерфейс користувача було значно змінено та спрощено на основі результатів тестування зручності в користуванні. Усі формулювання в елементах графічного інтерфейсу та сповіщень ретельно відредаговано, а сам інтерфейс тепер підтримує мови із записом справа наліво, зокрема арабську й іврит. Онлайн-довідку тепер інтегровано в програму ESET NOD32 Antivirus. Її вміст постійно оновлюється.
Антивірус та антишпигун	Завчасне виявлення та видалення більшості зареєстрованих і невідомих вірусів, черв'яків, троянських програм і руткітів. Технологія розширеної евристики дає змогу визначати раніше не відомі шкідливі програми, гарантуючи захист від нових загроз і їх завчасне знешкодження. Захист доступу до Інтернету та Захист від фішингу здійснюється шляхом контролю зв'язків між веб-браузерами й віддаленими серверами (включно з протоколом SSL). Захист поштового клієнта забезпечує керування поштовими комунікаціями через протоколи POP3(S) та IMAP(S).
Регулярні оновлення	Регулярне оновлення обробника виявлення (попередня назва – "вірусна база даних") і модулів програми – найкращий спосіб гарантувати максимальний захист комп'ютера.
ESET LiveGrid® (репутація у хмарі)	Відстежуйте репутацію запущених процесів і файлів безпосередньо в ESET NOD32 Antivirus.
Контроль пристроїв	Автоматичне сканування всіх запам'ятовуючих пристроїв USB, карток пам'яті й компакт-/DVD-дисків. Блокування доступу до змінних носіїв за типом, виробником, розміром та іншими атрибутами.
Робота системи HIPS	Максимально оптимізуйте роботу системи: укажіть правила для системного реєстру, активних процесів і програм, а також налаштуйте засоби захисту.
Ігровий режим	Блокування показу всіх спливаючих вікон, відкладення оновлень або іншої активної діяльності системи, яке дозволяє спрямувати апаратні ресурси на підтримку ігор і роботу в повноекранному режимі.

Активуйте ліцензію, щоб отримати змогу користуватися всіма функціями ESET NOD32 Antivirus. Рекомендуємо оновлювати ліцензію на ESET NOD32 Antivirus за кілька тижнів до завершення її терміну дії.

Нові функції та можливості

Нове в ESET NOD32 Antivirus 15

ESET HOME (раніше — myESET)

Забезпечує покращену видимість і контроль безпеки. Інсталюйте захист для нових пристроїв, додавайте ліцензії й відкривайте спільний доступ до них, а також отримуйте важливі сповіщення через мобільну програму й веб-портал. Більш докладну інформацію див. в [онлайн-довідці ESET HOME](#).

Удосконалена система запобігання вторгненням (HIPS)

Сканує ділянки пам'яті, які можуть бути змінені в результаті дії ретельно розроблених методів вставлення шкідливого програмного забезпечення. Удосконалення розширюють технічну можливість виявляти найскладніші вторгнення шкідливого програмного забезпечення.

Зображення й додаткову інформацію про нові функції в ESET NOD32 Antivirus див. за посиланням [What's new in the latest version of ESET home products](#) (Нові функції в останніх версіях продуктів ESET для домашнього використання).

i Щоб вимкнути **сповіщення про нові функції й можливості**, клацніть **Додаткові параметри > Сповіщення > Сповіщення на робочому столі**. Натисніть **Редагувати** поруч із параметром **Сповіщення на робочому столі** й зніміть прапорець **Показувати сповіщення про нові функції та можливості**. Більш докладну інформацію про сповіщення див. в розділі [Сповіщення](#).

Визначення продукту

Нові продукти ESET пропонують кілька рівнів безпеки: від ефективних і надійних рішень для захисту від вірусів до комплексних засобів захисту з використанням мінімуму системних ресурсів.

- ESET NOD32 Antivirus
- ESET Internet Security
- ESET Smart Security Premium

Щоб визначити, який продукт інстальовано, відкрийте [головне меню програми](#). Назва продукту відображатиметься у вікні вгорі (див. [статтю з бази знань](#)).

У таблиці нижче вказано функції, доступні в кожному продукті.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Ядро виявлення	✓	✓	✓
Розширене машинне навчання	✓	✓	✓
Захист від експлойтів	✓	✓	✓
Захист від атак на основі сценаріїв	✓	✓	✓
Захист від фішинг-атак	✓	✓	✓
Захист доступу до Інтернету	✓	✓	✓
Система запобігання вторгненням (HIPS) (зокрема, захист від програм-вимагачів)	✓	✓	✓
Антиспам		✓	✓
Брандмауер		✓	✓
Інспектор мережі		✓	✓
Захист веб-камери		✓	✓
Захист мережі від атак		✓	✓
Захист від ботнетів		✓	✓
Захист банківських операцій і платежів		✓	✓
Батьківський контроль		✓	✓
Антикрадій		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

i Деякі зазначені вище продукти можуть бути недоступні залежно від мови/регіону.

Системні вимоги

Для належної роботи ESET NOD32 Antivirus система має відповідати вказаним нижче вимогам до апаратного та програмного забезпечення.

Підтримувані процесори

Процесор Intel або AMD, 32-розрядний (x86) із набором інструкцій SSE2 або 64-розрядний (x64), 1 ГБ або вище

Процесор на базі ARM64, 1 ГГц або більше

Підтримувані операційні системи*


Microsoft® Windows® 11

Microsoft® Windows® 10

Microsoft® Windows® 8.1

Microsoft® Windows® 8

[Microsoft® Windows® 7 SP1 з останніми оновленнями Windows](#)

 Завжди вчасно оновлюйте операційну систему.

Інше

Для активації ESET NOD32 Antivirus й належної роботи функції оновлення потрібне підключення до Інтернету.

Якщо дві антивірусні програми одночасно виконуються на одному пристрої, це спричиняє неминучі системні конфлікти ресурсів, наприклад уповільнення роботи системи аж до неможливості роботи з нею.

* З лютого 2021 року ESET не забезпечуватиме захист для невідтримуваних операційних систем.

Ваша версія Windows 7 застаріла

Проблема

Ви використовуєте застарілу версію операційної системи. Щоб не послаблювати захист, завжди вчасно оновлюйте операційну систему.

Рішення

Ви інсталиували ESET NOD32 Antivirus на {GET_OSNAME} {GET_BITNESS}.

Переконайтеся, що інсталиовано Windows 7 із пакетом оновлень 1 (SP1) і останніми оновленнями Windows (принаймні [KB4474419](#) і [KB4490628](#)).

Якщо для вашої Windows 7 не налаштоване автоматичне оновлення, клацніть **Меню "Пуск" > Панель керування > Система й безпека > Windows Update > Перевірка наявності оновлень**, а потім клацніть **Інсталиувати оновлення**.

Також див. розділ [Microsoft більше не підтримує Windows 7](#).

Windows 7 більше не підтримується Microsoft

Проблема

Корпорація Microsoft 14 січня 2020 року припинила підтримку Windows 7. [Що це означає?](#)

Якщо продовжити використовувати Windows 7 після завершення підтримки, комп'ютер працюватиме, але він може стати більш уразливим до вірусів і загроз безпеки. На ваш комп'ютер більше не надходитимуть оновлення Windows (зокрема, оновленнями системи безпеки).

Рішення

Оновлюєтесь із Windows 7 до Windows 10? Оновіть продукт ESET

Процес оновлення відносно простий, і в багатьох випадках ви можете зробити це без втрати файлів. Перед оновленням до Windows 10 виконайте наведені нижче дії.

1. [Перевірте/оновіть наявний продукт ESET](#)
2. Резервне копіювання важливих даних
3. Ознайомтесь зі статтею Microsoft [Оновлення до Windows 10: запитання й відповіді](#) й оновіть операційну систему Windows

Плануєте використовувати новий комп'ютер або пристрій? Перенесіть продукт ESET

Якщо плануєте використовувати новий комп'ютер або пристрій, дізнайтеся більше про [перенесення наявного продукту ESET на новий пристрій](#).

i Див. також [Підтримку Windows 7 завершено](#).

Windows Vista більше не підтримується

Проблема

Через технічні обмеження ОС Windows Vista ESET NOD32 Antivirus не зможе забезпечувати захист, починаючи з **лютого 2021 року**. Продукт ESET **припинить роботу**. Через це ваша система може стати вразливою до загроз.

11 квітня 2017 року корпорація Microsoft припинила підтримку Windows Vista. [Що це означає?](#)

Якщо продовжити використовувати Windows Vista після завершення підтримки, комп'ютер працюватиме, але він може стати більш уразливим до вірусів і загроз безпеки. На ваш комп'ютер більше не надходитимуть оновлення Windows (зокрема, оновленнями системи безпеки).

Рішення

Виконуєте оновлення з Windows Vista до Windows 10? Перенесіть продукт ESET на новий пристрій

Перед оновленням до Windows 10 виконайте наведені нижче дії.

1. Резервне копіювання важливих даних
2. Ознайомтесь зі статтею Microsoft [Оновлення до Windows 10: запитання й відповіді](#) й оновіть операційну систему Windows
3. Установіть або [перенесіть наявний продукт ESET на новий пристрій](#).

i Див. також статтю [Support for Windows Vista has ended \(Підтримка Windows Vista завершилася\)](#).

Запобігання зараженню комп'ютера

Коли ви працюєте за комп'ютером (а особливо переглядаєте веб-сторінки в Інтернеті), пам'ятайте, що жодна антивірусна система у світі не зможе повністю усунути ризик, який несуть [інфіковані об'єкти](#) й [віддалені атаки](#). Щоб забезпечити максимальний захист і зручність під час роботи, важливо правильно користуватися рішеннями захисту від вірусів і дотримуватися кількох корисних правил.

Регулярне оновлення

Згідно зі статистичними даними від ESET LiveGrid® тисячі нових унікальних шкідливих кодів створюються щодня. Їх мета – обійти наявні захисні бар'єри та принести прибуток своїм авторам. Задля безперервного покращення захисту наших клієнтів спеціалісти дослідницької лабораторії ESET щодня аналізують ці загрози, а потім розробляють і випускають оновлення на основі отриманих даних. Максимальний рівень ефективності таких оновлень може гарантувати лише їхня належна конфігурація в системі. Щоб отримати додаткові відомості про спосіб налаштування оновлень, див. розділ [Параметри оновлення](#).

Завантаження оновлень для операційних систем та інших програм

Як правило, автори шкідливих програм використовують уразливість різних систем для збільшення дієвості поширення шкідливого коду. Тому компанії, що випускають програмне забезпечення, пильно слідкують за появою нових слабких місць у своїх програмах і регулярно випускають оновлення безпеки, які усувають потенційні загрози. Важливо завантажувати ці оновлення одразу після їх випуску. Microsoft Windows і веб-браузери, такі як Internet Explorer, – це дві програми, оновлення для яких випускаються на постійній основі.

Резервне копіювання важливих даних

Зловмисники, які створюють шкідливі програми, не переймаються потребами користувачів, а робота таких програм часто призводить до повної непрацездатності операційної системи та втрати важливих даних. Важливо регулярно створювати резервні копії важливих і конфіденційних даних на зовнішні носії, наприклад DVD- або зовнішній жорсткий диск. Так буде значно легше та швидше відновити дані у випадку збою системи.

Регулярне сканування комп'ютера на наявність вірусів

Модуль захисту файлової системи в режимі реального часу виявляє відомі й нові віруси, черв'яки, троянські програми та руткіти. Тож під час кожного відкриття або переходу до файлу виконується його перевірка на наявність шкідливого коду. Рекомендується щонайменше раз на місяць виконувати повне сканування комп'ютера, оскільки шкідливі програми постійно змінюються, а обробник виявлення оновлюється кожного дня.

Дотримання основних правил безпеки

Будьте обережні – це найкорисніше й найефективніше з усіх правил. На сьогодні для виконання та поширення багатьох загроз потрібне втручання користувача. Будьте обережні,

відкриваючи нові файли: це заощадить вам багато часу та зусиль, які інакше довелося б витратити на усунення проникнень. Нижче наведено деякі корисні правила:

- Не відвідуйте підозрілі веб-сайти з багатьма спливаючими вікнами та рекламою.
- Будьте обережні під час інсталяції безкоштовних програм, пакетів кодеків тощо. Користуйтеся тільки безпечними програмами й відвідуйте лише перевірені веб-сайти.
- Будьте обережні під час відкривання вкладених файлів електронних листів, зокрема в масово розісланих повідомленнях і повідомленнях від невідомих відправників.
- Не користуйтеся обліковим записом із правами адміністратора для повсякденної роботи на комп'ютері.

Довідкові сторінки

Вітаємо в посібнику користувача ESET NOD32 Antivirus! Наведена тут інформація допоможе краще ознайомитися з продуктом і зробити роботу з комп'ютером безпечнішою.

Початок роботи

Перш ніж починати працювати з ESET NOD32 Antivirus, радимо дізнатися про різноманітні [типи загроз](#) і [віддалених атак](#), які можуть виникати під час використання комп'ютера.

Ми уклали список [нових функцій](#) ESET NOD32 Antivirus, а також посібник, у якому наводяться інструкції щодо установки базових параметрів.

Принципи використання довідкових сторінок ESET NOD32 Antivirus

Теми сторінок розділено на кілька розділів і підрозділів. Натисніть **F1**, щоб переглянути інформацію про вікно, яке наразі відкрито.

Програма дає змогу шукати теми серед сторінок довідки за ключовими словами, а також вміст на цих сторінках за словами й фразами. Різниця між цими двома способами полягає в тому, що ключове слово може бути логічно пов'язане зі сторінками довідки, які не містять цього слова в тексті. Пошук за допомогою слів і фраз виконується у вмісті сторінок та відображає лише сторінки, які містять пошукове слово або фразу в самому тексті.

Щоб забезпечити узгодженість і уникнути плутанини, у цьому посібнику використовується термінологія на основі назв параметрів ESET NOD32 Antivirus. Щоб виділити важливі теми, ми також використовуємо стандартні набори символів.



Це лише коротке зауваження. Примітку можна пропустити, проте в ній зазначається цінна інформація, як-от про спеціальні функції або посилання на пов'язані теми.



Це повідомлення, на яке потрібно обов'язково звернути увагу. Зазвичай у ньому вказується некритична, але важлива інформація.



Це інформація, на яку потрібно звернути особливу увагу. Її розміщено для того, щоб застерегти користувача від потенційно небезпечних помилок. Уважно ознайомлюйтеся з попередженнями, оскільки в них подається інформація про надзвичайно важливі параметри системи або дії чи налаштування, пов'язані з ризиком.



Цей приклад використання допоможе зрозуміти, як можна застосовувати певну функцію чи опцію.

Позначення	Значення
Жирний текст	Назви елементів інтерфейсу, наприклад полів і кнопок опцій.
Текст курсивом	Поля, які користувач має заповнити даними. Наприклад, назва файлу або шлях означають, що необхідно ввести фактичну назву файлу або шлях.
Courier New	Зразки кодів і команд.
Гіперпосилання	Елемент для швидкого й легкого доступу до перехресних посилань і зовнішніх розташувань у мережі. Гіперпосилання виділені синім кольором і можуть бути підкреслені.
%ProgramFiles%	Системний каталог Windows, у якому зберігаються встановлені програми.

Інтерактивна довідка – основне джерело довідкової інформації. Найновіша версія інтерактивної довідки відображатиметься автоматично, якщо під час роботи у вас буде доступ до мережі.

Інсталяція

Існує кілька способів інсталяції ESET NOD32 Antivirus на комп'ютері. Способи інсталяції можуть відрізнятися залежно від країни й засобів розповсюдження.

- [Live installer](#) – завантажується з веб-сайту ESET або компакт- чи DVD-диску. Інсталяційний пакет універсальний для всіх мов (виберіть потрібну мову). Інсталятор Live installer – це файл невеликого розміру; додаткові файли, необхідні для інсталяції ESET NOD32 Antivirus, буде завантажено автоматично.
- [Інсталяція в автономному режимі](#) передбачає використання файлу з розширенням .exe, який більший за розміром, ніж файл Live installer, і не потребує підключення до Інтернету або додаткових файлів для завершення інсталяції.



Перш ніж інсталювати ESET NOD32 Antivirus, переконайтеся, що на комп'ютері відсутня будь-яка інша антивірусна програма. Якщо на комп'ютері інстальовано кілька антивірусних програм, вони можуть конфліктувати одна з одною. Рекомендується видалити із системи інші антивірусні програми. Див. [статтю бази знань ESET](#), у якій представлений список засобів видалення типового антивірусного ПЗ (доступно англійською та кількома іншими мовами)..

Інсталятор Live installer

Після завантаження [пакета інсталяції Live installer](#) двічі клацніть інсталяційний файл і дотримуйтеся покрокових інструкцій, що відображатимуться у вікні майстра інсталяції.

! Цей тип інсталяції вимагає підключення до Інтернету.

eSet SECURITY

— ×

Інсталювати програму ESET Security

Користуйтеся Інтернетом, грайте та спілкуйтеся, а про безпеку потурбується ESET.

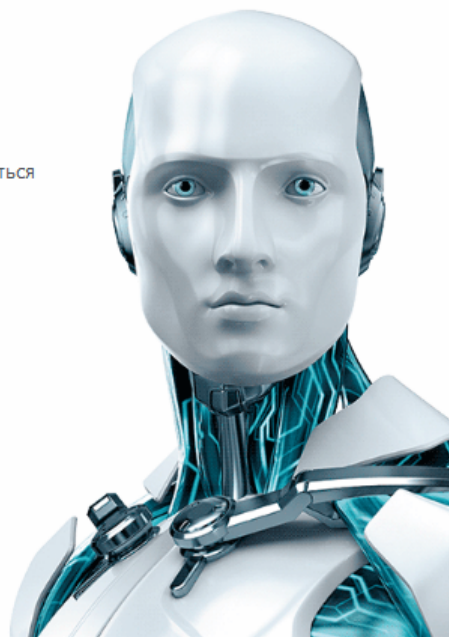
15.1.12.0

Потрібна допомога з інсталяції?

- Відкрити інструкції з інсталяції
- Відкрити посібник користувача

Продовжити

Українською



1. Виберіть потрібну мову з розкривного меню й натисніть **Продовжити**.



Якщо ви інсталюєте новішу версію поверх попередньої версії з параметрами, захищеними паролем, уведіть пароль. Пароль для налаштувань можна задати в [налаштуваннях доступу](#).

2. Виберіть параметри для наведених нижче функцій, ознайомтеся з умовами документів [Ліцензійна угода з кінцевим користувачем](#) і [Політика конфіденційності](#) й клацніть **Продовжити** або **Дозволити все й продовжити** (щоб увімкнути всі функції):

- [Система зворотного зв'язку ESET LiveGrid®](#)
- [Потенційно небажані програми](#)
- [Програма підвищення якості програмного забезпечення](#)



Натискаючи кнопку **Продовжити** або **Прийняти й продовжити**, ви погоджуєтеся з умовами документів "Ліцензійна угода з кінцевим користувачем" і "Політика конфіденційності".

3. Щоб активувати засоби захисту для пристрою, керувати ними й переглядати їхні дані в ESET HOME, [підключіть свій пристрій до облікового запису ESET HOME](#). Клацніть **Пропустити вхід**, щоб продовжити без підключення до ESET HOME. Пристрій [можна підключити до облікового запису ESET HOME](#) пізніше.

4. Якщо продовжити без підключення до ESET HOME, виберіть [варіант активації](#). Під час інсталяції новішої версії поверх попередньої ліцензійний ключ вводиться автоматично.

5. Майстер інсталяції визначає, який продукт ESET інсталюється, за вашою ліцензією. Завжди попередньо вибирається версія з найбільшим набором функцій захисту. Щоб [інсталювати](#)

[іншу версію продукту ESET](#), натисніть **Змінити продукт**. Клацніть **Продовжити**, щоб розпочати процес інсталяції. На це може знадобитися певний час.

i Якщо є залишки (файли або папки) від продуктів ESET, видалених у минулому, з'явиться запит на дозвіл для їх видалення. Щоб продовжити, клацніть **Інсталювати**.

6. Натисніть кнопку **Готово**, щоб вийти з майстра інсталяції.

! [Засіб виправлення неполадок під час інсталяції](#).

i Після інсталяції та активації продукту починається завантаження модулів. Триває запуск програми захисту. Поки завантаження не завершиться, деякі функції можуть працювати не в повній мірі.

Інсталяція в автономному режимі

Завантажте й інсталюйте домашню версію продукту ESET для Windows за допомогою автономного інсталюатора (.exe) нижче. [Виберіть версію домашнього продукту ESET для завантаження](#) (32-розрядну, 64-розрядну або ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Завантажити 64-розрядну версію	Завантажити 64-розрядну версію	Завантажити 64-розрядну версію
Завантажити 32-розрядну версію	Завантажити 32-розрядну версію	Завантажити 32-розрядну версію
Завантаження ARM	Завантаження ARM	Завантаження ARM

! Якщо у вас установлено підключення до Інтернету, [інсталюйте продукт ESET за допомогою Live Installer](#).

Після запуску автономного інсталюатора (файл .exe) майстер інсталяції допоможе вам виконати налаштування.

Інсталювати програму ESET Security

Користуйтеся Інтернетом, грайте та спілкуйтеся, а про безпеку потурбується ESET.

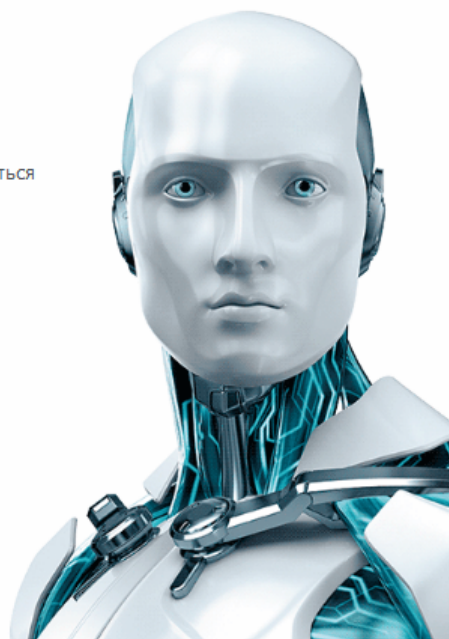
15.1.12.0

Потрібна допомога з інсталяції?

- 🔗 Відкрити інструкції з інсталяції
- 🔗 Відкрити посібник користувача

Продовжити

Українською



1. Виберіть потрібну мову з розкривного меню й натисніть **Продовжити**.



Якщо ви інсталюєте новішу версію поверх попередньої версії з параметрами, захищеними паролем, уведіть пароль. Пароль для налаштувань можна задати в [налаштуваннях доступу](#).

2. Виберіть параметри для наведених нижче функцій, ознайомтеся з умовами документів [Ліцензійна угода з кінцевим користувачем](#) і [Політика конфіденційності](#) й клацніть **Продовжити** або **Дозволити все й продовжити** (щоб увімкнути всі функції):

- [Система зворотного зв'язку ESET LiveGrid®](#)
- [Потенційно небажані програми](#)
- [Програма підвищення якості програмного забезпечення](#)



Натискаючи кнопку **Продовжити** або **Прийняти й продовжити**, ви погоджуєтеся з умовами документів "Ліцензійна угода з кінцевим користувачем" і "Політика конфіденційності".

3. Натисніть **Пропустити вхід**. Якщо у вас є підключення до Інтернету, можна [підключити пристрій до облікового запису ESET HOME](#).

4. Натисніть **Пропустити активацію**. Щоб працювали всі функції програми ESET NOD32 Antivirus, її потрібно активувати після інсталяції. Для [активації продукту](#) потрібне активне підключення до Інтернету.

5. Майстер інсталяції показує, який продукт ESET буде інстальовано відповідно до завантаженого автономного інсталювача. Клацніть **Продовжити**, щоб розпочати процес інсталяції. На це може знадобитися певний час.

i Якщо є залишки (файли або папки) від продуктів ESET, видалених у минулому, з'явиться запит на дозвіл для їх видалення. Щоб продовжити, клацніть **Інсталиювати**.

6. Натисніть кнопку **Готово**, щоб вийти з майстра інсталяції.

! [Засіб виправлення неполадок під час інсталяції](#).

Активація продукту

Активувати продукт можна кількома способами. У вікні активації можуть бути відсутні деякі сценарії активації, залежно від країни вашого перебування, а також засобів розповсюдження (компакт-/DVD-диск, веб-сторінка ESET тощо).

- Якщо ви придбали роздрібну версію продукту або отримали електронний лист із відомостями про ліцензію, активуйте продукт. Для цього клацніть **Скористайтесь придбаним ліцензійним ключем**. Як правило, ліцензійний ключ вказується всередині або на звороті упаковки. Для успішної активації потрібно вводити ключ в указаній послідовності. Ліцензійний ключ — це унікальний рядок символів у форматі XXXX-XXXX-XXXX-XXXX-XXXX або XXXX-XXXXXXXX, який використовується для активації ліцензії й ідентифікації її власника.
- Якщо вибрано параметр [Використовувати обліковий запис ESET HOME](#), вам буде запропоновано увійти у свій обліковий запис ESET HOME.
- Якщо вам потрібно оцінити якість ESET NOD32 Antivirus, перш ніж придбати, виберіть опцію [Безкоштовна пробна версія](#). Введіть адресу електронної пошти й назву країни, щоб активувати ESET NOD32 Antivirus на обмежений час. Тестову ліцензію вам буде надіслано електронною поштою. Пробну версію можна активувати лише раз.
- Якщо у вас немає ліцензії й ви хочете її придбати, клацніть "**Придбати ліцензію**". Програма спрямує вас на веб-сайт місцевого дистриб'ютора ESET. Для домашніх версій продуктів ESET для Windows [повні ліцензії не є безкоштовними](#).

Ви завжди можете змінити інформацію про ліцензію на продукт. Для цього в [головному меню](#) натисніть **Довідка та підтримка > Змінити ліцензію**. Відобразиться ідентифікатор відкритої ліцензії, який потрібно вказати у відповідь на запит служби підтримки ESET.

Якщо у вас є ім'я користувача й пароль, які використовувалися для активації продуктів ESET більш ранніх версій, і ви не знаєте, як активувати ESET NOD32 Antivirus, [перетворіть застарілі облікові дані в ліцензійний ключ](#).

! [Не вдалося активувати продукт?](#)

Виберіть варіант активації



Скористайтесь придбаним ліцензійним ключем

Скористайтесь ліцензією, яку ви придбали онлайн або в магазині.



Використовувати обліковий запис ESET HOME

Увійдіть у ESET HOME і виберіть ліцензію для активації продукту ESET на вашому пристрої.



Придбати ліцензію

Щоб придбати ліцензію, зверніться до торговельного партнера. Якщо ви точно не знаєте, хто є відповідним торговельним партнером, зверніться в нашу службу підтримки.

Введення ліцензійного ключа під час активації

Автоматичні оновлення допомагають убезпечити користувачів. ESET NOD32 Antivirus оновлюватиметься лише після активації.

Коли вводите **Ліцензійний ключ**, важливо стежити за відсутністю помилок.

- Ліцензійний ключ – це унікальний рядок символів у форматі xxxx-xxxx-xxxx-xxxx-xxxx, який використовується для ідентифікації власника ліцензії та її активації.

Ми рекомендуємо скопіювати ліцензійний ключ із повідомлення про реєстрацію, щоб не помилитися.

Якщо після інсталяції не ввести ліцензійний ключ, продукт не активується. Щоб активувати ESET NOD32 Antivirus, відкрийте [головне вікно програми](#) і виберіть пункти **Довідка та підтримка** > **Активувати ліцензію**.

Для домашніх версій продуктів ESET для Windows [повні ліцензії не є безкоштовними](#).

Використовувати обліковий запис ESET HOME

Підключіть свій пристрій на [ESET HOME](#), щоб переглядати всі активовані ліцензії та пристрої ESET і керувати ними. Ви можете поновити, оновити або розширити ліцензію та переглянути важливу інформацію про неї. На порталі керування ESET HOME або в мобільній програмі можна

додавати інші ліцензії, завантажувати продукти на пристрої, перевіряти статус безпеки продукту або надавати спільний доступ до ліцензій електронною поштою. Щоб дізнатися більше, відвідайте [онлайн-довідки ESET HOME](#).

Після вибору параметр **Використовувати обліковий запис ESET HOME** як метод активації або під час підключення до облікового запису ESET HOME у процесі інсталяції:

1. [Увійдіть в обліковий запис ESET HOME](#).

i Якщо у вас немає облікового запису ESET HOME, клацніть **Створити обліковий запис** для реєстрації або дотримуйтеся відповідних інструкцій в [онлайн-довідці ESET HOME](#).
Якщо ви забули пароль, клацніть **Забули пароль?** і дотримуйтеся вказівок на екрані або перегляньте інструкції в [онлайн-довідці ESET HOME](#).

2. Задайте **назву** для пристрою, яке використовуватиметься в усіх службах ESET HOME і натисніть **Продовжити**.

3. Виберіть ліцензію для активації або [додайте нову ліцензію](#). Натисніть **Продовжити**, щоб активувати програму ESET NOD32 Antivirus.

Активація ліцензії для ознайомлювальної версії

Щоб активувати пробну версію ESET NOD32 Antivirus, введіть дійсну електронну адресу в полях **Адреса електронної пошти** та **Підтвердження адреси електронної пошти**. Після активації буде згенеровано й надіслано електронною поштою ліцензію ESET. На цю адресу також

надсилатимуться сповіщення про завершення терміну дії продукту та інші повідомлення від ESET. Пробну версію можна активувати лише раз.

Виберіть свою країну з розкривного меню **Країна**, щоб зареєструвати ESET NOD32 Antivirus у місцевого дистриб'ютора, який надаватиме технічну підтримку.

Безкоштовний ліцензійний ключ ESET

Повна ліцензія для ESET NOD32 Antivirus не безкоштовна.

Ліцензійний ключ ESET – це унікальна послідовність літер і цифр, розділених тире, що надається компанією ESET для використання ESET NOD32 Antivirus відповідно до умов [ліцензійної угоди з кінцевим користувачем](#). Кожен кінцевий користувач має право використовувати ліцензійний ключ тільки в тих межах, які визначені правом користування ESET NOD32 Antivirus у залежності від кількості ліцензій, наданих ESET. Ліцензійний ключ є конфіденційним, тому ви не можете ділитися ним з третіми особами. При цьому ви можете [ділитися ліцензійними робочими місцями на ESET HOME](#).

В Інтернеті можна знайти джерела, де пропонуються так звані "безкоштовні" ліцензійні ключі ESET. З цього приводу слід пам'ятати таке:

- Переходячи за посиланнями на зразок "Безкоштовна ліцензія ESET", ви ризикуєте безпекою свого комп'ютера або пристрою й можете інфікувати його шкідливим програмним забезпеченням. Шкідливе програмне забезпечення може бути приховане в неофіційному веб-вмісті (наприклад, у відео), на веб-сайтах із рекламою заробітку за відвідування певних сторінок тощо. Зазвичай такі ресурси використовуються для заманювання користувачів.
- ESET може заблокувати й блокує піратські ліцензії.
- Використання піратського ліцензійного ключа суперечить умовам [ліцензійної угоди з кінцевим користувачем](#), які ви маєте прийняти перед інсталяцією ESET NOD32 Antivirus.
- Купуйте ліцензії ESET тільки з офіційних джерел продажу — на веб-сайті www.eset.com, у дистриб'юторів або торговельних партнерів ESET (не купуйте ліцензії на неофіційних сторонніх веб-сайтах (eBay) або в третіх осіб).
- ESET NOD32 Antivirus [Завантажуються](#) безкоштовно, проте для їх активації під час інсталяції потрібен дійсний ліцензійний ключ ESET. Продукт можна завантажити й інсталювати, проте він не працюватиме без активації
- Не надавайте доступ до вашого ліцензійного ключа в Інтернеті або соціальних мережах, де його можуть поширити мережею.

Щоб ідентифікувати піратський ліцензійний ключ ESET і повідомити про нього, дотримуйтесь інструкцій [у нашій статті бази знань](#).

Якщо ви ще не визначилися з покупкою продукту захисту ESET, ви можете використовувати пробну версію протягом пробного періоду:

1. [Активуйте ESET NOD32 Antivirus із використанням безкоштовної пробної ліцензії](#)
2. [Візьміть участь у програмі тестування бета-версій продуктів ESET](#)
3. [Інсталюйте ESET Mobile Security](#) на мобільному пристрої Android. Це безкоштовна версія з платними функціями.

Щоб отримати знижку / подовжити термін дії ліцензії:

- [Порекомендуйте ESET NOD32 Antivirus друзям](#)
- [Поновіть ліцензію вашого продукту ESET](#) (якщо ви мали її раніше) або активуйте продукт на додатковий період часу

Помилка активації: поширені сценарії

Далі наведено можливі причини того, що продукт ESET NOD32 Antivirus не вдалось активувати.

- Ліцензійний ключ уже використовується
- Недійсний ліцензійний ключ. Помилка форми активації продукту
- Додаткові відомості, необхідні для активації, відсутні або недійсні.
- Помилка зв'язку з базою даних активації. Повторіть спробу через 15 хвилин.
- Відсутнє або вимкнене підключення до серверів активації ESET

Переконайтеся, що ви ввели правильний ліцензійний ключ, і спробуйте активувати його ще раз. Якщо для активації використовується обліковий запис ESET HOME, перегляньте інформацію в розділі [онлайн-довідки для керування ліцензією ESET HOME](#).

Якщо продукт однаково не вдалось активувати, скористайтесь [засобом для вирішення проблем з активацією ESET](#). У ньому наведено відповіді на поширені запитання, описи помилок і проблем з активацією та ліцензуванням (доступно англійською та ще кількома мовами).

Не вдалося виконати активацію через перевикористану ліцензію

Проблема

- Вашу ліцензію можуть використовувати несанкціоновано або забагато осіб
- Не вдалося виконати активацію через перевикористану ліцензію

Рішення

Вашу ліцензію використовують більше пристроїв, ніж нею дозволено. Можливо, ви стали жертвою піратства або підробки програмних продуктів. Цю ліцензію неможливо використати

для активації будь-якого іншого продукту ESET. Цю проблему можна вирішити безпосередньо, скориставшись правом керування ліцензією в обліковому записі ESET HOME або придбавши ліцензію в законний спосіб. Якщо у вас іще немає облікового запису, створіть його.

Якщо ви є власником ліцензії й не отримували запит на введення своєї адреси електронної пошти:

1. Щоб керувати ліцензією ESET, відкрийте веб-браузер і перейдіть на сторінку <https://home.eset.com>. Відкрийте ESET License Manager і видаліть або деактивуйте робочі місця. Щоб дізнатися більше, перегляньте розділ [Що робити, якщо ліцензію перевикористано](#).
2. Щоб ідентифікувати піратський ліцензійний ключ ESET і повідомити про нього, дотримуйтесь інструкцій [у цій статті](#).
3. Якщо у вас є сумніви щодо цієї дії, натисніть кнопку "**Назад**" і [надішліть електронний лист у службу підтримки ESET](#).

Якщо ви не власник ліцензії, повідомте її власнику, що вам не вдається активувати продукт ESET через перевищення ліміту використання ліцензії. Власник може вирішити проблему на порталі [ESET HOME](#).

Якщо з'явиться запит на підтвердження адреси електронної пошти (лише кілька випадків), введіть адресу електронної пошти, що використовувалася для придбання або активації ESET NOD32 Antivirus.

Оновлення ліцензії

Це діалогове вікно відображається, якщо змінено ліцензію, яка використовувалася для активації продукту ESET. Нова ліцензія дає змогу активувати продукт із більшою кількістю функцій захисту. Якщо ліцензію не було змінено, ESET NOD32 Antivirus один раз покаже вікно сповіщення **Перейти на продукт із більшою кількістю функцій**.

Так (рекомендується): автоматична інсталяція продукту з більшою кількістю функцій безпеки.

Ні, дякую: зміни не вноситимуться, сповіщення не відображатимуться.

Інформацію про те, як змінити продукт пізніше, див. в нашій [статті бази знань ESET](#). Більш докладну інформацію про ліцензії ESET див. в розділі [щодо ліцензування](#) (Питання й відповіді щодо ліцензування).

У таблиці нижче вказано функції, доступні в кожному продукті.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Ядро виявлення	✓	✓	✓
Розширене машинне навчання	✓	✓	✓
Захист від експлойтів	✓	✓	✓
Захист від атак на основі сценаріїв	✓	✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Захист від фішинг-атак	✓	✓	✓
Захист доступу до Інтернету	✓	✓	✓
Система запобігання вторгненням (HIPS) (зокрема, захист від програм-вимагачів)	✓	✓	✓
Антиспам		✓	✓
Брандмауер		✓	✓
Інспектор мережі		✓	✓
Захист веб-камери		✓	✓
Захист мережі від атак		✓	✓
Захист від ботнетів		✓	✓
Захист банківських операцій і платежів		✓	✓
Батьківський контроль		✓	✓
Антикрадій		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Оновлення продукту

Ви завантажили інсталятор за замовчуванням і вирішили змінити продукт для активації або замінити інстальований продукт на продукт із більшою кількістю функцій безпеки.

[Змінення продукту під час інсталяції.](#)

У таблиці нижче вказано функції, доступні в кожному продукті.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Ядро виявлення	✓	✓	✓
Розширене машинне навчання	✓	✓	✓
Захист від експлойтів	✓	✓	✓
Захист від атак на основі сценаріїв	✓	✓	✓
Захист від фішинг-атак	✓	✓	✓
Захист доступу до Інтернету	✓	✓	✓
Система запобігання вторгненням (HIPS) (зокрема, захист від програм-вимагачів)	✓	✓	✓
Антиспам		✓	✓
Брандмауер		✓	✓
Інспектор мережі		✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Захист веб-камери		✓	✓
Захист мережі від атак		✓	✓
Захист від ботнетів		✓	✓
Захист банківських операцій і платежів		✓	✓
Батьківський контроль		✓	✓
Антикрадій		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Пониження рівня ліцензії

Це діалогове вікно відображається, якщо змінено ліцензію, яка використовувалася для активації продукту ESET. Нову ліцензію можна використовувати тільки з іншим продуктом ESET із меншою кількістю функцій захисту. Продукт змінено автоматично, щоб запобігти втраті захисту.

Більш докладну інформацію про ліцензії ESET див. в розділі [щодо ліцензування](#) (Питання й відповіді щодо ліцензування).

У таблиці нижче вказано функції, доступні в кожному продукті.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Ядро виявлення	✓	✓	✓
Розширене машинне навчання	✓	✓	✓
Захист від експлоїтів	✓	✓	✓
Захист від атак на основі сценаріїв	✓	✓	✓
Захист від фішинг-атак	✓	✓	✓
Захист доступу до Інтернету	✓	✓	✓
Система запобігання вторгненням (HIPS) (зокрема, захист від програм-вимагачів)	✓	✓	✓
Антиспам		✓	✓
Брандмауер		✓	✓
Інспектор мережі		✓	✓
Захист веб-камери		✓	✓
Захист мережі від атак		✓	✓
Захист від ботнетів		✓	✓
Захист банківських операцій і платежів		✓	✓
Батьківський контроль		✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Антикравдій		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Пониження версії продукту

Щойно інстальований продукт має більше функцій захисту, ніж продукт, який ви збираєтесь активувати.

У таблиці нижче вказано функції, доступні в кожному продукті.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Ядро виявлення	✓	✓	✓
Розширене машинне навчання	✓	✓	✓
Захист від експлойтів	✓	✓	✓
Захист від атак на основі сценаріїв	✓	✓	✓
Захист від фішинг-атак	✓	✓	✓
Захист доступу до Інтернету	✓	✓	✓
Система запобігання вторгненням (HIPS) (зокрема, захист від програм-вимагачів)	✓	✓	✓
Антиспам		✓	✓
Брандмауер		✓	✓
Інспектор мережі		✓	✓
Захист веб-камери		✓	✓
Захист мережі від атак		✓	✓
Захист від ботнетів		✓	✓
Захист банківських операцій і платежів		✓	✓
Батьківський контроль		✓	✓
Антикравдій		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Засіб виправлення неполадок під час

інсталяції

Якщо під час інсталяції виникнуть проблеми, у майстрі інсталяції буде запропоновано скористатися засобом виправлення неполадок, який усуває проблему, якщо це можливо.

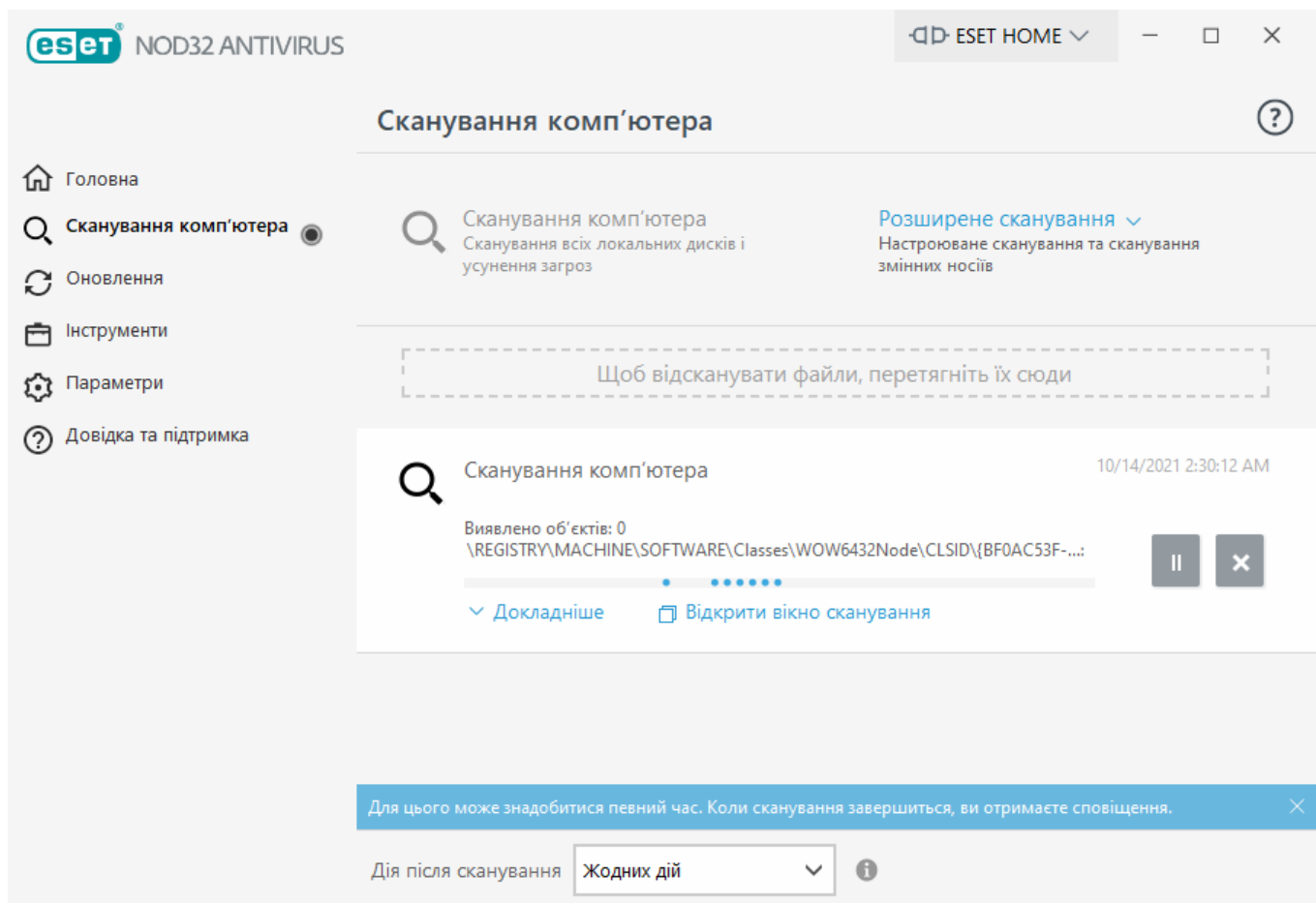
Клацніть **Запустити засіб виправлення неполадок**, щоб запустити його. Коли засіб виправлення неполадок завершить роботу, виконайте рекомендовані дії.

Якщо все одно не вдається вирішити проблему, див. список [поширених помилок інсталяції та рішень](#).

Перше сканування після інсталяції

Після інсталяції продукту ESET NOD32 Antivirus й першого успішного оновлення програма починає сканувати комп'ютер на наявність зловмисного коду.

Сканування комп'ютера також можна запустити вручну, натиснувши **Сканування комп'ютера** > **Сканування комп'ютера** у [головному вікні програми](#). Докладніші відомості про перевірку комп'ютера див. у розділі [Сканування комп'ютера](#).



Оновлення до останньої версії

Нові версії ESET NOD32 Antivirus містять програмні вдосконалення й виправлення помилок, які не можна усунути під час автоматичного оновлення програмних модулів. Оновити програму до

новішої версії можна кількома способами:

1. Автоматично, за допомогою оновлення програми.

Оновлення програми надсилаються всім без винятку користувачам і можуть впливати на певні системні конфігурації. Тому оновлення стають доступними лише після тривалого тестування: це гарантує, що програма належним чином працюватиме з усіма можливими системними конфігураціями. Якщо ви хочете інстальовати новішу версію відразу після її випуску, скористайтесь одним із наведених нижче методів.

Переконайтеся, що ввімкнено параметр **Оновлення функцій програми** в розділі **Додаткові параметри (F5) > Оновлення > Профілі > Оновлення**.

2. Уручну. Для цього в [головному вікні програми](#) відкрийте розділ **Оновлення** й клацніть **Перевірка наявності оновлень**.

3. Уручну, завантаживши й [інстальовавши новішу версію](#) поверх попередньої.


Додаткову інформацію й ілюстровані інструкції див. в таких статтях:

- [Оновлення продуктів ESET: перевірка наявності оновлень для модулів продукту](#)
- [Чим оновлення продукту ESET відрізняється від типів випуску?](#)

Автоматичне оновлення застарілих продуктів

Версія вашого продукту ESET більше не підтримується. Ваш продукт оновлено до останньої версії.

 [Поширені проблеми під час інсталяції](#)

 Кожна нова версія продуктів ESET містить багато виправлень і покращень. Клієнти з дійсною ліцензією на продукт ESET можуть отримати його актуальну версію безкоштовно.

Порядок завершення інсталяції

1. Клацніть **Прийняти й продовжити**, щоб прийняти умови [ліцензійної угоди з кінцевим користувачем](#) і [політики конфіденційності](#). Якщо ви не погоджуєтесь з умовами ліцензійної угоди з кінцевим користувачем, клацніть **Видалити**. Повернутися до попередньої версії неможливо.

2. Натисніть **Дозволити все й продовжити**, щоб дозволити [Систему зворотного зв'язку ESET LiveGrid®](#) і [Програму підвищення якості програмного забезпечення](#), або натисніть **Продовжити**, якщо ви не хочете брати участь.

3. Після активації нового продукту ESET за допомогою ліцензійного ключа відобразиться головна сторінка. Якщо інформацію про ліцензію не вдасться знайти, продукт працюватиме з новою пробною ліцензією. Якщо ліцензія, використовувана в попередньому продукті, недійсна, [активуйте продукт ESET](#).

4. Для завершення інсталяції необхідно перезавантажити комп'ютер.

Рекомендація продукту ESET другу або подрузі

У цій версії ESET NOD32 Antivirus передбачено бонуси за залучення нових користувачів, щоб заохотити вас ділитися враженнями від продукту ESET із членами родини або друзями. Ви можете залучати нових користувачів навіть із продукту, який активовано пробною ліцензією. Якщо ви використовуєте пробну версію, за кожного успішно залученого користувача (реферала), який у кінцевому підсумку активує продукт, ви й ваш друг (подруга) отримаєте додатковий час користування пробною ліцензією.


Ви можете запросити користувачів, використовуючи для цього інстальований ESET NOD32 Antivirus. Продукт, який ви можете рекомендувати, залежить від продукту, з якого ви надаєте рекомендації. Див. таблицю нижче.

Ваш інстальований продукт	Продукт, який ви можете порекомендувати
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Рекомендація продукту

Щоб надіслати реферальне посилання, виберіть пункт **Запросіть друга** в головному меню ESET NOD32 Antivirus. Клацніть **Поділитися реферальним посиланням**. Ваш продукт згенерує реферальне посилання, яке буде відображатись у новому вікні. Скопіюйте посилання й надішліть його членам родини та друзям. Є декілька способів поділитися реферальним посиланням безпосередньо з продукту ESET, які представлено параметрами **Поділитися в Facebook**, **Запросіть користувачів із контактів Gmail** і **Поділитися в Twitter**.

Коли ваш друг бо подруга перейдуть за надісланим вами реферальним посиланням, для них буде відкрито веб-сторінку, де вони зможуть завантажити продукт безпеки й БЕЗКОШТОВНО використовувати його ще один місяць. Як користувач пробної версії ви отримаєте сповіщення для кожного реферального посилання, за яким було виконано активацію, після чого термін дії вашої ліцензії буде автоматично подовжено ще на місяць БЕЗКОШТОВНОГО захисту. У такий спосіб ви можете БЕЗКОШТОВНО подовжити дію ліцензії для продукту безпеки на термін до 5 місяців. Кількість реферальних посилань, за якими було виконано активацію, можна перевірити у вікні **Запросіть друга** вашого продукту ESET.

 Можливість рекомендувати продукт може бути недоступною для вашої мови або вашого регіону.

ESET NOD32 Antivirus буде інстальовано

Це діалогове вікно може відображатися в таких випадках:

- Під час інсталяції. Клацніть **Продовжити**, щоб інстальувати ESET NOD32 Antivirus.

- Під час зміни ліцензії в ESET NOD32 Antivirus. Клацніть **Активувати**, щоб змінити ліцензію та активувати ESET NOD32 Antivirus.

Параметр **Змінити продукт** дає змогу вибирати домашні версії продуктів ESET для Windows відповідно до наявної ліцензії ESET. Більш докладну інформацію див. в розділі [Визначення продукту](#).

Змінити на іншу продуктову лінійку

Відповідно до вашої ліцензії ESET можна вибирати домашні версії продуктів ESET для Windows. Більш докладну інформацію див. в розділі [Визначення продукту](#).

Реєстрація

Зареєструйте ліцензію, заповнивши всі поля відповідної форми, і натисніть Продовжити. Не пропускайте поля, які позначено в дужках як обов'язкові. Ця інформація використовуватиметься лише для вирішення питань із ліцензією ESET.

Хід активації

Зачекайте кілька секунд, доки активацію буде завершено (час, потрібний для виконання цієї операції, залежить від швидкості інтернет-з'єднання або роботи комп'ютера).

Успішне завершення активації

Активацію успішно завершено.

Через кілька секунд буде оновлено модуль. Негайно ввімкнеться регулярне оновлення програми ESET NOD32 Antivirus.

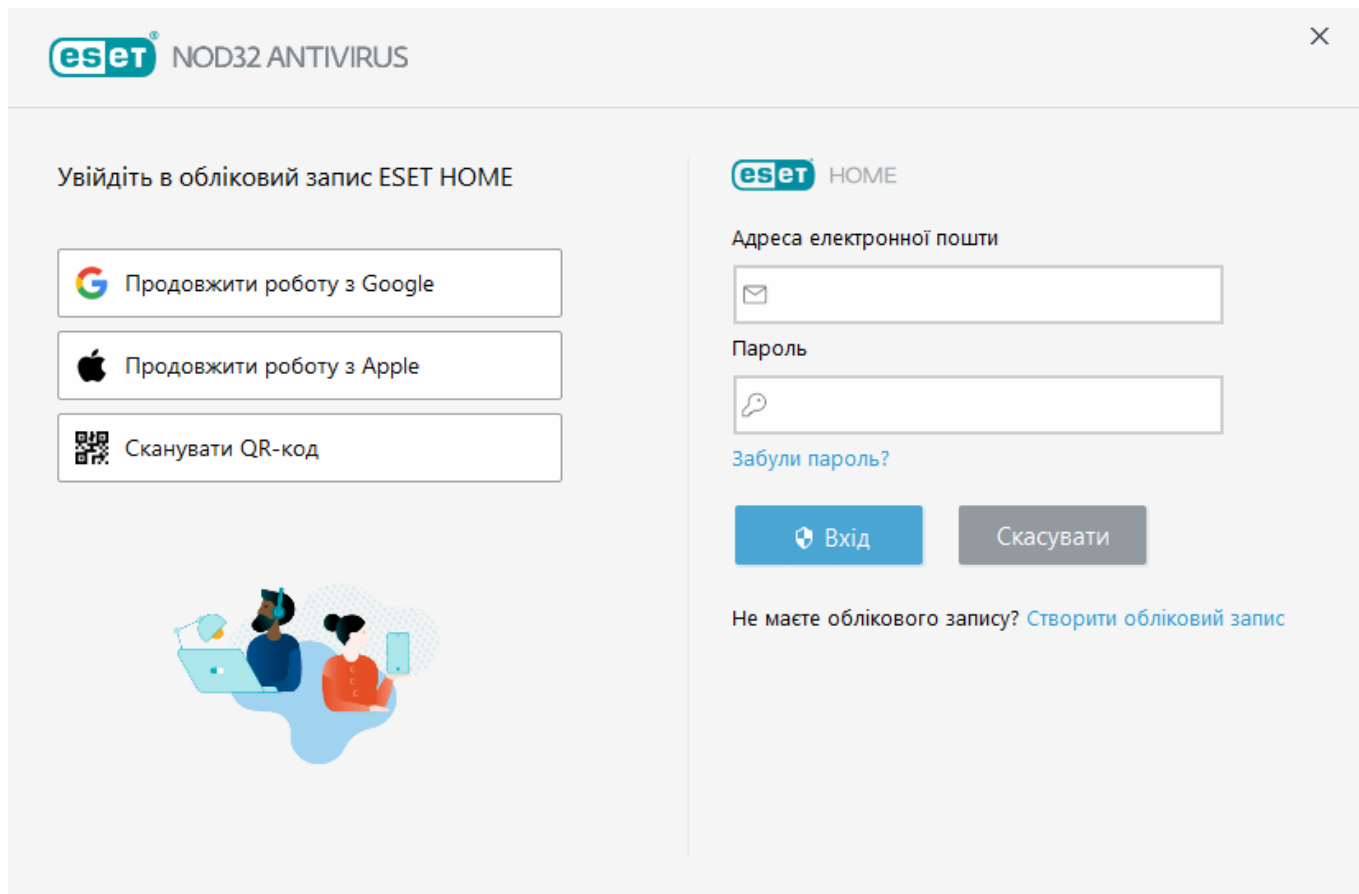
Перше сканування автоматично запуститься через 20 хвилин після оновлення модуля.

Посібник для початківців

У цьому розділі наведено загальний опис продукту ESET NOD32 Antivirus та його основних параметрів.

Підключіться до ESET HOME

Підключіть свій пристрій на [ESET HOME](#), щоб переглядати всі активовані ліцензії та пристрої ESET і керувати ними. Ви можете поновити, оновити або розширити ліцензію та переглянути важливу інформацію про неї. На порталі керування ESET HOME або в мобільній програмі можна додавати інші ліцензії, завантажувати продукти на пристрої, перевіряти статус безпеки продукту або надавати спільний доступ до ліцензій електронною поштою. Щоб дізнатися більше, відвідайте [онлайн-довідки ESET HOME](#).



Підключіть свій пристрій до ESET HOME:

Якщо ви підключаєтеся ESET HOME під час інсталяції або вибрали для активації метод **Використовувати обліковий запис ESET HOME**, дотримуйтеся інструкцій у темі [Використання облікового запису ESET HOME](#).

i Якщо ви вже інстальювали ESET NOD32 Antivirus і активували його за допомогою ліцензії, доданої в обліковому записі ESET HOME, ви можете підключити свій пристрій до ESET HOME на порталі ESET HOME. Див. інструкції в [онлайн-довідці ESET HOME](#) й [дозвольте підключення в ESET NOD32 Antivirus](#).

1. У [головному вікні програми](#) клацніть **ESET HOME > Підключитися до ESET HOME** або виберіть **Підключитися до ESET HOME** у сповіщенні **Підключіть цей пристрій до облікового запису ESET HOME**.

2. [Вхід в обліковий запис ESET HOME](#).

i Якщо у вас немає облікового запису ESET HOME, клацніть **Створити обліковий запис** для реєстрації або дотримуйтеся відповідних інструкцій в [онлайн-довідці ESET HOME](#). Якщо ви забули пароль, клацніть **Забули пароль?** і дотримуйтеся вказівок на екрані або перегляньте інструкції в [онлайн-довідці ESET HOME](#).

3. Задайте **назву пристрою** та натисніть **Продовжити**.

4. Після підключення з'явиться вікно відомостей. Натисніть **Готово**.


Вхід у ESET HOME

Існує кілька способів входу в обліковий запис ESET HOME.


- **За допомогою адреси електронної пошти й пароля ESET HOME:** уведіть **адресу електронної пошти й пароль**, які використовувалися для створення облікового запису ESET HOME, і клацніть **Увійти**.
- **За допомогою облікового запису Google/AppleID:** клацніть **Продовжити роботу з Google** або **Продовжити роботу з Apple** і увійдіть у відповідний обліковий запис. Після успішного входу відкриється веб-сторінка підтвердження ESET HOME. Щоб продовжити, поверніться у вікно продукту ESET. Більш докладну інформацію про вхід за допомогою облікового запису Google або AppleID див. в [онлайн-довідці ESET HOME](#).
- **Сканувати QR-код:** клацніть **Сканувати QR-код**, щоб показати QR-код. Відкрийте мобільну програму ESET HOME і відскануйте QR-код або спрямуйте камеру пристрою на QR-код. Більш докладну інформацію див. в інструкціях [онлайн-довідки ESET HOME](#).


i Якщо у вас немає облікового запису ESET HOME, клацніть **Створити обліковий запис** для реєстрації або дотримуйтеся відповідних інструкцій в [онлайн-довідці ESET HOME](#).
Якщо ви забули пароль, клацніть **Забули пароль?** і дотримуйтеся вказівок на екрані або перегляньте інструкції в [онлайн-довідці ESET HOME](#).


! [Не вдалося виконати вхід: поширені помилки.](#)





Увійдіть в обліковий запис ESET HOME

 Продовжити роботу з Google

 Продовжити роботу з Apple

 Сканувати QR-код





Адреса електронної пошти

Пароль

[Забули пароль?](#)

Вхід

Скасувати

Не маєте облікового запису? [Створити обліковий запис](#)

Не вдалося виконати вхід: поширені помилки

Не вдалося знайти обліковий запис, який відповідає вказаній адресі електронної пошти

Уведена адреса електронної пошти не відповідають жодному обліковому запису ESET HOME. Клацніть **Назад** і введіть правильну адресу електронної пошти й пароль.

Щоб увійти, необхідно створити обліковий запис ESET HOME. Якщо у вас немає облікового запису ESET HOME, клацніть **Назад > Створити обліковий запис** або див. інструкції в розділі [Створення нового облікового запису ESET HOME](#).

Ім'я користувача й пароль не збігаються

Уведений пароль не збігається з введеною адресою електронної пошти. Клацніть **Назад**, уведіть правильний пароль і переконайтеся, що вказана адреса електронної пошти правильна. Якщо вам не вдається увійти, клацніть **Назад > Забули пароль?**, щоб скинути пароль, і дотримуйтеся інструкцій на екрані, або див. розділ [Відновлення втраченого пароля ESET HOME](#).

Вибраний варіант входу не підтримується вашим обліковим записом

Ваш обліковий запис пов'язано з вашим обліковим записом у соціальній мережі. Щоб увійти в ESET HOME, клацніть **Продовжити роботу з Google** або **Продовжити роботу з Apple** і увійдіть у відповідний обліковий запис. Після успішного входу відкриється веб-сторінка підтвердження ESET HOME. Обліковий запис у соціальних мережах можна відключити від ESET HOME на порталі ESET HOME.

Неправильний пароль

Ця помилка може виникати, якщо ESET NOD32 Antivirus вже підключено до ESET HOME і ви вносите зміни, для яких потрібно виконати вхід (наприклад, вам потрібно вимкнути модуль Антикравд), а введений пароль не відповідає вашому обліковому запису. Клацніть **Назад** і введіть правильний пароль. Якщо вам не вдається увійти, клацніть **Назад > Забули пароль?**, щоб скинути пароль, і дотримуйтеся інструкцій на екрані, або див. розділ [Відновлення втраченого пароля ESET HOME](#).

Додавання пристрою в ESET HOME

Якщо ви вже інстальювали ESET NOD32 Antivirus і активували його за допомогою ліцензії, доданої в обліковому записі ESET HOME, ви можете підключити свій пристрій до ESET HOME на порталі ESET HOME:

1. [Надішліть запит на підключення на ваш пристрій.](#)

2. У ESET NOD32 Antivirus відкриється діалогове вікно **Підключити цей пристрій до облікового запису ESET HOME** з іменем облікового запису ESET HOME. Клацніть **Дозволити**, щоб підключити пристрій до вказаного облікового запису ESET HOME.

i Якщо зв'язок відсутній, запит на підключення буде скасовано автоматично приблизно через 30 хвилин.

Головне вікно програми

Головне вікно ESET NOD32 Antivirus розділено на дві основні частини. В основному вікні, що праворуч, відображається інформація, яка відповідає вибраній у головному меню зліва опції.

Ілюстровані інструкції

i У розділі [Open the main program window of ESET Windows products](#) (Відкриття головного вікна програми продуктів ESET для Windows) є ілюстровані інструкції, доступні англійською й деякими іншими мовами.

ESET HOME: [Підключіть пристрій до ESET HOME](#). У [ESET HOME](#) можна переглядати активовані ліцензії та пристрої ESET і керувати ними.

Нижче наведено опис опцій головного меню.

Головна – вміщує інформацію про стан захисту ESET NOD32 Antivirus.

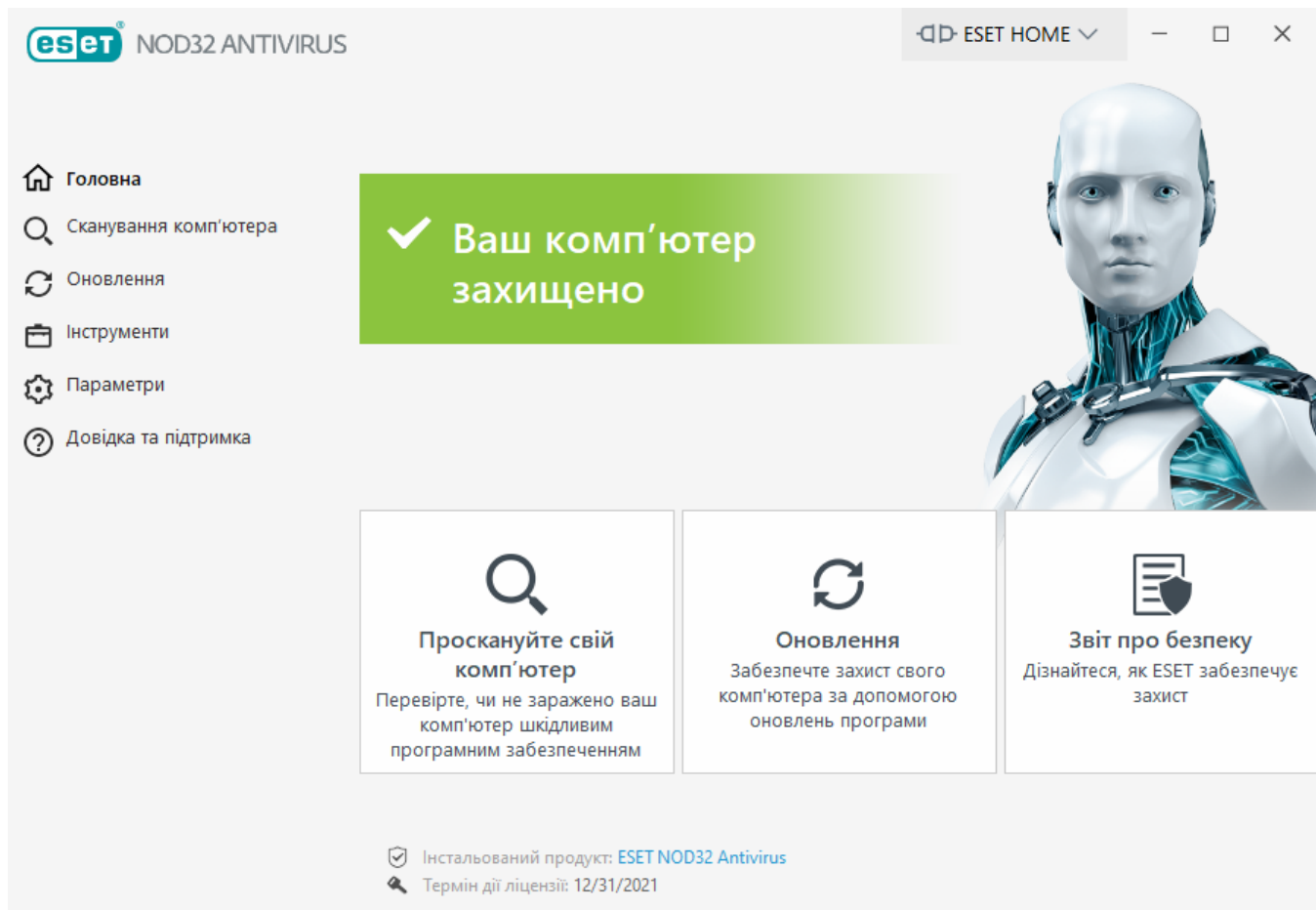
Сканування комп'ютера – налаштуйте й запустіть сканування комп'ютера або створіть спеціальне сканування.

Оновлення – відображення інформації про оновлення обробника виявлення.

Інструменти – надає доступ до модулів, завдяки яким спрощується адміністрування програми та відкриваються додаткові можливості для досвідчених користувачів. Докладну інформацію можна переглянути в розділі [інструментів у продукті ESET NOD32 Antivirus](#).

Параметри – виберіть цю опцію, щоб налаштувати рівень захисту для параметрів "Комп'ютер", "Інтернет".

Довідка та підтримка – доступ до файлів довідки, [бази знань ESET](#), веб-сайту ESET, а також посилань, за допомогою яких можна подати запит до служби підтримки.



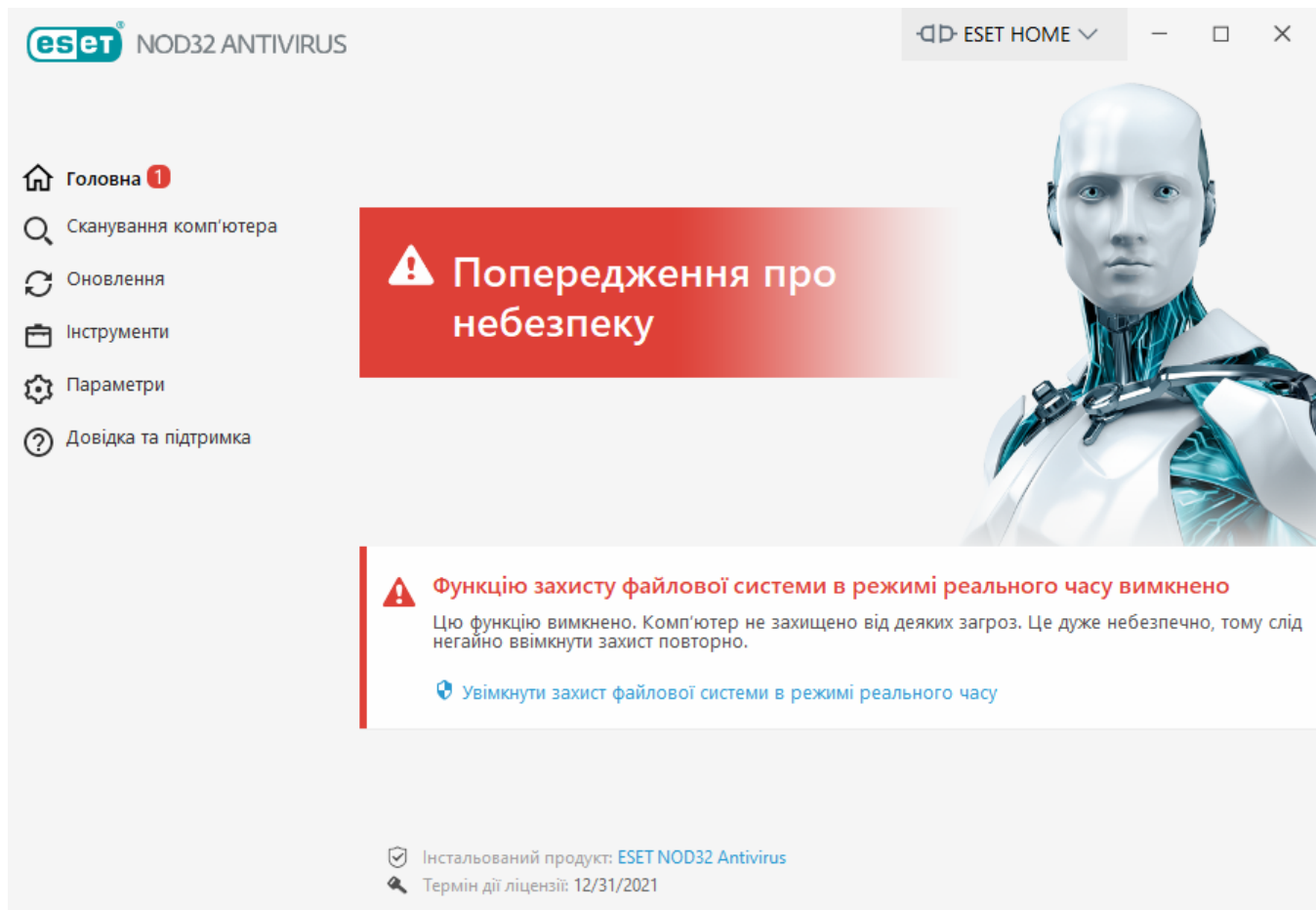
На **головному** екрані міститься важлива інформація про поточний рівень захисту комп'ютера. У вікні статусу відображаються часто використовувані функції програми ESET NOD32 Antivirus. Тут також наведено інформацію про інстальований продукт і дату завершення терміну дії ліцензії. Щоб інстальувати іншу версію продукту ESET, натисніть **ESET NOD32 Antivirus**. [Докладніше про функції кожного продукту](#).



Зелена піктограма і статус **Ваш комп'ютер захищено** вказують на максимально можливий рівень захисту системи.

Якщо програма не працює належним чином


Якщо модуль активного захисту працює правильно, відображається зелена піктограма статусу захисту. Якщо максимальний рівень захисту не забезпечується, відображається червоний знак оклику чи оранжева піктограма сповіщення. Додаткова інформація щодо статусу захисту кожного модуля та рекомендації щодо того, як відновити максимальний рівень безпеки, відображаються в розділі **Головна**. Щоб змінити статус окремих модулів, натисніть **Параметри** та виберіть потрібний модуль.



 Червона піктограма та червоний статус **Попередження про безпеку** свідчать про критичні проблеми.

Такий статус може з'являтися з кількох причин. Нижче наведено деякі з них.

- **Продукт не активовано або термін дії ліцензії завершився:** на цю проблему вказує червона піктограма статусу захисту. Після завершення терміну дії ліцензії програма не оновлюватиметься. Щоб оновити ліцензію, дотримуйтесь інструкцій, наведених у вікні тривоги.
- **Обробник виявлення застарілий:** ця помилка відображається після кількох невдалих спроб оновити обробник виявлення. Рекомендується перевірити параметри оновлення. Найпоширеніша причина помилки – неправильно введені [дані автентифікації](#) чи неналежним чином налаштовані [параметри підключення](#).
- **Функцію захисту файлової системи в режимі реального часу вимкнено:** захист у режимі реального часу вимкнено користувачем. Ваш комп'ютер не захищено від загроз. Клацніть **Увімкнути захист файлової системи в режимі реального часу**, щоб відновити дію функції.
- **Антивірус і антишпигун вимкнено** – антивірус і антишпигун можна повторно активувати, натиснувши **Увімкнути антивірус і антишпигун**.

 Оранжева піктограма свідчить про те, що захист обмежено (наприклад, через те що під час оновлення програми сталася помилка або термін дії ліцензії незабаром завершується).
Такий статус може з'являтися з кількох причин.

Такий статус може з'являтися з кількох причин. Нижче наведено деякі з них.

- **Ігровий режим активний** – коли [ігровий режим](#) увімкнено, системі може загрозувати небезпека. Після ввімкнення цієї функції вимикаються всі спливаючі вікна та припиняється виконання всіх запланованих завдань.
- **Термін дії ліцензії скоро закінчиться** – на цю проблему вказує піктограма статусу захисту, у якій відображається знак оклику поруч із системним годинником. Після завершення терміну дії ліцензії програма не оновлюватиметься, а піктограма статусу захисту стане червоною.

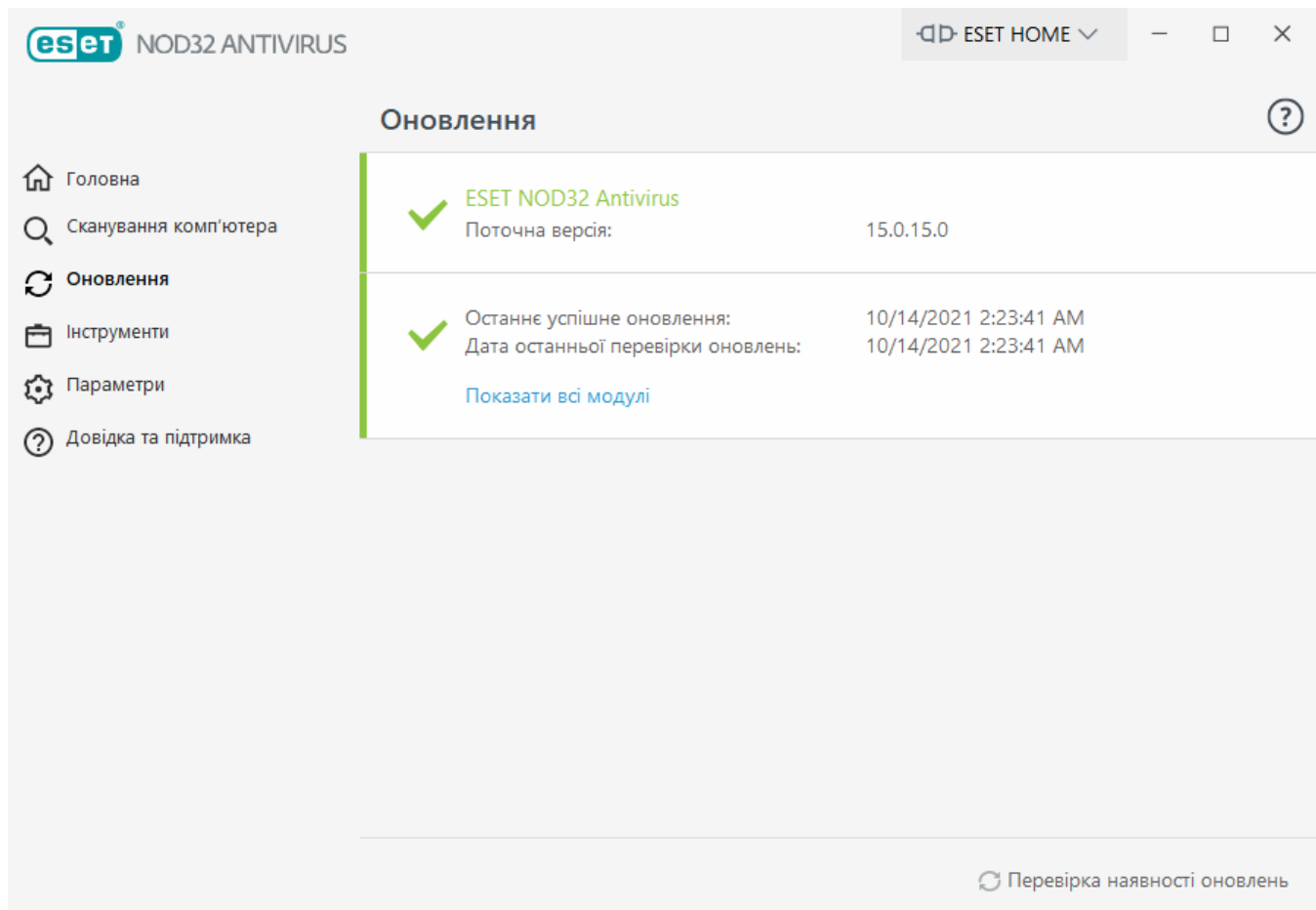
Якщо вирішити проблему за допомогою наведених рекомендацій не вдається, клацніть **Довідка та підтримка**, щоб перейти до файлів довідки, або виконайте пошук у [базі знань ESET](#). Якщо вам усе одно потрібна допомога, зверніться до служби підтримки. Спеціалісти служби технічної підтримки ESET швидко нададуть відповідь на ваші запитання й допоможуть знайти спосіб вирішення проблеми.

Оновлення

Регулярне оновлення ESET NOD32 Antivirus – найкращий спосіб забезпечити максимальний захист комп'ютера. Модуль оновлення гарантує, що модулі програми й компоненти системи завжди матимуть актуальний стан.

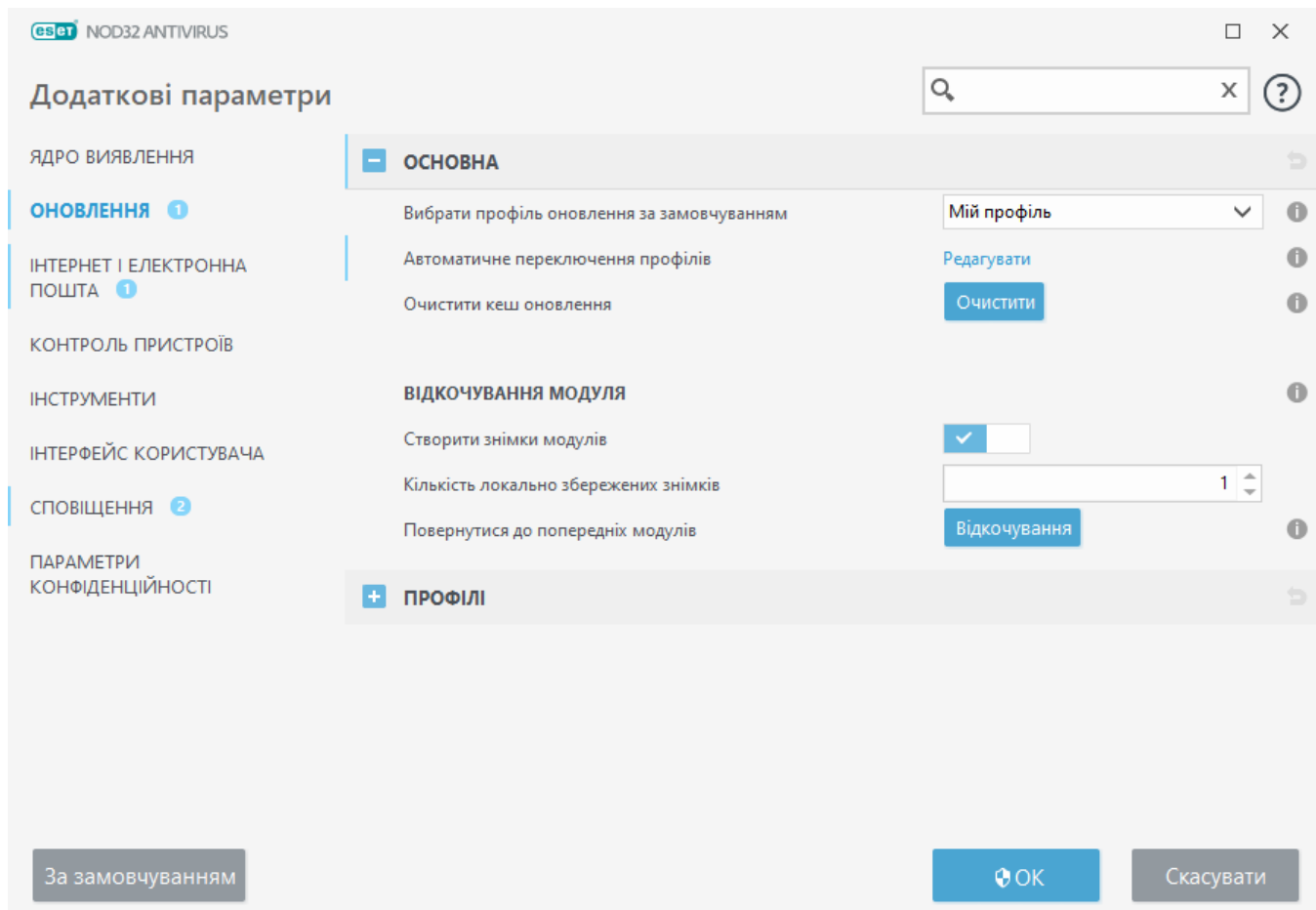
Натиснувши **Оновлення** в [головному вікні програми](#), можна переглянути поточний стан оновлення, відомості про дату й час останнього успішного оновлення, а також про те, чи потрібно його виконувати зараз.

Оновлення можна виконувати не лише автоматично. Також можна натиснути **Перевірити наявність оновлень**, щоб ініціювати оновлення вручну.



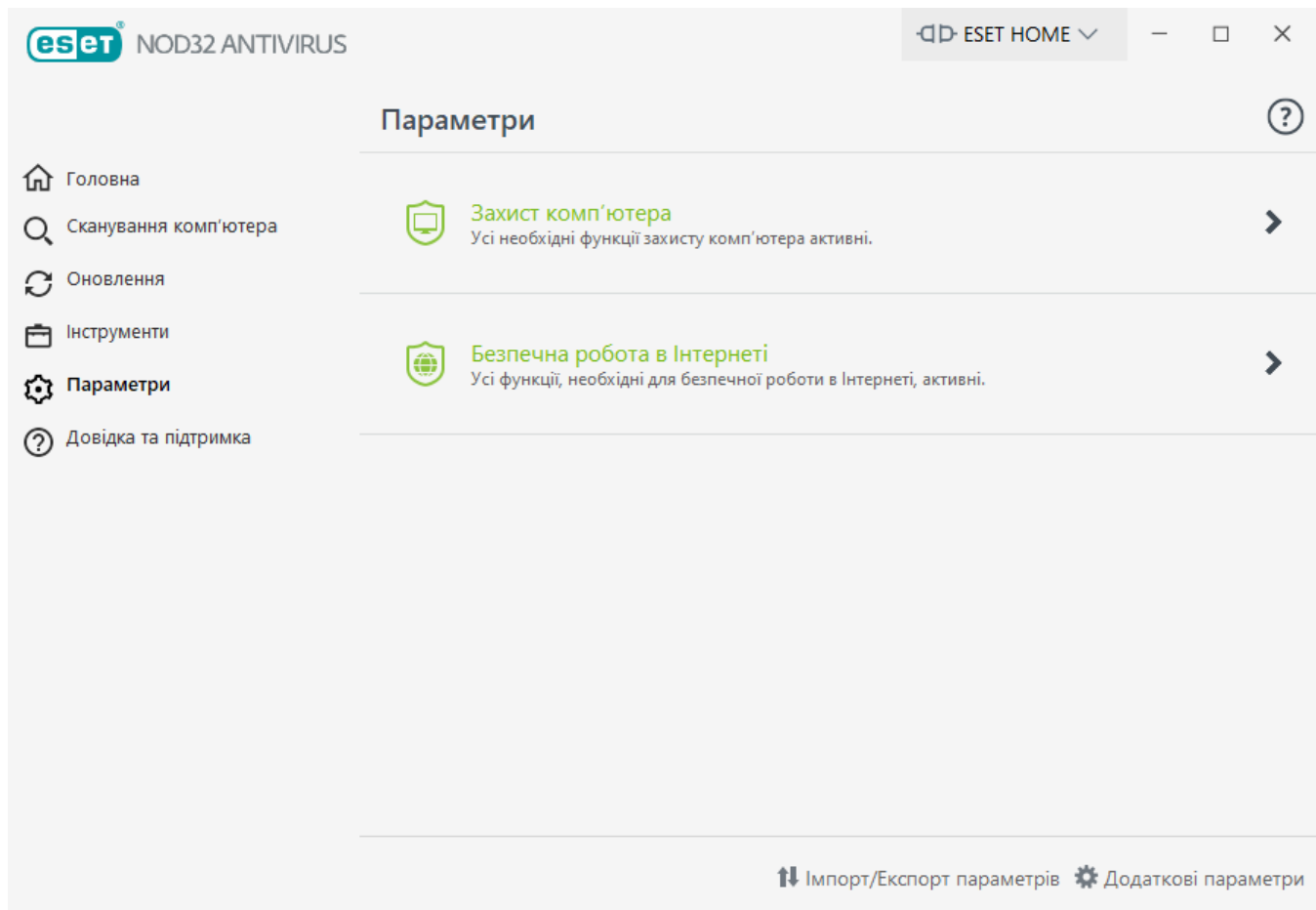
Вікно додаткових параметрів (у головному меню клацніть **Параметри**, потім виберіть **Додаткові параметри** або натисніть **F5** на клавіатурі) містить додаткові опції оновлення (наприклад, режим оновлення, доступ до проксі-сервера, підключення до локальної мережі тощо). Щоб налаштувати їх, у дереві "Додаткові параметри" клацніть **Оновити**.

Якщо виникнуть проблеми з оновленням, клацніть **Очистити** й видаліть усі файли кешу оновлення. Якщо все одно не вдається оновити модулі програми, див. статтю [Виправлення неполадок, пов'язаних із появою повідомлення "Помилка оновлення модулів"](#).



Робота з ESET NOD32 Antivirus

Параметри ESET NOD32 Antivirus дають можливість коригувати рівні захисту комп'ютера.



Меню **Параметри** поділено на наведені нижче розділи.



Захист комп'ютера



Безпечна робота в Інтернеті

Натисніть один із компонентів, щоб налаштувати додаткові параметри для відповідного модуля захисту.



За допомогою параметрів захисту в розділі **Комп'ютер** можна увімкнути або вимкнути такі компоненти:


- **Захист файлової системи в режимі реального часу:** усі файли перевіряються на наявність шкідливого коду під час відкриття, створення або запуску.
- **Контроль пристроїв** – за допомогою цього модуля користувач може сканувати та блокувати пристрої, налаштовувати розширені фільтри/дозволи, а також контролювати доступ до певних пристроїв і користування ними (компакт-/DVD-диск/запам'ятовуючий пристрій USB тощо).
- **Система запобігання вторгненням (HIPS)** – система [HIPS](#) стежить за системними подіями й реагує на них відповідно до спеціально визначеного набору правил.
- **Ігровий режим** – увімкнення або вимкнення [ігрового режиму](#). Після увімкнення ігрового режиму відобразиться попередження (потенційна загроза для безпеки), а колір головного

вікна зміниться на оранжевий.

Налаштування **Захист від загроз з Інтернету** дає змогу вмикати й вимикати наведені нижче компоненти.

- **Захист доступу до Інтернету:** якщо ввімкнено, увесь трафік, який проходить через протокол HTTP або HTTPS, сканується на наявність шкідливого програмного забезпечення.
- **Захист поштового клієнта:** відстеження обміну даними через протоколи POP3(S) та IMAP(S).
- **Захист від фішинг-атак** – відфільтровує веб-сайти, які підозрюються в поширенні вмісту для маніпулювання користувачами й отримання конфіденційної інформації.

Щоб повторно ввімкнути вимкнутий компонент захисту, натисніть повзунок . Має відображатися зелена позначка .


 Якщо вимкнути захист у такий спосіб, усі вимкнуті компоненти буде ввімкнуто знову після перезапуску комп'ютера.


У нижній частині вікна параметрів доступні додаткові опції. Перейдіть за посиланням **Додаткові параметри**, щоб налаштувати детальніші параметри для кожного модуля. Скористайтесь опцією **Параметри імпорту/експорту**, щоб завантажити параметри з файлу конфігурації формату .xml або зберегти поточні параметри в такий файл.


Захист комп'ютера


Натисніть **Захист комп'ютера** у вікні **Параметри**, щоб переглянути загальні відомості про всі модулі захисту:

- [Захист файлової системи в режимі реального часу](#)
- [Контроль пристроїв](#)
- [Систему запобігання вторгненням \(HIPS\)](#)
- [Ігровий режим](#)

Щоб призупинити або вимкнути певні модулі захисту, клацніть піктограму повзунка .

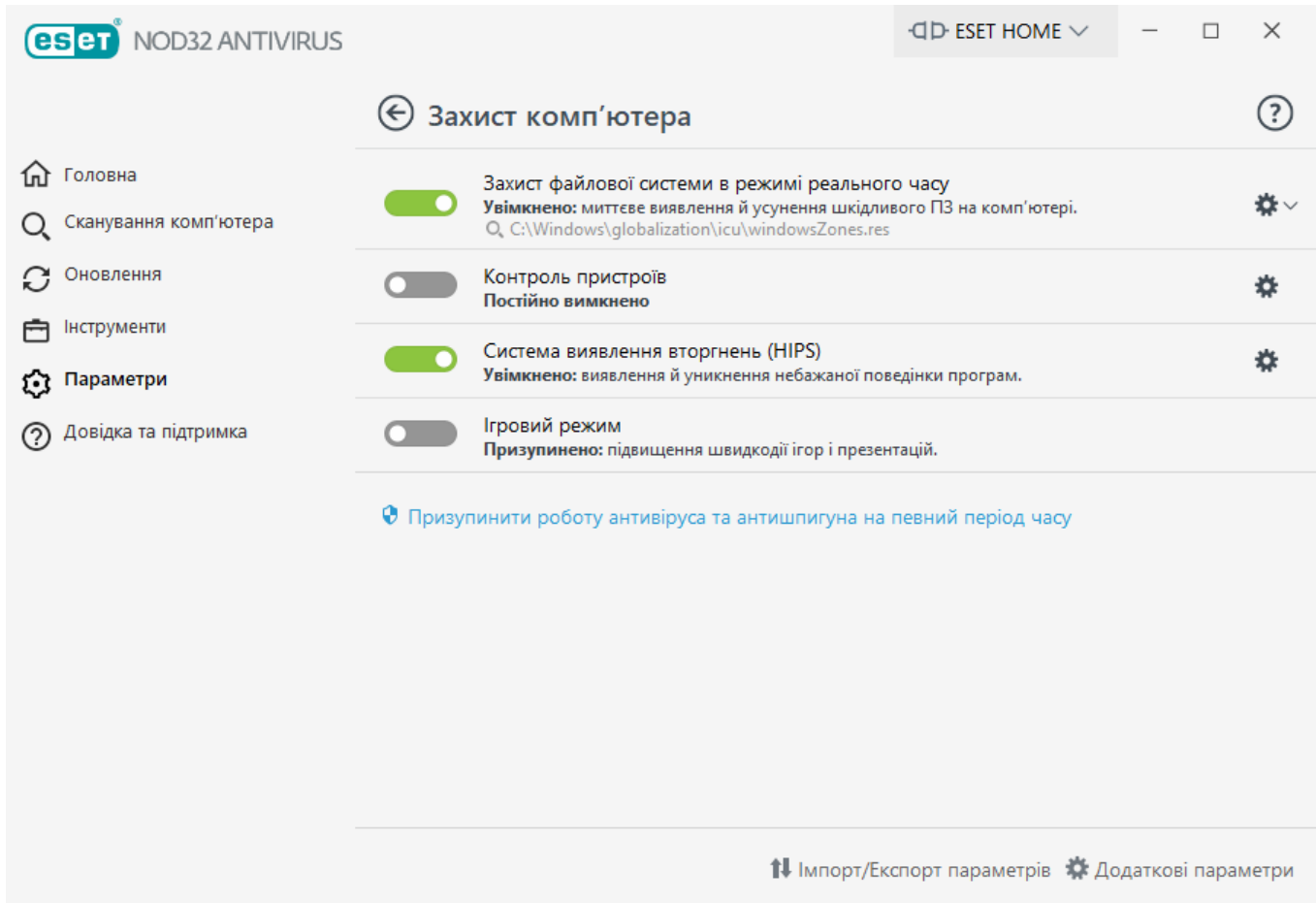
 Вимкнення модулів захисту може зменшити рівень захисту комп'ютера.

Клацніть піктограму шестерні  поруч із потрібним модулем захисту, щоб відкрити його додаткові налаштування.

Щоб увімкнути **Захист файлової системи в режимі реального часу**, клацніть піктограму шестерні  і виберіть один із таких параметрів:

- **Налаштувати:** відкриває додаткові параметри захисту файлової системи в режимі реального часу.

- **Змінити виключення:** відкриває [вікно налаштування виключень](#), де можна вибрати файли й папки, які не потрібно сканувати.



Призупинити роботу антивірусу та антишпигуна на певний період часу: вимкнення всіх антивірусних і антишпигунських модулів. Коли ви вимкнете захист, відкриється вікно, де в розкривному меню **Проміжок часу** можна вибрати час, протягом якого його буде вимкнено. Цей параметр слід застосовувати лише досвідченим користувачам або в тих випадках, коли цього вимагають спеціалісти служби технічної підтримки ESET.

Ядро виявлення

Ядро виявлення захищає систему від зловмисних атак шляхом контролю файлів, повідомлень електронної пошти й обміну даними в Інтернеті. Наприклад, якщо об'єкт класифіковано як шкідливе програмне забезпечення, запускається його виправлення. Ядро виявлення може знешкодити його: спочатку він блокується, потім очищається, видаляється або переміщується до карантину.

Щоб налаштувати параметри ядра виявлення, клацніть **Додаткові параметри** або натисніть клавішу **F5**.



Зміни в налаштування ядра виявлення має вносити лише досвідчений користувач. Неправильна конфігурація параметрів може призвести до зниження рівня захисту.

У цьому розділі:

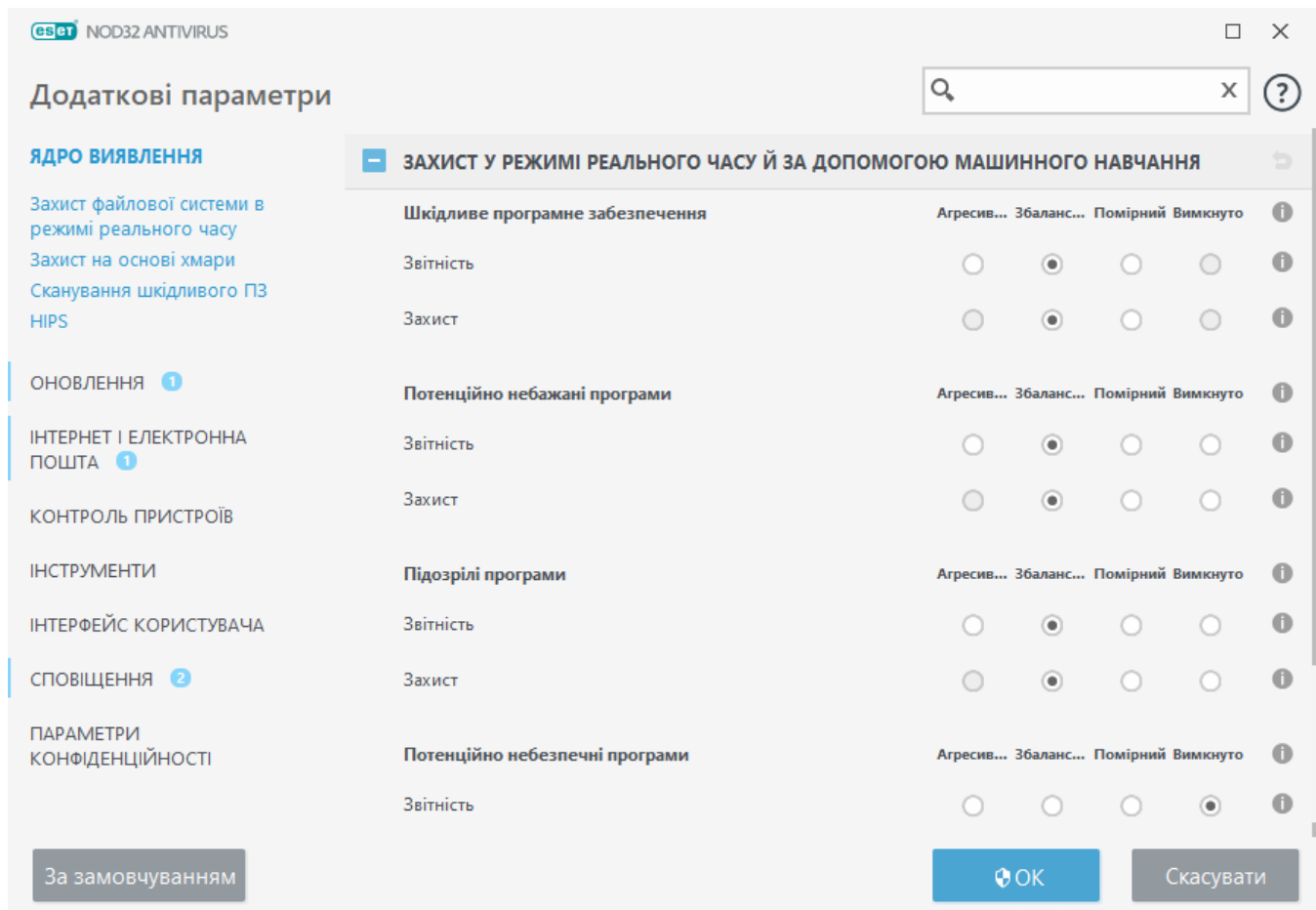
- [Категорії захисту в режимі реального часу й за допомогою машинного навчання](#)

- [Сканування шкідливого програмного забезпечення](#)
 - [Налаштування звітування](#)
 - [Налаштування захисту](#)
-

Категорії захисту в режимі реального часу й за допомогою машинного навчання

Захист у реальному часі й за допомогою машинного навчання для всіх модулів захисту (наприклад, "Захист файлової системи в режимі реального часу", "Захист доступу до інтернету" тощо) дозволяє налаштувати рівні звітування й захисту для наведених нижче категорій:

- **Шкідливе програмне забезпечення** (вірус) — це певний шкідливий код, який додається на початок або кінець коду наявних файлів на комп'ютері. Проте, термін "вірус" часто вживають помилково. Більш точний термін — "шкідливе програмне забезпечення (шкідливі програми)". Виявлення шкідливого програмного забезпечення здійснюється ядром виявлення в поєднанні з компонентом машинного навчання. Докладніше про ці типи програм див. в [гlossарії](#).
- **Потенційно небажані програми** - умовно шкідливе ПЗ або потенційно небажані програми (PUA, Potentially Unwanted Application) — це широка категорія програмного забезпечення, яке не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни. Ці програми можуть інстальювати додаткове небажане ПЗ, змінювати поведінку або налаштування цифрового пристрою, а також виконувати неочікувані для користувача дії або не підтверджені ним. Докладніше про ці типи програм див. в [гlossарії](#).
- **Підозрілі програми** - це програми, стиснуті [пакувальниками](#) або протекторами. Зловмисники часто використовують такі типи захисту, щоб запобігти виявленню шкідливого програмного забезпечення.
- **Потенційно небезпечні програми** - комерційне легальне програмне забезпечення, що може використовуватися для зловмисних цілей. До потенційно небезпечних програм належать інструменти віддаленого доступу, програми для зламу паролів і клавіатурні шпигуни (програми, які записують кожне натискання клавіш, зроблене користувачем). Докладніше про ці типи програм див. в [гlossарії](#).



Покращений захист

i У ядрі виявлення тепер впроваджено розширене машинне навчання — удосконалений рівень захисту, який покращує виявлення на основі машинного навчання. Докладніше про цей тип захисту див. в [глосарії](#).

Сканування шкідливого програмного забезпечення

Параметри сканера можна налаштувати окремо від параметрів сканування в реальному часі й [сканування за вимогою](#). За замовчуванням увімкнено параметр **Використовувати параметри захисту в режимі реального часу**. Коли цей параметр увімкнено, відповідні параметри сканування за вимогою успадковуються з розділу **Захист у реальному часі й на основі машинного навчання**. Більш докладну інформацію див. в темі щодо [сканування на наявність шкідливого програмного забезпечення](#).

Налаштування звітування

Коли виявлено певний об'єкт (наприклад, знайдено загрозу, класифіковану як шкідливе програмне забезпечення), інформація про це записується в [журнал виявлених об'єктів](#), а на робочому столі з'являються [сповіщення](#), якщо це налаштовано в ESET NOD32 Antivirus.

Пороговий рівень звітування налаштовується для кожної з таких категорій (далі — КАТЕГОРІЯ):

- 1.Шкідливе програмне забезпечення
- 2.Потенційно небажані програми
- 3.Потенційно небезпечні програми
- 4.Підозрілі програми

Операції звітування виконуються ядром виявлення, зокрема й компонентом машинного навчання. Можна задати більш високий поріг звітування, ніж поточний поріг [захисту](#). Ці параметри звітування не впливають на блокування, [очищення](#) чи видалення [об'єктів](#).

Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) звітування для КАТЕГОРІЇ:

Поріг	Пояснення
Агресивний	Для звітування про КАТЕГОРІЮ налаштована максимальна чутливість. Програма буде повідомляти про більшу кількість виявлених об'єктів. Використання параметрів рівня Агресивний може призвести до помилкового визначення об'єктів як таких, що належать до КАТЕГОРІЇ.
Збалансований	Для звітування про КАТЕГОРІЮ налаштовано збалансований рівень. Цей параметр дає змогу збалансувати продуктивність і точність виявлення й кількість помилково визначених об'єктів.
Помірний	Для звітування про КАТЕГОРІЮ налаштовано мінімізацію кількості помилково визначених об'єктів зі збереженням достатнього рівня захисту. Об'єкти реєструються тільки тоді, коли ймовірність очевидна й відповідає поведінці КАТЕГОРІЇ.
Вимкнено	Звітування про КАТЕГОРІЮ не активовано. Пошук (очищення) об'єктів цього типу не виконується. У результаті цей параметр вимикає захист від об'єктів цього типу. Параметр "Вимкнено" недоступний для звітування про шкідливе програмне забезпечення; його встановлено за замовчуванням для потенційно небезпечних програм.

✓ [Доступність модулів захисту ESET NOD32 Antivirus](#)

Нижче наведено інформацію про доступність модуля захисту (увімкнено або вимкнено) модуля захисту для вибраного порога КАТЕГОРІЇ:

	Агресивний	Збалансований	Помірний	Вимкнено**
Модуль розширеного машинного навчання*	✓ (агресивний режим)	✓ (консервативний режим)	х	х
модуль ядра виявлення	✓	✓	✓	х
Інші модулі захисту	✓	✓	✓	х

* Доступно в ESET NOD32 Antivirus версії 13.1 й новіших.

** Не рекомендовано

✓ [Визначення версії продукту, версій модуля продукту й дат збірки](#)

1. Клацніть **Довідка та підтримка > Про програму ESET NOD32 Antivirus**.
2. На екрані **Про програму** в першому рядку тексту відображається номер версії вашого продукту ESET.
3. Щоб отримати дані про певні модулі, клацніть **Інстальовані компоненти**.

Тези

Наводимо кілька тез щодо налаштування відповідного порогового рівня для вашого середовища:

- Поріг **Збалансований** рекомендується для більшості налаштувань.
- Поріг **Помірний** відповідає рівню захисту в попередніх версіях ESET NOD32 Antivirus (13.0 і попередніх версій). Він рекомендується для тих середовищ, де пріоритетом є мінімізація хибно виявлених об'єктів програми безпеки.
- Що вище рівень звітування, то вище частота виявлення й імовірність хибно ідентифікувати об'єкти.
- Фактично не існує гарантії виявлення 100 % шкідливих об'єктів, як і гарантії повного уникнення неправильної категоризації нешкідливих об'єктів як шкідливих.
- [Своєчасно оновлюйте ESET NOD32 Antivirus і його модулі](#), щоб забезпечити максимально оптимальний баланс між продуктивністю й точністю виявлення та кількістю хибно виявлених об'єктів.

Налаштування захисту

Якщо повідомляється про об'єкт, віднесений до КАТЕГОРІЇ, програма захисту блокує його, а потім [очищає](#), видаляє або переміщує його в [карантин](#).

Ознайомтеся з наведеною нижче інформацією, перш ніж змінювати поріг (або рівень) для захисту КАТЕГОРІЇ:

Поріг	Пояснення
Агресивний	Об'єкти, виявлені із застосуванням агресивного (або нижчого) рівня параметрів, блокуються. Після цього розпочинається автоматичне виправлення (очищення). Цей параметр рекомендований, якщо всі кінцеві точки проскановані з використанням параметрів агресивного рівня, а помилково визначені об'єкти додані в список виключень.
Збалансований	Об'єкти, виявлені із застосуванням збалансованого (або нижчого) рівня параметрів, блокуються. Після цього розпочинається автоматичне виправлення (очищення).
Помірний	Об'єкти, виявлені із застосуванням помірної рівня параметрів, блокуються. Після цього розпочинається автоматичне виправлення (очищення).

Поріг	Пояснення
Вимкнено	Корисно для ідентифікації й виключення помилково визначених об'єктів. Параметр "Вимкнено" недоступний для захисту від шкідливого програмного забезпечення; його встановлено за замовчуванням для потенційно небезпечних програм.

✓ [Таблиця відповідності для ESET NOD32 Antivirus 13.0 і попередніх версій](#)

Після оновлення з версій 13.0 і попередніх до версії 13.1 й новіших новий стан порогових рівнів буде таким:

Перемикач категорії до оновлення	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Новий поріг КАТЕГОРІЇ після оновлення	Збалансований	Вимкнено

Розширені параметри ядра виявлення

Технологія Антируткіт – це найсучасніша система виявлення небезпечних програм, наприклад [руткітів](#), здатних приховувати свою присутність у системі. Це означає, що їх неможливо виявити за допомогою звичайних методів перевірки.

Увімкнути розширену перевірку за допомогою AMSI: активувати інструмент перевірки Microsoft Antimalware Scan Interface, який надає розробникам нові засоби захисту від шкідливих програм (лише для ОС Windows 10).

Дії в разі виявлення загрози

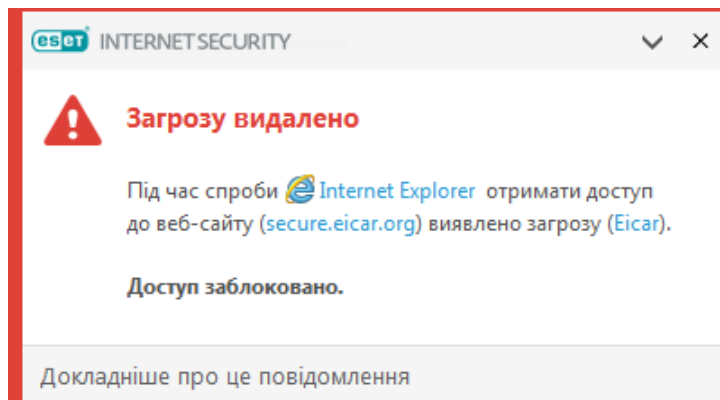
Загрози можуть проникати в систему через різні точки входу, наприклад [веб-сторінки](#), спільні папки, електронну пошту або [знімні пристрої](#) (USB, зовнішні диски, CD-диски, DVD-диски, тощо).

Стандартна поведінка

ESET NOD32 Antivirus захищає систему, виявляючи загрози за допомогою наведених нижче методів.

- [Захист файлової системи в режимі реального часу](#)
- [Захист доступу до Інтернету](#)
- [Захист поштового клієнта](#)
- [Сканування комп'ютера за вимогою](#)

Для кожного з цих параметрів використовується стандартний рівень очистки й виконується спроба видалити файл і перемістити його до [карантину](#) або перервати підключення. В області сповіщень у нижньому правому куті екрана відображається вікно сповіщень. Більш докладні відомості про виявлені/очищені об'єкти див. в розділі [Файли журналу](#). Більш докладні відомості про рівні очистки й поведінку див. в розділі [Рівень очистки](#).



Перевірка комп'ютера на інфіковані файли

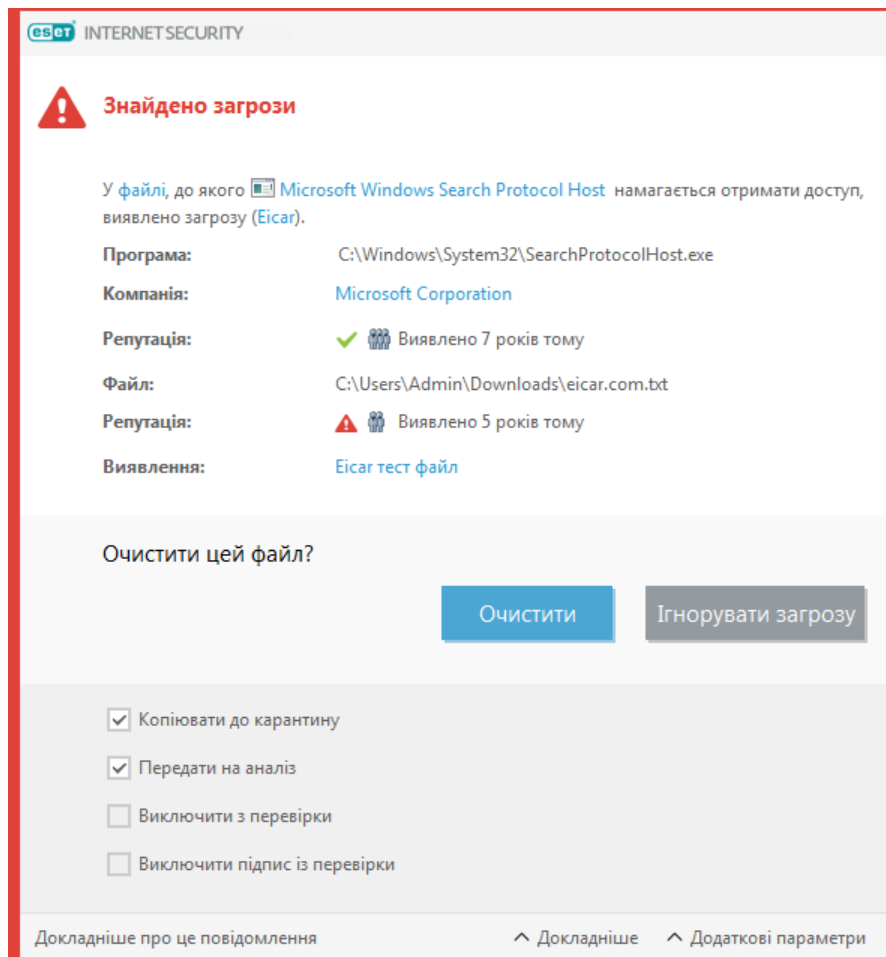
Якщо на комп'ютері спостерігаються ознаки діяльності шкідливих програм (наприклад, система працює повільніше, ніж звичайно, часто зависає тощо), рекомендується виконати наведені нижче дії.

1. Відкрийте ESET NOD32 Antivirus і натисніть "**Сканування комп'ютера**".
2. Натисніть **Сканування комп'ютера** (докладніше можна прочитати в розділі [Сканування комп'ютера](#)).
3. Після завершення сканування перегляньте в журналі кількість перевірених, інфікованих і очищених файлів.

Якщо необхідно перевірити лише певну частину диска, натисніть **Вибіркове сканування** та виберіть об'єкти для сканування на наявність вірусів.

Очистка та видалення

Якщо попередньо визначеної дії для модуля захисту файлової системи в режимі реального часу немає, на екрані відобразиться вікно тривоги, у якому вам буде запропоновано вибрати дію самостійно. Зазвичай у цьому вікні доступні такі дії: **Очистити**, **Видалити** та **Пропустити**. Не рекомендується вибирати опцію **Пропустити**, оскільки в такому разі інфіковані файли залишатимуться неочищеними. Винятком є випадки, коли ви впевнені, що файл безпечний і його виявлено помилково.



Очистку слід виконувати, якщо файл атаковано вірусом, який додав до нього шкідливий код. У цьому разі спершу потрібно спробувати очистити файл, щоб повернути його до початкового стану. Якщо файл складається виключно зі шкідливого коду, файл видаляється.

Якщо інфікований файл "заблоковано" або він використовується системним процесом, його буде видалено лише після розблокування (зазвичай після перезапуску системи).

Відновлення з карантину

Щоб відкрити карантин, у [головному вікні програми](#) ESET NOD32 Antivirus натисніть **Інструменти > Карантин**.

Файли з карантину також можна відновити й повернути до початкових місць розташування.

- Для цього натисніть правою кнопкою файл у карантині та виберіть опцію **Відновити** в контекстному меню.
- Якщо файл позначено як [потенційно небажану програму](#), доступна опція **Відновити та виключити з перевірки**. Також див. [Виключення](#).
- У контекстному меню також доступна опція **Відновити в**, за допомогою якої користувач може відновити файли в інше місце, а не туди, звідки їх було видалено.
- У деяких випадках функція відновлення недоступна, наприклад, якщо файли знаходилися на мережевому диску, доступному лише для читання.

Кілька загроз

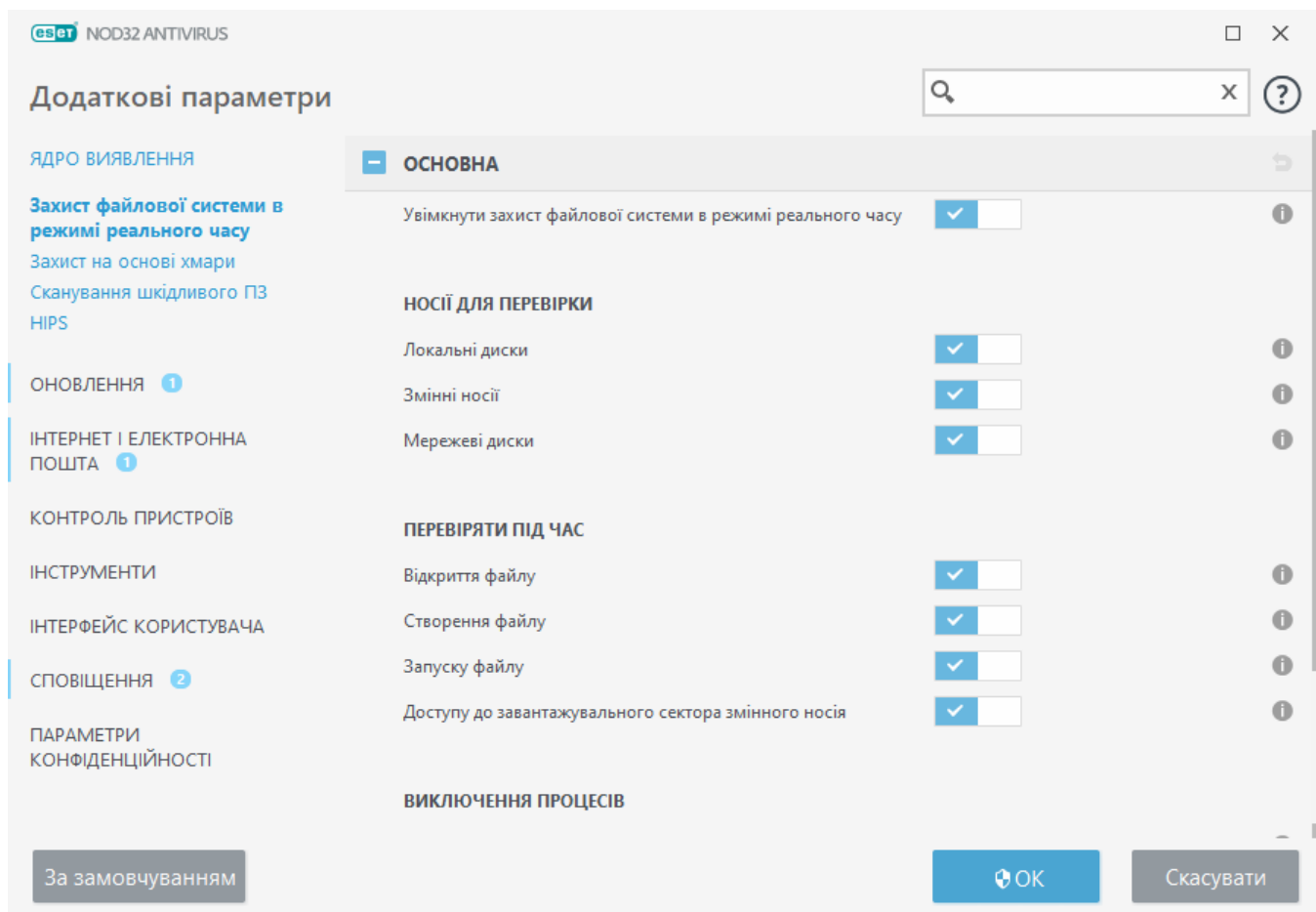
Якщо певні інфіковані файли не вдалось очистити під час сканування комп'ютера (або для [рівня очистки](#) вибрано значення **Без очистки**), відкривається вікно тривоги із пропозицією вибрати для них дію. Виберіть дії для файлів (дії встановлюються окремо для кожного файлу у списку), після чого клацніть **Готово**.

Видалення файлів з архівів

У режимі очистки за замовчуванням архів буде видалятися повністю лише в тому випадку, якщо містить виключно інфіковані файли й жодного чистого. Іншими словами, якщо архів також містить безпечні файли, він не видалятиметься. Будьте обережні, запускаючи сканування з ретельною очисткою. У ході цієї процедури архів видалятиметься, якщо в ньому виявлено принаймні один інфікований файл, незалежно від стану інших.

Захист файлової системи в режимі реального часу

Функція "Захист файлової системи в режимі реального часу" контролює всі файли в системі на наявність шкідливого коду під час їх відкриття, створення або запуску.



За замовчуванням модуль захисту файлової системи в режимі реального часу запускається разом із системою та виконує безперервне сканування. Не рекомендуємо вимикати параметр **Увімкнути захист файлової системи в режимі реального часу** в меню **Додаткові**

параметри (Ядро виявлення > Захист файлової системи в режимі реального часу > Базові).

Перевірка носіїв

За замовчуванням усі типи носіїв скануються на наявність потенційних загроз:

- **Локальні диски:** скануються всі системні й незмінні жорсткі диски (наприклад, C:\, D:\).
- **Змінний носій:** скануються CD/DVD-диски, USB-пристрої, карти пам'яті тощо
- **Мережеві диски:** скануються всі підключені мережеві диски (наприклад, H:\ як \\store04) або мережеві диски з безпосереднім доступом (наприклад, \\store08).

Рекомендується використовувати параметри за замовчуванням і змінювати їх лише у крайньому разі, наприклад, коли сканування певних носіїв значно сповільнює передачу даних.

Період перевірки

За замовчуванням усі файли скануються під час відкриття, створення або запуску. Рекомендується використовувати параметри за замовчуванням, оскільки вони забезпечують максимальний рівень захисту комп'ютера в режимі реального часу.

- **Відкриття файлу:** файли скануються під час відкриття.
- **Створення файлу:** скануються створені або змінені файли.
- **Запуск файлу:** файли скануються під час виконання або запуску.
- **Доступ до завантажувального сектора змінного носія:** під час підключення змінного носія із завантажувальним сектором до пристрою завантажувальний сектор відразу ж сканується. Цей параметр не вмикає сканування файлів на змінному носії. Щоб увімкнути сканування файлів на змінному носії, виберіть **Перевірка носіїв > Змінний носій**. Для належної роботи **доступу до завантажувального сектора на змінному носії** не вимикайте **Завантажувальні сектори/UEFI** в параметрах ThreatSense.

Модуль захисту файлової системи в режимі реального часу перевіряє всі типи носіїв. Його активують різноманітні системні події, наприклад відкриття файлу. Методи виявлення загроз, які використовуються в технології ThreatSense (див. розділ [Налаштування параметрів підсистеми ThreatSense](#)), дають змогу налаштувати модуль захисту файлової системи в режимі реального часу так, щоб він діяв по-різному відносно новостворених і вже наявних файлів. Наприклад, модуль може більш ретельно аналізувати новостворені файли.

Щоб зменшити споживання системних ресурсів, уже проскановані файли повторно не перевіряються (якщо їх не було змінено). Файли скануються повторно відразу після кожного оновлення обробника виявлення. Виконання цієї процедури контролюється за допомогою функції **Smart-оптимізація**. Якщо **Smart-оптимізацію** вимкнено, усі файли скануються щоразу, коли користувач до них звертається. Щоб змінити цей параметр, натисніть **F5**, щоб відкрити **Додаткові параметри**, потім розгорніть меню **Обробник виявлення > Захист файлової системи в режимі реального часу**. Натисніть **Параметр ThreatSense > Інше** й установіть або зніміть прапорець **Увімкнути Smart-оптимізацію**.

Рівні очистки

Щоб відкрити параметри рівня очищення для бажаного модуля захисту, розгорніть **параметри ThreatSense** (наприклад, **Захист файлової системи в режимі реального часу**), а потім виберіть **Очистка > Рівень очистки**.


Параметри ThreatSense дозволяють задати наведені нижче рівні виправлення (очищення).

Виправлення в ESET NOD32 Antivirus

Рівень очистки	Опис
Завжди виправляти виявлені об'єкти	Спробувати виправити виявлений об'єкт під час очищення об'єктів без втручання кінцевого користувача. У деяких випадках (наприклад, для системних файлів) виявлений об'єкт неможливо виправити, тому він залишатиметься у вихідному розташуванні.
Виправити виявлені об'єкти, якщо безпечно. В іншому разі залишити все як є	Спробувати виправити виявлений об'єкт під час очищення об'єктів без втручання кінцевого користувача. У деяких випадках (наприклад, системні файли або архіви з чистими та інфікованими файлами), якщо виявлений об'єкт не можна виправити, він залишається у вихідному розташуванні.
Виправити виявлені об'єкти, якщо безпечно. В іншому разі надіслати запит	Спробувати виправлення виявленого об'єкта під час очищення об'єктів. У деяких випадках, коли жодну операцію виконати неможливо, кінцевий користувач отримує інтерактивне сповіщення, де необхідно вибрати операцію виправлення (наприклад, видалити або пропустити). Цей параметр рекомендовано в більшості випадків.
Завжди запитувати кінцевого користувача	Під час очищення об'єктів для кінцевого користувача відкривається вікно, у якому необхідно вибрати операцію виправлення (наприклад, видалити або пропустити). Цей рівень призначений для більш досвідчених користувачів, які знають, що потрібно зробити у випадку виявлення.

Можливі причини для змінення конфігурації захисту в режимі реального часу

Захист у режимі реального часу – це найголовніший модуль, від якого залежить загальна безпека системи. Змінювати його параметри завжди слід дуже обережно. Зміни до параметрів рекомендується вносити лише у виключних випадках.

Після інсталяції ESET NOD32 Antivirus усі параметри оптимізовано таким чином, щоб досягти максимального рівня безпеки користувацької системи. Щоб відновити налаштування за замовчуванням, натисніть  поруч із кожною вкладкою у вікні (**Додаткові параметри > Обробник виявлення > Захист файлової системи в режимі реального часу**).

Перевірка захисту в режимі реального часу

Щоб переконатися, що захист у режимі реального часу працює та виявляє віруси, скористайтеся тестовим файлом із сайту www.eicar.com. Це безпечний файл, який виявляється всіма антивірусними програмами. Файл було створено Європейським інститутом комп'ютерних антивірусних досліджень (European Institute for Computer Antivirus Research, EICAR) для тестування функціональності антивірусних програм.

Цей файл можна завантажити за посиланням <http://www.eicar.org/download/eicar.com>. Після вводу цієї URL-адреси в браузер, відкриється повідомлення про те, що загрозу було видалено.

Необхідні дії, коли не працює захист у режимі реального часу

У цьому розділі описуються проблеми, які можуть виникнути під час використання захисту в режимі реального часу, і способи їх усунення.

Захист у режимі реального часу вимкнено

Якщо користувач випадково вимкнув захист у режимі реального часу, знову ввімкніть його. Щоб повторно активувати захист у режимі реального часу, перейдіть у меню **Налаштування** в [головному вікні програми](#) й натисніть **Захист комп'ютера > Захист файлової системи в режимі реального часу**.

Якщо модуль захисту в режимі реального часу не запускається під час запуску системи, можливо, параметр **Увімкнути захист файлової системи в режимі реального часу** вимкнено. Щоб переконатися, що цю опцію ввімкнуто, перейдіть у меню **Додаткові параметри (F5)** і натисніть **Обробник виявлення > Захист файлової системи в режимі реального часу**.

Захист у режимі реального часу не виявляє й не усуває загрози

Переконайтеся, що на комп'ютері не інстальовано жодної іншої антивірусної програми. Якщо на комп'ютері інстальовано дві антивірусні програми, вони можуть конфліктувати між собою. Перш ніж установлювати ESET, рекомендується видалити із системи інші антивірусні програми.

Модуль захисту в режимі реального часу не запускається

Якщо захист у режимі реального часу не активується під час запуску системи, а параметр **Увімкнути захист файлової системи в режимі реального часу** ввімкнено, можливо, має місце конфлікт з іншими програмами. Щоб вирішити проблему, [створіть журнал SysInspector й надішліть його на перевірку в службу технічної підтримки ESET](#).

Виключення процесів

Функція «Виключення процесів» дозволяє виключати процеси програм із компонента «Захист файлової системи в режимі реального часу». Щоб підвищити швидкість резервного копіювання, забезпечити цілісність процесу й доступність служб під час резервного копіювання застосовуються деякі методи, які конфліктують із системою захисту від шкідливого програмного забезпечення на рівні файлів. Єдиний дієвий спосіб уникнути обох ситуацій — деактивувати програму захисту від шкідливого програмного забезпечення. Якщо певні процеси (наприклад, процеси резервного копіювання) виключено, усі операції з файлами, пов'язані з цими виключеними процесами, ігноруються й розглядаються як безпечні. Це дозволяє мінімізувати перешкоди для процесу резервного копіювання. До створення виключень необхідно підходити обачно, адже виключений із перевірки інструмент резервного копіювання може отримати доступ до інфікованих файлів, а відповідне попередження системи безпеки не буде ініційоване. Саме тому розширені дозволи доступні тільки в модулі захисту в режимі реального часу.

i Слід чітко розуміти значення параметрів [Виключені розширення файлів](#), [Виключення NIPS](#), [Виключення об'єктів виявлення](#) або [Виключення в роботі](#).

Виключення процесів допомагають мінімізувати ризик потенційних конфліктів і підвищити швидкодію виключених програм, що позитивно впливає на загальну швидкодію й стабільність операційної системи. Виключення процесу (програми) — це виключення відповідного виконуваного файлу (.exe).

Можна додати виконуваний файл в список виключених процесів у розділі **Додаткові параметри (F5) > Ядро виявлення > Захист файлової системи в режимі реального часу > Виключення процесів**.

Ця функція призначена для виключення інструментів резервного копіювання. Виключення процесу інструмента резервного копіювання зі сканування не тільки забезпечує стабільність системи, але й виключає негативний вплив сканування на продуктивність резервного копіювання, оскільки воно не вповільнюється під час сканування.

Щоб відкрити вікно керування **Виключення процесів**, клацніть **Змінити**. У цьому вікні можна [додати](#) виключення й знайти виконуваний файл (наприклад, *Backup-tool.exe*), який буде виключено зі сканування.



✓ Щойно файл .exe буде додано до виключень, активність цього процесу не буде відстежуватись програмою ESET NOD32 Antivirus. Окрім того, сканування не запускатиметься для жодної операції з файлами, виконуваної цим процесом.



Якщо для вибору виконуваних файлів ви не використовуєте файловий провідник, необхідно вручну ввести повний шлях до виконуваного файлу. Інакше виключення не буде працювати правильно, а [система запобігання вторгненням \(NIPS\)](#) може повертати помилки.

Можна також **Змінити** наявні процеси або **Видалити** їх із виключень.



i Це виключення ігнорується модулем [захисту доступу до інтернету](#), тому якщо виключити виконуваний файл веб-браузера, завантажені файли все одно скануватимуться. Це дозволяє виявляти загрози. Цей сценарій наведено лише для довідки. Ми не рекомендуємо створювати виключення для веб-браузерів.

Додавання або зміна виключень процесів

У цьому діалоговому вікні можна **додавати** процеси, виключені з ядра виявлення. Виключення процесів допомагають мінімізувати ризик потенційних конфліктів і підвищити швидкодію виключених програм, що позитивно впливає на загальну швидкодію й стабільність операційної системи. Виключення процесу (програми) — це виключення відповідного виконуваного файлу (.exe).

Виберіть шлях до файлу потрібної програми. Для цього клацніть ... (наприклад, *C:\Program Files\Firefox\Firefox.exe*). НЕ вводьте назву програми.

✓ Щойно файл .exe буде додано до виключень, активність цього процесу не буде відстежуватись програмою ESET NOD32 Antivirus. Окрім того, сканування не запускатиметься для жодної операції з файлами, виконуваної цим процесом.

ⓘ Якщо для вибору виконуваних файлів ви не використовуєте файловий провідник, необхідно вручну ввести повний шлях до виконуваного файлу. Інакше виключення не буде працювати правильно, а [система запобігання вторгненням \(HIPS\)](#) може повертати помилки.

Можна також **Змінити** наявні процеси або **Видалити** їх із виключень.

Захист із використанням хмари

Технологію ESET LiveGrid® створено на основі системи завчасного попередження ThreatSense.Net. Вона збирає дані від користувачів ESET з усього світу й передає до дослідницької лабораторії ESET. Вона збирає дані від користувачів ESET з усього світу й передає до дослідницької лабораторії ESET. Отримуючи підозрілі зразки та метадані від ESET LiveGrid®, ми можемо миттєво реагувати на потреби користувачів і своєчасно оновлювати системи ESET.

Доступні наведені нижче варіанти:

Увімкніть систему репутації ESET LiveGrid®.

Система репутації ESET LiveGrid® дає змогу використовувати білі й чорні списки на основі хмарних технологій.

Репутацію [запущених процесів](#) і файлів можна дізнатися безпосередньо в інтерфейсі програми чи контекстному меню. Додаткова інформація доступна завдяки технології ESET LiveGrid®.

Увімкніть систему зворотного зв'язку ESET LiveGrid®.

Окрім системи репутації ESET LiveGrid®, система зворотного зв'язку ESET LiveGrid® збиратиме інформацію щодо нових загроз на вашому комп'ютері. Зокрема, це такі дані:

- Зразок або копія файлу, у якому з'явилася загроза
- Шлях до файлу
- Назва файлу

- Дата й час
- Процес, пов'язаний із загрозою, яка з'явилася на вашому комп'ютері
- Інформація про операційну систему вашого комп'ютера

За замовчуванням у ESET NOD32 Antivirus налаштовано передачу підозрілих файлів для детального аналізу до антивірусної лабораторії ESET. Файли з певними розширеннями, наприклад .doc або .xls, завжди виключаються. До списку виключень можна додати інші розширення файлів, які ви чи ваша організація не бажаєте надсилати.

i Докладніше про надсилання релевантних даних див. в [Політиці конфіденційності](#).

Можна не вмикати ESET LiveGrid®.

Функціональні можливості програми не будуть обмежені, але в деяких випадках продукт ESET NOD32 Antivirus швидше реагує на нові загрози, коли ввімкнено ESET LiveGrid®. Якщо ви раніше використовували систему ESET LiveGrid®, а потім вимкнули її, на комп'ютері ще можуть залишатися пакети даних, підготовлені до надсилання. Навіть після вимкнення системи завчасного попередження ці пакети будуть надіслані до ESET. Після надсилання всієї поточної інформації пакети не створюватимуться.

i Більш докладну інформацію про ESET LiveGrid® див. в [глосарії](#).
У наших [ілюстрованих інструкціях](#), які доступні англійською та іншими мовами, наочно показано, як умикати або вимикати ESET LiveGrid® у ESET NOD32 Antivirus.

Конфігурація захисту з використанням хмари в додаткових параметрах

Щоб отримати доступ до параметрів ESET LiveGrid®, відкрийте розділ **Додаткові параметри (F5)** > **Ядро виявлення** > **Захист із використанням хмари**.

- **Увімкнути систему репутації ESET LiveGrid® (рекомендується):** система репутації ESET LiveGrid® підвищує ефективність рішень ESET для захисту від шкідливого ПЗ, порівнюючи проскановані файли з хмарною базою даних об'єктів, доданих до білих і чорних списків.
- **Увімкнути систему зворотного зв'язку ESET LiveGrid®:** надсилає відповідні дані (описані в розділі **Надсилання зразків** нижче), а також звіти про аварійне завершення роботи й статистичні дані в дослідницьку лабораторію ESET для подальшого аналізу.
- **Надсилати звіти про аварійне завершення роботи й дані діагностики:** надсилатимуться пов'язані з ESET LiveGrid® діагностичні дані, зокрема звіти про аварійне завершення й дампи пам'яті модулів. Рекомендуємо не вимикати цю функцію, щоб допомагати ESET покращувати продукти й захист кінцевих користувачів.
- **Надіслати анонімну статистику** – дає змогу компанії ESET збирати інформацію про нові виявлені загрози, зокрема їхні імена, дати й час виявлення, методи виявлення та пов'язані метадані, версії та конфігурації продуктів із відомостями про систему.

- **Контактна адреса електронної пошти (необов'язково):** ваша контактна адреса електронної пошти може відправлятися з будь-якими підозрілими файлами й використовуватися для зв'язку з вами, якщо для проведення аналізу знадобляться додаткові відомості. Ви не отримаєте відповіді від ESET, якщо додаткова інформація не буде потрібна.

Надсилання зразків

Ручне надсилання зразків: дає змогу вручну надіслати зразки в ESET із контекстного меню, [карантину](#) або команди [Інструменти](#).

Автоматичне надсилання виявлених зразків

Виберіть типи зразків, які надсилатимуться в ESET для аналізу та покращення виявлення об'єктів у майбутньому (за замовчуванням розмір зразка може становити щонайбільше 64 МБ). Доступні наведені нижче варіанти:

- **Усі виявлені зразки:** усі [об'єкти](#), визначені [ядром виявлення](#) (включно з потенційно небажаними програмами, якщо ввімкнено в налаштуваннях сканера).
- **Усі зразки, за винятком документів:** усі виявлені об'єкти, окрім **документів** (див. нижче).
- **Не відправляти:** виявлені об'єкти не надсилатимуться до ESET.

Автоматичне надсилання підозрілих зразків

Ці зразки також надсилатимуться в ESET, якщо ядро виявлення не розпізнає їх. Наприклад, зразки, яким майже вдалось уникнути виявлення або які видалися підозрілими для [модулів захисту](#) ESET NOD32 Antivirus, зокрема, через свою незрозумілу поведінку.

- **Виконувані файли:** виконувані файли типу .exe, .dll, .sys.
- **Архіви:** архівні файли типу .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Сценарії:** файли сценаріїв типу .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Інше:** файли з розширенням .jar, .reg, .msi, .sfw, .lnk.
- **Повідомлення електронної пошти з підозрою на спам:** дає змогу надіслати вірогідний або вкрай вірогідний спам для подальшого аналізу спеціалістами ESET. Увімкнення цього параметра дає змогу вдосконалити глобальне виявлення спаму зараз і в майбутньому.
- **Документи:** документи Microsoft Office або PDF з активним вмістом чи без нього.

✓ [Розгорніть список усіх охоплюваних типів документів](#)

ACCEDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Виключення

[Фільтр виключень](#) дає можливість запобігати відправленню для аналізу типів файлів або папок. Наприклад, доцільно виключити файли, які можуть містити конфіденційну інформацію (документи, електронні таблиці тощо). Указані файли ніколи не надсилатимуться на аналіз до лабораторії ESET, навіть якщо вони містять підозрілий код. Найпоширеніші типи файлів виключено за замовчуванням (.doc тощо). За потреби можна доповнити список виключених файлів.

✓ Щоб виключити файли, завантажені з `download.domain.com`, перейдіть у меню **Додаткові параметри > Ядро виявлення > Захист на основі хмари > Надсилання зразків** і натисніть **Змінити** біля пункту **Виключення**. Додайте виключення `.download.domain.com`.

Максимальний розмір зразків (МБ): визначає максимальний розмір зразків (1-64 МБ).

Фільтр виключень для хмарного захисту

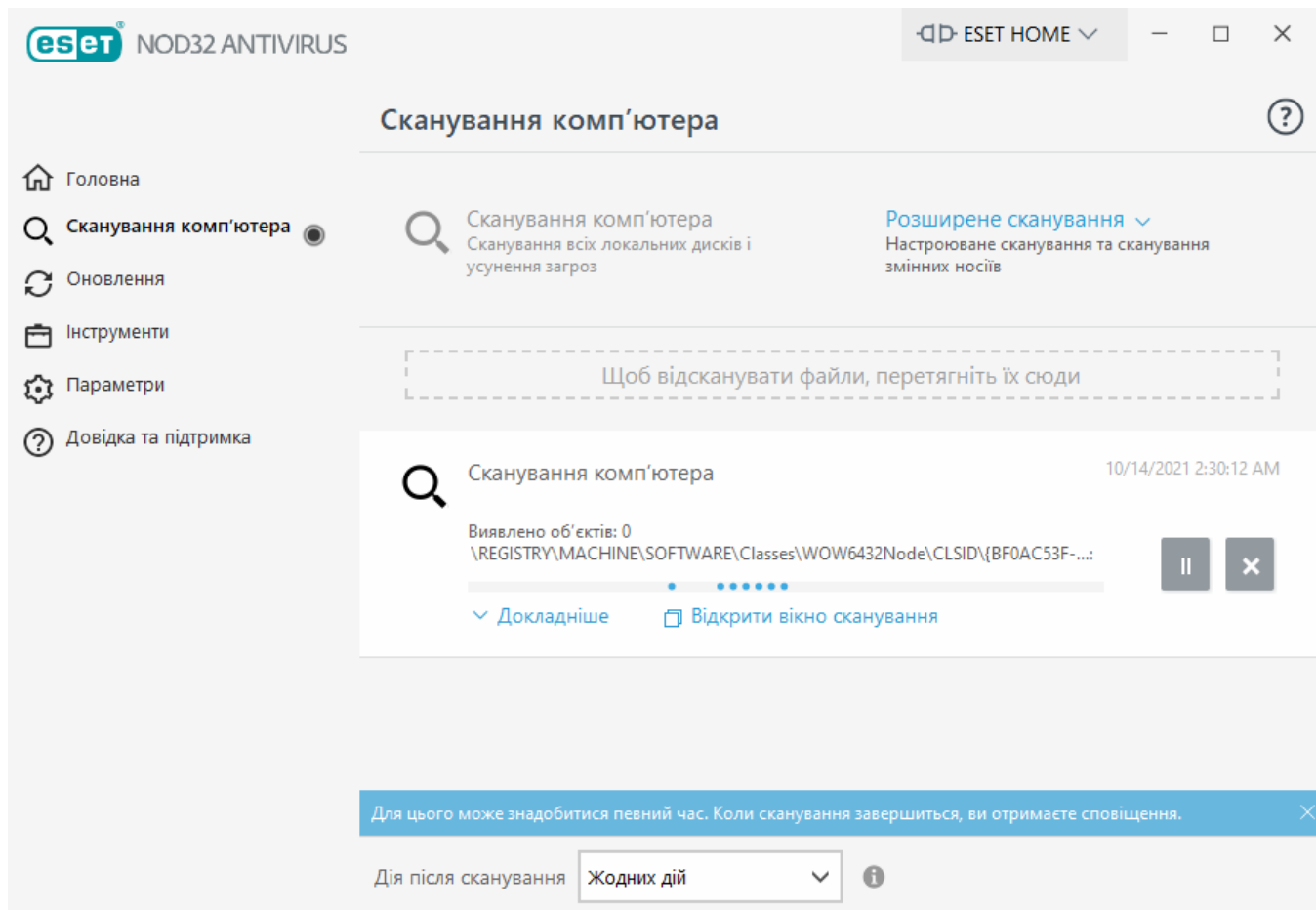
Фільтр виключень дає можливість не відправляти для аналізу певні файли або папки. Указані файли ніколи не надсилатимуться на аналіз до лабораторії ESET, навіть якщо вони містять підозрілий код. Найпоширеніші типи файлів виключено за замовчуванням (.doc тощо).

i Доцільно виключити файли, які можуть містити конфіденційну інформацію (документи, електронні таблиці тощо).

✓ Щоб виключити файли, завантажені на сайті `download.domain.com`, натисніть **Додаткові параметри > Ядро виявлення > Захист на основі хмари > Надсилання зразків > Виключення** та додайте виключення `*download.domain.com*`.

Сканування комп'ютера

Сканер за вимогою – це важлива частина антивірусного програмного забезпечення. Він використовується для сканування файлів і папок на комп'ютері. З точки зору безпеки важливо перевіряти комп'ютер не лише в разі підозри на наявність зараження, а й регулярно – як превентивний захід захисту. Рекомендується регулярно виконувати ретельне сканування системи, щоб виявляти віруси, які не розпізнаються модулем [захисту файлової системи в режимі реального часу](#) під час запису на диск. Це може статися, якщо наразі захист файлової системи в режимі реального часу вимкнено, обробник виявлення застарів або файл не класифіковано як вірус під час збереження на диск.



Доступні два типи **Сканування комп'ютера**. Функція **Сканування комп'ютера** дає змогу швидко запустити сканування системи без налаштування параметрів сканування. **Вибіркове сканування** (у розділі "Розширене сканування") передбачає вибір попередньо визначених профілів для спеціальних розташувань, а також дає змогу вказати окремі об'єкти сканування.

Додаткову інформацію про процедуру сканування див. у розділі [Хід сканування](#).



За замовчуванням ESET NOD32 Antivirus намагається автоматично очистити або видалити об'єкти, виявлені під час сканування комп'ютера. У деяких випадках, якщо програмі не вдається виконати жодної дії, користувач отримує інтерактивне сповіщення, у якому потрібно вказати, як очистити об'єкт (наприклад, видалити або проігнорувати). Змінити рівень очистки й переглянути докладнішу інформацію можна в меню [Очистка](#). Переглянути результати попередніх сканувань можна у [файлах журналу](#).

Сканування комп'ютера

Ця функція дає змогу швидко запускати **скануван комп'ютера** й очищати інфіковані файли без втручання користувача. Перевага функції "**Сканування комп'ютера**" полягає в тому, що нею просто користуватися й не потрібно детально налаштовувати сканування. Цей тип сканування перевіряє всі файли на локальних дисках і автоматично очищає або видаляє виявлені загрози. Для рівня очистки автоматично вибирається параметр за замовчуванням. Докладніше про типи очистки можна прочитати в розділі [Очистка](#).

Також можна скористатися функцією **Сканування перетягуванням**. Щоб просканувати файл або папку вручну, натисніть відповідний елемент і, не відпускаючи кнопку миші, перемістіть курсор у позначену область, а потім відпустіть кнопку. після цього програма переміститься на

передній план.

У меню **Параметри розширеного сканування** доступні наведені нижче опції.



Вибіркове сканування

Параметр **Вибіркове сканування** дає змогу вказати параметри (наприклад, об'єкти й методи). Перевага функції **Вибіркове сканування** полягає в тому, що користувач може детально налаштувати всі параметри. Конфігурації можна зберегти в користувацьких профілях сканування. Такий метод ефективний, якщо сканування регулярно виконується з однаковими параметрами.



Сканування змінних носіїв

Цей тип сканування схожий на функцію "**Сканування комп'ютера**", оскільки виконується швидкий запуск перевірки змінних носіїв (наприклад, CD/DVD/USB), наразі під'єднаних до комп'ютера. Такий тип сканування може знадобитися, коли ви під'єднуєте до комп'ютера флеш-пам'ять USB, і вам потрібно перевірити її на відсутність шкідливого ПЗ й інших загроз.

Цей тип сканування також можна запустити, якщо натиснути **Вибіркове сканування**, вибрати пункт **Змінний носій** у розкривному меню **Об'єкти сканування**, після чого натиснути **Сканувати**.



Повторити останнє сканування

Дає змогу швидко запустити сканування з налаштуваннями, які застосовувалися під час останнього сканування.

У розкривному меню **Дія після сканування** можна задати дію, яка автоматично виконуватиметься після завершення сканування:

- **Нічого не робити:** після завершення сканування жодна дія не виконується.
- **Завершити роботу:** комп'ютер вимикається після завершення сканування.
- **Перезавантажити:** після завершення сканування всі відкриті програми закриваються, а комп'ютер перезавантажується.
- **Перезавантажити за необхідності:** комп'ютер перезавантажується, лише якщо потрібно завершити очищення виявлених загроз.
- **Примусове перезавантаження:** після завершення сканування всі відкриті програми закриваються, а комп'ютер перезавантажується без втручання користувача.
- **Примусово перезавантажити за потреби:** комп'ютер перезавантажується, лише якщо потрібно завершити очищення виявлених загроз.
- **Режим сну:** сеанс зберігається, а комп'ютер переводиться в режим зниженого енергоспоживання, щоб можна було швидко відновити роботу.
- **Режим глибокого сну:** всі запущені в оперативній пам'яті процеси зберігаються в

окремому файлі на жорсткому диску. Комп'ютер вимикається, проте після запуску він відновлює попередній робочий стан.

i Дії **Сон** або **Глибокий сон** доступні залежно від налаштувань живлення та режиму сну в операційній системі або можливостей комп'ютера чи ноутбука. Зверніть увагу, що в режимі сну комп'ютер усе одно працює. Базові функції продовжують виконуватися, споживаючи енергію батареї (якщо комп'ютер живиться від неї). Щоб зберегти заряд, наприклад, коли ви залишили місце роботи, рекомендується користуватися режимом глибокого сну.

Вибрана дія запуститься після завершення всіх виконуваних процесів сканування. Якщо вибрано параметр **Завершити роботу** або **Перезавантажити**, протягом 30-секундного зворотного відліку відображатиметься діалогове вікно для підтвердження (клацніть **Скасувати**, щоб деактивувати запитувану дію).

i Сканування комп'ютера рекомендується виконувати принаймні раз на місяць. Сканування можна налаштувати як заплановане завдання в меню **Інструменти > Планувальник. Додавання до розкладу завдання щотижневого сканування комп'ютера**

Модуль запуску вибіркового сканування

За допомогою цієї опції можна просканувати оперативну пам'ять, мережу або окремі частини диска. Для цього натисніть **Розширене сканування > Вибіркове сканування** та знайдіть потрібні об'єкти у структурі папок (дерева).

У розкритому меню **Профіль** можна вибрати профіль, що використовуватиметься для перевірки вибраних об'єктів. За замовчуванням використовується профіль **Інтелектуальне сканування**. Інші три попередньо визначені профілі — **Детальне сканування**, **Сканування контекстного меню** й **Сканування комп'ютера**. Вони використовують різні [параметри ThreatSense](#). Доступні настройки наведено в розділі **Додаткові параметри (F5) > Ядро виявлення > Сканування шкідливого програмного забезпечення > Сканування за вимогою > Параметри ThreatSense.**

Структура папки (дерево) також містить певні об'єкти сканування.

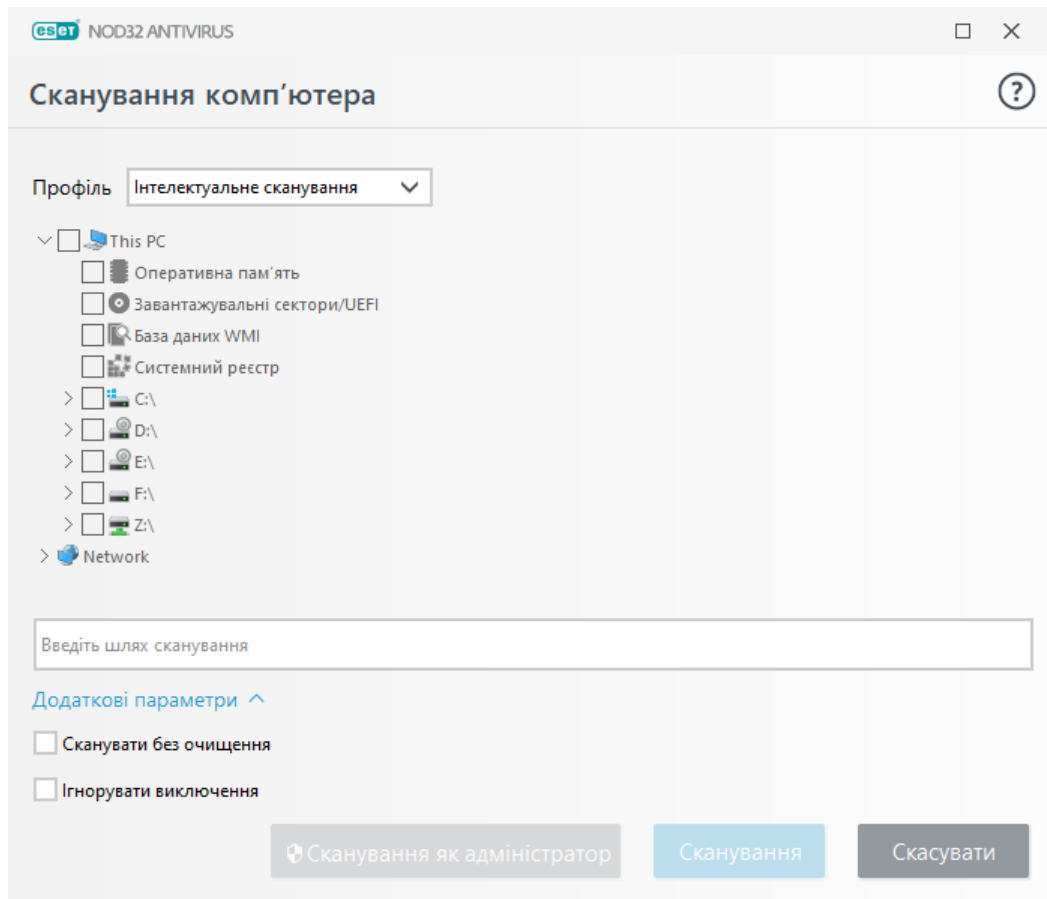
- **Оперативна пам'ять:** сканування всіх процесів і даних, які наразі використовуються оперативною пам'яттю.
- **Завантажувальні сектори/UEFI:** сканування завантажувальних секторів і UEFI наявність шкідливого програмного забезпечення. Більш докладну інформацію про сканер UEFI див. [в глосарії](#).
- **База даних WMI:** сканування всієї бази даних Windows Management Instrumentation (WMI), усіх областей імен, екземплярів класів і властивостей. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване під виглядом даних.
- **Системний реєстр:** сканування всього системного реєстру, усіх розділів і підрозділів. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване під виглядом даних. Після очищення реєстру посилання залишатиметься в ньому, що вбезпечить користувачів від втрати важливих даних.

Щоб швидко перейти до об'єкта сканування (файлу або папки), введіть шлях у текстове поле під структурою дерева. Шлях чутливий до регістру. Щоб додати об'єкт до сканування, установіть відповідний прапорець у структурі дерева.

Додавання до розкладу завдання щотижневого сканування комп'ютера



Щоб запланувати регулярне завдання, див. розділ [Додавання до розкладу завдання щотижневого сканування комп'ютера](#).



Щоб налаштувати для сканування параметри очистки, виберіть **Додаткові параметри (F5) > Обробник виявлення > Сканування комп'ютера за вимогою > Параметри ThreatSense > Очистка**. Щоб просканувати об'єкти, але не виконувати очистку, натисніть **Додаткові параметри** й виберіть **Сканувати без очистки**. Історія сканування зберігається в однойменний журнал.

Якщо вибрано параметр **Ігнорувати виключення**, усі файли з розширеннями, які раніше було виключено, скануватимуться без винятку.

Натисніть **Сканувати**, щоб виконати перевірку на основі встановлених спеціальних параметрів.

Кнопка **Виконати сканування як адміністратор** запускає сканування від імені облікового запису адміністратора. Натисніть цю кнопку, якщо в поточного користувача немає прав доступу до файлів, які потрібно просканувати. Ця кнопка недоступна, якщо поточний користувач не може виконувати дії УАС як адміністратор.



Щоб переглянути журнал, коли сканування завершиться, натисніть посилання [Показати журнал](#).

Хід сканування

У вікні ходу сканування відображається поточний стан процесу сканування, а також інформація про те, скільки файлів містять шкідливий код.



Деякі файли, наприклад захищені паролем або ті, що ексклюзивно використовуються системою (зазвичай *pagefile.sys* і деякі журнали), просканувати неможливо. Більш докладні відомості див. у нашій [статті бази знань](#).



Додавання до розкладу завдання щотижневого сканування комп'ютера

Щоб запланувати регулярне завдання, див. розділ [Додавання до розкладу завдання щотижневого сканування комп'ютера](#).

Хід сканування^ індикатор стану виконання процедури відображає, скільки об'єктів уже проскановано та скільки ще потрібно просканувати. Цей показник вираховується на основі загальної кількості об'єктів, доданих до списку сканування.

Ціль: ім'я об'єкта, який наразі сканується, а також шлях до нього.

Знайдено загроз – загальна кількість просканиваних файлів, а також виявлених і видалених у процесі сканування загроз.

Пауза: призупинення процедури сканування.

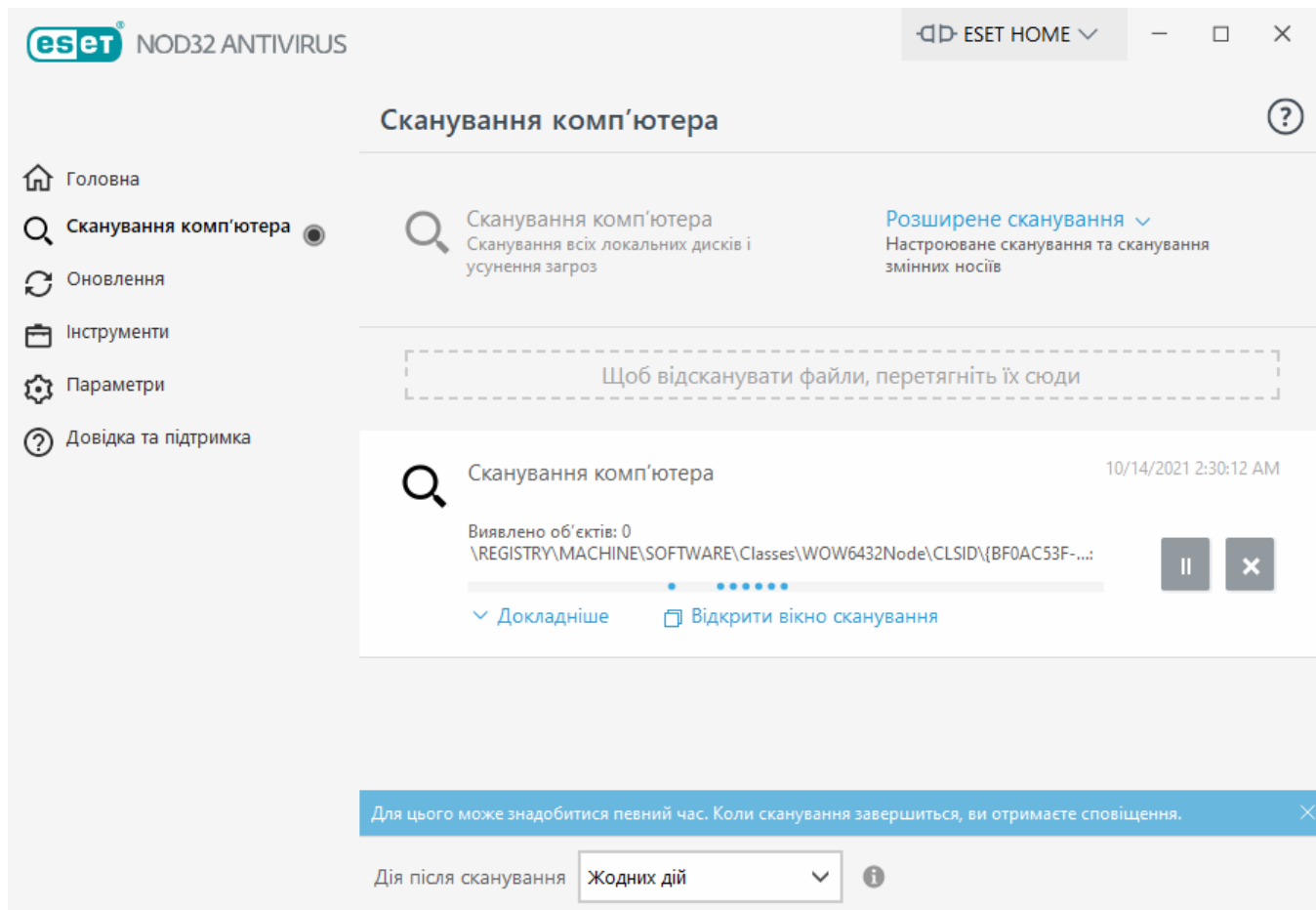
Продовжити: цей параметр доступний у режимі паузи. Натисніть **Продовжити**, щоб відновити сканування.

Зупинити: зупинення сканування.

Прокручування журналу перевірки: якщо вибрано цей параметр, журнал перевірки буде прокручуватися автоматично під час додавання нових записів, щоб останні з них були постійно видимі.



Клацніть стрілку чи піктограму лупи, щоб переглянути докладні відомості про поточну перевірку. Ви можете запустити паралельно ще одне сканування. Для цього натисніть **Сканування комп'ютера** або **Розширене сканування > Вибіркове сканування**.



У розкритому меню **Дія після сканування** можна задати дію, яка автоматично виконуватиметься після завершення сканування:

- **Нічого не робити:** після завершення сканування жодна дія не виконується.
- **Завершити роботу:** комп'ютер вимикається після завершення сканування.
- **Перезавантажити:** після завершення сканування всі відкриті програми закриваються, а комп'ютер перезавантажується.
- **Перезавантажити за необхідності:** комп'ютер перезавантажується, лише якщо потрібно завершити очищення виявлених загроз.
- **Примусове перезавантаження:** після завершення сканування всі відкриті програми закриваються, а комп'ютер перезавантажується без втручання користувача.
- **Примусово перезавантажити за потреби:** комп'ютер перезавантажується, лише якщо потрібно завершити очищення виявлених загроз.
- **Режим сну:** сеанс зберігається, а комп'ютер переводиться в режим зниженого енергоспоживання, щоб можна було швидко відновити роботу.
- **Режим глибокого сну:** всі запущені в оперативній пам'яті процеси зберігаються в окремому файлі на жорсткому диску. Комп'ютер вимикається, проте після запуску він відновлює попередній робочий стан.

i Дії **Сон** або **Глибокий сон** доступні залежно від налаштувань живлення та режиму сну в операційній системі або можливостей комп'ютера чи ноутбука. Зверніть увагу, що в режимі сну комп'ютер усе одно працює. Базові функції продовжують виконуватися, споживаючи енергію батареї (якщо комп'ютер живиться від неї). Щоб зберегти заряд, наприклад, коли ви залишили місце роботи, рекомендується користуватися режимом глибокого сну.

Вибрана дія запуститься після завершення всіх виконуваних процесів сканування. Якщо вибрано параметр **Завершити роботу** або **Перезавантажити**, протягом 30-секундного зворотного відліку відобразиться діалогове вікно для підтвердження (клацніть **Скасувати**, щоб деактивувати запитувану дію).

Журнал сканування комп'ютера

Після завершення сканування відкриється [журнал сканування комп'ютера](#) з усією релевантною інформацією, пов'язаною з певним скануванням. Журнал сканування містить, зокрема, наведену нижче інформацію.

- версія обробника виявлення;
- дата й час початку сканування;
- список просканиваних дисків, папок і файлів;
- Назва сканування за розкладом (лише [сканування за розкладом](#))
- Статус сканування
- кількість просканиваних об'єктів;
- кількість виявлених об'єктів;
- час виконання;
- загальний час сканування.

i Новий запуск [завдання сканування комп'ютера за розкладом](#) буде пропущено, якщо все ще виконується те саме заплановане завдання, яке було запущено раніше. Пропущене завдання сканування за розкладом створить журнал сканування комп'ютера з 0 просканиваних об'єктів і статусом **Сканування не запущено, оскільки попереднє сканування все ще виконується**.

Щоб знайти журнали попередніх сканувань, у [головному вікні програми](#) виберіть пункти **Інструменти > Файли журналу**. У розкритому меню виберіть **Сканування комп'ютера** й двічі натисніть потрібний запис.



Сканування комп'ютера

Журнал перевірки

Версія ядра виявлення: 22237 (20201030)

Дата: 10/30/2020 Час: 12:49:13 PM

Перевірено дисків, папок і файлів: Оперативна пам'ять; C:\Завантажувальні сектори/UEFI; C:\База даних WMI; Системний реєстр

Сканування перервано користувачем.

Перевірено об'єктів: 1163

Кількість виявлених об'єктів: 0

Час виконання: 12:49:25 PM Загальний час сканування: 12 секунд (00:00:12)

☐ Фільтрація

i Більш докладну інформацію про записи "не вдається відкрити", "помилка відкриття" й/або "архів пошкоджено" див. в статті бази знань ESET [за цим посиланням](#).

Клацніть повзунок ☐ **Фільтрація**, щоб відкрити вікно [Фільтрація журналів](#), де можна звузити пошук, указавши спеціальні критерії. Щоб відкрити контекстне меню, натисніть правою кнопкою миші певний запис журналу.

Дія	Використання
Відфільтровувати однакові записи	Активує фільтрацію журналу. У журналі відображатимуться записи лише вибраного типу.
Фільтр	Ця опція відкриває вікно фільтрації журналу й дає змогу визначити критерії для відображення певних записів. Сполучення клавіш: Ctrl+Shift+F
Увімкніть фільтр	Активує параметри фільтра. Якщо фільтр активується вперше, потрібно налаштувати відповідні параметри, після чого відкриється вікно фільтрації журналу.
Вимкнути фільтр	Вимикає фільтр (ту ж саму дію можна виконати, натиснувши перемикач унизу).
Копіювати	Дає змогу скопіювати виділені записи в буфер обміну. Сполучення клавіш: Ctrl+C
Копіювати все	Дає змогу скопіювати всі записи, що відображаються у вікні.
Експорт	Дає змогу експортувати виділені записи у файл XML.

Дія	Використання
Експортувати все	Дає змогу експортувати у файл XML всі записи, що відображаються у вікні.
Опис об'єкта	Відкриває енциклопедію загроз ESET, у якій міститься докладна інформація про небезпеки та симптоми виділеної загрози.

Сканування шкідливого програмного забезпечення

У розділі **Сканування шкідливого ПЗ (Додаткові параметри (F5) > Ядро виявлення > Сканування шкідливого ПЗ)** й виберіть параметри сканування. Цей розділ містить наведені нижче елементи.

Вибраний профіль: набір параметрів, які використовуються під час сканування за вимогою. Щоб створити його, натисніть **Змінити** поруч з елементом **Список профілів**. Більш докладну інформацію див. в розділі [Профілі сканування](#).

Об'єкти сканування: щоб просканувати певний об'єкт, натисніть **Змінити** поруч з елементом **Об'єкти сканування** й виберіть потрібну опцію в розкривному меню або вкажіть конкретні цілі в структурі папок (дерева). Більш докладну інформацію див. в розділі [Об'єкти сканування](#).

Параметри ThreatSense: у цьому розділі можна знайти додаткові параметри, наприклад розширення файлів, які бажано перевіряти, використовувані методи виявлення тощо. Натисніть, щоб відкрити вкладку додаткових параметрів сканера.

Сканування в неактивному стані

Сканування в неактивному стані можна увімкнути в розділі **Додаткові параметри**. Для цього виберіть **Ядро виявлення > Сканування шкідливого ПЗ > Сканування в неактивному стані**.

Сканування в неактивному стані

Щоб активувати цю функцію, увімкніть параметр **Увімкнути сканування в режимі очікування** за допомогою повзунка. Коли комп'ютер не використовуватиметься, програма виконуватиме сканування всіх локальних дисків без виводу даних на екран.

За замовчуванням сканування в неактивному стані не здійснюється, якщо комп'ютер (портативний комп'ютер) працює від батареї. Цей параметр можна змінити, активувавши за допомогою повзунка пункт **Запускати, навіть якщо комп'ютер живиться від батареї** в розділі "Додаткові параметри".

У розділі "Додаткові параметри" увімкніть параметр **Вести журнал** за допомогою повзунка, щоб вихідні дані сканування комп'ютера реєструвалися в розділі [Файли журналу](#). Для цього в [головному вікні програми](#) клацніть **Інструменти > Файли журналу**, а потім виберіть **Сканування комп'ютера** в розкривному меню **Журнал**.

Виявлення неактивного стану

Повний перелік умов, обов'язкових для запуску сканування в неактивному стані, наведено в розділі [Умови ініціювання виявлення неактивного стану](#).

Натисніть [Налаштування параметрів підсистеми ThreatSense](#), щоб змінити параметри сканування (наприклад, методи виявлення) для неактивного стану.

Профілі сканування

У ESET NOD32 Antivirus є чотири попередньо визначених профіля сканування:

- **Інтелектуальне сканування** – цей профіль розширеного сканування використовується за замовчуванням. Профіль "Інтелектуальне сканування" використовує технологію Smart-оптимізації, що виключає зі сканування файли, які в процесі попереднього сканування визначені як непошкоджені й з цього моменту не змінювалися. Це дозволяє знизити час сканування з мінімальним впливом на безпеку системи.
- **Сканування з контекстного меню** – у контекстному меню можна запустити сканування за вимогою для будь-якого файлу. Профіль сканування з контекстного меню дозволяє визначити конфігурацію сканування, яка буде використовуватися в разі запуску такого сканування.
- **Детальне сканування** – профіль детального сканування за замовчуванням не використовує технологію Smart-оптимізації, тому за умови використання цього профілю жоден файл не виключається зі сканування.
- **Сканування комп'ютера** – цей профіль використовується за замовчуванням під час стандартного сканування комп'ютера.

Потрібні параметри сканування можна зберегти для майбутнього використання. Рекомендується створити окремі профілі (з різними об'єктами сканування, способами сканування та іншими параметрами) для кожного типу сканування, які регулярно застосовуються.

Щоб створити новий профіль, відкрийте вікно додаткових параметрів (F5) і натисніть **Обробник виявлення > Сканування на шкідливе ПЗ > Сканування комп'ютера за вимогою > Список профілів**. У вікні **Менеджер профілів** міститься розкриттє меню **Вибраний профіль** зі списком наявних профілів перевірки й опцією для створення нового. Щоб створити профіль, який точно відповідатиме вашим вимогам, ознайомтесь із вмістом розділу [Налаштування параметрів підсистеми ThreatSense](#), у якому окремо описуються функції кожного параметра сканування.

Припустімо, що вам потрібно створити власний профіль сканування, для якого частково підходить конфігурація функції **Сканування комп'ютера**, але ви не бажаєте сканувати [упаковані](#) або [потенційно небезпечні програми](#) й додатково хочете застосувати параметр **Завжди виправляти виявлені об'єкти**. Введіть ім'я нового профілю у вікні **Менеджер профілів** і натисніть **Додати**. Виберіть новий профіль у розкриттєму меню **Вибраний профіль** і відкоригуйте решту параметрів відповідно до своїх потреб. Потім натисніть **ОК**, щоб зберегти свій новий профіль.

Об'єкти сканування

У розкривному меню **Об'єкти сканування** можна вибрати попередньо визначені набори об'єктів.

- **За параметрами профілю** – вибір об'єктів, зазначених у відповідному профілі сканування.
- **Змінні носії**: вибір дискет, запам'ятовуючих пристроїв USB, компакт-/DVD-дисків.
- **Локальні диски**: вибір усіх жорстких дисків системи.
- **Мережеві диски**: вибір усіх підключених мережевих дисків.
- **Налаштований вибір**: скасування вибору для всіх раніше вибраних об'єктів.

Структура папки (дерево) також містить певні об'єкти сканування.

- **Оперативна пам'ять**: сканування всіх процесів і даних, які наразі використовуються оперативною пам'яттю.
- **Завантажувальні сектори/UEFI**: сканування завантажувальних секторів і UEFI на наявність шкідливого програмного забезпечення. Більш докладну інформацію про сканер UEFI див. [в глосарії](#).
- **База даних WMI**: сканування всієї бази даних Windows Management Instrumentation (WMI), усіх областей імен, екземплярів класів і властивостей. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване під виглядом даних.
- **Системний реєстр**: сканування всього системного реєстру, усіх розділів і підрозділів. Пошук посилань на інфіковані файли або шкідливе програмне забезпечення, вбудоване під виглядом даних. Після очищення реєстру посилання залишатиметься в ньому, що вбезпечить користувачів від втрати важливих даних.

Щоб швидко перейти до об'єкта сканування (файлу або папки), введіть шлях у текстове поле під структурою дерева. Шлях чутливий до регістру. Щоб додати об'єкт до сканування, установіть відповідний прапорець у структурі дерева.

Контроль пристроїв

ESET NOD32 Antivirus дає змогу автоматично керувати носіями (CD/DVD/USB тощо). За допомогою цього модуля можна блокувати й налаштовувати розширені фільтри чи дозволи, а також контролювати доступ користувачів до пристрою та роботу з ним. Такі функції можуть бути корисними, якщо адміністратор комп'ютера хоче запобігти використанню пристроїв із недозволеним вмістом.

Підтримувані зовнішні пристрої:

- Дисківий накопичувач (жорсткий диск, змінний диск USB)
- Компакт-диск/DVD

- USB Принтер
- Сховище FireWire
- Bluetooth Пристрій
- Пристрій для читання смарт-карток
- Пристрій обробки зображень
- Модем
- LPT/COM порт
- Портативний пристрій
- Усі типи пристроїв

Параметри контролю пристроїв можна змінити в розділі **Додаткові параметри (F5) > Контроль пристроїв**.

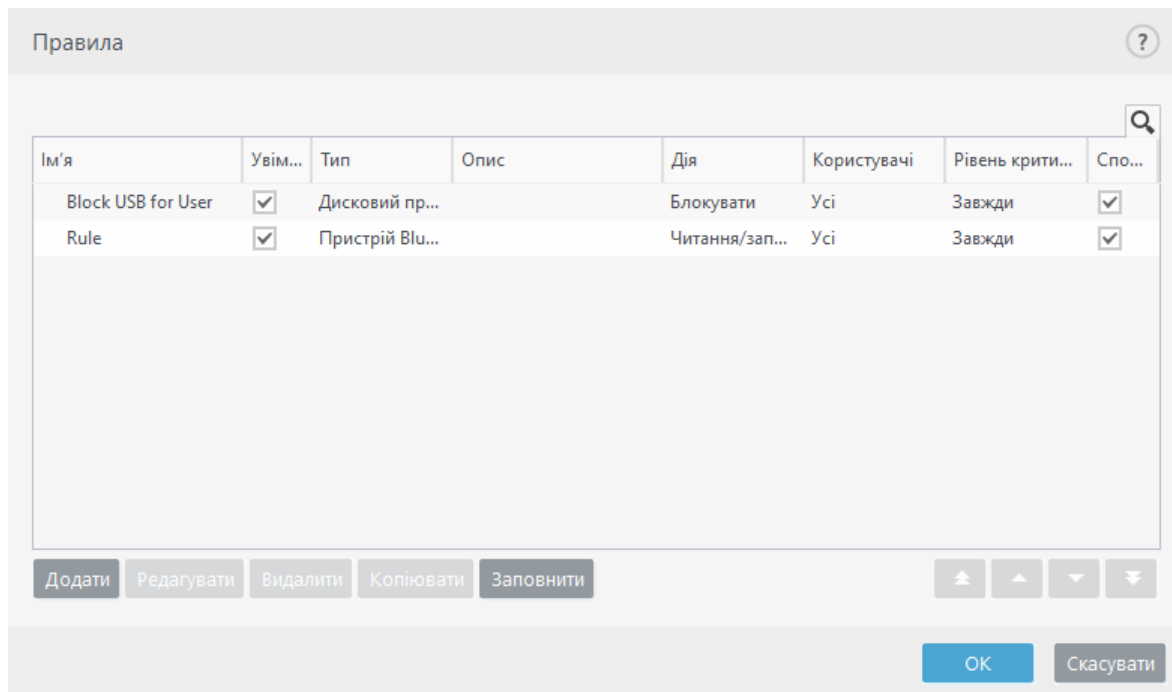
Увімкнення параметра **Увімкнути контроль пристроїв** за допомогою повзунка активує функцію контролю пристроїв у програмі ESET NOD32 Antivirus. Щоб зміни набули чинності, комп'ютер потрібно перезавантажити. Після цього стане доступним параметр **Правила**, за допомогою якого можна відкрити вікно [Редактор правил](#).

i Можна створювати різні групи пристроїв, до яких застосовуватимуться різні правила. Наприклад, можна створити тільки одну групу пристроїв, до яких застосовуватиметься правило з дією **Читання/запис** або **Лише читання**. Таким чином засіб контролю пристроїв блокуватиме нерозпізнані пристрої в разі їх підключення до комп'ютера.

Якщо під'єднати пристрій, який блокується поточним правилом, на екрані відобразиться вікно сповіщення, а доступ до пристрою буде заборонено.

Редактор правил контролю пристроїв

У вікні **Редактор правил контролю пристроїв** можна переглянути наявні правила, а також налаштувати детальні правила контролю зовнішніх пристроїв, які користувачі підключають до комп'ютера.



Можна дозволяти та блокувати певні пристрої для користувачів (індивідуально або для груп), а також на основі додаткових параметрів пристрою, які можна вказати в конфігурації правила. У переліку правил зазначено кілька описів правила, зокрема ім'я, тип зовнішнього пристрою, дію, яку потрібно виконати після підключення наявного зовнішнього пристрою до комп'ютера, а також зареєстрований у журналі рівень суворості. Перегляньте інформацію про те, [як додавати правила контролю пристроїв](#).

Натисніть **Додати** або **Змінити**, щоб керувати правилом. Натисніть **Копіювати**, щоб створити нове правило з попередньо визначеними параметрами, які вже використовуються для іншого вибраного правила. Рядки XML, які відображаються після натискання правила, можна скопіювати до буфера. Це допоможе системним адміністраторам експортувати/імпортувати вказані дані та застосовувати їх.

Щоб вибрати кілька правил, клацніть їх, водночас натиснувши й утримуючи клавішу **CTRL**. Після цього можна буде застосувати до всіх вибраних правил такі дії, як видалення або переміщення вгору чи вниз у списку. Прапорець **Увімкнено** відповідає за ввімкнення або вимкнення правила. Ця опція стане в пригоді, якщо використовувати правило не потрібно, але ви не хочете видаляти його остаточно.

Контроль здійснюється за допомогою правил, відсортованих згідно з пріоритетом (правила з вищим пріоритетом розміщуються вгорі списку).


Записи журналу можна переглянути в головному вікні ESET NOD32 Antivirus у розділі **Інструменти** > [Журнали](#).

У журналі контролю пристроїв фіксуються всі випадки застосування відповідної функції.

Виявлені пристрої

За допомогою кнопки **Заповнити** можна відобразити огляд усіх наразі підключених пристроїв з інформацією про їх тип, постачальника, модель і серійний номер (якщо доступно).

Виберіть пристрій у списку виявлених пристроїв і клацніть **ОК**, щоб [додати правило контролю пристроїв](#) із попередньо визначеною інформацією (усі параметри можна змінювати).

Пристрої в режимі зниженого енергопостачання (у режимі сну) позначено піктограмою попередження . Щоб активувати кнопку **ОК** і додати правило для цього пристрою, дотримуйтеся таких інструкцій:

- Заново підключіть пристрій
- Використовуйте пристрій (наприклад, запустіть програму "Камера" у Windows, щоб активувати веб-камеру)

Групи пристроїв

 Пристрій, під'єднаний до комп'ютера, може становити загрозу безпеці.

Вікно "Групи пристроїв" розділено на дві частини. У правій частині вікна міститься список пристроїв, що належать до відповідної групи, а в лівій – створені групи. Виберіть групу, а також пристрої, які потрібно відобразити в області справа.

Якщо відкрити вікно "Групи пристроїв" і вибрати одну з груп, можна додати пристрої до списку чи видалити їх. Інший спосіб додавання пристроїв до групи – імпорт із файлу. Також можна натиснути кнопку **Заповнити**. Після цього список усіх пристроїв, підключених до комп'ютера, відобразиться у вікні **Виявлені пристрої**. Виберіть пристрої в заповненому списку, а потім натисніть **ОК**, щоб додати їх до групи.

Елементи керування


Додати: можна додати групу, ввівши її ім'я, або додати пристрій до наявної групи (додатково можна вказати інші дані, наприклад постачальника, модель і серійний номер), залежно від того, у якій частині вікна було натиснуто кнопку.

Змінити: дає змогу редагувати ім'я вибраної групи або параметри пристрою (постачальника, модель і серійний номер).

Видалити: видаляє вибрану групу або пристрій залежно від того, у якій частині вікна натиснуто кнопку.

Імпорт: імпортує список пристроїв із текстового файлу. Для імпорту пристроїв із текстового файлу потрібне правильне форматування:

- Кожен пристрій починається з нового рядка.
- Для кожного пристрою через кому необхідно вказати **постачальника, модель і серійний номер**.

 Нижче наведено приклад вмісту текстового файлу:
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101

Експорт: експортує список пристроїв у файл.

За допомогою кнопки **Заповнити** можна відобразити огляд усіх наразі підключених пристроїв з інформацією про їх тип, постачальника, модель і серійний номер (якщо доступно).

Завершивши налаштування, натисніть **ОК**. Натисніть **Скасувати**, щоб закрити вікно **Групи пристроїв** без збереження змін.

i Можна створювати різні групи пристроїв, до яких застосовуватимуться різні правила. Наприклад, можна створити тільки одну групу пристроїв, до яких застосовуватиметься правило з дією **Читання/запис** або **Лише читання**. Таким чином засіб контролю пристроїв блокуватиме нерозпізнані пристрої в разі їх підключення до комп'ютера.

Зверніть увагу: для деяких типів пристроїв доступні не всі дії (дозволи). Для пристроїв збереження даних доступні всі чотири дії. Для пристроїв, не призначених для зберігання даних, доступні лише три дії (наприклад, дозвіл **Лише читання** недоступний для пристроїв Bluetooth, тому до них можна застосувати лише функції надання доступу, блокування чи попередження користувача).

Додавання правил контролю пристроїв

Правило контролю пристроїв визначає дію, що виконується після підключення до комп'ютера пристрою, який відповідає критеріям правила.

Змінити правило

Ім'я

Block USB for User

Правило ввімкнено

☒

Тип пристрою

Дисковий простір

Дія

Блокувати

Тип критеріїв

Пристрій

Постачальник

Модель

Серійний номер

Рівень критичності

Завжди

Список користувачів

Редагувати

Сповістити користувача

☒

ОК

Уведіть у поле **Ім'я** опис правила, щоб спростити його розпізнавання. За допомогою повзунка ввімкніть або вимкніть параметр **Правило ввімкнено**. Це може стати в пригоді, якщо ви не потрібно видаляти правило остаточно.

Тип пристрою

Вибір типу зовнішнього пристрою в розкритому меню (дисковий накопичувач, портативний пристрій, Bluetooth, FireWire тощо). Інформація про типи пристроїв надходить від операційної системи. Її можна переглянути в диспетчері пристроїв системи, попередньо під'єднавши пристрій до комп'ютера. До пристроїв збереження даних належать зовнішні диски та традиційні пристрої для читання карток пам'яті, які під'єднуються через USB або FireWire. До пристроїв для читання смарт-карток належать пристрої з підтримкою смарт-карток із вбудованою мікросхемою, зокрема SIM-картки або картки автентифікації. Прикладами пристроїв обробки зображень є сканери або фотокамери. Оскільки такі пристрої надають інформацію лише про свої дії, але не про користувачів, їх можна заблокувати лише повністю.

Дія

Можна дозволити або заборонити доступ до пристроїв, не призначених для зберігання даних. Натомість правила, які стосуються пристроїв для зберігання даних, дають змогу вибрати один із наведених нижче параметрів.

- **Читання/запис:** повний доступ до пристрою.
- **Блокування:** заборона доступу до пристрою.
- **Лише читання:** доступ лише для читання даних, збережених на пристрої.
- **Попереджати:** під час кожного підключення пристрою користувач отримуватиме сповіщення про виконану дію (дозволено/заблоковано), а в журналі фіксуватиметься відповідний запис. Пристрої не запам'ятовуються: сповіщення відображається щоразу, коли підключається навіть один і той самий пристрій.

Зверніть увагу: для деяких типів пристроїв доступні не всі дії (дозволи). Для пристроїв збереження даних доступні всі чотири дії. Для пристроїв, не призначених для зберігання даних, доступні лише три дії (наприклад, дозвіл **Лише читання** недоступний для пристроїв Bluetooth, тому до них можна застосувати лише функції надання доступу, блокування чи попередження користувача).

Тип критеріїв

Виберіть **Група пристроїв** або **Пристрій**.

Відповідно до використовуваних пристроїв можна налаштовувати правила за допомогою наведених нижче додаткових параметрів. Не залежать від реєстру:

- **Постачальник:** фільтрація за іменем постачальника або ID.
- **Модель:** поточне ім'я пристрою.
- **Серійний номер:** номер, який має більшість зовнішніх носіїв. Якщо це диск CD/DVD, серійний номер відповідає конкретному носію, а не дисководу CD.



Якщо певні параметри не вказано, під час застосування правила система ігноруватиме відповідні поля. В усіх полях параметри фільтрації вводяться без урахування реєстру. Символи узагальнення (*, ?) не підтримуються.



Щоб переглянути інформацію про пристрій, створіть для нього спеціальне правило, підключіть пристрій до комп'ютера та відкрийте [журнал контролю пристроїв](#).

Рівень критичності

Програма ESET NOD32 Antivirus записує всі важливі події в журнал, який можна відкрити безпосередньо в головному меню. Клацніть **Інструменти > Файли журналу**, а потім у розкритому меню **Журнал** виберіть пункт **Контроль пристроїв**.

- **Завжди:** фіксуються всі події.
- **Діагностика:** фіксується інформація, необхідна для оптимізації програми.
- **Інформація:** фіксуються інформаційні повідомлення, включно зі сповіщеннями про успішне оновлення, і всі зазначені вище елементи.
- **Попередження:** запис усіх критичних помилок і попереджувальних повідомлень.
- **Нічого:** жодні дані не фіксуватимуться.

Список користувачів

Можна обмежувати правила для окремих користувачів або для груп користувачів, додаючи їх у список користувачів. Для цього поруч із розділом **Список користувачів** клацніть **Змінити**.

- **Додати:** відкриває діалогове вікно **Типи об'єкта: користувачі або групи**, де можна вибрати потрібних користувачів.
- **Видалити** – видаляє вибраного користувача зі списку фільтрації.

Обмеження списку користувачів

Список користувачів не можна задати для правил, які мають відношення до певних [типів пристроїв](#):



- USB-принтер;
- Пристрій Bluetooth
- Пристрій для читання смарт-карток
- Пристрій обробки зображень
- Модем
- Порт LPT/COM

Сповістити користувача: якщо під'єднати пристрій, який блокується поточним правилом, відкриється вікно сповіщення.

Систему запобігання вторгненням (HIPS)

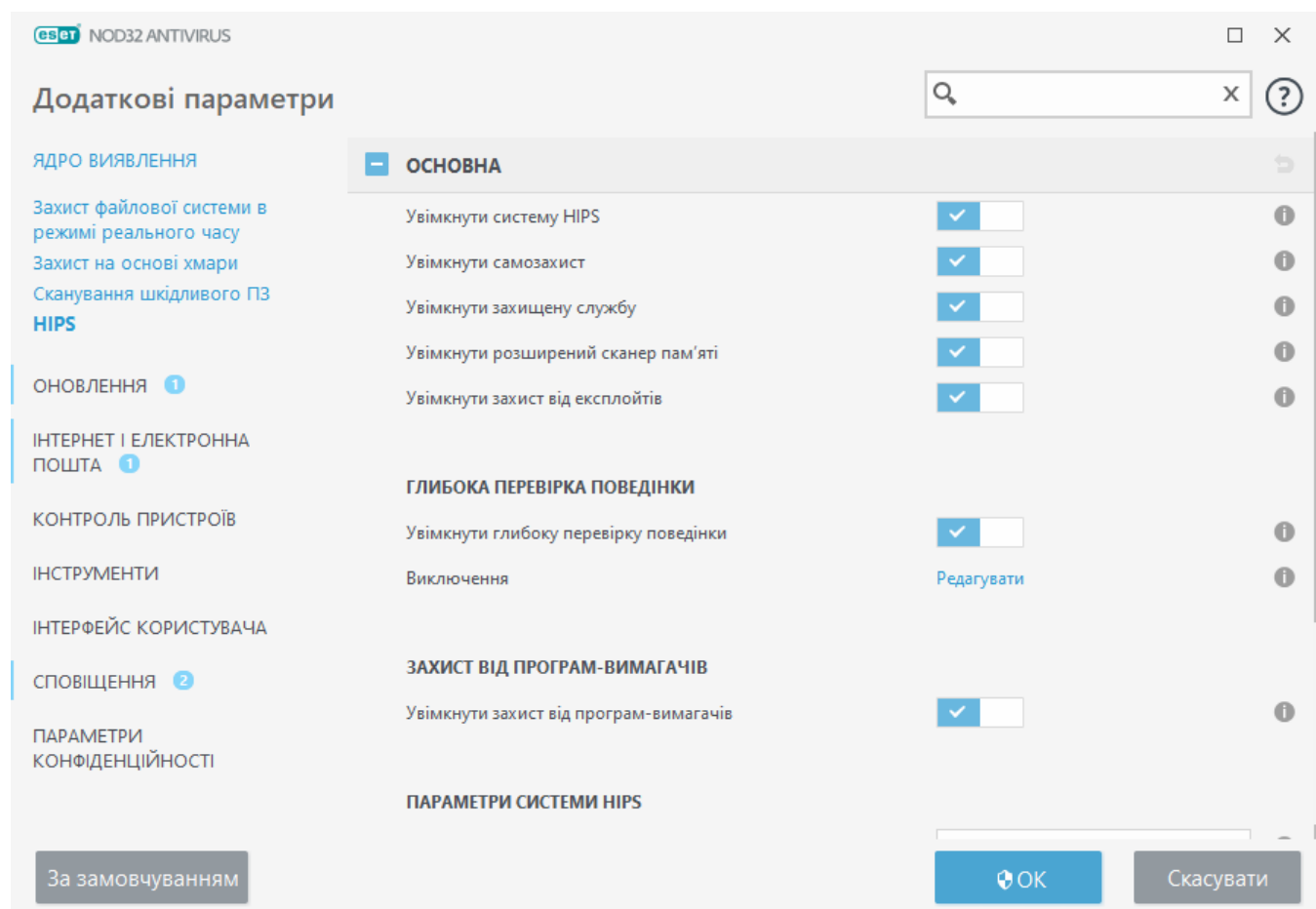


Зміни до параметрів HIPS має вносити лише досвідчений користувач. Оскільки помилка в налаштуваннях може призвести до нестабільності системи.

Система виявлення вторгнень (HIPS) захищає комп'ютер від шкідливих програм і небажаної активності, що негативно впливає на його роботу. Система HIPS використовує розширений

поведінковий аналіз і можливості системи виявлення на основі мережного фільтра для стеження за запущеними процесами, файлами та розділами реєстру. Система HIPS працює окремо від захисту файлової системи в режимі реального часу та не є брандмауером: вона лише відстежує процеси, запущені в операційній системі.

Налаштування HIPS можна знайти в меню **Додаткові параметри**(F5) > **Обробник виявлення > HIPS > Основна**. Інформація про стан системи HIPS (увімкнено чи вимкнено) відображається в [головному вікні програми](#) ESET NOD32 Antivirus (розділ **Параметри > Захист комп'ютера**).



Основна

Увімкнути HIPS: систему запобігання вторгненням (HIPS) увімкнено за замовчуванням у ESET NOD32 Antivirus. Вимкнення HIPS призведе до деактивації решти функцій HIPS, зокрема функції «Захист від експлойтів».

Увімкнути самозахист: ESET NOD32 Antivirus використовує вбудовану технологію **самозахисту** (складова HIPS), яка не дозволяє шкідливому програмному забезпеченню пошкоджувати або відключати антивірусні та антишпигунські модулі. Система самозахисту захищає критично важливі процеси системи та програми ESET, розділи реєстру та файли від маніпуляцій.

Увімкнути захищену службу: вмикає захист для ESET Service (ekrn.exe). Якщо цей параметр увімкнено, ця служба запускається як захищений процес Windows, забезпечуючи захист від атак із боку шкідливого програмного забезпечення. Цей параметр доступний у Windows 8.1 і більш пізніх версій.

Увімкнути розширений сканер пам'яті: працює разом із засобом захисту від експлойтів. Він

посилює захист від зловмисного ПЗ, призначеного для обходу захисних продуктів за допомогою обфускації або шифрування. Удосконалений сканер пам'яті ввімкнено за замовчуванням. Докладніше про цей тип захисту див. в [гlossарії](#).

Увімкнути захист від експлойтів: служить для захисту програм, які зазвичай використовуються для зараження системи, зокрема веб-браузерів, засобів читання PDF, клієнтів електронної пошти й компонентів MS Office. Захист від експлойтів увімкнено за замовчуванням. Докладніше про цей тип захисту див. в [гlossарії](#).

Глибока перевірка поведінки

Увімкнути глибоку перевірку поведінки: це ще один засіб захисту, який включено до системи HIPS. Це розширення HIPS аналізує поведінку всіх програм, запущених на комп'ютері, та попереджає вас про підозрілу поведінку процесу.

У розділі [Виключення HIPS із глибокої перевірки поведінки](#) можна виключити процеси з перевірки. Щоб система сканувала всі процеси на наявність загроз, рекомендуємо створювати виключення лише за крайньої потреби.

Захист від програм, які вимагають викуп

Увімкнути захист від програм-вимагачів: це ще один засіб захисту, який включено до системи HIPS. Щоб такий тип захисту працював, потрібно мати систему перевірки репутації ESET LiveGrid®. [Докладніше про цей тип захисту можна прочитати тут](#).

Параметри системи HIPS

Режим фільтрації може виконуватися в одному з таких режимів:

Режим фільтрації	Опис
Автоматичний режим	операції ввімкнено (окрім заблокованих попередньо визначеними правилами, які захищають систему).
Інтелектуальний режим	користувач отримуватиме сповіщення лише про дуже підозрілі події.
Інтерактивний режим	користувач має підтверджувати виконання операцій.
Режим на основі положень політики	блокує всі операції, які не визначені певним правилом, що дозволяє їх.
Режим навчання	Операції ввімкнено, а після кожної операції створюється правило. Правила, створені в цьому режимі, можна переглядати в редакторі Правила HIPS , проте їх пріоритет нижчий за пріоритет правил, створених вручну або в автоматичному режимі. Якщо в розкривному меню Режим фільтрації вибрати Режим навчання , стане доступним налаштування Режим навчання стане неактивним о . Виберіть тривалість використання в режимі навчання (максимум — 14 днів). Після завершення зазначеного періоду відобразиться запит на зміну правил, створених системою HIPS у режимі навчання. Можна також вибрати інший режим фільтрації або відкласти рішення й користуватися режимом навчання далі.

Установлено після виходу з режиму навчання: укажіть режим фільтрації, який застосовуватиметься після завершення роботи в режимі навчання. Після завершення строку дії зміна режиму фільтрації NIPS за допомогою опції **Запитувати користувача** потребуватиме наявності прав адміністратора.

Система NIPS контролює події в операційній системі та реагує на них відповідно до правил, подібних до тих, які використовує брандмауер. Щоб відкрити редактор **правил NIPS**, натисніть **Змінити** біля елемента **Правила**. У вікні правил NIPS можна вибирати, додавати, змінювати й вилучати правила. Докладніше про створення правил і операції NIPS див. в розділі [Змінення правила NIPS](#).

Інтерактивне вікно NIPS

У вікні сповіщень системи запобігання вторгненням (NIPS) можна створити правило на основі будь-якої нової дії, виявленої системою NIPS, а потім визначити умови, за яких ця дія дозволятиметься або блокуватиметься.

Створені таким чином правила рівноцінні заданим уручну. Тому правило, створене у вікні сповіщень, може бути менш конкретним у порівнянні з тим правилом, що ініціювало появу цього вікна. Це означає, що після створення такого правила в діалоговому вікні одна операція може ініціювати появу того самого вікна. Більш докладну інформацію див. в розділі [Пріоритет для правил NIPS](#).

Якщо за замовчуванням для правила вибрано дію **Запитувати щоразу**, під час кожного його застосування відображатиметься відповідне діалогове вікно. Ви можете **Відхилити** або **Дозволити** певну операцію. Якщо за відведений час ви не вказали жодної дії, її буде вибрано на основі правил.

Параметр **Запам'ятати до закриття програми** ініціює використання дії (**Дозволити/Відхилити**) до наступної зміни правил або режимів фільтрації, оновлення модуля NIPS або перезапуску системи. Після будь-якої з цих трьох дій тимчасові правила буде видалено.

Параметр **Створити правило та запам'ятати безстроково** дозволяє створити нове правило NIPS, яке пізніше можна змінити в розділі [Керування правилами NIPS](#) (для цього потрібні права адміністратора).

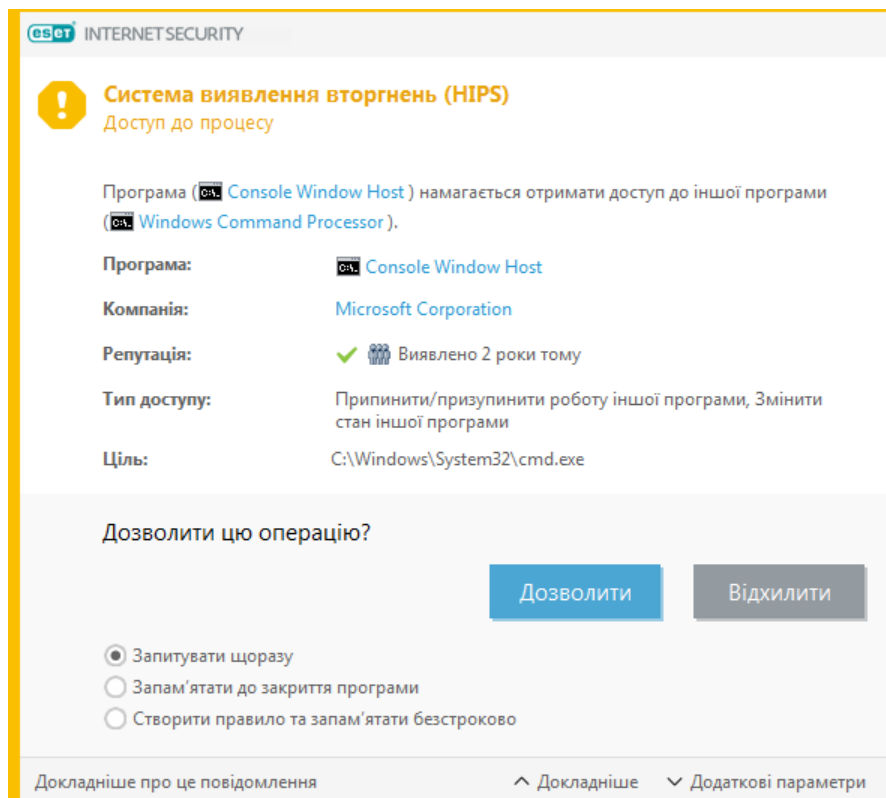
Клацніть **Докладніше** в нижній частині вікна, щоб дізнатися більше про програму, яка ініціює операцію, репутацію файлу або тип операції, яку вам потрібно підтвердити або відхилити.

Щоб відкрити розширені параметри правила, клацніть **Розширені параметри**. Якщо вибрати **Створити правило та запам'ятати безстроково**, будуть доступні вказані нижче параметри:

- **Створити правило, дійсне лише для цієї програми:** якщо зняти цей прапорець, правило буде створено для всіх вихідних програм.
- **Лише для операції:** виберіть операції правила для файлу (програми, реєстру). [Див. описи всіх операцій NIPS](#).
- **Лише для об'єкта:** виберіть об'єкти правила для файлу (програми, реєстру).

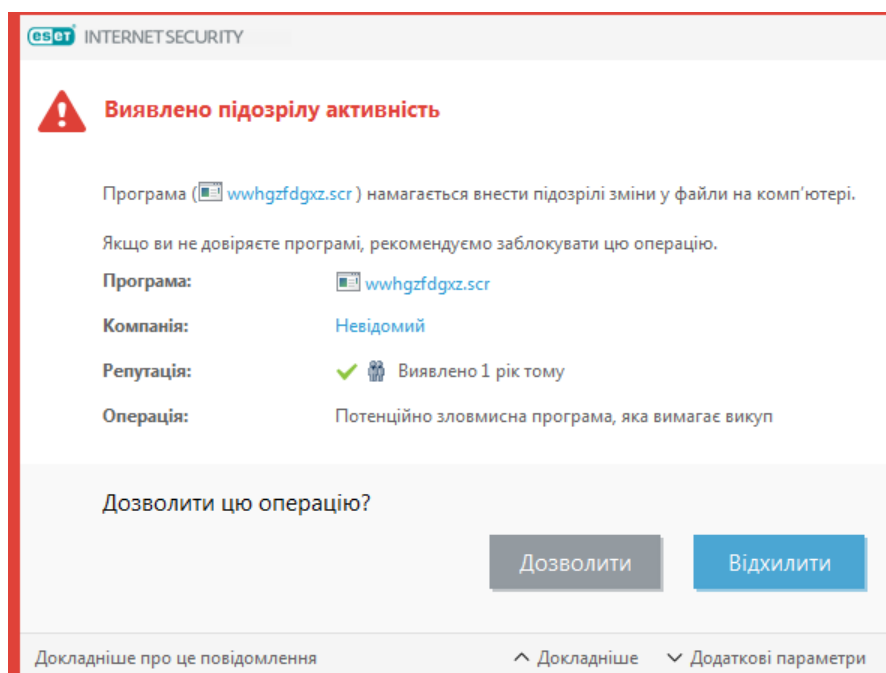
Набридли сповіщення HIPS?

- ! Щоб більше не показувати сповіщення, змініть режим фільтрації на **Автоматичний режим** у розділі **Додаткові параметри (F5) > Ядро виявлення > HIPS > Базові**.



Виявлено потенційно зловмисну програму, яка вимагає викуп

Це інтерактивне вікно з'являється, коли виявлено потенційно зловмисну програму. Ви можете **Відхилити** або **Дозволити** певну операцію.



Щоб переглянути окремі параметри виявлення, клацніть **Докладніше**. У діалоговому вікні можна **надіслати файл на аналіз** або **виключити з перевірки**.



Щоб функція [захисту від програм-вимагачів](#) працювала належним чином, потрібно ввімкнути ESET LiveGrid®.

Керування правилами HIPS

Список визначених користувачем і автоматично доданих правил із системи HIPS. Більш докладні відомості про створення правил і операції HIPS можна переглянути в розділі [Параметри правила HIPS](#). Див. також розділ [Загальні принципи роботи HIPS](#).

Стовпці

Правило: визначене користувачем або автоматично вибране ім'я правила.

Увімкнено: деактивуйте цей параметр за допомогою повзунка, якщо потрібно тільки зберегти правило в списку, а не використовувати його.

Дія: правило визначає дію (**Дозволити**, **Заблокувати** або **Запитувати**), яка виконуватиметься в разі дотримання відповідних умов.

Джерела: правило використовуватиметься лише в тому випадку, коли подію ініціює програма.

Об'єкти: правило використовуватиметься лише в тому випадку, коли операція пов'язана з певним файлом, програмою або записом реєстру.

Рівень критичності – якщо ввімкнути цей параметр, інформацію про таке правило буде записано в [журнал HIPS](#).

Сповіщати: у разі ініціювання події в правому нижньому куті відображається невелике спливаюче вікно.

Елементи керування

Додати: створити нове правило.

Редагувати: редагувати вибрані елементи.

Видалити: видалить вибрані записи.

Пріоритет для правил HIPS

Немає параметрів, які б дозволили змінити рівень пріоритету правил HIPS за допомогою кнопок переходу у верхню або нижню частину вікна.

- Усі створювані правила мають однаковий пріоритет
- Що більш конкретне правило, то вищий пріоритет (наприклад, правило для певної програми має вищий пріоритет відносно правил для всіх програм)

- Система запобігання вторгненням (HIPS) має внутрішні правила з більш високим пріоритетом, що недоступні для користувача (наприклад, користувач не може змінити визначені правила самозахисту)
- Якщо створюване правило може вповільнити роботу операційної системи, воно не буде застосовуватися (буде мати найнижчий пріоритет)

Змінення правила HIPS

Спочатку див. тему [Керування правилами HIPS](#).

Ім'я правила: визначене користувачем або автоматично вибране ім'я правила.

Дія: дає змогу визначити дію (**Дозволити**, **Заблокувати** або **Запитувати**), яка виконуватиметься в разі виконання відповідних умов.

Задіяні операції: потрібно вибрати тип операції, для якої застосовуватиметься правило. Правило використовуватиметься лише для цього типу операцій і для вибраної цілі.

Увімкнено: вимкніть цей параметр за допомогою повзунка, щоб зберегти правило у списку, але не застосовувати його.

Рівень критичності – якщо увімкнути цей параметр, інформацію про таке правило буде записано в [журнал HIPS](#).

Сповістити користувача: у разі ініціювання події в правому нижньому куті відображається невелике спливаюче вікно.

Правило складається з частин, що описують умови, які його ініціюють.

Програми-джерела: правило використовуватиметься лише в тому випадку, якщо подію ініціює ця програма. У розкритому меню виберіть **Окремі програми** й натисніть **Додати**, щоб додати нові файли. Також можна вибрати **Усі програми**, щоб додати всі програми.

Цільові файли: правило використовуватиметься лише в тому випадку, якщо операцію пов'язано з відповідним цільовим об'єктом. У розкритому меню виберіть **Окремі файли** й натисніть **Додати**, щоб додати нові файли чи папки, або виберіть **Усі файли**, щоб додати всі файли.

Програми: правило використовуватиметься лише в тому випадку, якщо операція пов'язана з відповідним цільовим об'єктом. У розкритому меню виберіть **Окремі програми** й натисніть **Додати**, щоб додати нові файли або папки, або виберіть **Усі програми**, щоб додати всі програми.

Записи реєстру: правило використовуватиметься лише в тому випадку, якщо операція пов'язана з відповідним цільовим об'єктом. У розкритому меню виберіть **Окремі записи** й натисніть **Додати**, щоб ввести вручну, або натисніть **Відкрити редактор реєстру**, щоб вибрати ключ із реєстру. Ви також можете вибрати в розкритому меню елемент **Усі записи**, щоб додати всі програми.

i Деякі операції за певними правилами, визначені заздалегідь системою HIPS, не можна заблокувати, і їх дозволено за замовчуванням. Окрім того, не всі системні операції контролюються HIPS. HIPS відстежує лише ті операції, які можуть вважатися небезпечними.

Опис важливих операцій

Операції з файлами

- **Видалити файл:** програма відображає запит про надання дозволу на видалення цільового файлу.
- **Виконати запис до файлу:** програма відображає запит про надання дозволу на запис до цільового файлу.
- **Безпосередній доступ до диска** – програма намагається розпочати читання з диска або запис на нього нестандартним способом, який дає змогу обійти звичайні процедури Windows. Це може призвести до зміни файлів без застосування відповідних процедур. Таку операцію може виконувати шкідливе ПЗ, яке намагається уникнути виявлення, програма резервного копіювання, що робить спробу створити точну копію диска, або менеджер розділів, який намагається повторно впорядкувати томи диска.
- **Установити глобальне перехоплення:** передбачає виклик функції SetWindowsHookEx із бібліотеки MSDN.
- **Завантажити драйвер:** інсталяція та завантаження драйверів у середовищі системи.

Операції з програмами

- **Налагодити іншу програму:** приєднання до процесу засобу налагодження. Під час виправлення неполадок у роботі іншої програми певні відомості про її поведінку можна переглядати й коригувати. Також можна отримати доступ до даних цієї програми.
- **Зупиняти події від іншої програми:** програма-джерело намагається перехопити події, пов'язані з певною програмою (наприклад, клавіатурний шпигун робить спробу перехопити події, пов'язані з браузером).
- **Припинити/призупинити роботу іншої програми:** призупинення, відновлення або припинення процесу (доступ можна отримати безпосередньо з диспетчера процесів або на вкладці "Процеси").
- **Запустити нову програму:** запуск нових програм або процесів.
- **Змінити стан іншої програми:** програма-джерело намагається здійснити запис у пам'ять цільової програми або виконати певний код від її імені. Така функція може бути корисною для захисту важливої програми: просто визначте її як цільову у правилі, що блокує використання подібної операції.

i Не можна зупинити виконання процесу на 64-розрядній версії Windows XP.

Операції з реєстром

- **Змінити параметри запуску** – будь-які зміни в параметрах запуску програм під час завантаження Windows. Їх можна знайти, наприклад, здійснивши пошук за назвою розділу Run у реєстрі Windows.
- **Видалити з реєстру:** видалення розділу або його значення.
- **Перейменувати розділ реєстру:** перейменування розділів реєстру.
- **Внести зміни до реєстру:** створення нових значень розділів реєстру, зміна наявних значень, переміщення даних у дереві бази даних або налаштування прав доступу до розділів реєстру для користувачів і груп.

Під час введення цілі можна користуватися символами узагальнення (з певними обмеженнями). Замість назви конкретного розділу у шляху реєстру можна ввести символ * (астериск). Наприклад, `HKEY_USERS*\software` може означати `HKEY_USER\default\software`, але не може означати



`HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\default\software`.

`HKEY_LOCAL_MACHINE\system\ControlSet*` – не дійсний шлях до розділу реєстру. Шлях до розділу реєстру, який містить *, означає "цей шлях або будь-який шлях на будь-якому рівні після цього символу". Символи узагальнення для цільових файлів можна використовувати лише таким чином. Спершу перевіряється визначена частина шляху, а потім шлях після символу узагальнення (*).

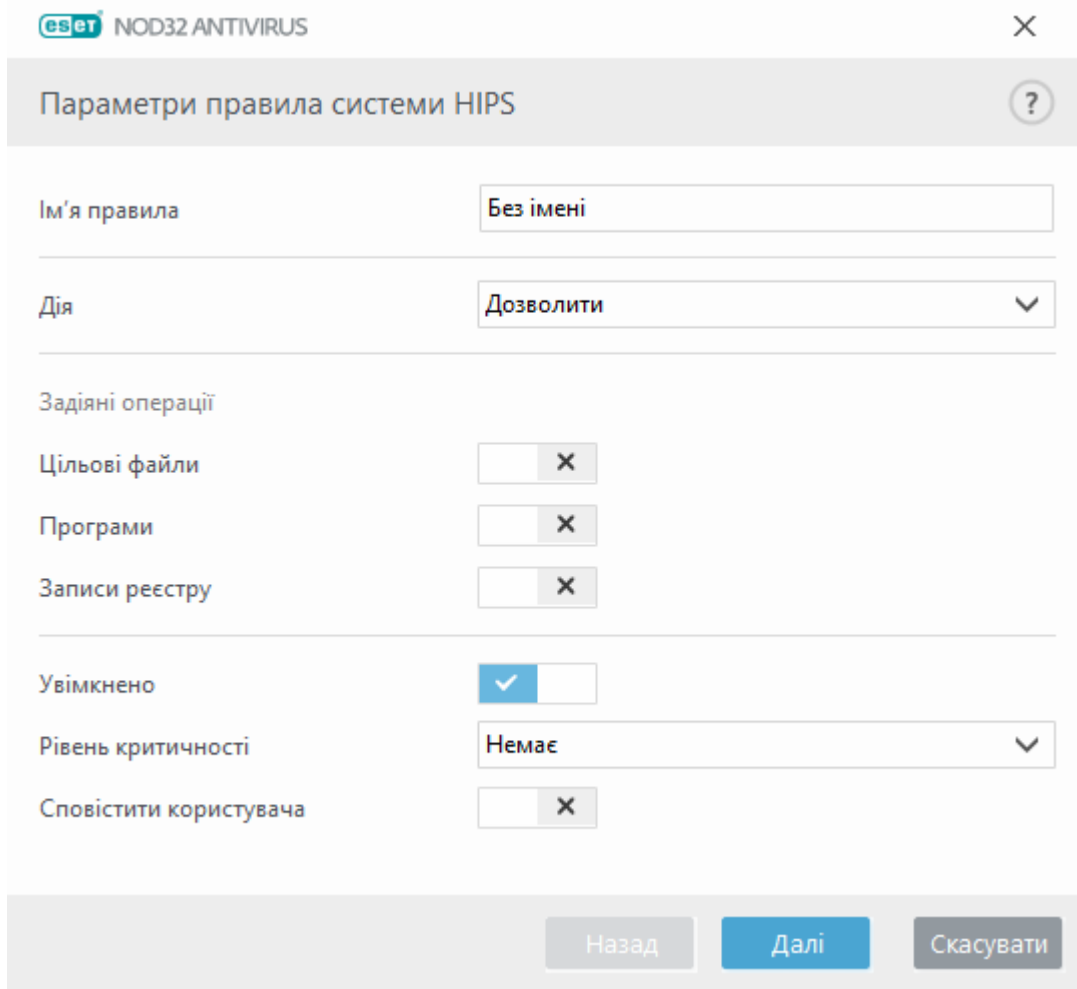


Якщо створити дуже загальне правило, з'явиться відповідне попередження.

На наведеному нижче прикладі ми продемонструємо, як обмежити небажану поведінку окремої програми.

1. Призначте ім'я правилу й виберіть **Заблокувати** (або **Запитати**, якщо ви маєте намір вибрати дію пізніше) в розкритому меню **Дія**.
2. За допомогою повзунка ввімкніть параметр **Сповістити користувача**, щоб відображати сповіщення під час кожного застосування правила.
3. Виберіть щонайменше одну операцію в списку **Операції для розділу**, до якого застосовуватиметься правило.
4. Натисніть кнопку **Далі**.
5. У розкритому меню вікна **Програми-джерела** виберіть **Окремі програми**, щоб застосувати нове правило до всіх програм, які намагаються виконати будь-яку з вибраних операцій з указаними програмами.
6. Клацніть **Додати**, а потім ..., щоб вибрати шлях до певної програми, і натисніть кнопку **ОК**. За бажанням додайте більше програм.
Приклад: `C:\Program Files (x86)\Untrusted application\application.exe`
7. Виберіть операцію **Записати у файл**.
8. У розкритому меню виберіть пункт **Усі файли**. Після цього будуть блокуватися будь-які спроби програм, вибраних у попередньому кроці, виконати запис у будь-які файли.

9. Натисніть кнопку **Готово**, щоб зберегти нове правило.



eset NOD32 ANTIVIRUS

Параметри правила системи HIPS

Ім'я правила: Без імені

Дія: Дозволити

Задіяні операції

Цільові файли: X

Програми: X

Записи реєстру: X

Увімкнено: ☒

Рівень критичності: Немає

Сповістити користувача: X

Назад Далі Скасувати

Додавання шляху до програми/реєстру для HIPS

Виберіть шлях до файлу програми, клацнувши опцію Якщо вибрати папку, додадуться всі програми, що містяться в ній.

Опція **Відкрити редактор реєстру** дає змогу запустити редактор реєстру Windows (regedit). Під час додавання шляху реєстру введіть потрібний розділ у поле **Значення**.

Приклади шляху файлу або реєстру:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Додаткові параметри HIPS

Наведені нижче опції стануть у пригоді під час налагодження програми й аналізу її поведінки.

Драйвери, які дозволено завжди завантажувати: виберіть драйвери, які можна

завантажувати в усіх режимах фільтрації, якщо їх не блокує правило користувача.

Запис усіх заблокованих дій: усі заблоковані операції буде записано в журнал HIPS. Використовуйте цю функцію лише для вирішення проблеми або за запитом служби підтримки ESET, оскільки вона може створювати великий файл журналу й сповільнювати роботу комп'ютера.

Повідомляти, коли в автоматично виконувані програми вносяться зміни: на робочому столі відображатимуться сповіщення щоразу, коли програма додається до списку завантажуваних під час запуску системи або видаляється з нього.

Драйвери, які дозволено завантажувати завжди

Драйвери в цьому списку можна завантажувати в усіх режимах фільтрації HIPS, якщо їх не блокує правило користувача.

Додати: додати новий драйвер.

Змінити: редагувати дані вибраного драйвера.



Видалити – видалити драйвер зі списку.

Скинути: перезавантажити набір системних драйверів.

i Натисніть **Скинути**, якщо ви не бажаєте включати драйвери, додані вручну. Це може бути корисно, якщо вам не вдається вручну видалити зі списку додані драйвери.

Ігровий режим

Ігровий режим – це функція для користувачів, які не хочуть переривати роботу програм, відволікатися на спливаючі вікна й надмірно навантажувати CPU. Ігровий режим також може використовуватися під час презентацій, які небажано переривати антивірусною перевіркою. Після ввімкнення цієї функції всі спливаючі вікна вимикаються, а робота планувальника повністю зупиняється. Функції захисту системи продовжують роботу у фоновому режимі, не вимагаючи втручання користувача.

Ви можете ввімкнути або вимкнути ігровий режим у [головному вікні програми](#) в розділі **Параметри > Захист комп'ютера**, натиснувши  або  поруч із параметром **Ігровий режим**. Увімкнення ігрового режиму становить потенційний ризик безпеки, тому колір піктограми статусу захисту на панелі завдань стане оранжевим, а також відобразиться відповідне попередження. Це попередження також відображатиметься в [головному вікні програми](#), де з'явиться сповіщення оранжевим кольором **Ігровий режим активний**.

Щоб ігровий режим вмикався щоразу, коли ви запускаєте програму в повноекранному режимі, і вимикався, щойно ви її закриєте, перейдіть у меню **Додаткові параметри (F5) > Інструменти > Ігровий режим** й активуйте параметр **Автоматично вмикати ігровий режим під час запуску програм у повноекранному режимі**.

Виберіть **Автоматично вимикати ігровий режим через**, щоб ігровий режим автоматично вимикався через заданий проміжок часу.

Сканування під час запуску

За замовчуванням автоматична перевірка файлу під час запуску виконується після запуску системи або під час оновлення обробника виявлення. Цей процес перевірки залежить від параметрів і завдань, визначених у розділі [Завдання за розкладом](#).

Параметри перевірки під час запуску є частиною запланованого завдання **Перевірка файлів під час запуску системи**. Щоб змінити його налаштування, відкрийте **Інструменти > Розклад**, натисніть **Автоматична перевірка файлу під час запуску**, а тоді – **Змінити**. На останньому кроці відобразиться вікно [Автоматична перевірка файлів під час запуску системи](#) (див. наступний розділ для отримання докладніших відомостей).

Детальні інструкції щодо створення запланованого завдання та керування див. у розділі [Створення нових завдань](#).

Автоматична перевірка файлів під час запуску системи

Створюючи заплановане завдання перевірки файлів під час запуску, можна змінити перелічені нижче параметри.

У розкритому меню **Об'єкт сканування** визначається глибина перевірки файлів, що виконується під час запуску системи, на основі прогресивного алгоритму. Відповідно до вказаних критеріїв файли розташовуються за спаданням:

- **Всі зареєстровані файли** (перевіряється більшість файлів)
- **Файли, які рідко використовуються**
- **Файли, які зазвичай використовуються**
- **Файли, які часто використовуються**
- **Тільки файли, які найчастіше використовуються** (перевірка виконується на мінімальній кількості файлів)

Включено також дві конкретні групи:

- **Файли, запущені перед входом користувача в систему:** файли з розташувань, доступні без обов'язкового входу користувача в систему (практично всі розташування під час запуску, зокрема служби, додаткові компоненти браузера, сповіщення winlogon, записи інструмента "Завдання за розкладом", відомі dll тощо).
- **Файли, що запускаються після входу користувача в систему** – файли з розташувань, які дають змогу запускати їх лише після входу користувача в систему (файли, які запускаються лише для певного користувача, зокрема файли в розташуванні `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`).

Списки файлів для сканування є фіксованими для кожної з наведених вище груп. Якщо вибрати нижчу глибину сканування для файлів, які виконуються під час запуску системи, то файли, які не будуть проскановані, перевірятимуться під час відкриття або виконання.

Пріоритет сканування: рівень пріоритетності, що визначається перед початком сканування:

- **Під час простою:** завдання виконуватиметься лише тоді, коли система неактивна.
- **Найнижчий:** за мінімально можливого рівня завантаження системи.
- **Низький:** за низького завантаження системи.
- **Нормальний:** за середнього завантаження системи.

Захист документів

Модуль захисту документів сканує документи Microsoft Office перед їх відкриттям, а також файли, автоматично завантажені браузером Internet Explorer (такі як елементи Microsoft ActiveX). Функція захисту документів забезпечує ще один рівень безпеки, додатково до захисту файлової системи в режимі реального часу. Для підвищення продуктивності її можна вимкнути в системах, робота яких не пов'язана з опрацюванням великої кількості документів Microsoft Office.

Щоб увімкнути захист документів, відкрийте розділ **Додаткові параметри** (F5), виберіть пункти **Ядро виявлення > Сканування на шкідливе ПЗ > Захист документів** і клацніть повзунок **Увімкнути захист документів**.

i Цю функцію активують програми, у яких використовується прикладний інтерфейс Microsoft Antivirus API (наприклад, Microsoft Office 2000 та пізніших версій або Microsoft Internet Explorer 5.0 та пізніших версій).

Виключення

У розділі **Виключення** можна виключити **об'єкти** з ядра виявлення. Щоб система сканувала всі об'єкти, рекомендується створювати виключення лише за необхідності. Існують ситуації, коли може виникнути потреба виключити об'єкт. Прикладом таких ситуацій, коли потрібно виключити об'єкт зі списку сканування, може бути сканування елементів великих баз даних, що значно сповільнить роботу комп'ютера, або програмного забезпечення, яке конфліктує зі сканером.

У розділі **Виключення в роботі** можна виключити файли й папки зі сканування. Виключення в роботі стають у пригоді для виключення зі сканування певних файлів для ігор, або коли сканування певних файлів спричиняє відхилення в роботі або продуктивності системи.

Виключення об'єктів виявлення дозволяє виключати об'єкти з виявлення об'єктів за їх іменем, шляхом і хешем. Виключення об'єктів виявлення не виключає файли й папки зі сканування, як виключення в роботі. Виключення об'єктів виявлення стосуються тільки виявлених ядром виявлення об'єктів, для яких є застосовуване правило в списку виключень.

Не слід плутати з іншими типами виключень:

- [Виключення процесу](#): усі операції з файлами, які відносяться до виключених програмних процесів, виключаються зі сканування (це може знадобитися для підвищення швидкості резервного копіювання або рівня доступності сервісу).
- [Виключені розширення файлів](#)
- [Виключення NIPS](#)
- [Фільтр виключень для хмарного захисту](#)

Виключення в роботі

У розділі "Виключення в роботі" можна виключити файли й папки зі сканування.

Щоб система сканувала всі об'єкти на наявність загроз, рекомендуємо створювати виключення в роботі лише за крайньої потреби. Проте існують ситуації, коли може виникнути потреба виключити об'єкт. Це, наприклад, можуть бути елементи великих баз даних, сканування яких значно сповільнить роботу комп'ютера, або програмне забезпечення, що конфліктує зі сканером.

Щоб виключити файли й папки зі сканування, додайте їх у список виключень: **Додаткові параметри (F5) > Ядро виявлення > Виключення > Виключення в роботі > Змінити**.

i Слід чітко розуміти значення параметрів [Виключення об'єктів виявлення](#), [Виключені розширення файлів](#), [Виключення NIPS](#) або [Виключення процесів](#).

Щоб [виключити об'єкт](#) (шлях до файлу або папки) зі сканування, клацніть **Додати** й уведіть відповідний шлях або виберіть його в структурі дерева.

Виключити шлях	Коментар
C:\Backup*	
C:\pagefile.sys	

i Загрозу у файлі не буде виявлено модулем **захисту файлової системи в режимі реального часу** або модулем **перевірки комп'ютера**, якщо файл відповідає критеріям виключення під час сканування.

Елементи керування

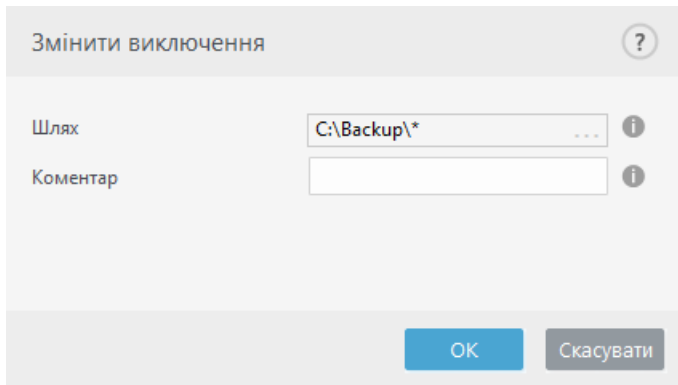
- **Додати:** виключити об'єкти з перевірки.
- **Редагувати:** редагувати вибрані елементи.
- **Видалити:** видаляє вибрані записи (щоб вибрати кілька записів, клацніть їх мишею, утримуючи клавішу CTRL).

Додавання або зміна виключення в роботі

У цьому діалоговому вікні можна виключити певний шлях (файл або каталог) для цього комп'ютера.

Виберіть шлях або введіть його вручну

- i** Щоб вибрати певний шлях, клацніть ... у полі **Шлях**.
Якщо ви вводите файл уручну, ознайомтеся з наведеними нижче прикладами [прикладями формату виключення](#).



Щоб виключити групу файлів, можна використовувати символи узагальнення. Знак запитання (?) позначає окремий символ, а зірочка (*) представляє рядок, який складається з нуля або більшої кількості символів.

Формат виключень

- Якщо необхідно виключити всі файли та підпапки в папці, введіть шлях до папки та скористайтесь маскою *
- Щоб виключити лише файли у форматі doc, скористайтесь маскою *.doc
- Якщо ім'я виконуваного файлу має певну кількість символів (і вони різняться), а точно відомий лише перший (наприклад, "D"), використовуйте такий формат:
D?????.exe (знаки запитання замінюють відсутні або невідомі символи)



Приклади

- C:\Tools* – для виключення папки та всього вмісту в ній (файлів і підпапок) шлях має закінчуватися зворотною скісною рисою (\) і зірочкою (*).
- C:\Tools*. * – те саме, що й з C:\Tools*
- C:\Tools: папку Tools не буде виключено. Для сканера Tools може бути іменем.
- C:\Tools*.dat: цей шлях дозволяє виключити всі файли .dat в папці Tools.
- C:\Tools\sg.dat: цей шлях дозволяє виключити лише конкретний указаний файл.

Системні змінні у виключеннях

Для визначення виключень зі сканування %PROGRAMFILES% можна використовувати системні змінні.

- Щоб виключити папку Program Files, використовуючи цю системну змінну, скористайтесь шляхом %PROGRAMFILES%* (обов'язково вкажіть зворотну скісну риску й зірочку в кінці шляху).
- Щоб виключити всі файли й папки в підкаталозі %PROGRAMFILES%, використовуйте шлях %PROGRAMFILES%\Excluded_Directory*

✓ [Розгорнути список підтримуваних системних змінних](#)

У шлях до виключень можна використовувати такі змінні:

- ✓ • %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

Системні змінні, визначені користувачем (наприклад, %TEMP% або %USERPROFILE%) та змінні оточення (наприклад, %PATH%) не підтримуються.

Символи узагальнення в середині шляху не підтримуються

! Символи узагальнювання в середині шляху (наприклад, C:\Tools*|Data\file.dat) можуть працювати, але офіційно не підтримуються у виключеннях. Щоб дізнатися більше, перегляньте цю [статтю бази знань](#).

Якщо використовується [виключення виявлених об'єктів](#), символи узагальнення можна використовувати в середині шляху без обмежень.

Порядок виключень

- Немає параметрів, які б дозволили змінити рівень пріоритету виключень за допомогою кнопок переходу у верхню або нижню частину вікна.
- ✓ • Коли сканер виявить відповідність до першого застосовного правила, друге застосовне правило не буде оцінюватися.
- Що менше правил, то вище швидкодія сканування.
- Не створюйте паралельні правила.

Формат виключення шляху

Щоб виключити групу файлів, можна використовувати символи узагальнення. Знак запитання (?) позначає окремий символ, а зірочка (*) представляє рядок, який складається з нуля або більшої кількості символів.

Формат виключень

- Якщо необхідно виключити всі файли та підпапки в папці, введіть шлях до папки та скористайтеся маскою *
- Щоб виключити лише файли у форматі doc, скористайтеся маскою *.doc
- Якщо ім'я виконуваного файлу має певну кількість символів (і вони різняться), а точно відомий лише перший (наприклад, "D"), використовуйте такий формат:
✓ *D?????.exe* (знаки запитання замінюють відсутні або невідомі символи)

Приклади

- *C:\Tools** – для виключення папки та всього вмісту в ній (файлів і підпапок) шлях має закінчуватися зворотною скісною рисою (\) і зірочкою (*).
- *C:\Tools*.** – те саме, що й з *C:\Tools**
- *C:\Tools:* папку *Tools* не буде виключено. Для сканера *Tools* може бути іменем.
- *C:\Tools*.dat:* цей шлях дозволяє виключити всі файли .dat в папці *Tools*.
- *C:\Tools\sg.dat:* цей шлях дозволяє виключити лише конкретний указаний файл.

Системні змінні у виключеннях

Для визначення виключень зі сканування %PROGRAMFILES% можна використовувати системні змінні.

- Щоб виключити папку Program Files, використовуючи цю системну змінну, скористайтеся шляхом %PROGRAMFILES%* (обов'язково вкажіть зворотну скісну риску й зірочку в кінці шляху).
- Щоб виключити всі файли й папки в підкаталозі %PROGRAMFILES%, використовуйте шлях %PROGRAMFILES%\Excluded_Directory*

✓ [Розгорнути список підтримуваних системних змінних](#)

У шлях до виключень можна використовувати такі змінні:

- ✓ • %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

Системні змінні, визначені користувачем (наприклад, %TEMP% або %USERPROFILE%) та змінні оточення (наприклад, %PATH%) не підтримуються.

Виключення об'єктів виявлення

У розділі "Виключення об'єктів виявлення" можна виключити об'єкти з виявлення об'єктів за допомогою фільтрації імен виявлених об'єктів, шляху до них або їх хешу.

Принцип роботи виключення об'єктів виявлення

Виключення об'єктів виявлення не виключає файли й папки зі сканування, як [виключення в роботі](#). Виключення об'єктів виявлення стосуються тільки виявлених ядром виявлення

✓ об'єктів, для яких є застосовуване правило в списку виключень.

У прикладі, який наведено в першому рядку, виявлено об'єкт Win32/Adware.Optmedia у файлі *C:\Recovery\file.exe*. У другому рядку є правило, згідно з яким кожен файл із відповідним хешем SHA-1 завжди буде виключати незалежно від імені виявленого об'єкта.

Виключення об'єктів виявлення

?

Q

Критерій об'єкта	Виключити виявлення	Коментар
C:\Recovery*.*	Win32/Advare.Optmedia	
678C1422DE867141B947EA700E8A2D6114AFAE97	Будь-який об'єкт виявлення	SuperApi.exe

Додати
Редагувати
Видалити
Імпортувати
Експортувати

ОК
Скасувати

Щоб система виявила всі загрози, рекомендується створювати виключення лише за необхідності.

Щоб додати файли й папки в список виключень, виберіть **Додаткові параметри (F5) > Ядро виявлення > Виключення > Виключення об'єктів виявлення > Змінити**.

i Слід чітко розуміти значення параметрів [Виключення в роботі](#), [Виключені розширення файлів](#), [Виключення NIPS](#) або [Виключення процесів](#).

Щоб [виключити об'єкт \(за іменем виявленого в ньому об'єкта або хеша\)](#) з ядра виявлення, клацніть **Додати**.

Нижче наведено способи створення виключення для [потенційно небажаних](#) і [потенційно небезпечних](#) програм за іменем виявленого об'єкта:

- У вікні сповіщень з інформацією про виявлений об'єкт клацніть **Показати додаткові параметри**, а потім виберіть пункт **Виключити виявлення**.
- У контекстному меню "Файли журналу" за допомогою [майстрі створення виключень виявлених об'єктів](#).
- Натисніть **Інструменти > Карантин**, натиснути правою кнопкою миші файл у карантині й вибрати в контекстному меню пункт **Відновити та виключити з перевірки**.

Критерій об'єкта виключення

- **Шлях:** обмежити виключення виявлених об'єктів для певного шляху.
- **Ім'я виявленого об'єкта:** якщо поруч із виключеним файлом указано ім'я [об'єкта виявлення](#), це означає, що файл виключений не цілком, а лише для відповідного об'єкта. Якщо цей файл пізніше буде інфіковано іншою шкідливою програмою, її буде виявлено.
- **Хеш:** дозволяє виключити файл у залежності від указанного хешу SHA-1 незалежно від

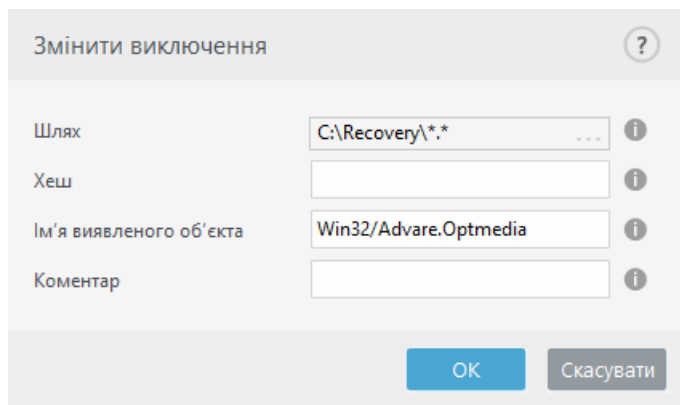
типу, розташування, імені або розширення файлу.

Додавання або зміна виключення об'єкта виявлення

Виключити виявлення

Потрібно вказати правильне ім'я виявленого об'єкта ESET. Правильне ім'я виявленого об'єкта див. в розділі [Файли журналу](#): у розкривному меню "Файли журналу" виберіть пункт **Виявлені об'єкти**. Це корисно, коли в ESET NOD32 Antivirus виявляються [помилкові зразки](#). Створювати виключення для реальних проникнень дуже небезпечно. Рекомендуємо виключати тільки певні файли або каталоги (клацніть ... у полі **Маска шляху** та (або) застосовуйте виключення лише на певний період часу. Виключення також застосовуються до [потенційно небажаних програм](#), потенційно небезпечних і підозрілих програм.

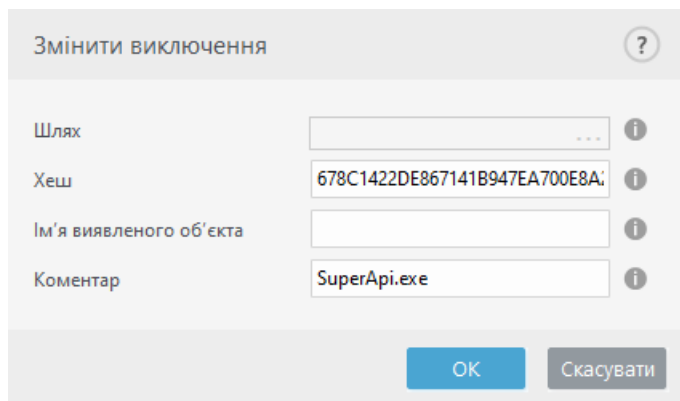
Див. також [Формат виключення шляху](#).



Див. пункт [Приклад виключень виявленого об'єкта](#).

Виключити хеш

Дозволяє виключити файл у залежності від вказаного хешу SHA-1 незалежно від типу, розташування, імені або розширення файлу.



Виключення за ім'ям об'єкта виключення

Щоб виключити певний об'єкт виключення за його ім'ям, уведіть його дійсне ім'я:
Win32/Adware.Optmedia

✓ Якщо для виявленого об'єкта виключення створюється у вікні сповіщень ESET NOD32 Antivirus, можна також використовувати такий формат:

@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt

@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan

@NAME=Win32/Bagle.D@TYPE=worm

Елементи керування

- **Додати:** виключити об'єкти з перевірки.
- **Редагувати:** редагувати вибрані елементи.
- **Видалити:** видаляє вибрані записи (щоб вибрати кілька записів, клацніть їх мишею, утримуючи клавішу CTRL).

Майстер створення виключень виявлених об'єктів

Виключення виявлених об'єктів також можна створити в контекстному меню [Файли журналу](#) (ця можливість недоступна для виявлених об'єктів шкідливого програмного забезпечення):

1. У [головному вікні програми](#) натисніть **Журнали > Файли журналу**.
2. Правою кнопкою миші клацніть виявлений об'єкт у **журналі виявлених об'єктів**.
3. Клацніть **Створити виключення**.

Щоб виключити один або кілька виявлених об'єктів, у розділі **Критерій виключення** клацніть **Змінити критерій**:

- **Точно вказані файли:** виключити кожен файл із певним хешем SHA-1.
- **Виявлений об'єкт:** виключити кожен файл за певним іменем виявленого об'єкта.
- **Шлях + виявлений об'єкт:** виключити кожен файл за певним іменем виявленого об'єкта й шляхом, у якому вказано ім'я файлу (наприклад, *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Рекомендований параметр попередньо вибраний за типом виявлення.

Перш ніж натиснути **Створити виключення**, можна додати **коментар**.

NOD32 ANTIVIRUS

—
□
×

Створити виключення
 ?

Не ініціювати виявлення для:
 Будь-які файли з шифруванням SHA-1: **00117F70C86ADB0F979021391A8AEAA497C2C8DF**

Критерій виключення

- ☒ **Точно вказані файли**
 Виключити кожен файл із певним хешем SHA-1
- ☐ **Виявлений об'єкт**
 Виключити кожен файл за певним іменем виявленого об'єкта
- ☐ **Шлях + виявлений об'єкт**
 Виключити кожен файл за певним іменем виявленого об'єкта й шляхом

Коментар (для всіх виключень)

Створити виключення

Скасувати

Виключення HIPS

Виключення дозволяють виключати процеси із системи глибокої перевірки поведінки HIPS.

Щоб змінити виключення HIPS, клацніть **Додаткові параметри (F5) > Ядро виявлення > HIPS > Базові > Виключення > Змінити**.

Слід чітко розуміти значення параметрів [Виключені розширення файлів](#), [Виключення об'єктів виявлення](#), [Виключення в роботі](#) або [Виключення процесів](#).

Щоб виключити об'єкт, клацніть **Додати** й уведіть шлях до об'єкта або виберіть його в структурі дерева. Окрім того, вибрані записи можна змінити або видалити.

Параметри ThreatSense

ThreatSense – це технологія, яка складається з багатьох комплексних методів виявлення загроз. Вона проактивна, тобто забезпечує захист навіть у перші години поширення нової загрози. У ній поєднуються різні методи (аналіз коду, емуляція коду, родові сигнатури, сигнатури вірусів), які працюють узгоджено, що суттєво підвищує рівень захисту системи. Підсистема сканування може контролювати одночасно кілька потоків даних, тим самим збільшуючи ефективність системи та швидкість виявлення загроз. Окрім того, технологія ThreatSense успішно знищує руткити.

У налаштуваннях підсистеми ThreatSense можна задати кілька параметрів сканування:

- типи й розширення файлів, які потрібно сканувати;
- комбінація різних методів виявлення;
- рівні очистки тощо.

Щоб відкрити вікно параметрів, натисніть **Параметри ThreatSense** у вікні додаткових параметрів будь-якого модуля, у якому використовується технологія ThreatSense (її описано нижче). Для різних сценаріїв інколи потрібно налаштувати індивідуальні конфігурації. Зважаючи на це, підсистему ThreatSense можна налаштовувати окремо для кожного з таких модулів захисту:

- Захист файлової системи в режимі реального часу
- Сканування в неактивному стані
- Сканування під час запуску
- Захист документів
- Захист поштового клієнта
- Захист доступу до Інтернету
- Сканування комп'ютера

Параметри ThreatSense оптимізовано для кожного модуля, тому їх змінення може суттєво вплинути на роботу системи. Наприклад, якщо ввімкнути обов'язкове сканування упакованих програм або розширену евристику для модуля захисту файлової системи в режимі реального часу, робота системи може значно сповільнитися (зазвичай такі методи використовуються лише для сканування щойно створених файлів). Не рекомендуємо змінювати параметри ThreatSense за замовчуванням для всіх модулів, окрім перевірки комп'ютера.

Перевірити об'єкти

У цьому розділі можна визначати компоненти комп'ютера та файли, які скануватимуться на наявність проникнень.

Оперативна пам'ять: сканування на предмет проникнень, орієнтованих на оперативну пам'ять комп'ютера.

Завантажувальні сектори/UEFI: сканування завантажувальних секторів на наявність шкідливого програмного забезпечення в головному завантажувальному записі. [Докладніше про UEFI див. в глосарії.](#)

Файли електронної пошти: програма підтримує такі розширення: DBX (Outlook Express) і EML.

Архіви: програма підтримує розширення ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UAE, WISE, ZIP, ACE та багато інших.

Саморозпакувальні архіви: ці архіви (SFX) можуть розпаковуватися самостійно.

Упаковані програми: після виконання ці програми (на відміну від стандартних типів архіву) розпаковуються в пам'яті. Окрім стандартних статичних пакувальників (UPX, yoda, ASPack, FSG та інших), сканер здатен розпізнати кілька додаткових типів пакувальників завдяки емуляції коду.

Опції сканування

Виберіть методи сканування системи на наявність проникнень. Доступні наведені нижче варіанти:

Евристика: алгоритм, який аналізує зловмисні дії програм. Основна перевага цієї технології – можливість виявляти шкідливе програмне забезпечення, яке не існувало під час формування попередньої версії обробника виявлення або не було в ній зареєстроване. Недолік – (дуже мала) імовірність помилкових сигналів.

Розширені евристики/DNA-підписи – у розширеній евристиці реалізовано унікальний евристичний алгоритм, розроблений компанією ESET, який оптимізовано для виявлення комп'ютерних черв'яків, троянських програм і написано мовами програмування високого рівня. Використання розширеної евристики значно розширює можливості продуктів ESET для виявлення загроз. Сигнатури – надійний засіб виявлення й визначення вірусів. Автоматична система оновлення дає змогу отримувати нові сигнатури протягом кількох годин із моменту виявлення загрози. Недолік використання сигнатур полягає в тому, що визначити можна лише відомі віруси (або їх дещо змінені версії).

Очистка

Параметри очистки визначають поведінку ESET NOD32 Antivirus під час очистки інфікованих об'єктів. Існує 4 рівні очистки.

Параметри ThreatSense дозволяють задати наведені нижче рівні виправлення (очищення).

Виправлення в ESET NOD32 Antivirus

Рівень очистки	Опис
Завжди виправляти виявлені об'єкти	Спробувати виправити виявлений об'єкт під час очищення об'єктів без втручання кінцевого користувача. У деяких випадках (наприклад, для системних файлів) виявлений об'єкт неможливо виправити, тому він залишатиметься у вихідному розташуванні.
Виправити виявлені об'єкти, якщо безпечно. В іншому разі залишити все як є	Спробувати виправити виявлений об'єкт під час очищення об'єктів без втручання кінцевого користувача. У деяких випадках (наприклад, системні файли або архіви з чистими та інфікованими файлами), якщо виявлений об'єкт не можна виправити, він залишається у вихідному розташуванні.
Виправити виявлені об'єкти, якщо безпечно. В іншому разі надіслати запит	Спробувати виправлення виявленого об'єкта під час очищення об'єктів. У деяких випадках, коли жодну операцію виконати неможливо, кінцевий користувач отримує інтерактивне сповіщення, де необхідно вибрати операцію виправлення (наприклад, видалити або пропустити). Цей параметр рекомендовано в більшості випадків.

Рівень очистки	Опис
Завжди запитувати кінцевого користувача	Під час очищення об'єктів для кінцевого користувача відкривається вікно, у якому необхідно вибрати операцію виправлення (наприклад, видалити або пропустити). Цей рівень призначений для більш досвідчених користувачів, які знають, що потрібно зробити у випадку виявлення.

Виключення

Розширення – це частина імені файлу, відокремлена крапкою. Розширення визначає тип і вміст файлу. Цей розділ налаштування параметрів підсистеми ThreatSense дає змогу визначити типи файлів, які потрібно сканувати.

Інше

Під час налаштування параметрів підсистеми ThreatSense для сканування комп'ютера за вимогою доступні також наведені нижче опції розділу **Інше**.

Перевіряти альтернативні потоки даних (ADS) – файлова система NTFS використовує альтернативні потоки даних, тобто асоціації файлів і папок, невидимі в разі застосування звичайних методів перевірки. Багато загроз намагаються обійти виявлення, маскуючись як альтернативні потоки даних.

Запускати фонові перевірки з низьким пріоритетом: на кожну процедуру сканування витрачається певний обсяг ресурсів системи. Якщо запущено програму, яка спричиняє значне використання ресурсів системи, можна активувати фонову перевірку з низьким пріоритетом і зберегти ресурси для програм.

Реєструвати всі об'єкти: у [журналі сканування](#) будуть відображені всі файли, проскановані в саморозпакувальних архівах, навіть неінфіковані (можуть генеруватися великі об'єми даних, що збільшуватиме розмір файлу журналу).

Увімкнути Smart-оптимізацію: коли Smart-оптимізацію увімкнено, система використовує оптимальні параметри для забезпечення найефективнішого рівня сканування, одночасно підтримуючи найвищу швидкість цього процесу. Різноманітні модулі захисту виконують інтелектуальне сканування, використовуючи різні методи й застосовуючи їх до відповідних типів файлів. Якщо Smart-оптимізацію вимкнено, під час сканування застосовуються лише визначені користувачем у ядрі ThreatSense параметри для певних модулів.

Зберегти час останнього доступу: установіть цей прапорець, щоб зберігати початковий час доступу до сканованих файлів, а не оновлювати їх (наприклад, якщо цього потребує робота систем резервного копіювання даних).

Обмеження

У розділі "Обмеження" можна вказати максимальний розмір об'єктів і число рівнів вкладених архівів, які необхідно сканувати.

Параметри об'єкта

Максимальний розмір об'єкта: визначає максимальний розмір об'єктів, які потрібно сканувати. Після встановлення цього параметра відповідний антивірусний модуль скануватиме лише об'єкти, розмір яких не перевищуватиме зазначений. Цей параметр рекомендується змінювати тільки досвідченим користувачам, у яких може виникнути потреба виключити з перевірки великі об'єкти. Значення за замовчуванням: необмежено.

Максимальний час перевірки об'єкта (с): визначає максимальний час перевірки файлів у контейнері (наприклад, архіві RAR/ZIP або електронному листі з кількома вкладеннями). Не застосовується для окремих файлів. Якщо в поле введено користувацьке значення, після завершення часу перевірка завершиться за найближчої можливості, навіть якщо в контейнері залишаться неперевірені файли.

Якщо в архіві містяться великі файли, перевірка завершиться лише після того, як з архіву буде видобуто файл (наприклад, якщо користувач указав 3 секунди, а на видобування потрібно щонайменше 5 секунд). Інші файли в архіві не будуть перевірятися після завершення вказаного часу.

Щоб обмежити час перевірки, зокрема для великих архівів, скористайтеся параметрами

Максимальний розмір об'єкта й **Максимальний розмір файлу в архіві** (не рекомендується через ризики для безпеки).

Значення за замовчуванням: необмежено.

Параметри перевірки архівів

Глибина архіву: визначає максимальну глибину сканування архіву. За замовчуванням використовується файл: 10.

Максимальний розмір файлу в архіві: за допомогою цього параметра можна вказати максимальний розмір для файлів, що містяться в архівах (у видобутому стані), які потрібно просканувати. Максимальне значення **3 ГБ**.



Змінювати значення за замовчуванням не рекомендується, оскільки за нормальних обставин для цього немає причин.

Список розширень файлів, виключених із перевірки

Виключені розширення файлів є частиною [параметрів ThreatSense](#). Щоб налаштувати виключені розширення файлів, клацніть **параметри ThreatSense** у вікні "Додаткові параметри" для будь-якого [модуля, що використовує технологію ThreatSense](#).

Розширення – це частина імені файлу, відокремлена крапкою. Розширення визначає тип і вміст файлу. Цей розділ налаштування параметрів підсистеми ThreatSense дає змогу визначити типи файлів, які потрібно сканувати.



Слід чітко розуміти значення параметрів [Виключення процесів](#), [Виключення HIPS](#) та [Виключення папки \(файлу\)](#).

За замовчуванням скануються всі файли. Будь-яке розширення можна додати до списку

файлів, виключених із перевірки.

Іноді доцільно виключити з перевірки певні типи файлів, якщо сканування таких файлів заважає належній роботі відповідних програм. Наприклад, рекомендується виключати файли з розширеннями `.edb`, `.eml` і `.tmp` в разі використання серверів Microsoft Exchange.

✓ Щоб додати до списку нове розширення, натисніть кнопку **Додати**. Уведіть розширення в пусте поле (наприклад, `tmp`) та натисніть кнопку **ОК**. Якщо вибрати параметр **Введіть кілька значень**, можна додати декілька розширень файлів, розділяючи їх рисками, комами або крапкою з комою. Наприклад, у розкритому меню виберіть **Крапка з комою** для розділового знаку та введіть `edb;eml;tmp`. Можна використовувати спеціальний символ `?` (знак питання). Він позначає будь-який символ (наприклад, `?db`).

i Щоб дізнатися точне розширення (якщо є) файлу в ОС Windows, відкрийте сторінку **Панель керування**, виберіть **Параметри папки** та перейдіть на вкладку **Вигляд**. Після цього зніміть прапорець **Приховувати розширення для зареєстрованих типів файлів**.

Додаткові параметри ThreatSense

Щоб змінити ці параметри, виберіть **Додаткові параметри (F5) > Ядро виявлення > Захист файлової системи в режимі реального часу > Додаткові параметри ThreatSense**.

Додаткові параметри ThreatSense для нових і змінених файлів

Імовірність виявити інфікування в новостворених або змінених файлах порівняно вища, ніж у наявних. Саме тому програма перевіряє ці файли за допомогою додаткових параметрів сканування. У ESET NOD32 Antivirus використовуються розширені евристики, які дають змогу виявляти нові загрози до оновлення ядра виявлення, у поєднанні з методами сканування на основі сигнатур вірусів.

Окрім новостворених файлів, сканування також поширюється на **саморозпакувальні архіви** (`.sfh`) і **упаковані програми** (запаковані виконувані файли). За замовчуванням архіви перевіряються до 10-го рівня вкладення, причому сканування виконується незалежно від їхнього фактичного розміру. Щоб змінити параметри сканування архіву, зніміть прапорець **Параметри сканування архівів за замовчуванням**.


Додаткові параметри ThreatSense для виконуваних файлів


Розширена евристика під час запуску файлу – за замовчуванням [розширена евристика](#) використовується під час запуску файлів. Коли цей параметр увімкнено, наполегливо рекомендуємо також активувати [Smart-оптимізацію](#) й [ESET LiveGrid®](#), щоб запобігти зниженню продуктивності системи.

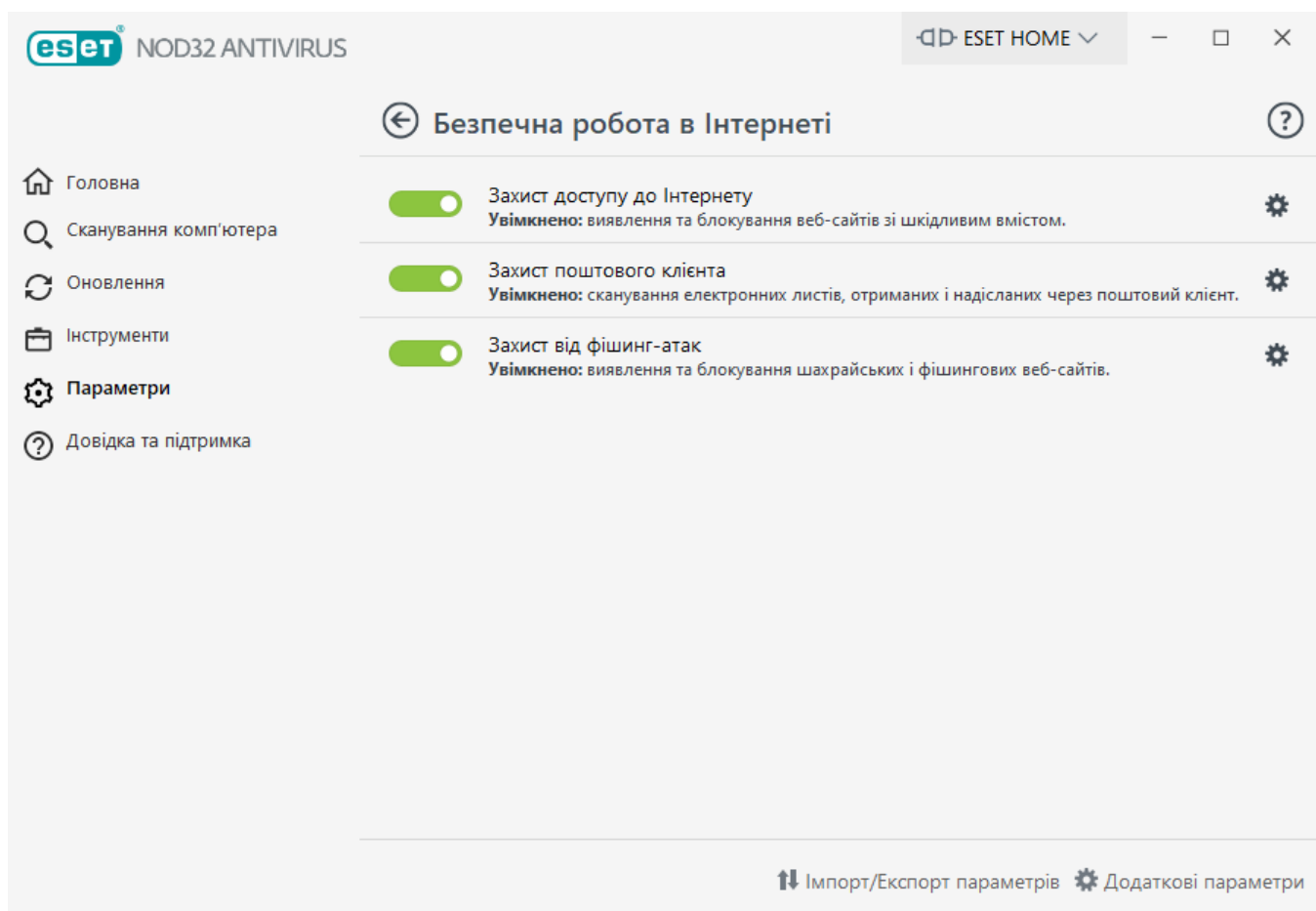
Розширена евристика під час запуску файлів зі змінного носія – розширена евристика емулює код у віртуальному середовищі й оцінює його поведінку, перш ніж дозволити запускати код зі змінного носія.


Безпечна робота в Інтернеті

Щоб налаштувати функцію захисту "Інтернет і електронна пошта", у вікні **Параметри** клацніть **Безпечна робота в Інтернеті**. З цього вікна можна отримати доступ до додаткових параметрів програми.

Щоб призупинити або вимкнути певні модулі захисту, клацніть піктограму повзунка .

 Вимкнення модулів захисту може зменшити рівень захисту комп'ютера.



Клацніть піктограму шестерні , щоб відкрити налаштування для інтернету/електронної пошти/захисту від фішинг-атак у вікні додаткових параметрів.

Підключення до Інтернету – це стандартна функція персонального комп'ютера. На жаль, Інтернет став основним засобом для передачі шкідливого коду. Тому [Захист доступу до Інтернету](#) – це одна з функцій, якій слід приділяти особливу увагу.

[Захист поштового клієнта](#) забезпечує керування поштовими комунікаціями через протоколи POP3(S) та IMAP(S). За допомогою модуля plug-in для поштового клієнта ESET NOD32 Antivirus забезпечує керування поштовими комунікаціями.

[Захист від фішинг-атак](#) дає змогу блокувати веб-сторінки, про які відомо, що вони поширюють фішинговий вміст. Настійно рекомендується залишити модуль захисту від фішинг-атак увімкненим.

Фільтрація протоколів

Антивірусний захист для протоколів програм забезпечується ядром сканування ThreatSense, у яке повністю інтегровано всі вдосконалені методики виявлення шкідливих програм. Фільтрація протоколів здійснюється автоматично, незалежно від використовуваного веб-браузера або клієнта електронної пошти. Щоб змінити параметри зашифрованого підключення (SSL/TLS), виберіть **Додаткові параметри (F5) > Інтернет і електронна пошта > [SSL/TLS](#)**.

Увімкнути фільтрацію вмісту протоколів програм: може використовуватися для вимкнення фільтрації протоколів. Зверніть увагу, що робота багатьох модулів програми ESET NOD32 Antivirus (захист доступу до Інтернету, захист протоколів електронної пошти, захист від фішингу, батьківський контроль) неможлива без цього компонента.

Виключені програми: дає змогу виключати певні програми з фільтрації протоколів. Цей параметр доцільно використовувати в разі виникнення проблем із сумісністю, пов'язаних із фільтрацією протоколів.

Виключені IP-адреси: дає змогу виключати певні віддалені адреси з фільтрації протоколів. Цей параметр доцільно використовувати в разі виникнення проблем із сумісністю, пов'язаних із фільтрацією протоколів.

Додає (наприклад, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Підмережа – підмережа (група комп'ютерів), визначена IP-адресою та маскою (наприклад, *2002:c0a8:6301:1::1/64*).

Приклад виключених IP-адрес

Адреса IPv4 та маска:

- *192.168.0.10* – додайте IP-адресу окремого комп'ютера, до якого має застосовуватися правило.
- *192.168.0.1–192.168.0.99* - введіть першу й останню IP-адреси, щоб визначити діапазон (для кількох комп'ютерів), до якого має застосовуватися правило.
- ✓ Підмережа (група комп'ютерів), визначена IP-адресою та маскою. Наприклад, *255.255.255.0* – це маска мережі для префіксу *192.168.1.0/24*, що позначає діапазон адрес від *192.168.1.1* до *192.168.1.254*.

Адреса IPv6 і маска:

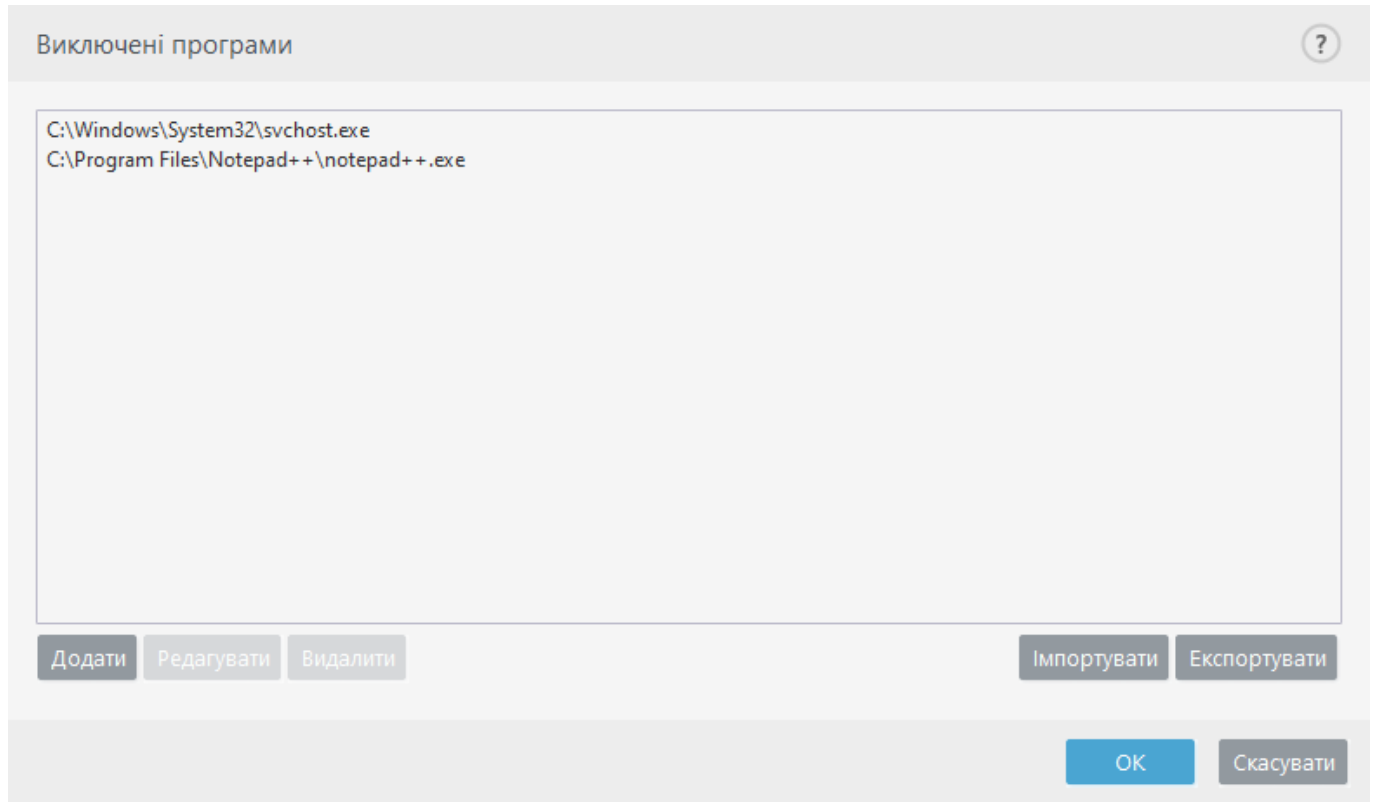
- *2001:718:1c01:16:214:22ff:fec9:ca5* – додайте адресу IPv6 окремого комп'ютера, до якого має застосовуватися правило.
- *2002:c0a8:6301:1::1/64* – адреса IPv6 із префіксом довжиною 64 біти, що означає від *2002:c0a8:6301:0001:0000:0000:0000:0000* до *2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

Виключені програми

Щоб виключити певні мережеві програми зі сфери охоплення фільтра вмісту, виберіть їх у списку. Підключення HTTP/POP3/IMAP, які встановлюватимуться за участю вибраних програм, не перевірятимуться на наявність загроз. Рекомендуємо використовувати цей параметр лише в тих випадках, коли перевірка встановлюваних підключень порушує нормальну роботу програми.

Запущені програми та служби відображатимуться в цьому списку автоматично. Натисніть

Додати, щоб додати програму вручну, якщо вона не відображається у списку фільтрування протоколу.



Виключені IP-адреси

До адрес у цьому списку не застосовується функція фільтрації вмісту протоколу. Підключення HTTP/POP3/IMAP, які встановлюватимуться за участю вказаних адрес, не перевірятимуться на наявність загроз. Рекомендується використовувати цей параметр лише для довірених адрес.

Натисніть **Додати**, щоб виключити IP-адресу/діапазон адрес/підмережу віддаленої точки, що не відображається у списку фільтрації протоколів.

Клацніть **Видалити**, щоб видалити вибрані записи зі списку.

Виключені IP-адреси?

10.1.2.3
10.2.1.1-10.2.1.10
192.168.1.0/255.255.255.0
fe80::b434:b801:e878:5975
2001:21:420::/64

ДодатиРедагуватиВидалитиІмпортуватиЕкспортувати

ОКСкасувати

Додати адресу IPv4

Додавання адреси, діапазону адрес або підмережі IP віддаленої точки, до якої має застосовуватися правило. Протокол IP версії 4 – стара, проте й досі найпоширеніша версія.

Одна адреса – додайте IP-адресу окремого комп'ютера, до якого має застосовуватися правило (наприклад, *192.168.0.10*).

Діапазон адрес – введіть першу й останню IP-адреси, щоб визначити діапазон (для кількох комп'ютерів), до якого має застосовуватися правило (наприклад, *192.168.0.1–192.168.0.99*).

Підмережа – підмережа (група комп'ютерів), визначена IP-адресою та маскою.

Наприклад, *255.255.255.0* – це маска мережі для префіксу *192.168.1.0/24*, що позначає діапазон адрес від *192.168.1.1* до *192.168.1.254*.

Додати адресу IPv6

Додавання адреси чи підмережі IPv6 віддаленої точки, до якої має застосовуватися правило. Це найновіша версія протоколу Інтернету, яка замінить стару версію 4.

Одна адреса – додайте IP-адресу окремого комп'ютера, до якого має застосовуватися правило (наприклад, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Підмережа – підмережа (група комп'ютерів), визначена IP-адресою та маскою (наприклад, *2002:c0a8:6301:1::1/64*).

SSL/TLS

Програма ESET NOD32 Antivirus здатна перевіряти наявність загроз зв'язки, у яких використовується протокол SSL. Можна використовувати різні режими фільтрації для перевірки захищених SSL-зв'язків, коли застосовуються довірені сертифікати, невідомі сертифікати або сертифікати, виключені з перевірки захищених SSL-зв'язків.

Увімкнути фільтрацію протоколу SSL/TLS – якщо фільтрацію протоколу вимкнено, програма не скануватиме SSL-зв'язки.

для параметра **Режим фільтрації протоколу SSL/TLS** доступні наведені нижче опції.

Режим фільтрації	Опис
Автоматичний режим	Режим за замовчуванням, у якому скануються лише відповідні програми, зокрема веб-браузери та поштові клієнти. Його можна обійти, вибравши програми, чиї зв'язки потрібно сканувати.
Інтерактивний режим	Якщо ввести адресу веб-сайту із захистом SSL (з невідомим сертифікатом), з'явиться діалогове вікно вибору дії . У цьому режимі можна створити список сертифікатів SSL або програм, які не перевірятимуться.
Режим політики	Виберіть цей параметр, щоб сканувати всі захищені SSL-зв'язки, окрім тих, які захищено виключеними з перевірки сертифікатами. Якщо встановлюється новий зв'язок із використанням невідомого підписаного сертифіката, вас не буде сповіщено про це й зв'язок буде автоматично відфільтровано. Якщо сервер має недовірений сертифікат, позначений як довірений (доданий до списку довірених), зв'язок із сервером буде дозволено, а вміст каналу зв'язку відфільтровуватиметься.

Список програм, до яких застосовуються фільтри SSL/TLS: дає змогу коригувати поведінку ESET NOD32 Antivirus відносно окремих програм.

Список відомих сертифікатів – також дає змогу коригувати поведінку програми ESET NOD32 Antivirus відносно окремих сертифікатів SSL.

Виключити зв'язок із довіреними доменами: якщо увімкнено цей параметр, обмін даними між довіреними доменами не буде перевірятись. Довірені домени визначаються вбудованим білим списком.

Блокувати зашифрований зв'язок, що використовує застарілий протокол SSL v2: автоматично блокує зв'язки, для встановлення яких використовується попередня версія протоколу SSL.

Кореневий сертифікат

Додати кореневий сертифікат до відомих браузерів – для належного функціонування зв'язків за протоколом SSL у браузерах і клієнтах електронної пошти важливо, щоб до списку відомих корневих сертифікатів (видавців) було додано кореневий сертифікат для ESET. Якщо цей параметр увімкнено, ESET NOD32 Antivirus автоматично додасть сертифікат ESET SSL Filter CA до відомих браузерів (наприклад, Opera). Для браузерів, які використовують системне сховище сертифікатів, він додається автоматично. Наприклад, Firefox автоматично налаштовано на

довіру кореневим центрам у системному сховищі сертифікатів.

Щоб застосувати сертифікат до непідтримуваних браузерів, виберіть **Переглянути сертифікат > Відомості > Копіювати у файл...**, після чого вручну імпортуйте його до браузера.

Дійсність сертифікатів

Якщо сертифікат не вдається перевірити (інколи сертифікат не можна перевірити за допомогою сховища довірених корневих сертифікатів (TRCA). Це означає, що сертифікат підписаний певною особою (наприклад, адміністратором веб-сервера чи невеликої компанії), тому вважати його довіреним не завжди ризиковано. Більшість великих комерційних організацій (наприклад, банки) використовують сертифікати, підписані TRCA. Якщо прапорець **Запитувати про дійсність сертифіката** встановлено (за замовчуванням), користувач побачить запит на вибір дії, яку потрібно виконати в разі встановлення зашифрованого зв'язку. Можна встановити прапорець **Блокувати зв'язок, який використовує сертифікат**, щоб завжди переривати зашифровані підключення до сайтів, які використовують неперевірені сертифікати.

Якщо сертифікат пошкоджено, це означає, що його неправильно підписано або пошкоджено. У такому випадку ESET не рекомендує знімати прапорець **Блокувати зв'язок, який використовує сертифікат**. Якщо вибрано параметр **Запитувати про дійсність сертифіката**, користувачу буде запропоновано вибрати дію для виконання в разі утворення зашифрованого з'єднання.

Ілюстровані приклади

Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:

- і • [Сповіщення про сертифікати в домашніх версіях продуктів ESET для Windows](#)
- [«Зашифрований мережевий трафік: недовірений сертифікат» відображається під час відвідування веб-сторінок](#)

Сертифікати

Для належного функціонування зв'язків за протоколом SSL у браузерах і клієнтах електронної пошти важливо, щоб до списку відомих корневих сертифікатів (видавців) було додано кореневий сертифікат для ESET. Параметр **Додати кореневий сертифікат до відомих браузерів** має бути ввімкнено. Установіть цей прапорець, щоб автоматично додати кореневий сертифікат ESET до відомих браузерів (наприклад, Opera і Firefox). Для браузерів, які використовують системне сховище сертифікатів, сертифікат додається автоматично (наприклад, до Internet Explorer). Щоб застосувати сертифікат до непідтримуваних браузерів, виберіть **Переглянути сертифікат > Відомості > Копіювати в файл**, після чого вручну імпортуйте його до браузера.

У деяких випадках сертифікат неможливо перевірити за допомогою сховища довірених корневих сертифікатів (наприклад, VeriSign). Це означає, що сертифікат самостійно підписаний певною особою (наприклад, адміністратором веб-сервера або невеликої компанії), тому вважати його довіреним не завжди небезпечно. Більшість великих комерційних організацій (наприклад, банки) використовують сертифікати, підписані TRCA.

Якщо прапорець **Запитувати про дійсність сертифіката** встановлено (за замовчуванням),

користувач побачить запит на вибір дії, яку потрібно виконати в разі встановлення зашифрованого зв'язку. З'явиться діалогове вікно вибору дії, у якому можна позначити сертифікат як довірений або виключений. Якщо сертифіката немає у списку TRCA, вікно відображається червоним. Якщо сертифікат зазначено у списку TRCA, вікно відображається зеленим.

Можна встановити прапорець **Блокувати зв'язок, який використовує сертифікат**, щоб завжди переривати зашифровані підключення до сайту, який використовує неперевірений сертифікат.

Якщо сертифікат недійсний або пошкоджений, це означає, що термін його дії минув або його неправильно підписано. У такому випадку рекомендується блокувати зв'язок, що використовує такий сертифікат.

Зашифрований мережевий трафік

Якщо систему налаштовано на використання сканування трафіку за SSL-протоколом, у двох наведених нижче ситуаціях відображатиметься діалогове вікно з пропозицією вибрати дію.

Перша: якщо веб-сайт використовує недійсний сертифікат або такий, що не можна перевірити, і програму ESET NOD32 Antivirus налаштовано запитувати вказівки користувача (за замовчуванням "Так" — для сертифікатів, які не вдається перевірити, а "Ні" — для недійсних), відображатиметься діалогове вікно із запитом про дію, яку потрібно застосувати до відповідного підключення (**Заблокувати** чи **Дозволити**). Якщо сертифікат не знайдено в Trusted Root Certification Authorities store (TRCA), він вважається недовіреним.

Друга: якщо для параметра **Режим фільтрації протоколу SSL** встановлено значення **Інтерактивний режим**, для кожного веб-сайту відображатиметься діалогове вікно із запитом про дію, яку потрібно застосувати до трафіку (**Сканувати** чи **Ігнорувати**). Деякі програми перевіряють, чи не зазнавав змін або перевірок оброблюваний ними SSL-трафік. У такому разі ESET NOD32 Antivirus має **ігнорувати** трафік, щоб забезпечити роботу цих програм.

Ілюстровані приклади

Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:

- і • [Сповіщення про сертифікати в домашніх версіях продуктів ESET для Windows](#)
- [«Зашифрований мережевий трафік: недовірений сертифікат» відображається під час відвідування веб-сторінок](#)

В обох випадках користувач може зафіксувати вибрану ним дію. Збережені дії можна знайти в розділі [Список відомих сертифікатів](#).

Список відомих сертифікатів

Список відомих сертифікатів можна використовувати для коригування поведінки ESET NOD32 Antivirus стосовно певних сертифікатів SSL, а також для запам'ятовування вибраних дій, коли в розділі **Режим фільтрації протоколу SSL/TLS** вибрано параметр **Інтерактивний режим**. Список можна переглянути й відредагувати в меню **Додаткові параметри (F5) > Інтернет і електронна пошта > SSL/TLS > Список відомих сертифікатів**.

Вікно **Список відомих сертифікатів** складається з наведених нижче елементів.

Стовпці

Ім'я: ім'я сертифіката.

Видавець сертифіката: ім'я автора сертифіката.

Предмет сертифіката: тема, пов'язана з відкритим ключем, указаним у відповідному полі.

Доступ: виберіть значення **Дозволити** або **Заблокувати** для параметра **Доступ**, щоб дозволити чи заблокувати зв'язок, захищений відповідним сертифікатом незалежно від його надійності. Виберіть **Автоматично**, щоб програма дозволяла довірені сертифікати й запитувала про недовірені. Виберіть **Запитувати**, щоб система завжди зверталася за вказівками до користувача.

Перевірка: виберіть значення **Перевіряти** або **Ігнорувати** для параметра **Перевірка**, щоб перевіряти або ігнорувати зв'язок, захищений відповідним сертифікатом. Виберіть **Автоматично**, щоб в автоматичному режимі система виконувала перевірку, а в інтерактивному – зверталася за вказівками до користувача. Виберіть **Запитувати**, щоб система завжди зверталася за вказівками до користувача.

Елементи керування

Додати – додати сертифікат і налаштувати його відповідно до параметрів доступу та сканування.

Змінити: виберіть сертифікат, який потрібно налаштувати, і натисніть **Змінити**.

Видалити : виберіть потрібний сертифікат і натисніть **Видалити**.

ОК/Скасувати: натисніть **ОК**, щоб зберегти зміни, або виберіть **Скасувати**, щоб залишити налаштування без змін.

Список програм, до яких застосовуються фільтри SSL/TLS

Параметр **Список програм, до яких застосовуються фільтри SSL/TLS** можна використовувати, щоб налаштувати роботу ESET NOD32 Antivirus у певних програмах, а також зберегти вибрані дії, коли в розділі **Режим фільтрації протоколу SSL/TLS** активовано **Інтерактивний режим**. Щоб переглянути й відредагувати список, відкрийте меню **Додаткові параметри (F5) > Інтернет і електронна пошта > SSL/TLS > Список програм, до яких застосовуються фільтри SSL/TLS**.

Вікно **Список програм, до яких застосовуються фільтри SSL/TLS** складається з наведених нижче елементів.

Стовпці

Програма: виберіть виконуваний файл у дереві каталогів, натисніть кнопку ... або введіть шлях уручну.

Перевірка: виберіть **Перевіряти** чи **Ігнорувати**, щоб перевіряти або ігнорувати зв'язок. Виберіть **Автоматично**, щоб в автоматичному режимі система виконувала перевірку, а в інтерактивному – зверталася за вказівками до користувача. Виберіть **Запитувати**, щоб система завжди зверталася за вказівками до користувача.

Елементи керування

Додати: додати відфільтровані програми.

Змінити: виберіть програму, яку потрібно налаштувати, і натисніть **Змінити**.

Видалити: виберіть програму, яку потрібно видалити, і натисніть **Видалити**.

Імпорт/Експорт: імпорт програм із файлу або збереження поточного списку програм у файл.

ОК/Скасувати: натисніть **ОК**, щоб зберегти зміни, або виберіть **Скасувати**, щоб залишити налаштування без змін.

Захист поштового клієнта

Процедуру налаштування інтеграції див. в розділі [Інтеграція ESET NOD32 Antivirus із поштовим клієнтом](#).

Параметри поштового клієнта доступні в меню **Додаткові параметри (F5) > Інтернет і електронна пошта > Захист поштового клієнта > Поштові клієнти**.

Поштові клієнти

Увімкнути захист електронної пошти за допомогою плагінів клієнта: якщо цей параметр вимкнено, захист за допомогою плагінів клієнта не працює.

Електронні листи для сканування

Виберіть електронні листи для сканування:

- Отримані листи
- Відправлені листи
- Прочитані листи
- Змінений електронний лист



Рекомендуємо не вимикати параметр **Увімкнути захист електронної пошти за допомогою плагінів клієнта**. Навіть якщо інтеграцію вимкнено або вона не працює, поштовий зв'язок усе одно захищено функцією [фільтрації протоколу](#) (IMAP/IMAPS і POP3/POP3S).

Дія, що виконуватимуться інфікованими повідомленнями електронної пошти

Пропустити – програма виявлятиме інфіковані вкладення, але не застосовуватиме жодних дій до повідомлень електронної пошти.

Видалити лист: програма повідомлятиме користувачу про виявлені загрози й видалятиме повідомлення.

Перемістити лист до папки «Видалені»: інфіковані повідомлення буде автоматично переміщено до папки "Видалені".

Перемістити лист до папки (дія за замовчуванням): інфіковані повідомлення будуть автоматично переміщені до вказаної папки.

Папка: укажіть спеціальну папку, куди потрібно переміщувати інфіковані повідомлення електронної пошти.

Інтеграція з поштовими клієнтами

Інтеграція ESET NOD32 Antivirus з поштовими клієнтами підвищує рівень активного захисту від шкідливих кодів у повідомленнях електронної пошти. Якщо ваш поштовий клієнт підтримується, інтеграцію можна активувати за допомогою елементів керування ESET NOD32 Antivirus. Якщо інтеграцію ввімкнено, панель інструментів ESET NOD32 Antivirus вставляється безпосередньо в поштовий клієнт, що підвищує ефективність захисту електронної пошти. Параметри інтеграції доступні в меню **Додаткові параметри (F5) > Інтернет і електронна пошта > Захист поштового клієнта > Інтеграція з поштовими клієнтами**.

Наразі підтримуються такі поштові клієнти: [Microsoft Outlook](#), [Outlook Express](#), [Windows Mail](#) і Windows Live Mail. Захист електронної пошти працює як плагін для цих програм. Головна перевага компонента plug-in – незалежність від використовуваного протоколу. Коли клієнт електронної пошти отримує зашифроване повідомлення, воно розшифровується й передається на обробку до антивірусного сканера. Щоб отримати повний список підтримуваних поштових клієнтів і їхніх версій, див. відповідну [статтю бази знань ESET](#).

Якщо під час отримання електронних листів робота системи вповільнюється, вимкніть параметри **Оптимізація обробки вкладень** і **Оптимізація обробки вкладень**.

Панель інструментів Microsoft Outlook

Захист клієнта Microsoft Outlook забезпечується за допомогою модуля plug-in. Після інсталяції ESET NOD32 Antivirus панель інструментів, яка містить параметри захисту від вірусів/ додається до Microsoft Outlook:

ESET NOD32 Antivirus: двічі клацніть цю піктограму, щоб відкрити головне вікно ESET NOD32

Antivirus.

Повторне сканування повідомлень: дає змогу вручну запустити перевірку електронної пошти. Можна вказати повідомлення, які потрібно просканувати, а також активувати повторне сканування отриманої електронної пошти. Докладніше див. у розділі [Захист поштового клієнта](#).

Налаштування сканера: відображає параметри [захисту поштового клієнта](#).

Панель інструментів Outlook Express і Windows Mail

Модуль захисту для Outlook Express і Windows Mail працює як компонент plug-in. Після інсталяції ESET NOD32 Antivirus панель інструментів, яка містить параметри захисту від вірусів/ додається до Outlook Express або Windows Mail:

ESET NOD32 Antivirus: двічі клацніть цю піктограму, щоб відкрити головне вікно ESET NOD32 Antivirus.

Повторне сканування повідомлень: дає змогу вручну запустити перевірку електронної пошти. Можна вказати повідомлення, які потрібно просканувати, а також активувати повторне сканування отриманої електронної пошти. Докладніше див. у розділі [Захист поштового клієнта](#).

Налаштування сканера: відображає параметри [захисту поштового клієнта](#).

Інтерфейс користувача

Настройка вигляду: вигляд панелі інструментів для поштового клієнта можна змінити. Зніміть цей прапорець, щоб налаштувати вигляд незалежно від параметрів поштової програми.

Показувати текст: відображення опису піктограм.

Текст праворуч: переміщення опису параметрів з області під піктограмою в область праворуч від неї.

Великі піктограми: відображення великих піктограм для пунктів меню.

Діалогове вікно підтвердження

Це повідомлення використовується для того, щоб переконатися, що користувач дійсно бажає виконати вибрану дію, і уникнути можливих помилок.

З іншого боку, це вікно також пропонує можливість скасувати підтвердження.

Повторне сканування повідомлень

Панель інструментів ESET NOD32 Antivirus, інтегрована в поштовий клієнт, дає змогу користувачам вибрати кілька опцій сканування електронної пошти. Опція **Повторне сканування повідомлень** пропонує два режими сканування:

Усі повідомлення в поточній папці: сканування всіх повідомлень у поточній папці.

Тільки вибрані повідомлення: сканування лише тих повідомлень, які позначив користувач.

Установивши прапорець **Повторне сканування вже просканованих повідомлень**, користувач може повторно просканувати повідомлення, які вже сканувалися раніше.

Протоколи електронної пошти

IMAP і POP3 – це найпоширеніші протоколи, які використовуються для поштового зв'язку в програмах поштових клієнтів. IMAP (Internet Message Access Protocol – протокол доступу до електронної пошти) – інший інтернет-протокол для отримання доступу до електронної пошти. Протокол IMAP має певні переваги над POP3: кілька клієнтів можуть одночасно підключатися до однієї поштової скриньки, не змінюючи стан повідомлення (прочитане/непрочитане, з відповіддю/видалене). Модуль захисту, який забезпечує контроль цього типу, ініціюється автоматично під час запуску операційної системи й залишається активним у пам'яті.

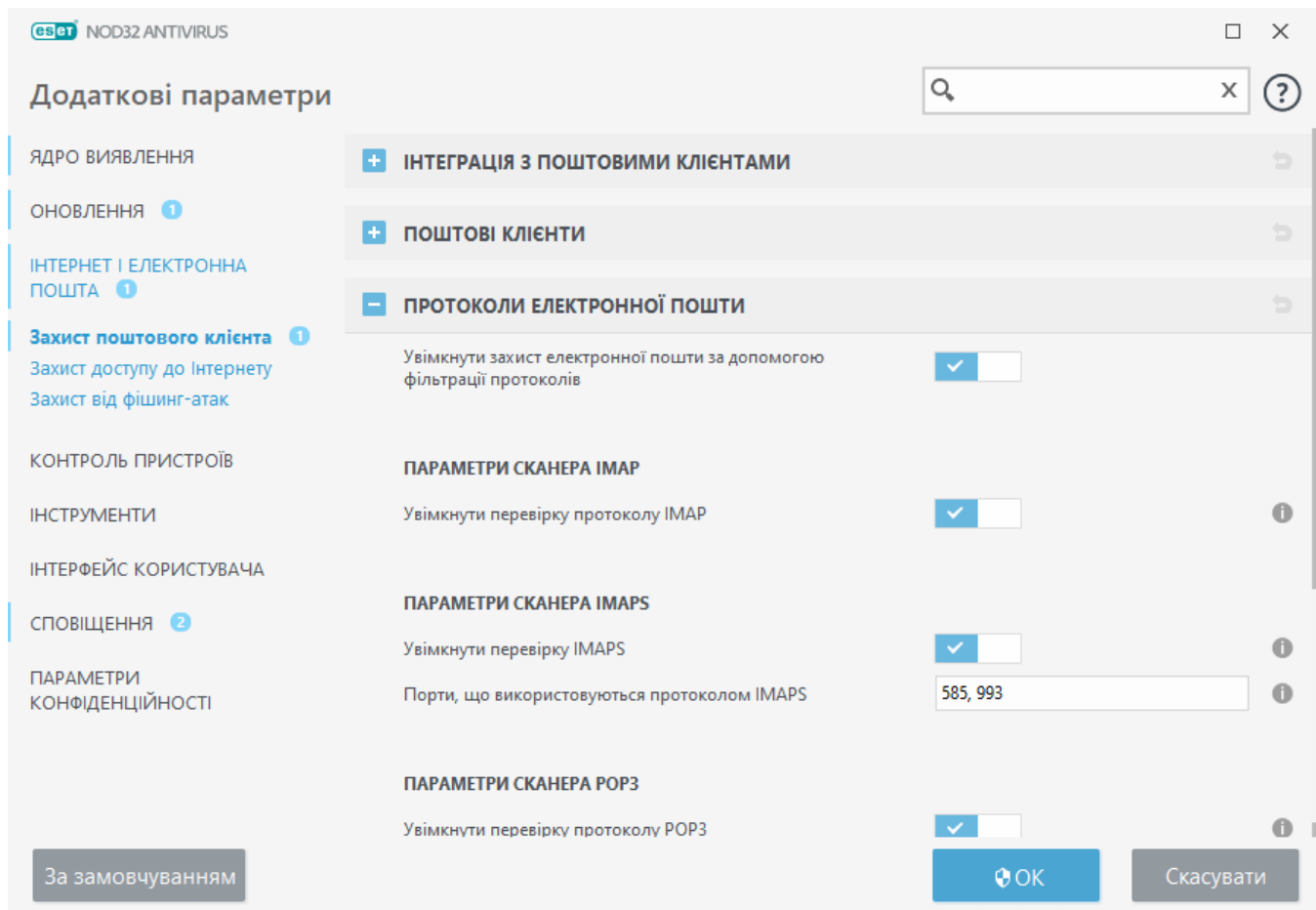
ESET NOD32 Antivirus забезпечує захист користувачів цього протоколу незалежно від їхнього поштового клієнта й без необхідності його повторного налаштування. За замовчуванням перевіряються всі операції обміну даними через протоколи POP3 й IMAP, незалежно від стандартних номерів портів POP3/IMAP.

Протокол IMAP не перевіряється. Проте обмін даними із сервером Microsoft Exchange може перевіряти [модуль інтеграції](#) з поштовими клієнтами, такими як Microsoft Outlook.

Рекомендуємо не вимикати параметр **Увімкнути захист електронної пошти за допомогою фільтрації протоколів**. Щоб налаштувати перевірку протоколів IMAP/IMAPS і POP3/POP3S, перейдіть у меню **Додаткові параметри > Інтернет і електронна пошта > Захист поштового клієнта > Протоколи електронної пошти**.

ESET NOD32 Antivirus також підтримує сканування протоколів IMAPS (585, 993) і POP3S (995), які використовують зашифрований канал для передачі інформації між сервером і клієнтом. ESET NOD32 Antivirus перевіряє комунікаційні зв'язки, що використовують протоколи SSL (Secure Socket Layer – рівень захищених сокетів) і TLS (Transport Layer Security – захист на транспортному рівні). Програма скануватиме лише трафік, який передається через **Порти, що використовуються протоколом IMAPS/POP3S**, незалежно від версії операційної системи. В разі необхідності можна додати інші комунікаційні порти. Якщо портів кілька, розділяйте їх номери комою.

Зашифровані зв'язки скануються за замовчуванням. Щоб переглянути налаштування сканера відкрийте розділ "Додаткові параметри" й виберіть пункти **Інтернет і електронна пошта > [SSL/TLS](#)**.



Фільтр POP3, POP3S

Протокол POP3 – це найпоширеніший протокол, який використовується для поштового зв'язку у програмах поштових клієнтів. ESET NOD32 Antivirus забезпечує захист користувачів цього протоколу незалежно від поштового клієнта, що використовується.

Модуль захисту, який забезпечує контроль цього типу, ініціюється автоматично під час запуску операційної системи й залишається активним у пам'яті. Перевірка протоколу POP3 виконується автоматично без повторного налаштування поштового клієнта. За замовчуванням перевіряється зв'язок через порт 110, але в разі необхідності можна додати інші комунікаційні порти. Якщо портів кілька, розділяйте їх номери комою.

Зашифровані зв'язки скануються за замовчуванням. Щоб переглянути налаштування сканера відкрийте розділ "Додаткові параметри" й виберіть пункти **Інтернет і електронна пошта** > [SSL/TLS](#).

У цьому розділі можна налаштувати параметри перевірки протоколів POP3 і POP3S.

Увімкнути перевірку протоколу POP3 – якщо прапорець встановлено, увесь трафік через протокол POP3 перевіряється на наявність шкідливого програмного забезпечення.

Порти, використовувані протоколом POP3 – список портів, використовуваних протоколом POP3 (за замовчуванням – 110).

ESET NOD32 Antivirus також підтримує перевірку протоколу POP3S. У разі використання цього типу зв'язку для передавання інформації між сервером і клієнтом використовується зашифрований

канал. ESET NOD32 Antivirus перевіряє зв'язки, для яких використовується шифрування за протоколами SSL (Secure Socket Layer – безпечний рівень сокета) і TLS (Transport Layer Security – захист транспортного рівня).

Не використовувати перевірку POP3S – зашифровані зв'язки не будуть перевірятися.

Використовувати перевірку протоколу POP3S для вибраних портів – виберіть цю опцію, щоб увімкнути перевірку POP3S лише для портів, зазначених у списку **Порти, використовувані протоколом POP3S**.

Порти, використовувані протоколом POP3S – список портів POP3S, які необхідно перевіряти (за замовчуванням – 995).

Теги електронної пошти

Параметри цієї функції доступні в меню **Додаткові параметри > Інтернет і електронна пошта > Захист поштового клієнта > Сигнали та сповіщення**.

Після завершення перевірки електронної пошти сповіщення з результатом сканування може бути додано до повідомлення. Можна вибрати параметр **Додавати повідомлення-ознаки до отриманої чи прочитаної пошти** або **Додавати повідомлення-ознаки до надісланої пошти**. Пам'ятайте, що іноді повідомлення-ознаки можуть опускатися в проблемних HTML-повідомленнях або підроблятися шкідливим ПЗ. Повідомлення-ознаки можуть додаватися до прочитаних вхідних повідомлень електронної пошти та до надісланих листів. Доступні наведені нижче варіанти:

- **Ніколи** – повідомлення-ознаки не додаватимуться.
- **Коли виявлено певний об'єкт** – як перевірені позначатимуться лише повідомлення, що містять шкідливе програмне забезпечення (за замовчуванням).
- **До всіх перевірених електронних листів** – програма додаватиме повідомлення до всієї перевіреної електронної пошти.

Текст, що додається до тем виявлених електронних листів – відредагуйте цей шаблон, якщо потрібно змінити формат префіксу теми інфікованої електронної пошти. Ця функція змінюватиме тему повідомлення "Вітаємо!" на такий формат: "виявлений об'єкт [%DETECTIONNAME%] Вітаємо!". Змінна %DETECTIONNAME% вказує на виявлений об'єкт.

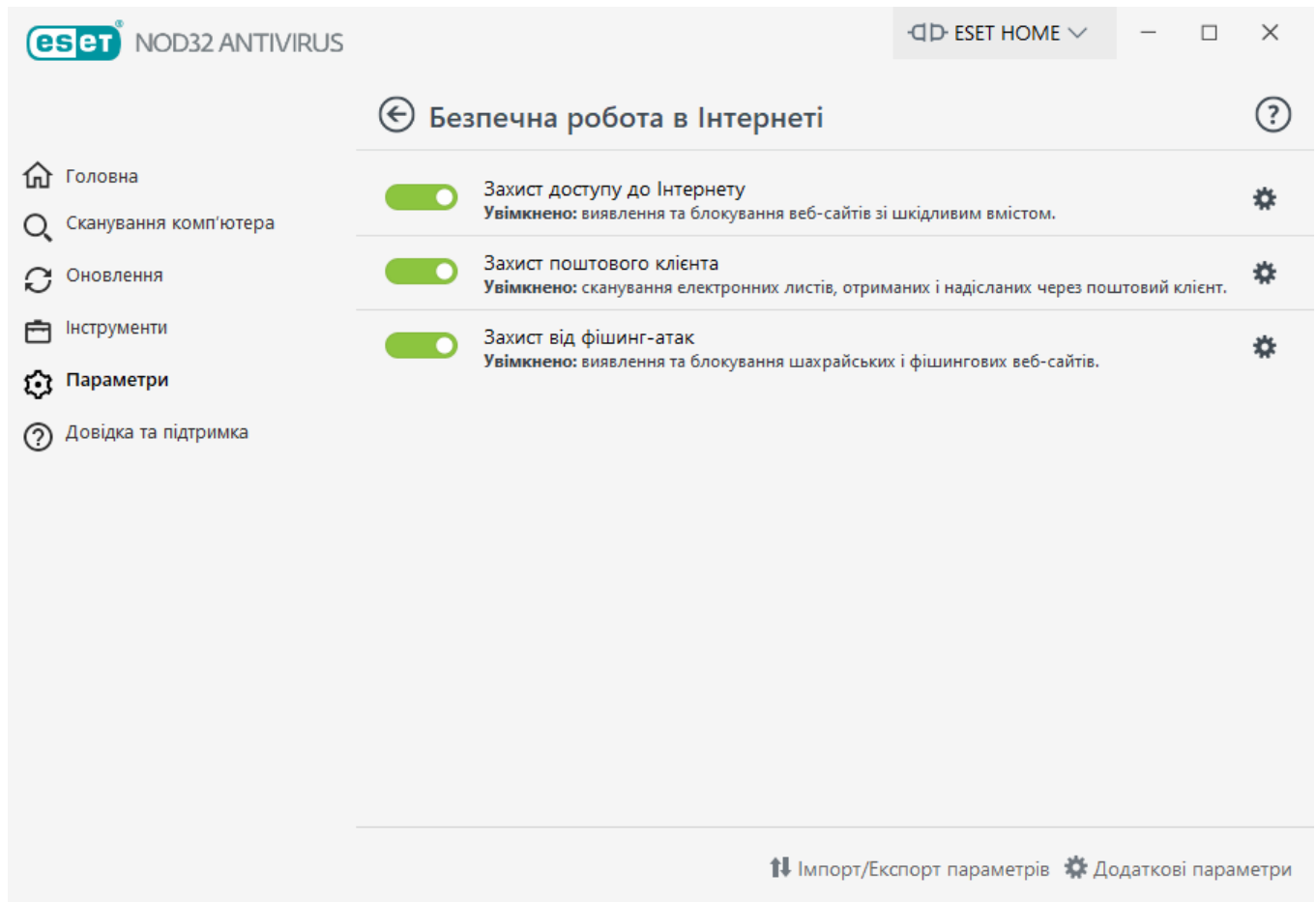
Захист доступу до Інтернету

Підключення до Інтернету – це стандартна функція персонального комп'ютера. На жаль, саме вона стала основним засобом для передачі шкідливого коду. Захист доступу до Інтернету здійснюється за допомогою контролю зв'язків між веб-браузерами й віддаленими серверами відповідно до правил протоколів HTTP (протокол передавання гіпертексту) і HTTPS (зашифрований HTTP).

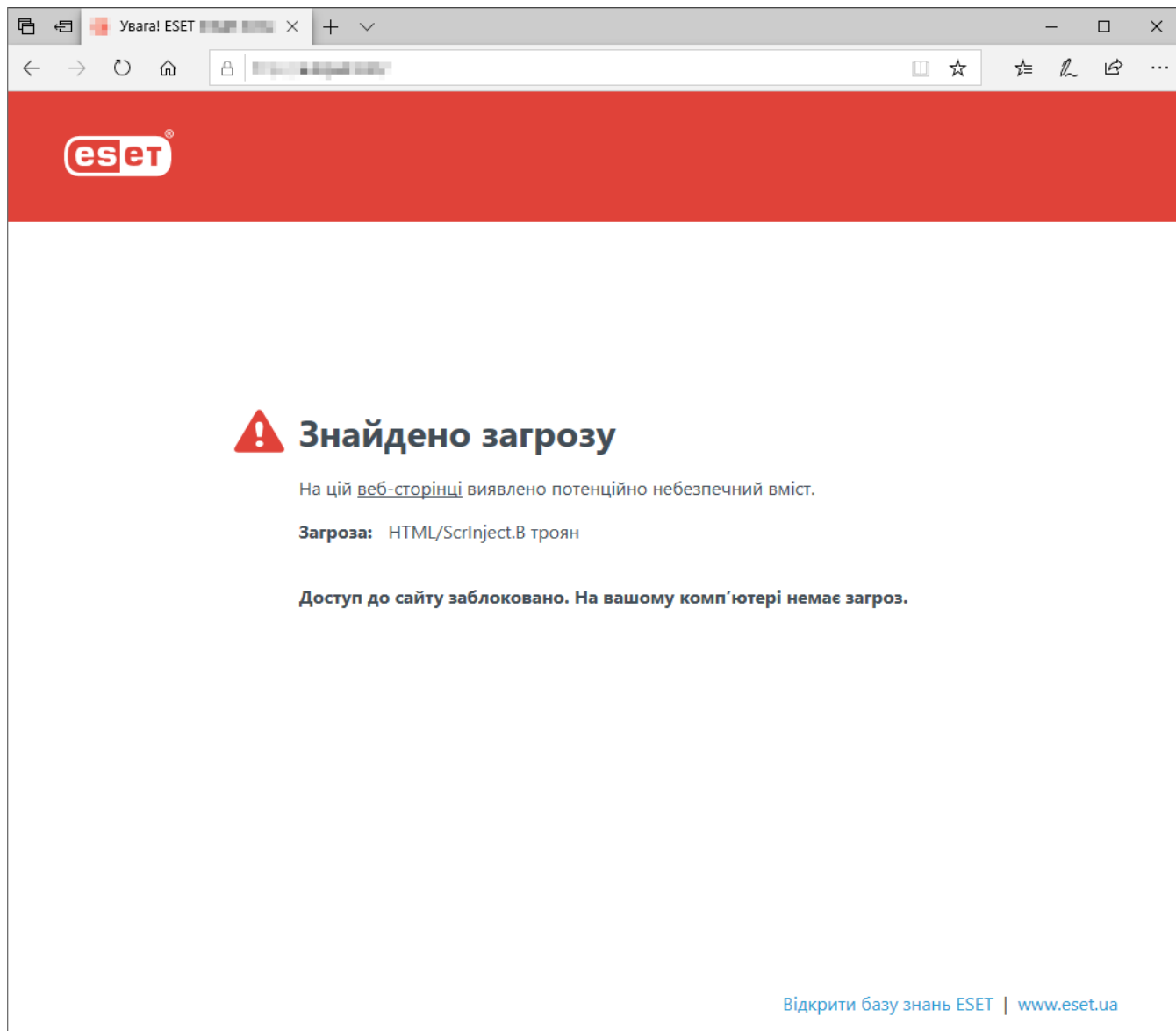
Доступ до відомих веб-сторінок зі шкідливим вмістом блокується до початку його завантаження. Усі інші веб-сторінки перевіряються підсистемою сканування ThreatSense під час завантаження та блокуються в разі виявлення зловмисного вмісту. Захист доступу до

Інтернету має два рівні: блокування за чорним списком і блокування за вмістом.

Наполегливо рекомендується активувати функцію захисту доступу до Інтернету. Щоб отримати доступ до цієї опції, у [головному вікні програми](#) > **Параметри** > **Захист від загроз з Інтернету** > **Захист доступу до Інтернету**.



Якщо функція "захист доступу до інтернету" заблокує веб-сайт, у веб-браузері відобразиться таке повідомлення:



Ілюстровані інструкції

- i** Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:
- [Виключити безпечний веб-сайт із блокування функцією захисту доступу до інтернету](#)
 - [Блокувати веб-сайт із використанням ESET NOD32 Antivirus](#)

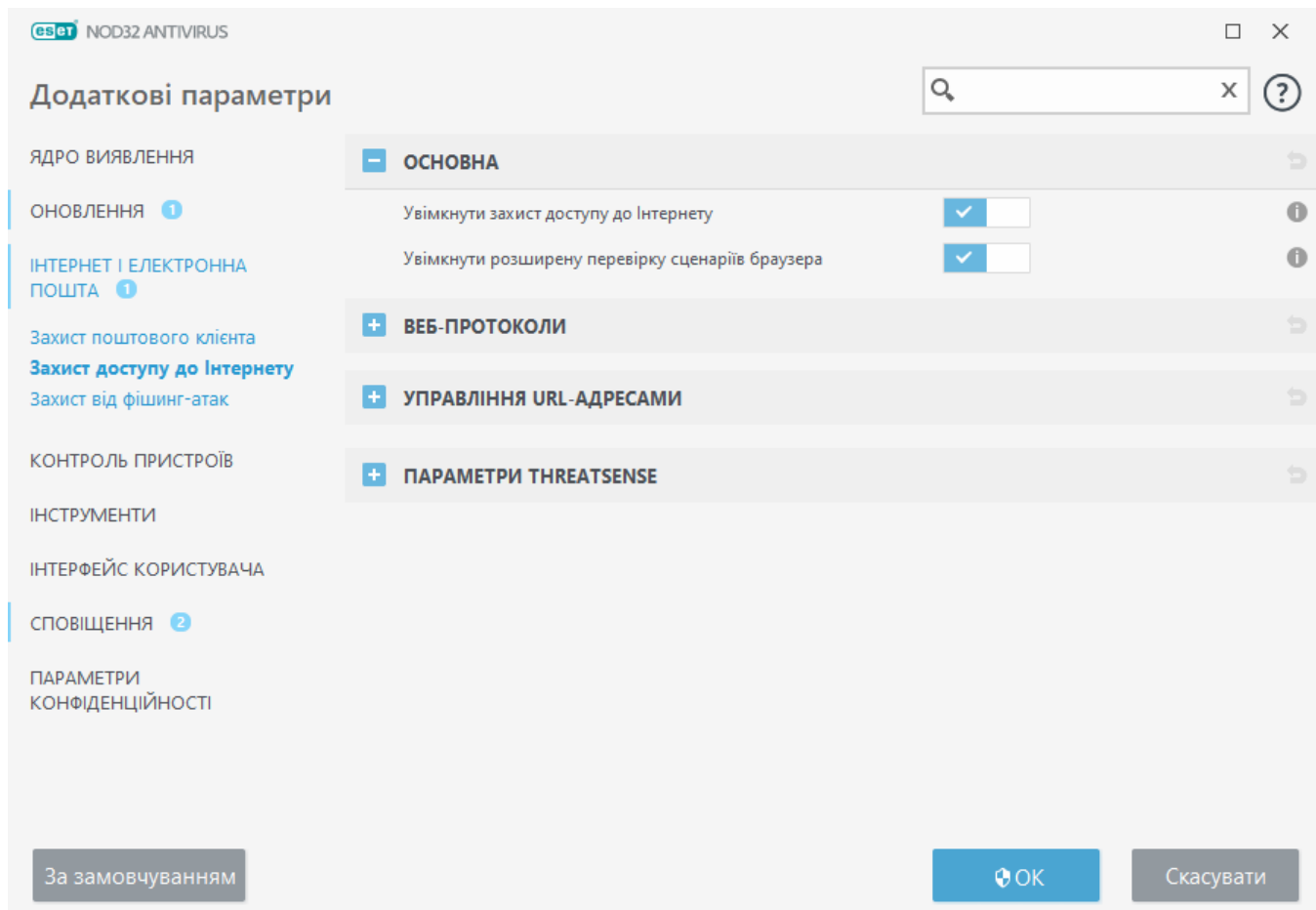
У меню **Додаткові параметри** (F5) > **Інтернет і електронна пошта** > **Захист доступу до Інтернету** доступні такі параметри:

Базові: дозволяє ввімкнути або вимкнути цю функцію в розділі "Додаткові параметри".

Веб-протоколи: дає змогу налаштувати моніторинг для стандартних протоколів, що використовуються більшістю веб-браузерів.

Керування URL-адресою: дає змогу вказати списки URL-адрес, які потрібно заблокувати, дозволити або виключити з перевірки.

Параметри підсистеми ThreatSense – додаткові параметри антивірусного сканера, за допомогою яких можна, зокрема, вказати типи об'єктів для перевірки (електронна пошта, архіви тощо), методи виявлення загроз для захисту доступу до Інтернету тощо.



Розширене налаштування функції захисту доступу до Інтернету

У меню **Додаткові параметри** (F5) > **Інтернет і електронна пошта** > **Захист доступу до Інтернету** > **Базові** доступні такі параметри:

Увімкнути захист доступу до Інтернету: коли цей параметр вимкнено, [захист від фішинг-атак](#) і [захист доступу до Інтернету](#) не забезпечуються. Ця опція доступна лише після ввімкнення фільтрації протоколу SSL/TLS.

Увімкнути розширену перевірку сценаріїв браузера: коли цей параметр увімкнено, ядро виявлення перевіряє всі програми JavaScript, що виконуються у веб-браузерах.

i Наполегливо рекомендуємо не вимикати функцію захисту доступу до Інтернету.

Веб-протоколи

За замовчуванням ESET NOD32 Antivirus налаштовано на відстеження протоколу HTTP, що використовується більшістю веб-браузерів.

Параметри сканера HTTP

Трафік за протоколом HTTP завжди відстежується на всіх портах для всіх програм.

Параметри сканера HTTPS

ESET NOD32 Antivirus також підтримує перевірку протоколу HTTPS. У разі застосування зв'язку HTTPS для передавання інформації між сервером і клієнтом використовується зашифрований канал. ESET NOD32 Antivirus перевіряє зв'язки, для яких використовується шифрування за протоколами SSL (Secure Socket Layer – рівень захищених сокетів) і TLS (Transport Layer Security – захист на транспортному рівні). Програма скануватиме лише трафік, порти (443, 0-65535), який передається через **Порти, що використовуються протоколом HTTPS**, незалежно від версії операційної системи.

Зашифровані зв'язки скануються за замовчуванням. Щоб переглянути налаштування сканера відкрийте розділ "Додаткові параметри" й виберіть пункти **Інтернет і електронна пошта > [SSL/TLS](#)**.

Управління URL-адресами

У розділі керування URL-адресами можна вказати списки HTTP-адрес, які буде заблоковано, дозволено чи виключено з перевірки вмісту.

Виберіть параметр [Увімкнути фільтрацію протоколу SSL/TLS](#), якщо крім веб-сторінок із протоколом HTTP потрібно також фільтрувати адреси HTTPS. Інакше додаватимуться лише домени відвіданих вами сайтів HTTPS, а не повні URL-адреси.

Веб-сайти зі **списку заблокованих адрес** будуть недоступні, якщо їх не перемістити до **списку дозволених адрес**. Веб-сайти зі **списку адрес, виключених зі сканування вмісту**, не скануються на наявність шкідливого програмного коду.

Щоб заблокувати всі HTTP-адреси, окрім включених в активний **список дозволених адрес**, додайте символ * в активний **список заблокованих адрес**.

У списках можна використовувати такі спеціальні символи, як-от * (зірочка) і ? (знак запитання). Зірочка означає будь-яку послідовність символів, а знак запитання – будь-який окремий символ. Необхідно дуже обережно визначати виключені адреси, тому що список має містити лише довірені та безпечні адреси. Окрім того, необхідно переконатися, що символи * та ? використовуються в списку правильно. Перегляньте розділ [Додати HTTP-адресу/маску домену](#), щоб дізнатися, як безпечно визначити весь домен разом із субдоменами. Щоб активувати список, виберіть опцію **Активний список**. Щоб отримувати попередження про введення адреси з поточного списку, виберіть **Сповіщати про застосування**.

Довірені домени



Адреси не будуть фільтруватися, якщо увімкнено параметр **Інтернет і електронна пошта > SSL/TLS > Виключити зв'язок із довіреними доменами** й домен вважається довіреним.

Список адрес?

Назва списку

Типи адрес

Опис списку

Список дозволених адрес	Дозволено	
Список заблокованих адрес	Заблоковано	
Список адрес, виключених зі скануван...	Знайдене шкідливе програмне забезпечен...	

Додати

Редагувати

Видалити

Імпортувати

Експортувати

Додайте до списку заблокованих адрес символ узагальнення (*), щоб заблокувати всі URL, окрім включених у список дозволених.

ОК

Скасувати

Елементи керування

Додати – створити список додатково до попередньо налаштованих. Це може знадобитися, коли потрібно розділити різні групи адрес за певною логікою. Наприклад, один список заблокованих адрес може містити веб-сторінки із зовнішнього загальнодоступного чорного списку, а другий – включати вашу особисту добірку небажаних сайтів. Це полегшить оновлення зовнішнього списку, натомість особистий список залишатиметься без змін.

Змінити – редагувати наявні списки. Використовуйте цю опцію, щоб додавати чи видаляти адреси.

Видалити: дає змогу видаляти наявні списки. Видаляти можна лише списки, створені за допомогою опції **Додати**, на відміну від списків за замовчуванням.

Список URL-адрес

У цьому розділі можна вказати списки адрес HTTP, які буде заблоковано, дозволено або виключено з перевірки.

За замовчуванням доступні такі три типи списків:

- **Список адрес, виключених зі сканування вмісту:** для будь-якої адреси, доданої до цього списку, перевірка на наявність шкідливого програмного коду не виконуватиметься.
- **Список дозволених адрес:** якщо встановлено прапорець "Дозволити доступ лише до URL-адрес, які містяться у списку дозволених", а список заблокованих адрес містить символ * (відповідає будь-якому символу), користувач зможе переходити лише за адресами, зазначеними в цьому списку. Перехід за адресами зі списку буде дозволено, навіть якщо їх включено до списку заблокованих.
- **Список заблокованих адрес:** користувачеві заборонено переходити за адресами з цього списку, доки їх також не буде додано до списку дозволених адрес.

Щоб створити новий список, клацніть **Додати**. Щоб видалити вибрані списки, клацніть **Видалити**.

Назва списку	Типи адрес	Опис списку
Список дозволених адрес	Дозволено	
Список заблокованих адрес	Заблоковано	
Список адрес, виключених зі скануван...	Знайдене шкідливе програмне забезпечен...	

Додайте до списку заблокованих адрес символ узагальнення (*), щоб заблокувати всі URL, окрім включених у список дозволених.

Ілюстровані інструкції



Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:

- [Виключити безпечний веб-сайт із блокування функцією захисту доступу до інтернету](#)
- [Блокування веб-сайту з використанням домашніх версій продуктів ESET для Windows](#)

Докладніші відомості наведено в розділі [Керування URL-адресами](#).

Створити новий список URL-адрес

У цьому розділі можна вказати списки URL-адрес/масок, які будуть заблоковані, дозволені або виключені з перевірки.

Під час створення нового списку можна налаштувати наведені нижче параметри.

Тип списку адрес – доступні три типи списків:

- **Виключені з перевірки:** для жодної адреси з цього списку перевірка шкідливого програмного коду виконуватися не буде.
- **Заблоковані** – користувач не зможе перейти за адресами з цього списку.
- **Дозволені** – якщо встановлено прапорець "Дозволити доступ лише до URL-адрес зі списку дозволених", а список заблокованих адрес містить символ * (зіставляти з усім), користувач зможе переходити лише за адресами з цього списку. Перехід за адресами зі списку буде дозволено, навіть якщо вони збігаються з елементами списку заблокованих.

Назва списку: укажіть назву списку. Під час редагування одного з трьох попередньо визначених списків це поле буде недоступним.

Опис списку – введіть короткий опис списку (необов'язково). Недоступне під час редагування одного з трьох попередньо визначених списків.

Щоб активувати список, виберіть поруч із ним параметр **Список активний**. Щоб отримувати сповіщення, коли певний список використовується для оцінювання відвіданого HTTP-сайту, виберіть **Сповіщати про застосування**. Наприклад, ви отримуватимете сповіщення, коли доступ до веб-сайту блокуватиметься або дозволятиметься відповідно до налаштувань списку заблокованих або дозволених адрес. У сповіщенні буде вказано назву списку, який містить зазначений веб-сайт.

Елементи керування

Додати: додати нову URL-адресу до списку (можна вказати кілька значень, використовуючи роздільник).

Редагувати: дає змогу редагувати адреси в списку. Цю команду можна застосувати лише до адрес, введених за допомогою функції **Додати**.

Видалити – дає змогу видалити наявні адреси зі списку. Цю команду можна застосувати лише до адрес, введених за допомогою функції **Додати**.

Імпортувати: імпортувати файл із URL-адресами (ім'я кожного файлу починається з нового рядка, наприклад, *.txt з використанням кодування UTF-8).

Додавання маски URL-адреси

Перед введенням потрібної адреси/маски домену виконайте інструкції, наведені в цьому діалоговому вікні.

Програма ESET NOD32 Antivirus дає змогу користувачеві заблокувати доступ до визначених веб-сайтів, перешкоджаючи веб-браузеру відображати їх вміст. Окрім того, можна вказати адреси, які мають бути виключені з перевірки. Якщо повне ім'я віддаленого сервера невідоме або користувач бажає вказати цілу групу віддалених серверів, для визначення такої групи можна використовувати так звані маски. Маски містять символи "?" та "*":

- "?" представляє окремий символ;
- "*" представляє текстовий рядок.

Наприклад, маска *.c?m описує всі адреси, остання частина яких починається з літери "c", закінчується літерою "m" і містить будь-який символ між ними (.com, .cam тощо).

До послідовності "*" застосовуються особливі правила, якщо вона стоїть на початку імені домену. По-перше, у цьому випадку символ узагальнення "*" не відповідає символу скісної риски (/). Це запобігає можливості обійти маску. Наприклад, маска *.domain.com не відповідатиме <http://anydomain.com/anypath#.domain.com> (такий суфікс можна додати до будь-якої URL-адреси, і це не вплине на завантаження). По-друге, у цьому особливому випадку послідовність "*" також відповідатиме пустому рядку. Саме тому за допомогою однієї маски можна охопити весь домен разом із субдоменами. Наприклад, маска *.domain.com також відповідатиме <http://domain.com>. Використання *.domain.com буде помилковим, оскільки така маска також відповідатиме <http://anotherdomain.com>.

Захист від фішинг-атак

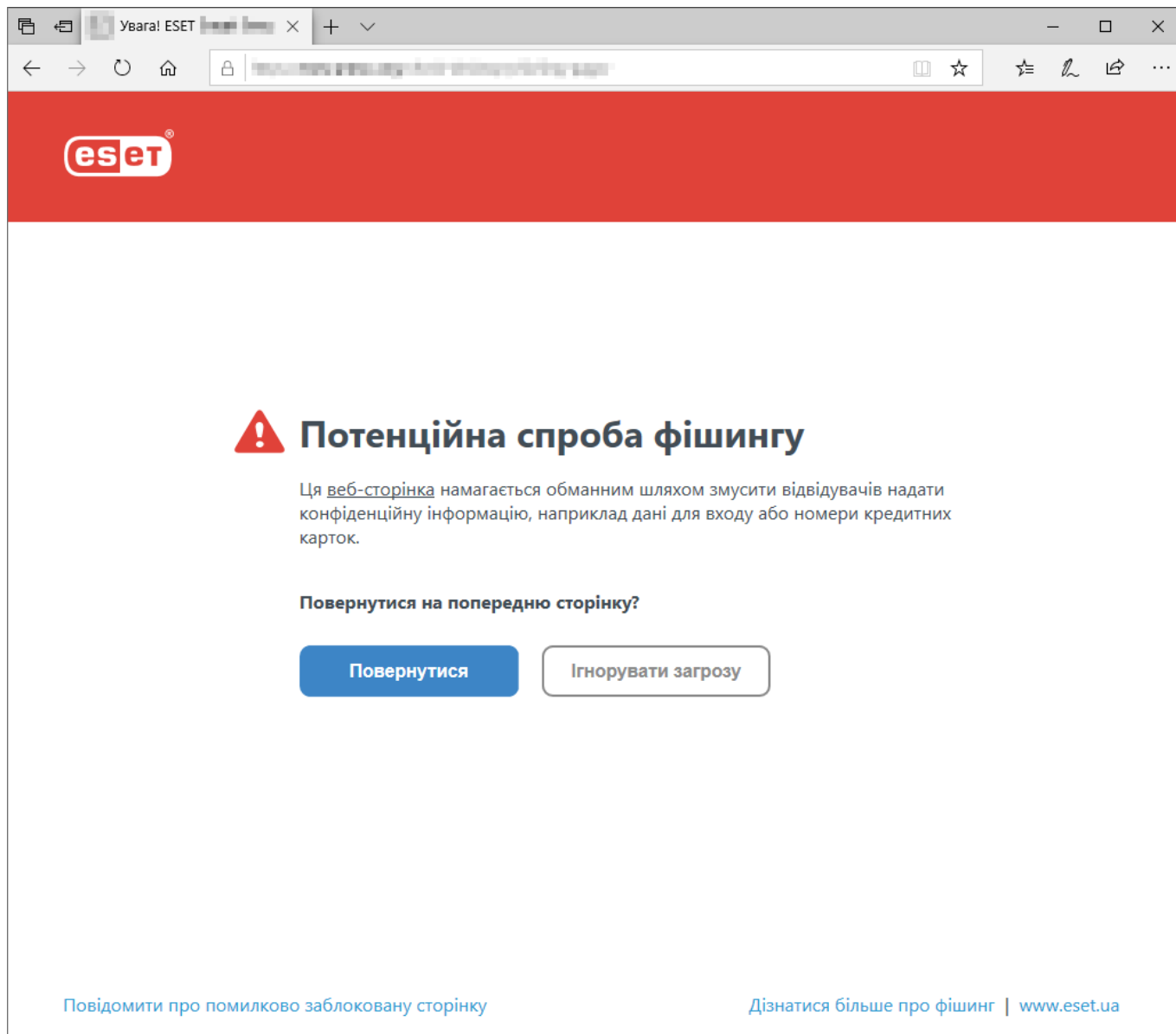
Терміном "фішинг" називається злочинна діяльність із використанням соціотехнік (маніпулювання користувачами для отримання конфіденційної інформації). Мета фішингу – отримати доступ до таких конфіденційних даних, як номери банківських рахунків, ПІН-коди тощо. Докладнішу інформацію про цю діяльність див. у [глосарії](#). ESET NOD32 Antivirus включає модуль захисту від фішинг-атак, який блокує веб-сторінки, що, як відомо, поширюють такий вміст.

Рекомендуємо активувати захист від фішингу в ESET NOD32 Antivirus. Для цього відкрийте меню **Додаткові параметри** (F5) і перейдіть до розділу **Інтернет і електронна пошта > Захист від фішинг-атак**.

Перегляньте цю [статтю в базі знань](#), щоб дізнатися більше про захист від фішинг-атак у ESET NOD32 Antivirus.

Відвідування шахрайського веб-сайту

Після переходу на фішинговий сайт у браузері відобразиться наведене нижче діалогове вікно. Якщо ви все одно бажаєте відвідати такий веб-сайт, натисніть **Ігнорувати загрозу** (не рекомендується).



За замовчуванням потенційні шахрайські веб-сайти, які було додано до білого списку, через кілька годин видаляються з нього. Щоб остаточно визначити веб-сайт як безпечний, скористайтесь інструментом [Управління URL-адресами](#). У меню **Додаткові параметри (F5) > Інтернет і електронна пошта > Захист доступу до Інтернету > Керування URL-адресою > Список адрес > Змінити** додайте до списку той веб-сайт, статус якого потрібно змінити.

Повідомлення про шахрайський сайт

Скористайтесь посиланням **Повідомити** й передайте дані про шахрайський/шкідливий веб-сайт компанії ESET для його подальшої перевірки.

Перш ніж відправляти дані про веб-сайт до ESET, упевніться, що виконується один або кілька перелічених нижче критеріїв.

- Веб-сайт узагалі не виявляється.
- Веб-сайт неправильно виявляється як загроза. У цьому випадку ви можете [повідомити про помилково заблоковану сторінку](#).

Дані про веб-сайт також можна відправити електронною поштою. Надішліть повідомлення на адресу samples@ eset.com. Обов'язково вкажіть тему повідомлення та надайте якомога більше

інформації про веб-сайт (наприклад, веб-сайт, з якого ви на нього перейшли, як про нього дізналися тощо).

Оновлення програми

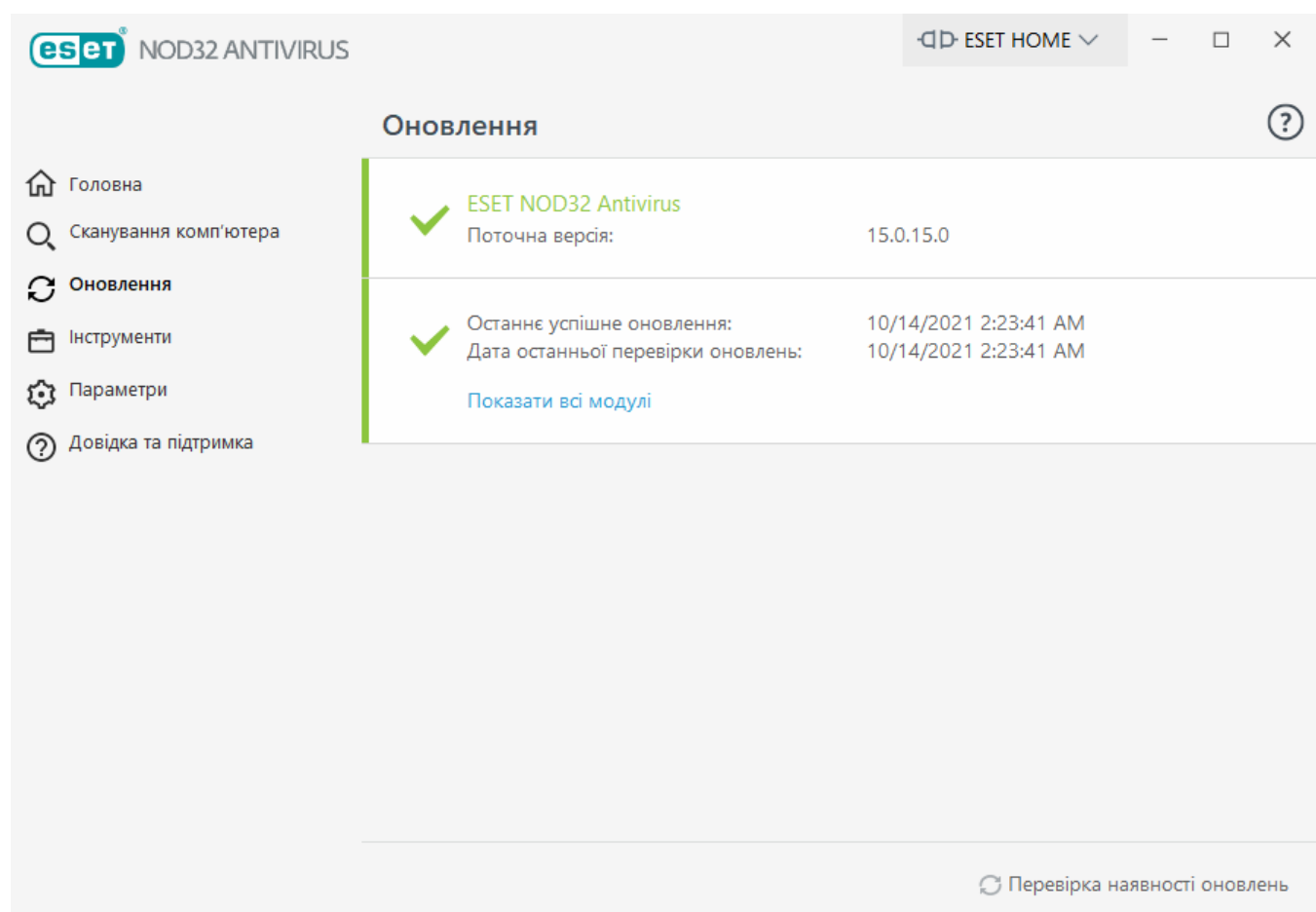
Регулярне оновлення ESET NOD32 Antivirus – найкращий спосіб забезпечити максимальний захист комп'ютера. Модуль оновлення гарантує, що модулі програми й компоненти системи завжди матимуть актуальний стан.

Натиснувши **Оновлення** в [головному вікні програми](#), можна переглянути поточний стан оновлення, відомості про дату й час останнього успішного оновлення, а також про те, чи потрібно його виконувати зараз.

Оновлення можна виконувати не лише автоматично. Також можна натиснути **Перевірити наявність оновлень**, щоб ініціювати оновлення вручну. Регулярне оновлення модулів і компонентів програми — це запорука повного захисту від шкідливого коду. Приділіть особливу увагу налаштуванню та роботі модулів продукту. Щоб отримувати оновлення, потрібно активувати продукт за допомогою ліцензійного ключа. Якщо ви не зробили цього під час інсталяції, уведіть ліцензійний ключ, щоб активувати свою копію продукту для доступу до серверів оновлення ESET.



Компанія ESET надіслала ліцензійний ключ електронною поштою після придбання продукту ESET NOD32 Antivirus.



Поточна версія – номер поточної інсталюваної версії продукту.

Останнє оновлення: дата останнього оновлення. Якщо відображається давня дата, можливо, версія модулів продукту застаріла.

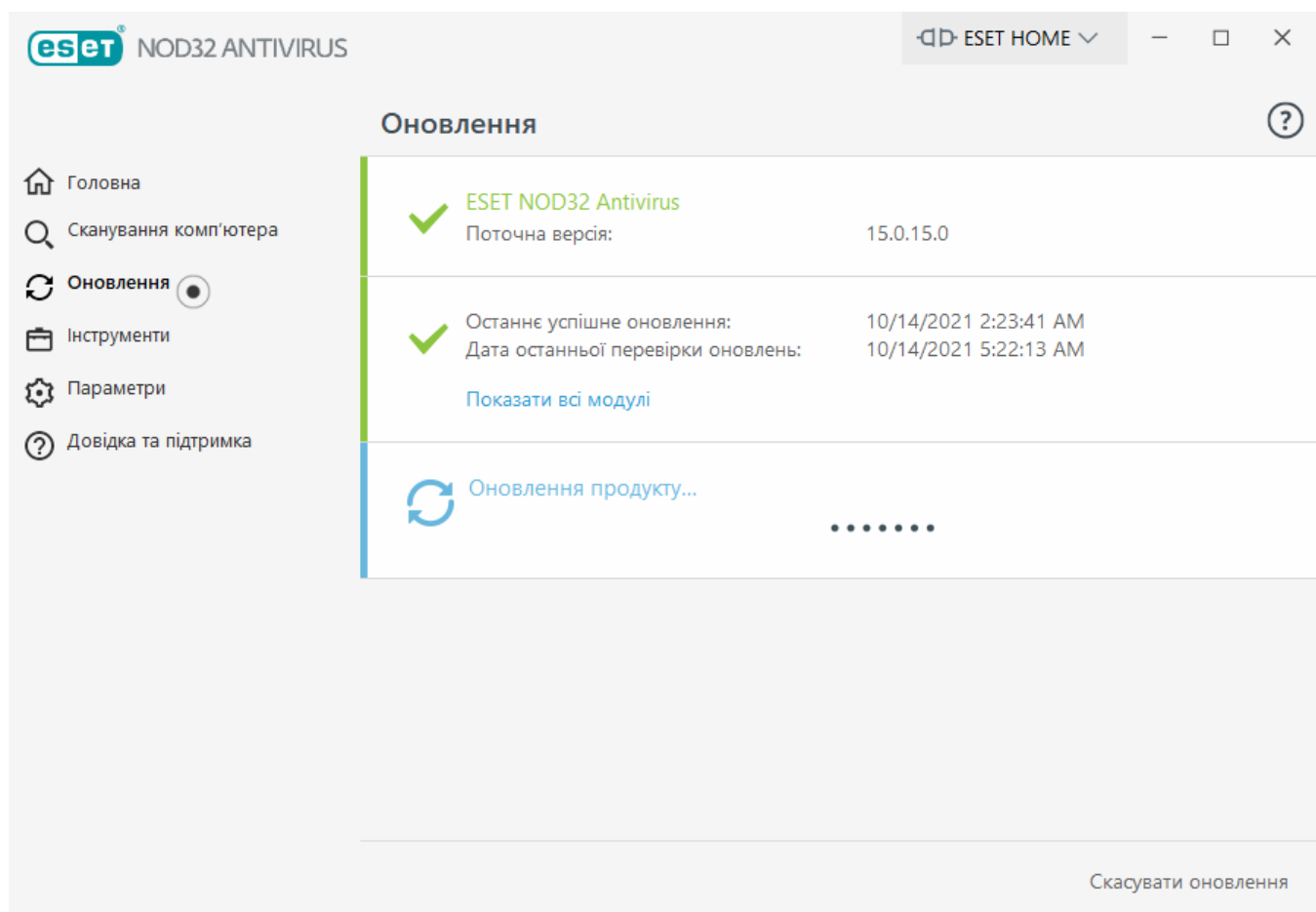
Дата останньої перевірки оновлень: дата останньої перевірки наявності оновлень.

Показати всі модулі – інформація про список інстальованих модулів програми.

Натисніть **Перевірити наявність оновлень**, щоб визначити останню доступну версію ESET NOD32 Antivirus.

Процес оновлення

Щойно ви натиснете **Перевірити наявність оновлень**, почнеться завантаження. На екрані відображається індикатор виконання та час до закінчення завантаження. Щоб перервати процес оновлення, натисніть **Скасувати оновлення**.



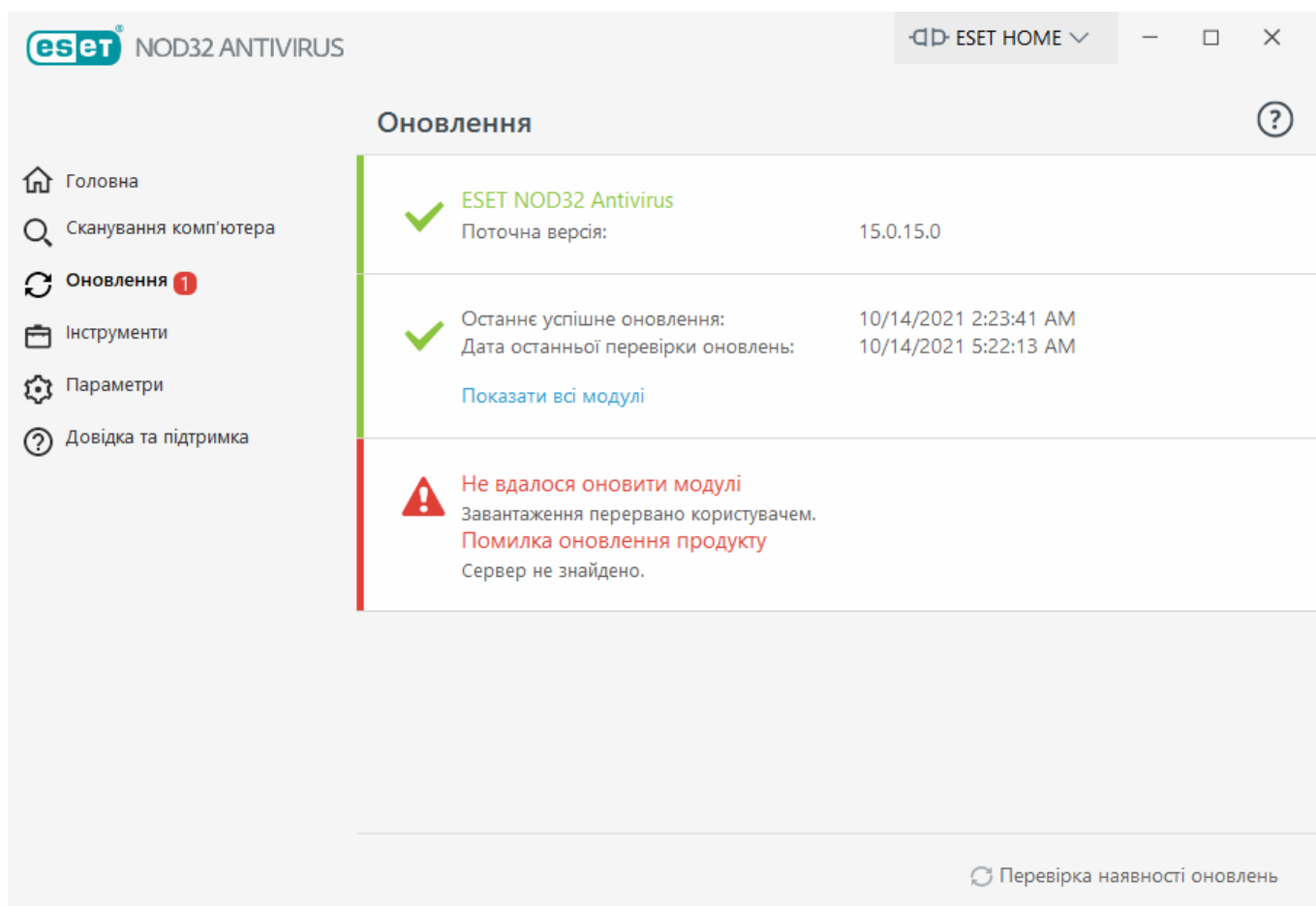
За нормальних умов у вікні **Оновлення** відображається зелена позначка, яка вказує, що для програми інстальовано всі потрібні оновлення. Якщо ця позначка не відображається, програма застаріла, тому вона є більш уразливою до зараження. Оновіть модулі програми якомога швидше.

Оновлення завершується помилкою

Якщо з'являється повідомлення про помилку оновлення модулів, це може бути з таких причин:

1. **Недійсна ліцензія:** ліцензія, що використовувалася для активації, недейсна або термін її дії минув. У [головному вікні програми](#) натисніть **Довідка та підтримка > Змінити ліцензію** та введіть новий ліцензійний ключ.

2. **Помилка під час завантаження файлів оновлення** – причиною появи такого повідомлення можуть бути неправильні [параметри підключення до Інтернету](#). Рекомендується перевірити підключення до Інтернету (наприклад, відкривши в браузері будь-який веб-сайт). Якщо веб-сайт не відкривається, імовірно, підключення Інтернету не встановлено або комп'ютер має проблеми з підключенням. Зверніться до свого інтернет-провайдера, якщо не вдається встановити активне підключення до Інтернету.



Після успішного оновлення ESET NOD32 Antivirus до новішої версії рекомендуємо перезапустити комп'ютер, щоб забезпечити коректне оновлення всіх модулів програми. Не потрібно перезапускати комп'ютер після завершення звичайних оновлень модулів.



Більш докладну інформацію див. за посиланням [Виправлення неполадок, пов'язаних із появою повідомлення "Помилка оновлення модулів"](#).

Параметри оновлення

Параметри налаштування оновлень розташовані в дереві **Додаткові параметри** (F5) у розділі **Оновлення > Базові**. У розділі параметрів оновлення вказується інформація про відповідне джерело (наприклад, сервери оновлення й дані автентифікації для них).

Основна

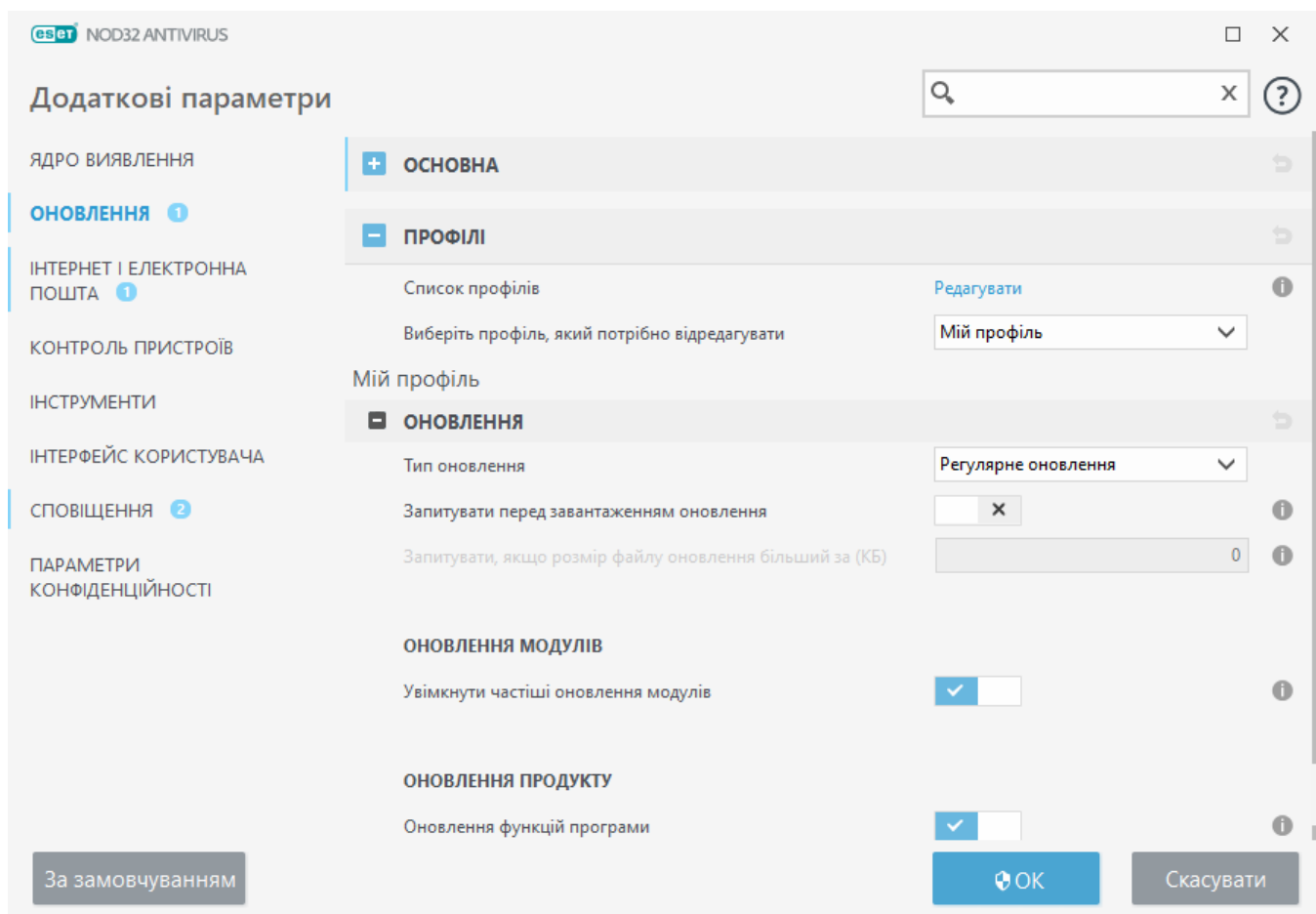
Поточний профіль оновлення (якщо його не визначено в розділі **Додаткові параметри > Брандмауер > Відомі мережі**) відображається в розкритому меню **Вибрати профіль оновлення за замовчуванням**.

Інформацію щодо створення нового профілю, див. в розділі [Профілі оновлення](#).

Якщо вам не вдається завантажити оновлення обробника виявлення або модулів, натисніть **Очистити**, щоб видалити тимчасові файли/кеш оновлення.

Відкочування модуля

Якщо ви підозрюєте, що останнє оновлення обробника виявлення та/або модулів програми нестабільне або пошкоджене, можна [повернутися до попередньої](#) версії та вимкнути всі оновлення для вибраного періоду часу.



Щоб оновлення були завантажені належним чином, важливо правильно вказати всі параметри. Якщо ви використовуєте брандмауер, переконайтеся, що програмі ESET дозволено взаємодіяти з

Інтернетом (тобто дозволено зв'язок за протоколом HTTP).

Профілі

Профілі оновлення можна створювати для різних конфігурацій і завдань оновлення. Зокрема ця функція стане в пригоді користувачам мобільних пристроїв, яким потрібен альтернативний профіль, оскільки їхні параметри підключення до Інтернету часто змінюються.

Активний профіль указано в розкритому меню **Виберіть профіль, який потрібно відредагувати** (за замовчуванням для цього параметра встановлено значення **Мій профіль**). Щоб створити новий профіль, клацніть **Змінити** поруч з елементом **Список профілів**, уведіть **Ім'я профілю** й натисніть **Додати**.

Оновлення

За замовчуванням для параметра **Тип оновлення** вибрано значення **Регулярне оновлення**. Так файли оновлень автоматично завантажуватимуться із сервера ESET із мінімальним споживанням мережевого трафіку. Оновлення попередніх версій (параметр **Бета-версії оновлень**) – це оновлення, які пройшли повну внутрішню перевірку й незабаром будуть доступні для широкого загалу. Перевага бета-версії оновлення – доступ до найновіших методів виявлення й виправлення. Однак бета-версії оновлення можуть бути недостатньо стабільними, тому їх НЕ МОЖНА використовувати на виробничих серверах і робочих станціях, де потрібен високий рівень доступності й стабільності.

Запитувати перед завантаженням оновлення: у сповіщенні можна буде підтвердити або скасувати завантаження файлу оновлення.

Запитувати, якщо розмір файлу оновлення більший за (КБ): якщо розмір файлу оновлення більший за вказаний, буде відображатися діалогове вікно з підтвердженням. Якщо вибрати розмір файлу 0 КБ, сповіщення відображатиметься завжди.

Не відображати сповіщення про успішне оновлення: дає змогу вимкнути показ сповіщень у системному треї в нижньому правому куті екрана. Це зручно, коли ви працюєте в повноекранному режимі або коли запущено комп'ютерну гру. Зверніть увагу, що в ігровому режимі всі сповіщення буде вимкнено.

Оновлення модуля

Увімкнути частіші оновлення вірусної бази даних: вірусна база даних буде оновлюватись через коротші проміжки часу. Якщо цей параметр вимкнено, це може негативно позначитися на ефективності виявлення.

Оновлення продукту

Оновлення функцій програми: автоматична інсталяція нових версій ESET NOD32 Antivirus.

Параметри підключення

Якщо потрібно використовувати проксі-сервер для завантаження оновлень, відповідну інформацію див. в розділі [Параметри підключення](#).

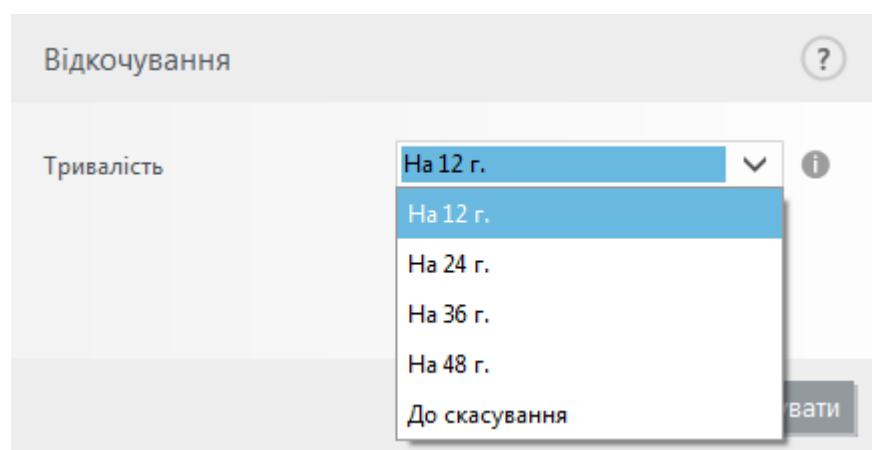
Відкочування оновлення

Якщо ви підозрюєте, що нове оновлення ядра виявлення або модулів програми нестабільне або пошкоджене, можна повернутися до попередньої версії й тимчасово вимкнути оновлення. Окрім того, можна активувати попередньо вимкнуті оновлення, якщо їх було призупинено на невизначений час.

ESET NOD32 Antivirus зберігає знімки ядра виявлення й модулів програми, які можна використовувати з функцією відкочування. Щоб створювати знімки вірусної бази даних, залиште перемикач **Створити знімки модулів** увімкненим. Якщо перемикач **Створити знімки модулів** увімкнено, під час першого оновлення створюється перший знімок. Наступний знімок створюється через 48 годин. У полі **Кількість локально збережених знімків** відображається кількість збережених знімків ядра виявлення.

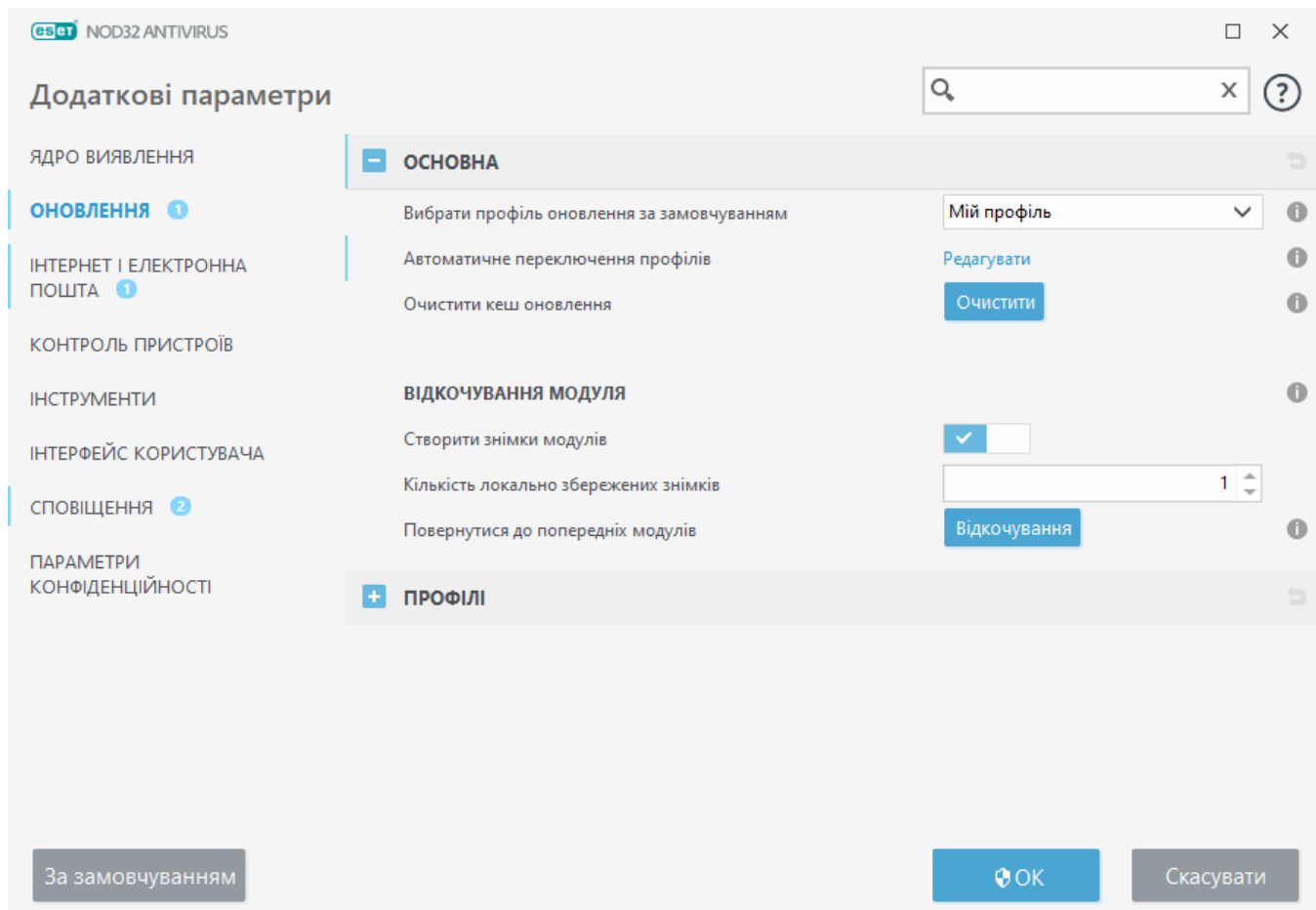
i Коли досягнуто максимальної кількості знімків (наприклад, три), найстаріший знімок замінюється новим знітком кожні 48 годин. ESET NOD32 Antivirus відкочує оновлення ядра виявлення й модуля програми до найстарішої версії знімка.

Якщо натиснути **Відкочування (Додаткові параметри (F5) > Оновлення > Базові)**, у розкритому меню **Тривалість** потрібно буде вибрати проміжок часу, на який оновлення обробника виявлення й програмних модулів призупиниться.



Для призупинення оновлень на невизначений час (доки отримання оновлень не буде відновлено вручну) виберіть **До скасування**. Оскільки цей параметр спричиняє потенційну загрозу для безпеки, ESET не рекомендує вибирати його.

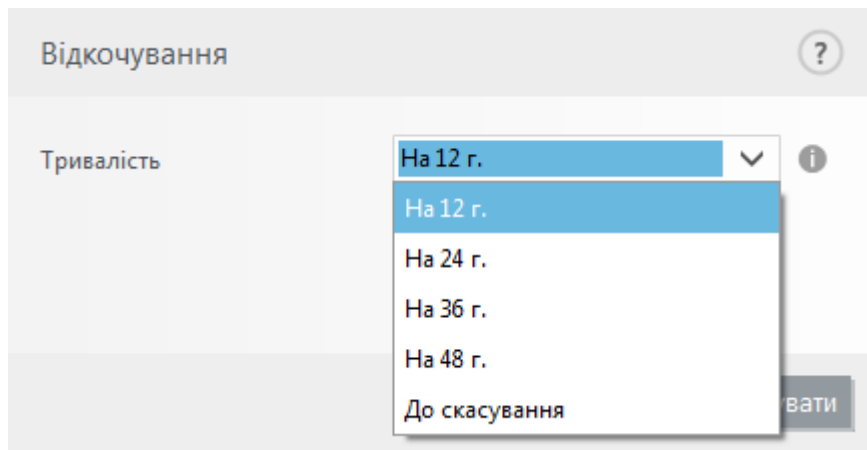
Якщо відкочування вже виконано, кнопка **Відкочування** замінюється на **Дозволити оновлення**. Протягом періоду, вибраного в розкритому меню **Призупинити оновлення**, оновлення не дозволятимуться. Версію ядра виявлення буде понижено до найстарішої серед доступних, тож вона зберігатиметься як знімок у файловій системі на локальному комп'ютері.



Припустімо, що найновішою версією обробника виявлення є версія 22700, а версії 22698 і 22696 зберігаються як знімки ядра виявлення. Зверніть увагу, що версія 22697 недоступна. У цьому прикладі комп'ютер було вимкнено, коли версія 22697 була актуальною, і ще до завантаження цієї версії вже з'явилася інша найновіша версія. Якщо в полі **Кількість локально збережених знімків** задано значення 2, і ви клацнули **Відкочування**, ядро виявлення (разом із модулями програми) буде відкочено до версії 22696. Цей процес може тривати деякий час. На екрані [Оновити](#) перевірте, чи було понижено версію ядра виявлення.

Інтервал часу відкочування

Якщо натиснути **Відкочування** (**Додаткові параметри** (F5) > **Оновлення** > **Базові**), у розкритому меню **Тривалість** потрібно буде вибрати проміжок часу, на який оновлення обробника виявлення й програмних модулів призупиниться.



Для призупинення оновлень на невизначений час (доки отримання оновлень не буде відновлено вручну) виберіть **До скасування**. Оскільки цей параметр спричиняє потенційну загрозу для безпеки, ESET не рекомендує вибирати його.

Оновлення продукту

Розділ **Оновлення продукту** дає змогу налаштувати автоматичну інсталяцію нових оновлень функцій щойно вони ставатимуть доступними.

Оновлення функцій програми містять нові функції або змінюють функції, наявні в попередніх версіях. Оновлення може бути застосовано автоматично без участі користувача або з відображенням відповідного сповіщення. Після інсталяції оновлення функцій програми може знадобитися перезавантажити комп'ютер.

Оновлення функцій програми: якщо цей параметр увімкнено, оновлення функцій програми будуть виконуватися автоматично.

Параметри підключення

Щоб отримати доступ до параметрів проксі-сервера для певного профілю оновлення, виберіть елемент **Оновлення** в дереві **Додаткові параметри** (F5) і натисніть **Профілі > Оновлення > Параметри оновлення**. Клацніть розкриттве меню **Режим проксі-сервера** й виберіть один із трьох наведених нижче параметрів.

- Не використовувати проксі-сервер
- Підключення через проксі-сервер
- Використовувати глобальні параметри проксі-сервера

Якщо вибрати параметр **Використовувати глобальні параметри проксі-сервера**, програма використовуватиме параметри проксі-сервера, уже вказані в гілці **Інструменти > Проксі-сервер** дерева додаткових параметрів.

Виберіть параметр **Не використовувати проксі-сервер**, щоб указати, що для оновлення ESET NOD32 Antivirus не потрібно використовувати проксі-сервер.

Параметр **Підключення через проксі-сервер** слід вибирати в наведених нижче випадках.

- Якщо для оновлення ESET NOD32 Antivirus використовується проксі-сервер, відмінний від указанного в меню **"Інструменти" > Проксі-сервер**. У цій конфігурації інформацію для нового проксі-сервера має бути вказано в полі адреси **Проксі-сервер**, у полі зв'язку **Порт** (за промовчанням – 3128), а також у полях **Ім'я користувача** та **Пароль** (якщо потрібно).
- Якщо параметри проксі-сервера для загального використання не було встановлено, але для оновлення програма ESET NOD32 Antivirus підключатиметься до проксі-сервера.
- Якщо комп'ютер підключено до Інтернету через проксі-сервер. Під час інсталяції програми значення параметрів беруться з конфігурації Internet Explorer, але якщо вони змінюються (наприклад, ви звертаєтесь до іншого постачальника послуг Інтернету), переконайтеся, що в цьому вікні вказано правильні параметри проксі-сервера. В іншому разі програма не зможе підключитися до серверів оновлень.

За замовчування для проксі-сервера застосовується параметр **Використовувати глобальні параметри проксі-сервера**.

Використовувати пряме підключення, якщо проксі-сервер недоступний – якщо проксі-сервер недоступний, у процесі оновлення буде виконано його обхід.

i У полях **Ім'я користувача** та **Пароль** указуються окремі дані для кожного проксі-сервера. Заповнюйте їх, лише якщо ці дані потрібні для підключення до проксі-сервера. Ці поля потрібно заповнювати, лише якщо ви точно знаєте, що для доступу до Інтернету через проксі-сервер потрібен пароль.

Створення завдань оновлення

Процес оновлення можна ініціювати вручну, натиснувши **Перевірити наявність оновлень** в основному вікні, яке відобразиться після вибору елемента **Оновлення** в головному меню.

Оновлення також можна виконувати як заплановані завдання. Щоб налаштувати заплановане завдання, натисніть **Інструменти > Завдання за розкладом**. За замовчуванням у програмі ESET NOD32 Antivirus активовано наведені нижче завдання.

- **Регулярне автоматичне оновлення**
- **Автоматичне оновлення після встановлення модемного підключення**
- **Автоматичне оновлення після входу користувача в систему**

Кожне завдання оновлення за бажанням можна змінювати. Окрім стандартних завдань оновлення, користувач може створювати нові завдання із власною користувацькою конфігурацією. Докладніше про створення й налаштування завдань оновлення див. у розділі [Завдання за розкладом](#).

Діалогове вікно "Необхідно перезавантажити комп'ютер"

Після оновлення ESET NOD32 Antivirus до нової версії необхідно перезавантажити комп'ютер. Наразі випущено нові версії ESET NOD32 Antivirus для вдосконалення або виправлення проблем,

які не вдається усунути через автоматичне оновлення модулів програми.

Нову версію ESET NOD32 Antivirus можна інстальовати автоматично залежно від [параметрів оновлення програми](#) або вручну, [завантаживши й інстальовавши новішу версію](#) поверх попередньої.

Клацніть **Перезавантажити зараз**, щоб перезавантажити комп'ютер. Якщо ви плануєте перезавантажити комп'ютер пізніше, клацніть **Нагадати пізніше**. Пізніше комп'ютер можна буде перезавантажити вручну в **головному** розділі [головного вікна програми](#).

Інструменти

У меню **Інструменти** представлено ряд модулів, які допомагають спростити адміністрування програми та надають додаткові можливості для досвідчених користувачів.

Докладнішу інформацію можна переглянути в розділі [Інструменти ESET NOD32 Antivirus](#).

Інструменти ESET NOD32 Antivirus

У меню **Інструменти** представлено ряд модулів, які допомагають спростити адміністрування програми та надають додаткові можливості для досвідчених користувачів.

Цей розділ містить такі елементи:



[Файли журналу](#)



[Звіт про безпеку](#)



[Запущені процеси](#) (якщо ESET LiveGrid® увімкнено в програмі ESET NOD32 Antivirus)



[ESET SysInspector](#)



[ESET SysRescue Live](#): виконує переспрямування на веб-сайт ESET SysRescue Live, де можна завантажити образ .iso для запису ESET SysRescue Live на диск CD/DVD.



[Планувальник](#)



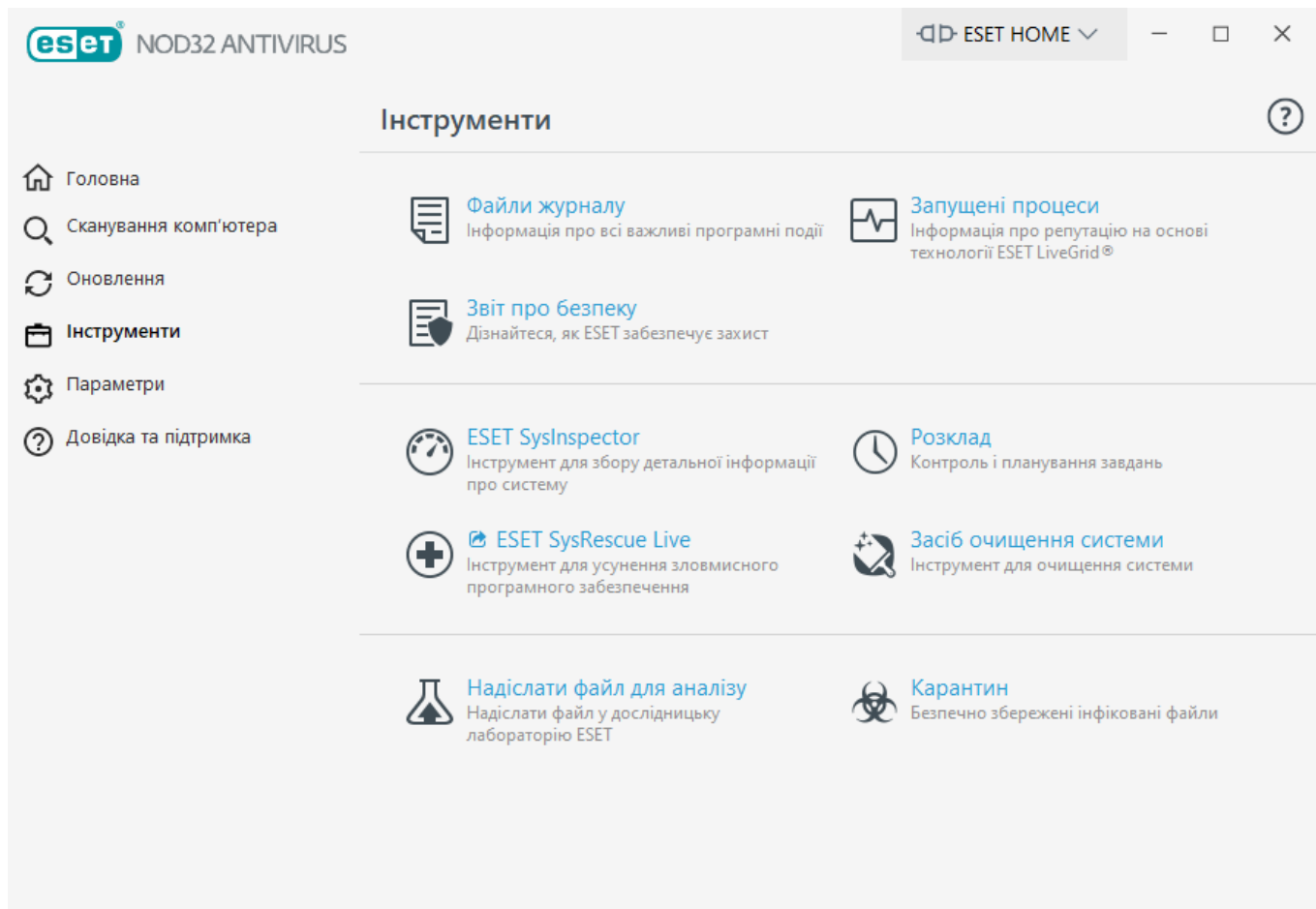
[Засіб очищення системи](#) – допомагає відновити працездатний стан комп'ютера після очищення загрози.



[Надіслати файл для аналізу](#) – дає змогу надсилати підозрілі файли на аналіз до дослідницької лабораторії ESET (доступність функції залежить від конфігурації ESET LiveGrid®).

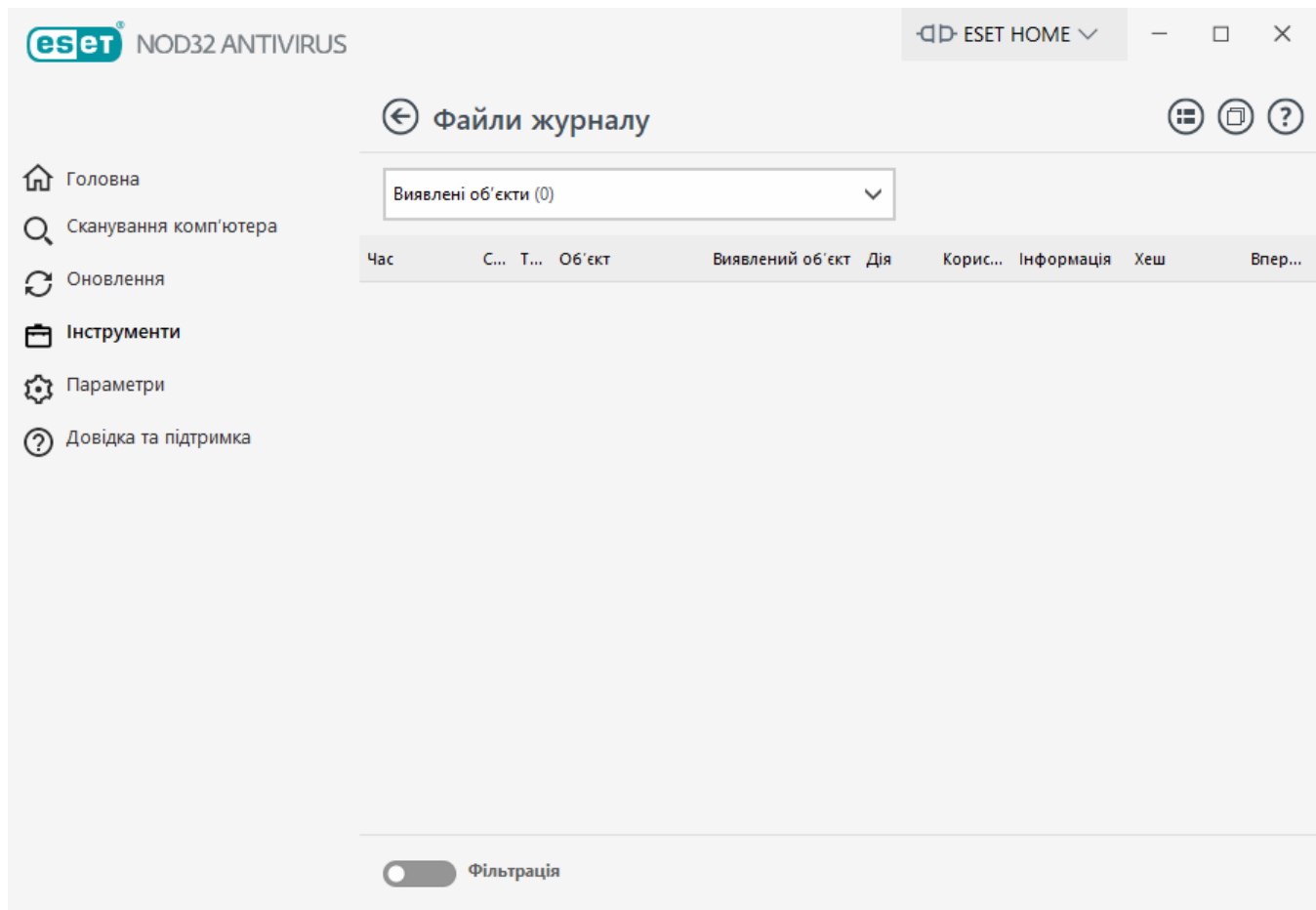


[Карантин](#)



Журнали

Журнали містять інформацію про важливі події, які відбулися у програмі, і надають огляд виявлених загроз. Ведення журналу є важливим засобом системного аналізу, виявлення загроз і виправлення неполадок. Запис у журнал відбувається у фоновому режимі без втручання користувача. Інформація, яка може записуватися в журнал, залежить від поточних параметрів деталізації журналу. Доступна можливість переглядати текстові повідомлення та журнали безпосередньо в інтерфейсі ESET NOD32 Antivirus, а також архівувати журнали.




Доступ до журналів можна отримати з [головного вікна програми](#). Для цього клацніть **Журнали** > **Файли журналу**. Виберіть потрібний тип журналу в розкритому меню **Журнал**. Доступні такі журнали:

- **Виявлені об'єкти:** цей журнал містить детальну інформацію про інфіковані об'єкти й загрози, виявлені продуктом ESET NOD32 Antivirus. У журналі зазначається час виявлення, тип сканера, тип об'єкта, назва загрози, виконана дія, ім'я користувача, який перебував у системі в момент виявлення загрози, хеш і дані про перше виникнення. Загрози, які не вдалось очистити, завжди позначаються червоним текстом на яскраво-червоному фоні. Очищені загрози позначаються жовтим текстом на білому фоні. Потенційно небезпечні програми, які не очищено, позначаються жовтим текстом на білому фоні.
- **Події:** усі важливі дії, виконані ESET NOD32 Antivirus, записуються в журналі подій. Журнал містить інформацію про події та помилки, які сталися в програмі. Він призначений для системних адміністраторів і користувачів, яким потрібна допомога з вирішенням проблем. Часто інформація в ньому допомагає знайти вирішення проблеми, яка виникла під час роботи програми.
- **Сканування комп'ютера:** у цьому вікні відображаються результати всіх виконаних сканувань. Кожний рядок відповідає одному скануванню комп'ютера. Двічі клацніть будь-який рядок, щоб переглянути докладну [інформацію про відповідний сеанс сканування](#).
- **HIPS** – містить записи певних правил [HIPS](#), позначених для запису. Протокол містить назву програми, яка викликала операцію, результат (правило було дозволено чи заборонено), а також ім'я правила.
- **Відфільтровані веб-сайти:** список веб-сайтів, заблокованих модулем [захисту доступу](#)

[до Інтернету](#). У кожному журналі вказується час, URL-адреса, ім'я користувача та програма, що встановила підключення з певним сайтом.

- **Контроль пристроїв:** містить записи про змінні носії та пристрої, підключені до комп'ютера. У файлі журналу реєструються тільки пристрої з відповідними правилами контролю. Якщо правило не відповідає підключеному пристрою, запис у журналі для підключеного пристрою не створюватиметься. У цьому ж журналі можна переглянути відомості про тип пристрою, серійний номер, ім'я постачальника та розмір носія (якщо доступно).


Виберіть вміст будь-якого журналу й натисніть комбінацію клавіш **CTRL + C**, щоб скопіювати його в буфер обміну. Натисніть і утримуйте **CTRL** або **SHIFT**, щоб вибрати кілька записів.

Натисніть елемент  **Фільтрація**, щоб відкрити вікно [Фільтрація журналу](#), де можна визначати критерії фільтрації.

Клацніть певний запис правою кнопкою миші, щоб відкрити контекстне меню. У контекстному меню ви зможете отримати доступ до наведених нижче параметрів.

- **Показати:** показ додаткової інформації про вибраний журнал у новому вікні.
- **Відфільтровувати однакові записи:** після активації цього фільтра відображатимуться лише записи певного типу (діагностичні, попереджувальні тощо).
- **Фільтрувати:** після натискання цієї опції у вікні [Фільтрація журналу](#) можна визначати критерії фільтрації для певних записів журналу.
- **Увімкнути фільтр:** активація параметрів фільтра.
- **Вимкнути фільтр:** очищення всіх параметрів фільтра (як описано вище).
- **Копіювати/Копіювати все:** копіювання інформації про вибрані записи у вікні.
- **Видалити / Видалити все:** видалення вибраних або всіх відображуваних записів (для виконання цієї дії необхідні права адміністратора). (для виконання цієї дії необхідні права адміністратора).
- **Експорт / Експортувати все:** експорт інформації про вибрані або всі записи у форматі XML.
- **Знайти / Знайти наступні / Знайти попередні:** після натискання цієї опції можна визначати критерії фільтрації для пошуку певних записів у вікні фільтрації журналу.
- **Опис об'єкта:** відкриває енциклопедію загроз ESET, у якій міститься докладна інформація про небезпеки й симптоми зафіксованих загроз.
- **Створити виключення:** дозволяє створити нове [виключення виявленого об'єкта з використанням майстра](#) (недоступно для виявленого шкідливого програмного забезпечення).

Фільтрація журналу

Натисніть **Фільтрація**  у розділі **Журнали > Файли журналу** для визначення критеріїв фільтрації.

Функція фільтрації журналів допоможе знайти потрібну інформацію. Особливо вона стане в нагоді, коли записів багато. Фільтрація дозволяє зменшити кількість відображуваних записів журналу, наприклад, для пошуку певних подій, станів або проміжків часу. Щоб відфільтрувати записи журналу, укажіть певні параметри пошуку. Після цього у вікні «Файли журналу» відображатимуться тільки записи, які відповідають параметрам пошуку.

Уведіть ключове слово для пошуку в поле **Знайти текст**. Щоб виокремити результати пошуку, скористайтеся розкривним меню **Знайти в стовпцях**. У розкривному меню **Типи журналів запису** виберіть один запис або кілька записів. Укажіть **проміжок часу**, за який потрібно відобразити результати. Можна також указати додаткові параметри пошуку, наприклад **Тільки слово повністю** або **З урахуванням регістру**.

Знайти текст

Уведіть рядок (слово або частину слова). Відображатимуться тільки ті записи, які містять цей рядок. Інші записи будуть пропущені.

Знайти в стовпцях

Виберіть стовпці, які прийматимуться до уваги під час пошуку. Можна вибрати один стовпчик або кілька стовпчиків, які будуть використовуватися для пошуку.

Типи запису

У розкривному меню виберіть один або кілька типів записів журналу:

- **Діагностика:** запис інформації, необхідної для оптимізації програми, і всіх зазначених вище елементів.
- **Інформаційні записи:** запис інформаційних повідомлень, включно зі сповіщеннями про успішне оновлення, і всіх зазначених вище елементів.
- **Попередження:** запис усіх критичних помилок і попереджувальних повідомлень.
- **Помилки:** запис таких помилок, як "Помилка під час завантаження файлу", і критичних помилок.
- **Критичні помилки:** запис лише критичних помилок (помилка запуску антивірусного захисту,

Проміжок часу

укажіть проміжок часу, за який потрібно відобразити результати.

- **Не вказано** (за замовчуванням): пошук буде здійснюватися по всьому журналу, а не тільки в межах певного проміжку часу.
- **Останній день**

- **Останній тиждень**
- **Останній місяць**
- **Проміжок часу:** можна вказати точний проміжок часу («Від»: і «До:») для фільтрації записів тільки в межах цього проміжку.

Тільки слово повністю

Це дозволяє отримати точніші результати пошуку за конкретними словами, уведеними повністю.

З урахуванням регістру

Увімкніть цей параметр, щоб під час фільтрації враховувалися верхній і нижній регістри літер. Після налаштування параметрів фільтрації/пошуку, натисніть кнопку **ОК**, щоб показати відфільтровані записи журналу, або кнопку **Знайти**, щоб розпочати пошук. Пошук у файлах журналу виконується згори вниз, починаючи з поточного місця (виділеного запису). Пошук зупиняється, коли буде знайдено перший відповідний запис. Для пошуку наступного запису натисніть клавішу **F3**. Щоб уточнити параметри пошуку, клацніть правою кнопкою миші й виберіть пункт **Знайти**.

Налаштування ведення журналу

Налаштувати параметри ведення журналу можна в [головному вікні](#) ESET NOD32 Antivirus.

Натисніть **Параметри > Додаткові параметри > Інструменти > Журнали**. Розділ журналів використовується для налаштування параметрів керування журналами. Для економії місця на жорсткому диску програма автоматично видаляє найстаріші журнали. Для журналів можна налаштувати такі параметри:

Мінімальна детальність журналу – визначає, наскільки докладно описуватимуться події в журналі.

- **Діагностика** – запис інформації, необхідної для оптимізації програми, і всіх зазначених вище елементів.
- **Інформаційні записи:** запис інформаційних повідомлень, включно зі сповіщеннями про успішне оновлення, і всіх зазначених вище елементів.
- **Попередження:** запис усіх критичних помилок і попереджувальних повідомлень.
- **Помилки:** запис таких помилок, як "Помилка під час завантаження файлу", і критичних помилок.
- **Критичні помилки** – запис лише критичних помилок (помилка запуску антивірусного захисту, тощо).



Якщо вибрати рівень детальності діагностики, система реєструватиме всі заблоковані підключення.

У полі **Автоматично видаляти записи, старіші за (дн.)** можна вказати термін зберігання записів журналу, після завершення якого вони видалятимуться автоматично.

Автоматично оптимізувати файли журналу – якщо цей прапорець встановлено, журнали автоматично дефрагментуються, коли відсоток фрагментації перевищує значення, указане в полі **Якщо кількість записів, що не використовуються, перевищує (%)**.

Натисніть **Оптимізувати**, щоб запустити дефрагментацію файлів журналів. Під час її виконання всі порожні записи видаляються, що підвищує ефективність і швидкість обробки журналів. Це вдосконалення особливо помітне, коли журнали містять велику кількість записів.

Параметр **Увімкнути текстовий протокол** дає змогу зберігати журнали у файлах іншого формату окремо від розділу [Журнали](#):

- **Цільовий каталог:** каталог, у якому зберігатимуться файли журналів (тільки для файлів TXT/CSV). Кожен розділ журналів містить окремий файл із попередньо визначеним іменем (наприклад, virlog.txt в розділі **Виявлені об'єкти**, якщо для збереження журналів використовується звичайний текстовий формат).
- **Тип:** якщо вибрати формат **Текст**, журнали зберігатимуться в текстовому файлі, а дані розділятимуться знаками табуляції. Те саме стосується формату **CSV** (файл із роздільниками-комами). Якщо вибрати параметр **Подія**, дані зберігатимуться в журнали подій Windows (їх можна переглянути за допомогою засобу перегляду подій на панелі керування), а не у файлі.
- **Видалити всі файли журналу:** видаляє всі збережені журнали, вибрані в розкритому меню **Тип** у цей момент. Відобразиться сповіщення про успішне видалення журналів.



Щоби прискорити вирішення деяких проблем, ESET може попросити вас надати копії журналів, збережених на комп'ютері. Інструмент ESET Log Collector полегшує збір потрібної інформації. Докладніше про ESET Log Collector можна прочитати у відповідній статті [бази знань ESET](#).

Запущені процеси

Модуль стеження за запущеними процесами відображає інформацію про програми або процеси на комп'ютері та є засобом негайного й постійного інформування ESET про нові загрози. ESET NOD32 Antivirus надає детальну інформацію про запущені процеси, захищаючи користувачів за допомогою технології [ESET LiveGrid®](#).

NOD32 ANTIVIRUS

ESET HOME

← Запущені процеси

Головна

Сканування комп'ютера

Оновлення

Інструменти

Параметри

Довідка та підтримка

У цьому вікні відображається список вибраних файлів із додатковою інформацією від ESET LiveGrid®. Окрім цього, зазначається рівень репутації, кількість користувачів і час першого виявлення.

Репутація	Процес	PID	Кількість корис...	Час виявлен...	Назва програми
★★★★★★	smss.exe	356	★★★★★★	3 місяці тому	Microsoft® Windows® Oper...
★★★★★★	csrss.exe	452	★★★★★★	1 рік тому	Microsoft® Windows® Oper...
★★★★★★	wininit.exe	524	★★★★★★	1 місяць тому	Microsoft® Windows® Oper...
★★★★★★	services.exe	572	★★★★★★	6 місяців тому	Microsoft® Windows® Oper...
★★★★★★	winlogon.exe	616	★★★★★★	1 місяць тому	Microsoft® Windows® Oper...
★★★★★★	lsass.exe	660	★★★★★★	6 місяців тому	Microsoft® Windows® Oper...
★★★★★★	svchost.exe	748	★★★★★★	1 рік тому	Microsoft® Windows® Oper...
★★★★★★	fontdrvhost.exe	760	★★★★★★	1 місяць тому	Microsoft® Windows® Oper...
★★★★★★	dwm.exe	980	★★★★★★	6 місяців тому	Microsoft® Windows® Oper...
★★★★★★	vboxservice.exe	1412	★★★★	1 рік тому	Oracle VM VirtualBox Guest A...
★★★★★★	wudfhost.exe	1472	★★★★★★	1 рік тому	Microsoft® Windows® Oper...

Шлях:

c:\windows\system32\smss.exe

Розмір:

152.3 КБ

Опис:

Windows Session Manager

Компанія:

Microsoft Corporation

Версія:

10.0.19041.1 (WinBuild.160101.0800)

Продукт:

Microsoft® Windows® Operating System

Дата створення:

5/12/2021 12:02:49 AM

Дата змінення:

5/12/2021 12:02:49 AM

Приховати подробиці

Репутація: у більшості випадків ESET NOD32 Antivirus і технологія ESET LiveGrid® призначають рівні ризику об'єктам (файлам, процесам, розділам реєстру тощо), використовуючи ряд евристичних правил, за якими досліджуються характеристики кожного об'єкта й потім визначається потенціал шкідливої активності. На основі цієї евристики об'єктам призначається певний рівень ризику — від 1 — безпечний (зелений) до 9 — небезпечний (червоний).

Процес – ім'я процесу або програми, запущеної на комп'ютері. Усі запущені процеси доступні для перегляду також у диспетчері завдань Windows. Щоб відкрити диспетчер завдань, клацніть правою кнопкою миші в пустій області на панелі завдань і виберіть пункт **Диспетчер завдань** або натисніть на клавіатурі **Ctrl + Shift + Esc**.

i Відомі програми з позначкою Безпечні (зелений) без сумніву безпечні (зазначені в білому списку), і з метою покращення ефективності вони не скануватимуться.

PID – числовий ідентифікатор процесу, який можна використовувати як параметр у викликах різноманітних функцій (наприклад, для регулювання пріоритетності процесів).

Кількість користувачів: кількість користувачів, які працюють із певною програмою. Збір цієї інформації виконує технологія ESET LiveGrid®.

Час виявлення: час, коли програму було виявлено технологією ESET LiveGrid®.

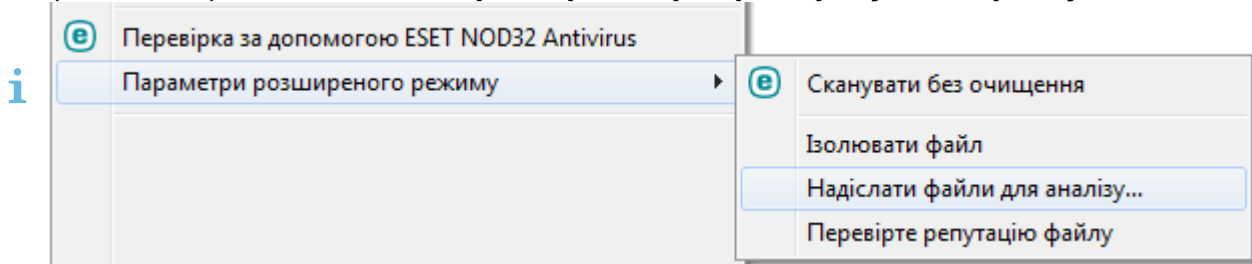
i Програми з позначкою Невідомі (червоний) не обов'язково шкідливі. Зазвичай таку позначку отримують нові програми. Якщо ви не впевнені, чи шкідливий певний файл, можна [надіслати його на аналіз](#) у дослідницьку лабораторію ESET. Якщо буде визначено, що файл шкідливий, ми додамо засоби для його виявлення в наступне оновлення.

Назва програми: ім'я, присвоєне програмі або процесу.

Натисніть програму, щоб переглянути вказані нижче відомості про неї.

- **Шлях:** розміщення програми на комп'ютері.
- **Розмір:** розмір файлу в кілобайтах (КБ) або мегабайтах (МБ).
- **Опис:** характеристики файлу на основі його опису операційною системою.
- **Компанія:** ім'я постачальника або прикладного процесу.
- **Версія:** інформація від видавця програми.
- **Продукт:** ім'я програми та/або фірмове найменування.
- **Дата створення/Дата змінення** – дата й час створення чи змінення.

Також можна перевірити репутацію файлів, які не є запущеними програмами або процесами. Для цього у файловому провіднику клацніть правою кнопкою миші потрібний файл і виберіть **Додаткові параметри > Перевірити репутацію файлу**.



Звіт про безпеку

Ця функція забезпечує короткий огляд статистичних даних для наведених нижче категорій.

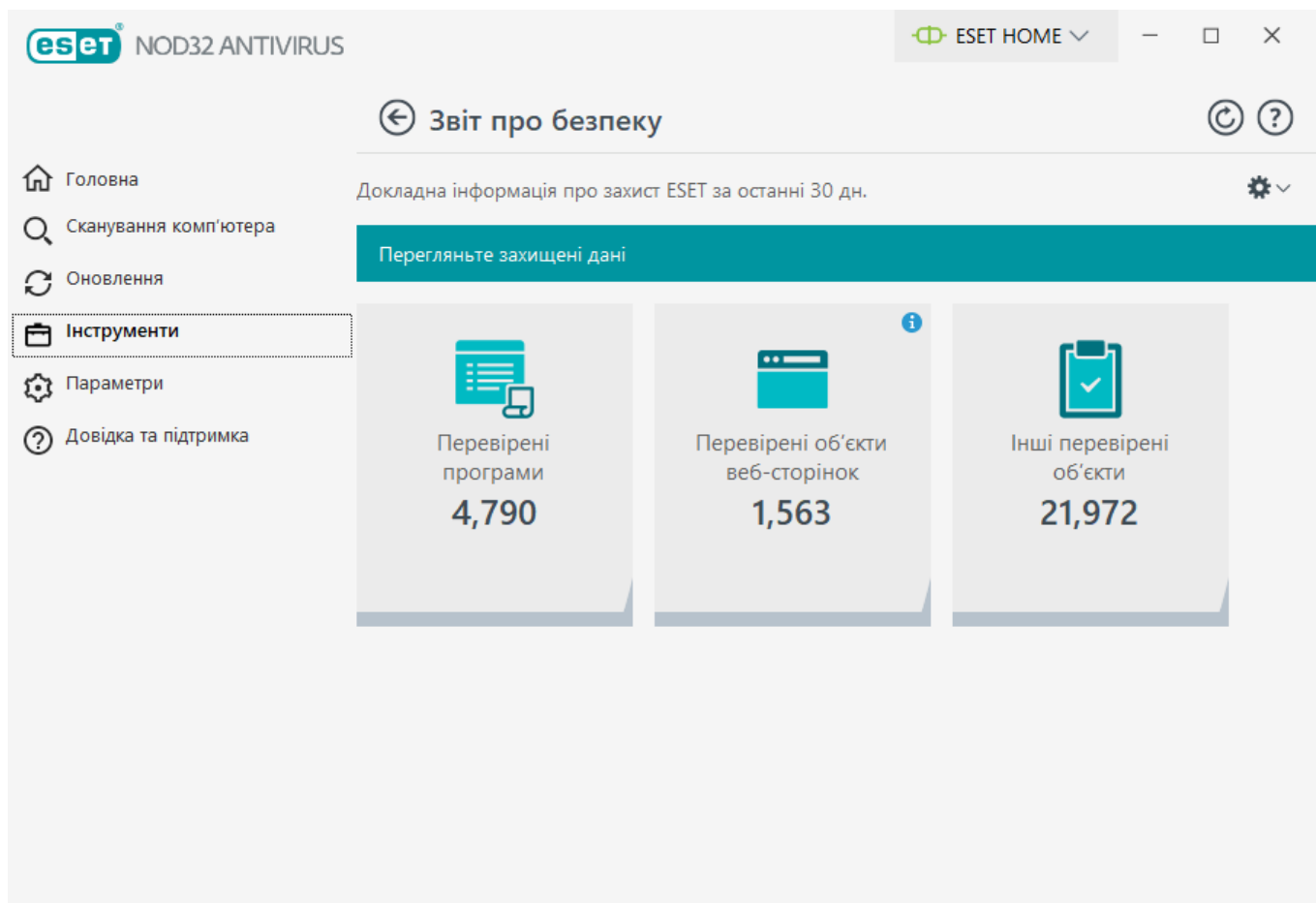
- **Заблоковані веб-сторінки:** відображає кількість заблокованих веб-сторінок (URL-адресу вказано в чорному списку потенційно небажаних програм, фішингових веб-сайтів, зламаних маршрутизаторів, небезпечних IP-адрес або ненадійних сертифікатів).
- **Інфіковані об'єкти, виявлені в електронній пошті:** відображає кількість таких [об'єктів](#).
- **Виявлені потенційно небажані програми:** відображає кількість [потенційно небажаних програм](#).
- **Перевірені документи:** відображає кількість таких документів.
- **Перевірені програми:** відображає кількість просканиваних виконуваних об'єктів.
- **Інші перевірені об'єкти:** відображає кількість таких об'єктів.
- **Перевірені об'єкти веб-сторінок:** відображає кількість перевірених об'єктів веб-сторінок.

- **Перевірені об'єкти електронних листів:** відображає кількість таких об'єктів.

Порядок відображення цих категорій визначається їх числовим значенням (від найвищого до найнижчого). Категорії з нульовими значеннями не відображаються. Натисніть "**Розгорнути**", щоб відобразити приховані категорії.

Після ввімкнення функція більше не відображатиметься у звіті про безпеку як неактивна.

Натисніть значок шестірні у верхньому правому куті, щоб **увімкнути чи вимкнути сповіщення звіту про безпеку** або вибрати період, за який збиратимуться дані (за останні 30 днів або з моменту активації продукту). Якщо ESET NOD32 Antivirus інстальовано менше ніж 30 днів тому, можна вибрати лише ту кількість днів, яка минула з моменту інсталяції. За замовчуванням вибрано 30 днів.



Скинути дані: очищає всю статистику й видаляє наявні дані звіту про безпеку. Цю дію необхідно підтверджувати, якщо не знято прапорець **Запитувати перед скиданням даних статистики** в меню **Додаткові параметри > Сповіщення > Інтерактивні сповіщення > Повідомлення про підтвердження > Редагувати**.

ESET SysInspector

ESET SysInspector — це програма, яка ретельно перевіряє комп'ютер і збирає докладну інформацію про такі системні компоненти, як драйвери та програми, мережеві підключення й важливі розділи реєстру. Крім того, вона оцінює рівень ризику для кожного компонента. Ця інформація може допомогти виявити причину підозрілого поведіння системи, яке може бути спричинено несумісністю програмного забезпечення або обладнання чи проникненням

шкідливої вірусної програми. Інструкції з використання ESET SysInspector див. в [онлайн-довідці ESET SysInspector](#).

У вікні ESET SysInspector відображається така інформація про журнали:

- **Час:** час створення журналу.
- **Коментар:** короткий коментар.
- **Користувач:** ім'я користувача, який створив журнал.
- **Статус:** статус створення журналу.

Можливі такі дії:

- **Показати:** відкриває вибраний журнал у ESET SysInspector. Також відповідний файл журналу можна натиснути правою кнопкою миші й вибрати **Показати** в контекстному меню.
- **Порівняти:** порівняти два наявні журнали.
- **Створити:** створити новий журнал. Перш ніж відкривати журнал, дочекайтеся, поки ESET SysInspector завершить його створення (статус журналу зміниться на **Створено**).
- **Видалити:** видалити вибрані журнали зі списку.

Для одного або кількох вибраних файлів журналу в контекстному меню доступні такі елементи:

- **Показати:** відкрити вибраний журнал в ESET SysInspector (аналогічно подвійному натисканню журналу).
- **Порівняти:** порівняти два наявні журнали.
- **Створити:** створити новий журнал. Перш ніж відкривати журнал, дочекайтеся, поки ESET SysInspector завершить його створення (статус журналу зміниться на **Створено**).
- **Видалити:** видалити вибрані журнали зі списку.
- **Видалити все:** видалити всі журнали.
- **Експорт:** експортувати файл у журнал .xml або стиснутий .xml. Журнал експортується в каталог C:\ProgramData\ESET\ESET Security\SysInspector.

Розклад

Інструмент "Розклад" керує запланованими завданнями та запускає їх із попередньо визначеною конфігурацією та заданими властивостями.

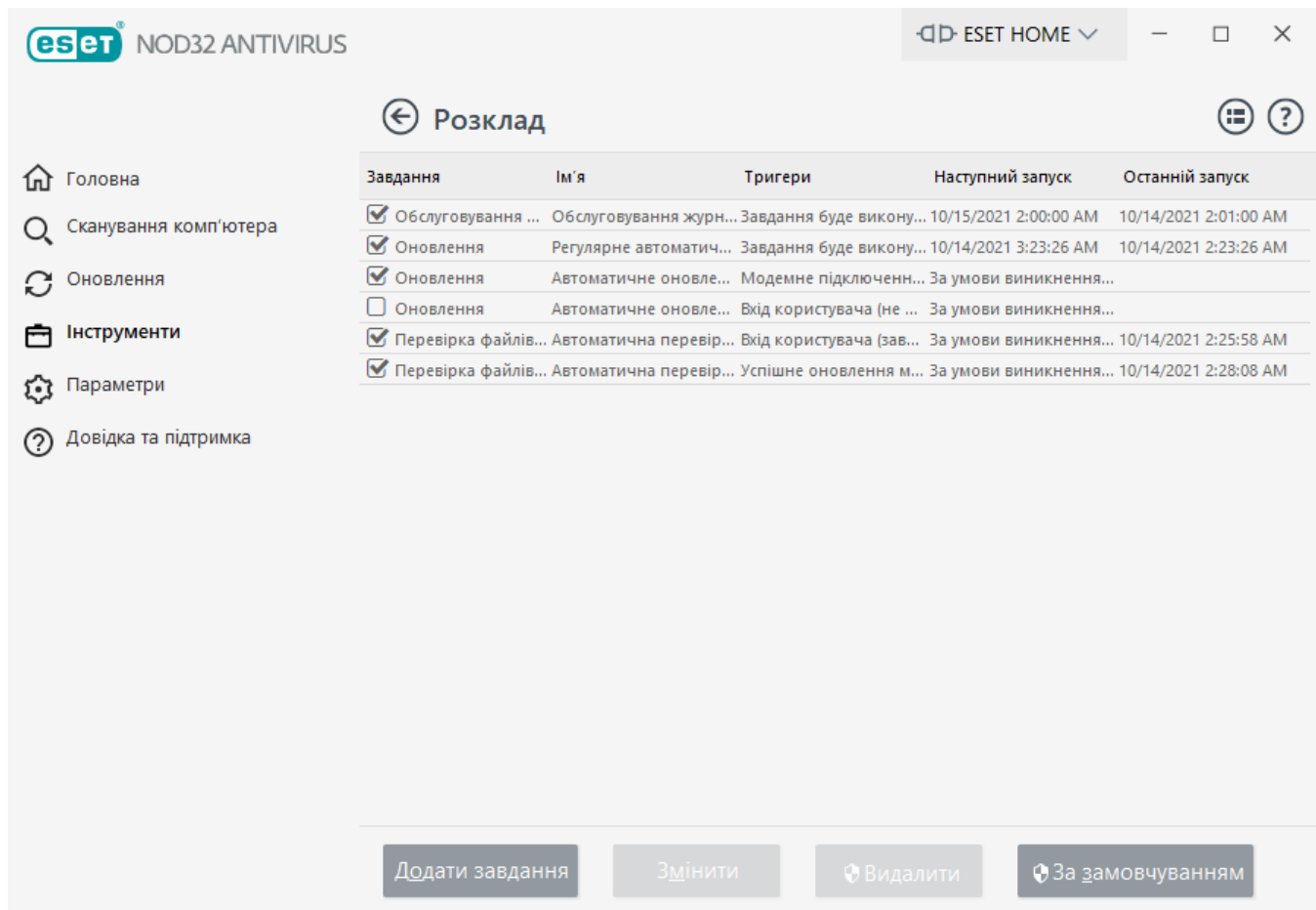
Щоб відкрити планувальник, у [головному вікні програми](#) ESET NOD32 Antivirus клацніть **Інструменти > Розклад**. У розділі **Розклад** міститься список усіх завдань і властивостей конфігурацій, зокрема такі параметри, як дата, час і профіль сканування.

Планувальник використовується для планування таких завдань: оновлення модулів, сканування за розкладом, сканування файлів під час запуску системи й обслуговування журналів. Завдання можна додавати або видаляти безпосередньо з головного вікна планувальника (натисніть у нижній частині **Додати завдання** або **Видалити**). Щоб відновити список запланованих завдань за замовчуванням і видалити всі зміни, натисніть **За замовчуванням**. Клацніть правою кнопкою миші в будь-якій частині вікна, щоб виконати такі дії: відобразити детальну інформацію, виконати завдання негайно, додати нове завдання або видалити наявне. Використовуйте прапорці на початку кожного запису, щоб активувати або вимкнути завдання.

За замовчуванням у вікні **Розклад** відображаються такі завдання:

- **Обслуговування журналу**
- **Регулярне автоматичне оновлення**
- **Автоматичне оновлення після встановлення модемного підключення**
- **Автоматичне оновлення після входу користувача в систему**
- **Автоматична перевірка файлів під час запуску системи** (після входу користувача в систему)
- **Автоматична перевірка файлів під час запуску** (після успішного оновлення обробника виявлення)

Щоб змінити конфігурацію наявного запланованого завдання (як стандартного, так і користувацького), клацніть завдання правою кнопкою миші та виберіть команду **Змінити** або виберіть потрібне завдання й натисніть **Змінити**.



Додавання нового завдання

1. Натисніть **Додати завдання** в нижній частині вікна.
2. Укажіть ім'я завдання.
3. Виберіть потрібне завдання з розкривного меню:
 - **Запуск зовнішньої програми:** планування запуску зовнішньої програми.
 - **Обслуговування журналу** – окрім усього іншого, у журналах також містяться залишки видалених записів. Це завдання регулярно оптимізовує записи в журналах для підвищення ефективності роботи.
 - **Перевірка файлів під час запуску системи:** перевірка файлів, що запускаються автоматично під час завантаження системи або входу до облікового запису.
 - **Створити знімок стану системи:** створення знімка системи засобом [ESET SysInspector](#), який збирає докладну інформацію про системні компоненти (наприклад, драйвери, програми) й оцінює рівень ризику для кожного з них.
 - **Сканування комп'ютера за вимогою:** сканування файлів і папок на комп'ютері.
 - **Оновлення** – планування завдання оновлення, у рамках якого оновлюються модулі програми.
4. Клацніть повзунок **Увімкнено**, щоб активувати завдання (це можна зробити пізніше,

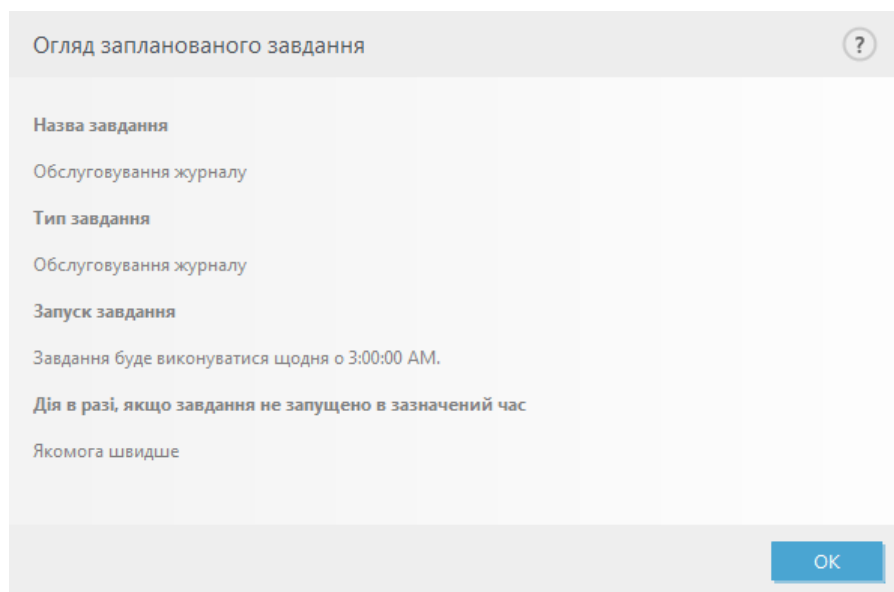
установивши/знявши прапорець у списку запланованих завдань), клацніть **Далі** й виберіть один із часових параметрів:

- **Один раз:** завдання буде виконано у визначений день і час.
- **Багаторазово:** завдання буде виконуватися багаторазово через зазначений інтервал часу.
- **Щодня:** завдання буде виконуватися багаторазово кожен день у визначений час.
- **Щотижня:** завдання буде виконуватись у вибраний день і час.
- **За умови виникнення події:** завдання буде виконано, якщо відбудеться зазначена подія.

5. Виберіть **Не запускати завдання, якщо комп'ютер працює від батареї**, щоб зменшити використання системних ресурсів, коли портативний комп'ютер працює від батареї. Завдання буде виконуватись у вибраний день і час відповідно до параметрів розділу **Запуск завдання**. Якщо завдання не вдалося запустити в заданий час, можна зазначити, коли його необхідно виконати наступного разу:

- **Під час наступного запланованого виконання**
- **Якомога швидше**
- **Негайно, якщо час з останнього запуску перевищує зазначений інтервал (у годинах):** час, що минув із моменту першого пропущеного запуску завдання. Якщо цей час перевищено, завдання запуститься негайно. Налаштуйте час за допомогою лічильника нижче.

Щоб переглянути інформацію про заплановане завдання, натисніть його правою кнопкою миші й виберіть **Показати деталі задачі**.



Параметри сканування за розкладом

У цьому вікні можна вказати розширені параметри для запланованої перевірки комп'ютера.

Щоб просканувати об'єкти, але не виконувати очистку, натисніть **Додаткові параметри** й виберіть **Сканувати без очищення**. Історія сканування зберігається в журналі сканування.

Якщо вибрано параметр **Ігнорувати виключення**, усі файли з розширеннями, які раніше було виключено зі сканування, перевірятимуться без винятку.

У розкритому меню можна вибрати дію, що виконуватиметься автоматично після завершення сканування:

- **Нічого не робити:** після завершення сканування жодна дія не виконується.
- **Завершити роботу:** комп'ютер вимикається після завершення сканування.
- **Перезавантажити:** після завершення сканування всі відкриті програми закриваються, а комп'ютер перезавантажується.
- **Перезавантажити за необхідності:** комп'ютер перезавантажується, лише якщо потрібно завершити очищення виявлених загроз.
- **Примусове перезавантаження:** після завершення сканування всі відкриті програми закриваються, а комп'ютер перезавантажується без втручання користувача.
- **Примусово перезавантажити за потреби:** комп'ютер перезавантажується, лише якщо потрібно завершити очищення виявлених загроз.
- **Режим сну:** сеанс зберігається, а комп'ютер переводиться в режим зниженого енергоспоживання, щоб можна було швидко відновити роботу.
- **Режим глибокого сну:** всі запущені в оперативній пам'яті процеси зберігаються в окремому файлі на жорсткому диску. Комп'ютер вимикається, проте після запуску він відновлює попередній робочий стан.

i Дії **Сон** або **Глибокий сон** доступні залежно від налаштувань живлення та режиму сну в операційній системі або можливостей комп'ютера чи ноутбука. Зверніть увагу, що в режимі сну комп'ютер усе одно працює. Базові функції продовжують виконуватися, споживаючи енергію батареї (якщо комп'ютер живиться від неї). Щоб зберегти заряд, наприклад, коли ви залишили місце роботи, рекомендується користуватися режимом глибокого сну.

Виберіть параметр **Сканування не може бути скасовано**, щоб користувачі без відповідних повноважень не могли переривати сканування, що виконуються після сканування.

Виберіть параметр **Перевірка може бути зупинена користувачем на (хв)**, щоб надати деяким користувачам можливість призупиняти сканування комп'ютера на визначений період часу.

Див. також [Хід сканування](#).

Огляд запланованого завдання

У цьому діалоговому вікні відображаються докладні відомості про вибране заплановане завдання. Щоб переглянути їх, двічі клацніть спеціальне заплановане завдання або натисніть його правою кнопкою миші й виберіть **Показати деталі задачі**.

Відомості про завдання

Введіть **Ім'я завдання** й виберіть один із параметрів **Тип завдання**, після чого натисніть **Далі**.

- **Запуск зовнішньої програми:** планування запуску зовнішньої програми.
- **Обслуговування журналу** – окрім усього іншого, у журналах також містяться залишки видалених записів. Це завдання регулярно оптимізовує записи в журналах для підвищення ефективності роботи.
- **Перевірка файлів під час запуску системи:** перевірка файлів, що запускаються автоматично під час завантаження системи або входу до облікового запису.
- **Створити знімок стану системи:** створення знімка системи засобом [ESET SysInspector](#), який збирає докладну інформацію про системні компоненти (наприклад, драйвери, програми) й оцінює рівень ризику для кожного з них.
- **Сканування комп'ютера за вимогою:** сканування файлів і папок на комп'ютері.
- **Оновлення** – планування завдання оновлення, у рамках якого оновлюються модулі програми.

Часовий параметр завдання

Завдання буде виконуватися багаторазово через зазначений інтервал часу. Виберіть один із часових параметрів:

- **Один раз:** завдання буде виконано один раз у зазначений день і час.
- **Багаторазово:** завдання буде виконуватися багаторазово через зазначений інтервал часу (у годинах).
- **Щодня:**– завдання буде виконуватися кожен день у визначений час.
- **Щотижня:** завдання буде виконуватись один або кілька разів на тиждень у зазначені дні та в заданий час.
- **За умови виникнення події:** завдання буде виконано, якщо відбудеться зазначена подія.

Не запускати завдання, якщо комп'ютер працює від батареї: завдання не виконуватиметься, якщо в момент його запуску комп'ютер працює від батареї. Це стосується також комп'ютерів, які працюють від джерела безперебійного живлення.

Часовий параметр завдання: одноразово

Запуск завдання: вибране завдання буде виконано один раз у зазначений день і час.

Часовий параметр завдання: щодня

Завдання буде виконуватися кожен день у визначений час.

Часовий параметр завдання: щотижня

Завдання буде виконуватися кожен тиждень у зазначені дні та в заданий час.

Часовий параметр завдання: за умови виникнення події

Завдання буде ініційовано однією з таких подій:

- кожного разу під час запуску комп'ютера;
- кожного дня під час першого запуску комп'ютера;
- Модемне підключення до Інтернету/VPN
- Успішне оновлення модуля
- Успішне оновлення продукту
- вхід користувача;
- виявлення загрози.

Під час планування завдання, ініційованого подією, можна зазначити мінімальний інтервал між двома процесами виконання завдання. Наприклад, якщо ви входите в обліковий запис на комп'ютері кілька разів протягом дня, виберіть 24 години, щоб завдання виконувалося лише під час першого входу до системи, а потім – наступного дня.

Невиконане завдання

Завдання пропускатиметься, якщо комп'ютер працює від батареї або вимкнений. Виберіть час виконання пропущеного завдання, скориставшись одним із наведених нижче параметрів, і натисніть **Далі**.

- **Під час наступного запланованого виконання:** завдання буде виконуватися, якщо комп'ютер увімкнено в той час, коли заплановано наступне виконання.
- **Якомога швидше:** завдання буде виконуватися, коли комп'ютер буде ввімкнено.

- **Негайно, якщо з часу останнього запланованого запуску пройшло більше (години):** час, що минув із моменту першого пропущеного запуску завдання. Якщо цей час перевищено, завдання запуститься негайно.

Негайно, якщо час з часу останнього запланованого запуску пройшло більше (години) – приклади

Для прикладу завдання налаштовано виконання щогодини. Вибирано параметр **Негайно, якщо час з часу останнього запланованого запуску пройшло більше (години)**, а

✓ для відповідного проміжку часу задано тривалість дві години. Завдання запускається о 13:00, а після його завершення комп'ютер переходить у режим сну:

- Комп'ютер вийде з режиму сну о 15:30. Запуск завдання вперше пропущено о 14:00. З 14:00 минуло лише 1,5 години, тому завдання буде запущено о 16:00.
- Комп'ютер вийде з режиму сну о 16:30. Запуск завдання вперше пропущено о 14:00. З 14:00 минуло дві з половиною години, тому завдання запуститься негайно.

Відомості про завдання: оновлення

Щоб здійснювати оновлення програми із двох серверів оновлень, потрібно створити два різних профілі оновлення. Якщо за допомогою першого профілю не вдається завантажити файли оновлення, програма автоматично переключається на альтернативний профіль. Це зручно, наприклад, у разі роботи на портативних комп'ютерах, які зазвичай оновлюються із сервера оновлень у локальній мережі, але їхні власники часто підключаються до Інтернету з інших мереж. Якщо перший профіль не може завантажити оновлення, другий автоматично завантажить файли оновлення із серверів оновлень ESET.

Відомості про завдання: запуск програми

У цьому завданні можна планувати роботу зовнішньої програми.

Відомості про завдання

?

Запустити програму

Програма:

C:\Program Files\Internet Explorer\iexplore.exe

×

Робоча папка:

Internet Explorer

×

Параметри:

www.eset.com

Назад

Завершити

Скасувати

Програма: виберіть виконуваний файл у дереві каталогів, натисніть кнопку ... або введіть шлях уручну.

Робоча папка: укажіть робочий каталог зовнішньої програми. Усі тимчасові файли вибраної програми створюватимуться в цьому каталозі.

Параметри: параметри командного рядка для програми (необов'язково).

Натисніть **Готово**, щоб застосувати завдання.

Засіб очищення системи

Засіб очищення системи – це інструмент, який допомагає відновити працездатний стан комп'ютера після очищення загрози. Шкідливе програмне забезпечення може вимикати такі утиліти системи, як редактор реєстру, диспетчер завдань або оновлення Windows. Засіб очищення системи одним натисканням дозволяє відновити значення за замовчуванням і параметри системи.

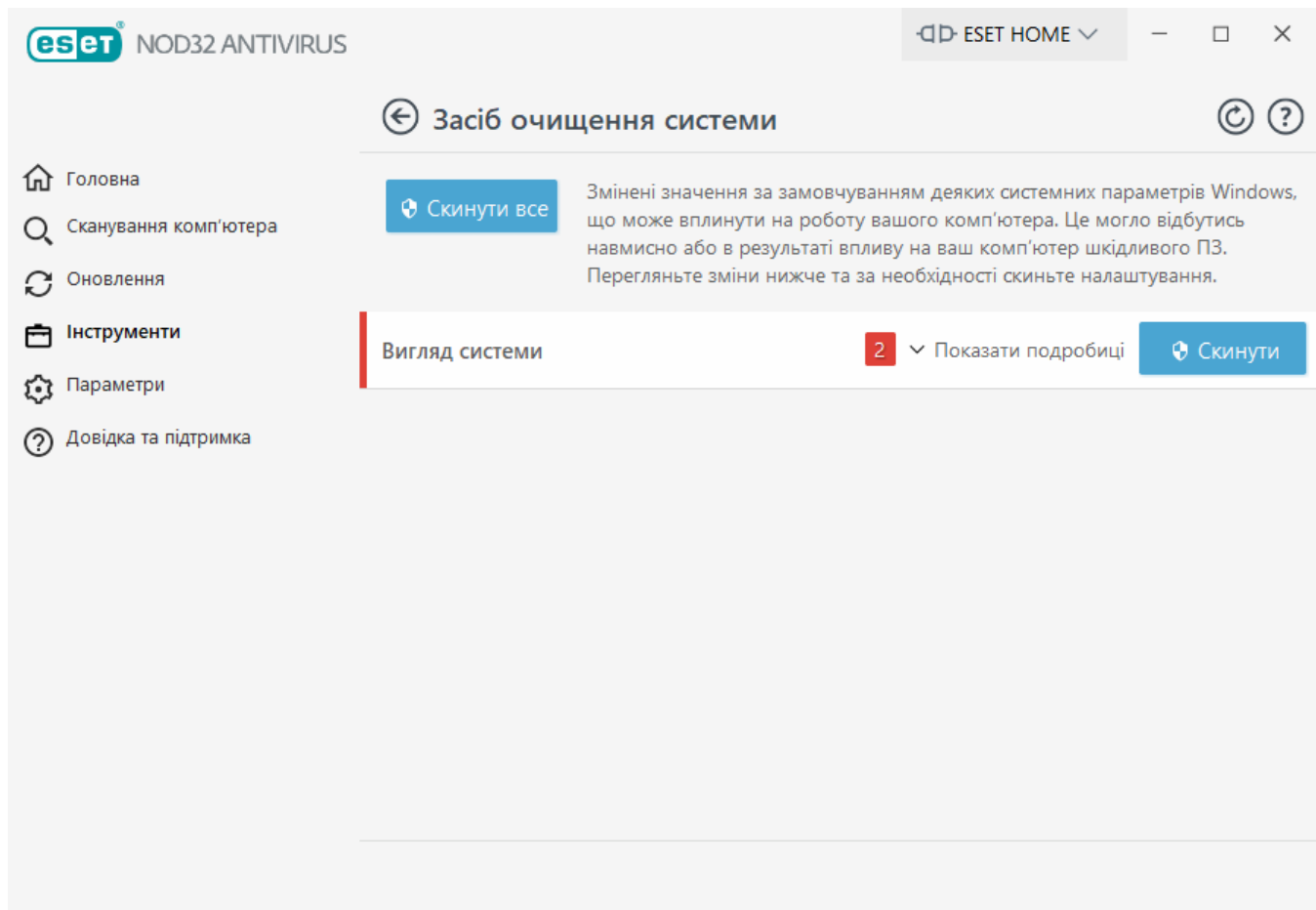
Засіб очищення системи повідомляє про проблеми в таких п'яти категоріях параметрів:

- **Параметри безпеки:** зміни параметрів, які можуть підвищити вразливість вашого комп'ютера, наприклад зміни параметрів Windows Update.
- **Параметри системи:** зміни в налаштуваннях системи, які можуть змінити поведінку комп'ютера, наприклад зміни асоціації файлів.
- **Вигляд системи:** налаштування, які можуть змінювати зовнішній вигляд системи, наприклад фонове зображення робочого стола.
- **Вимкнені функції:** деякі важливі функції та програми, які можуть бути вимкнені.
- **Відновлення системи Windows:** налаштування функції відновлення системи Windows, які дають змогу повернути систему до попереднього стану.

Очищення системи можна ініціювати в таких випадках:

- у разі виявлення загрози;
- у разі натискання користувачем кнопки **Скинути**.

Якщо потрібно, ви можете переглянути зміни й скинути налаштування.



i Застосовувати функції засобу очищення системи може лише користувач із правами адміністратора.

ESET SysRescue Live

ESET SysRescue Live — це безкоштовна утиліта, яка дозволяє створити завантажувальний компакт-диск (DVD-диск) або USB-носій. Ви можете завантажити інфікований комп'ютер із компакт-диска, щоб просканувати його на наявність шкідливого програмного забезпечення й очистити інфіковані файли.

Головна перевага утиліти ESET SysRescue Live полягає в тому, що вона запускається незалежно від базової операційної системи, проте має прямий доступ до диска й усієї файлової системи. Це дає змогу видаляти загрози, які неможливо видалити за звичайних умов (наприклад, коли операційну систему запущено тощо).

- [Інтерактивна довідка ESET SysRescue Live](#)

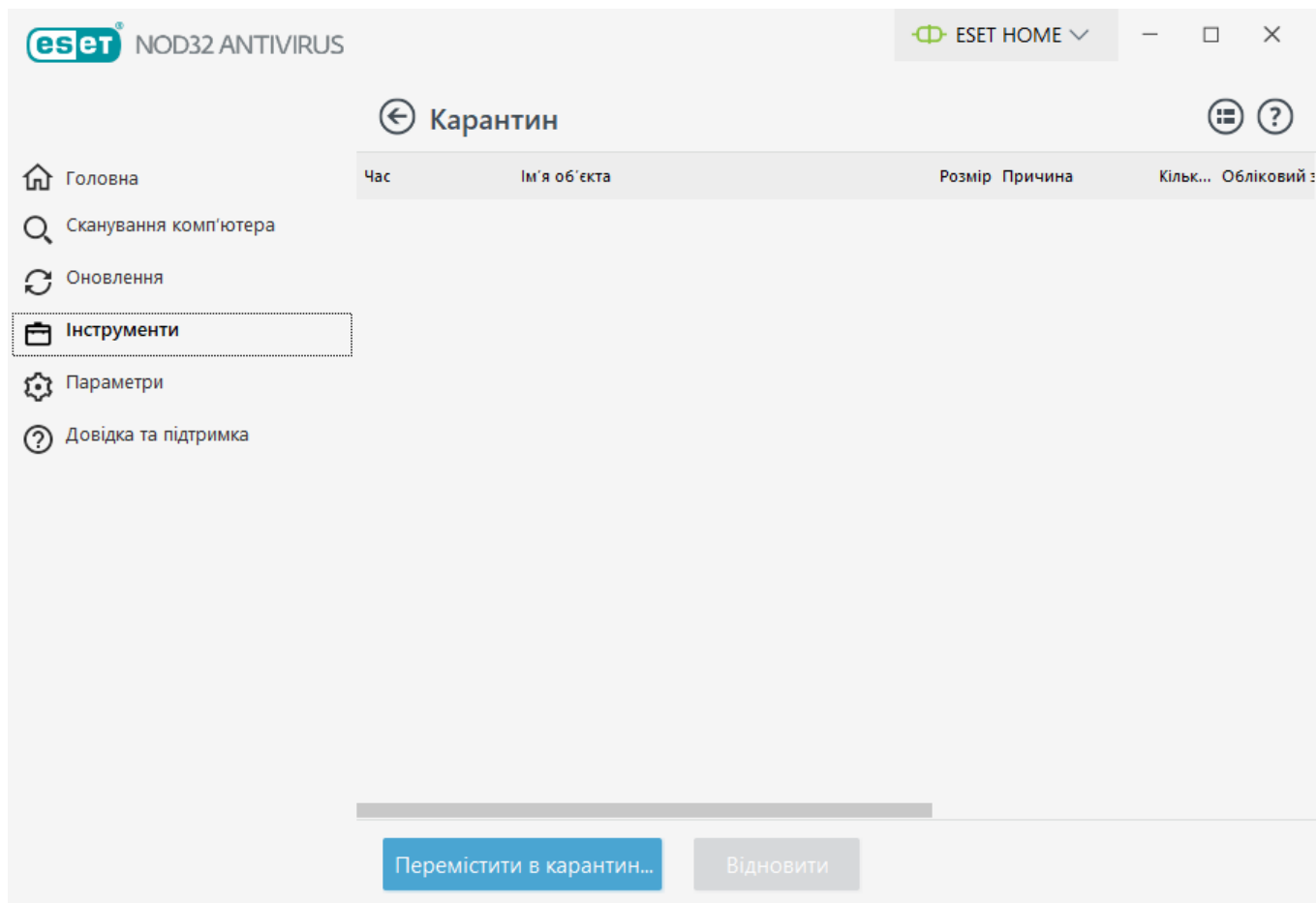
Карантин

Основна функція карантину — безпечно ізолювати виявлені об'єкти (наприклад, шкідливе програмне забезпечення, інфіковані файли або потенційно небажані програми).

Щоб відкрити карантин, у [головному вікні програми](#) ESET NOD32 Antivirus натисніть **Інструменти** > **Карантин**.

Файли, які зберігаються в папці карантину, можна переглядати в таблиці, де вказано:

- дату й час переміщення в карантин;
- шлях до вихідного місця розташування інфікованого файлу;
- розмір у байтах;
- причину (наприклад, об'єкт додано користувачем);
- кількість виявлених об'єктів (наприклад, багаторазове виявлення одного файлу, або якщо це архів із кількома загрозами).



Карантинування файлів

ESET NOD32 Antivirus автоматично переміщує в карантин видалені файли (якщо ви не скасували цю опцію у [вікні тривоги](#)).

Додаткові файли можна перемістити в карантин, якщо:

- а.їх не вдається очистити;
- б.вони небезпечні або їх рекомендується видалити;
- с.їх випадково виявлено програмою ESET NOD32 Antivirus;
- д.файл поводиться підозріло, але його не виявляє [сканер](#).

Перемістити файл у карантин можна кількома способами.

а. За допомогою перетягування – для цього вручну натисніть файл і, не відпускаючи кнопку миші, перемістіть курсор у позначену область, а потім відпустіть кнопку, щоб програма перемістилася на передній план. Щоб просканувати файл або папку вручну, натисніть відповідний елемент і, не відпускаючи кнопку миші, перемістіть курсор у позначену область, а потім відпустіть кнопку. Після цього програма переміститься на передній план.

б. Натисніть файл правою кнопкою миші та виберіть пункт **Додаткові параметри > Помістити файл на карантин**.

с. У вікні **Карантин** натисніть **Перемістити в карантин**.

д. Це також можна зробити за допомогою контекстного меню: натисніть правою кнопкою миші у вікні **Карантин** і виберіть **Карантин**.

Відновлення з карантину

Файли з карантину також можна відновити й повернути до початкових місць розташування.

- Для цього натисніть правою кнопкою файл у карантині та виберіть опцію **Відновити** в контекстному меню.
- Якщо файл позначено як [потенційно небажану програму](#), доступна опція **Відновити та виключити з перевірки**. Також див. [Виключення](#).
- У контекстному меню також доступна опція **Відновити в**, за допомогою якої користувач може відновити файли в інше місце, а не туди, звідки їх було видалено.
- У деяких випадках функція відновлення недоступна, наприклад, якщо файли знаходилися на мережевому диску, доступному лише для читання.

Видалення з карантину

Натисніть правою кнопкою миші відповідний елемент і виберіть **Видалити з карантину** або виберіть потрібний елемент і натисніть клавішу **Delete** на клавіатурі. Окрім того, можна виділяти й видаляти кілька елементів одночасно. Видалені елементи остаточно видаляються з вашого пристрою й карантину.

Відправка на аналіз файлів із карантину

Якщо ви помістили в карантин підозрілий файл, який програма не виявила, або файл помилково розпізнано як інфікований (наприклад, під час евристичного аналізу коду) і переміщено в карантин, [надішліть файл до дослідницької лабораторії ESET](#). Щоб відправити файл, клацніть його правою кнопкою миші та виберіть **Відправити на аналіз** у контекстному меню.

Опис об'єкта

Правою кнопкою миші натисніть елемент і виберіть параметр **Опис об'єкта**, щоб відкрити

енциклопедію загроз ESET, у якій міститься докладна інформація про небезпеки й симптоми зафіксованих загроз.

Ілюстровані інструкції

Указані нижче статті бази знань можуть бути доступними тільки англійською мовою:

- [Відновлення файлу з карантину в ESET NOD32 Antivirus](#)
- [Видалення файлу з карантину в ESET NOD32 Antivirus](#)
- [Продукт ESET повідомив про підозрілий об'єкт. Що робити?](#)

Не вдалося перемістити в карантин

Нижче наведено причини, через які певні файли не можна перемістити в карантин.

- **У вас немає дозволів на читання** – ви не можете переглядати вміст файлу.
- **У вас немає дозволів на запис** – ви не можете змінювати вміст файлу, наприклад додавати новий вміст або видаляти наявний.
- **Файл, який ви намагаєтеся помістити на карантин, занадто великий** – потрібно зменшити розмір файлу.

Коли з'являється повідомлення про помилку "Не вдалося помістити на карантин", натисніть **Додаткова інформація**. Відкриється вікно списку помилок карантину. У ньому буде вказано назву файлу та причину, чому його не можна помістити на карантин.

Проксі-сервер

У великих LAN проксі-сервер може керувати підключенням комп'ютерів до Інтернету. У такому випадку потрібно визначити наведені нижче параметри. Інакше програма не зможе автоматично оновлюватися. У програмі ESET NOD32 Antivirus параметри проксі-сервера доступні у двох розділах дерева додаткових параметрів.

По-перше, параметри проксі-сервера можна вказати в розділі **Додаткові параметри** меню **Інструменти > Проксі-сервер**. Указані на цьому рівні параметри визначають загальні налаштування проксі-сервера для всіх функцій ESET NOD32 Antivirus. Визначені тут параметри використовуватимуться всіма модулями, які вимагають підключення до Інтернету.

Щоб визначити параметри проксі-сервера на цьому рівні, установіть прапорець **Використовувати проксі-сервер**, після чого введіть його адресу в полі **Проксі-сервер** і номер порту в полі **Порт**.

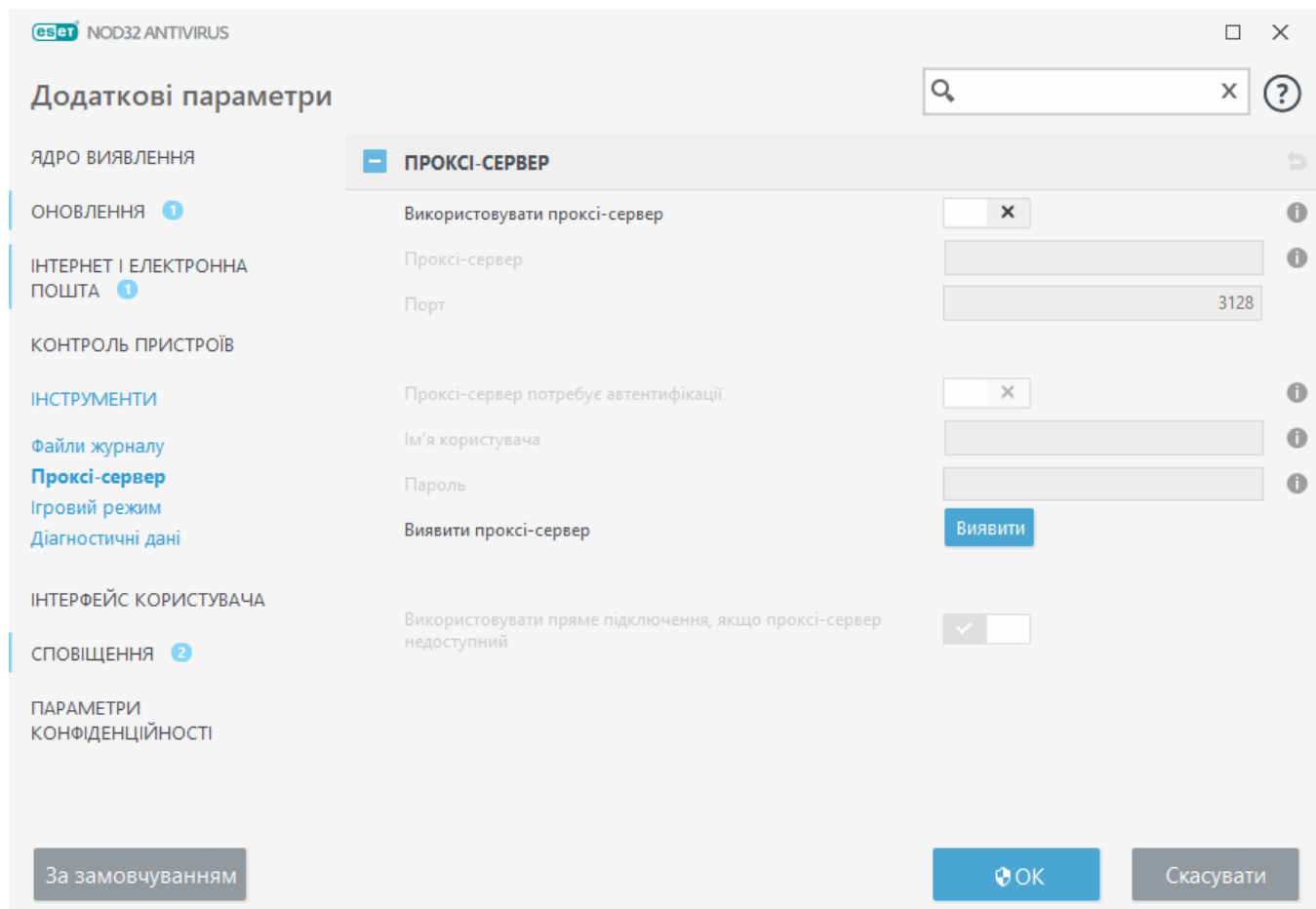
Якщо підключення за допомогою проксі-сервера вимагає автентифікації, установіть прапорець **Проксі-сервер потребує автентифікації** та введіть дійсні дані в полях **Ім'я користувача** й **Пароль**. Клацніть **Виявити проксі-сервер**, щоб налаштування проксі-сервера виявлялись і застосовувались автоматично. Буде скопійовано параметри властивостей браузера Internet Explorer або Google Chrome.

І Ім'я користувача й пароль потрібно вручну вказати в налаштуваннях **проксі-сервера**.

Використовувати пряме підключення, якщо проксі-сервер недоступний: якщо ESET NOD32

Antivirus настроєний на використання проксі-сервера, але той недоступний, то продукт ESET NOD32 Antivirus виконає обхід проксі-сервера й установить зв'язок безпосередньо із серверами ESET.

Параметри проксі-сервера також можна визначити в розділі додаткових параметрів оновлення (у розділі **Додаткові параметри** > **Оновлення** > **Профілі** > **Оновлення** > **Параметри підключення** виберіть елемент **Підключення через проксі-сервер** із розкритого меню **Режим проксі-сервера**). Ці налаштування застосовуються до відповідного профілю оновлення. Їх рекомендується вказувати на портативних комп'ютерах, оскільки вони часто отримують оновлення вірусної бази даних із віддалених місць розташування. Докладніше про ці налаштування можна прочитати в розділі [Додаткові параметри оновлення](#).



Вибір зразка для аналізу

Якщо ви виявили підозрілий файл на комп'ютері або підозрілий веб-сайт в Інтернеті, їх можна надіслати на аналіз у дослідницьку лабораторію компанії ESET (доступність функції залежить від конфігурації ESET LiveGrid®).

Переш ніж надсилати зразки в ESET

Не надсилайте зразок, якщо він не відповідає хоча б одному з наведених нижче критеріїв:

- Зразок взагалі не виявляється вашим продуктом ESET.
- Зразок неправильно визначається як загроза.
- ! • Ми не приймаємо особисті файли, що надсилаються нам як зразки для сканування на наявність шкідливого програмного забезпечення (дослідницька лабораторія ESET не виконує сканування на вимогу для користувачів)
- Укажіть інформативну тему повідомлення, а також надайте якомога більше інформації про файл (наприклад, надайте знімок або вкажіть веб-сайт, з якого його завантажено)

Щоб надіслати в ESET зразок (файл або веб-сайт) для аналізу, скористайтеся одним із наведених нижче методів.

1. Скористайтеся формою надсилання зразків у вашому продукті. Щоб відкрити її, виберіть **Інструменти > Надіслати файл для аналізу**. Розмір зразка, який надсилається, може становити щонайбільше 256 МБ.
2. Файл також можна відправити електронною поштою. Якщо цей варіант зручніший для вас, додайте відповідні файли до архіву WinRAR/WinZIP, установивши для нього пароль "infected", і надішліть на адресу samples@eset.com.
3. Щоб повідомити про спам або повідомлення, помилково розпізнані як спам, дотримуйтесь інструкцій, наведених у [цій статті бази знань ESET](#).

У формі **Вибір зразка для аналізу** клацніть розкривне меню **Причини відправлення файлу** й виберіть опис, який найкраще відповідає меті вашого повідомлення:

- [Підозрілий файл](#)
- [Підозрілий сайт](#) (веб-сайт, інфікований будь-яким шкідливим ПЗ)
- [Сайт, заблокований помилково](#)
- [Помилковий результат файлу](#) (файли, неправильно розпізнані як інфіковані)
- [Інше](#)

Файл/сайт – шлях до файлу або веб-сайту, який потрібно відправити.

Контактна адреса електронної пошти — контактна адреса електронної пошти, яка відправляється до ESET разом із підозрілими файлами і може використовуватися для зв'язку з вами, якщо для аналізу будуть потрібні додаткові відомості про надіслані файли. Додавати контактну адресу електронної пошти необов'язково. Щоб не вказувати її, виберіть **Надіслати анонімно**.

Ви можете не отримати відповіді від ESET

- i Ви не отримаєте відповіді від ESET (окрім тих випадків, коли для аналізу будуть потрібні додаткові відомості від вас). Щодня на наші сервери надходять десятки тисяч файлів, тому ми не маємо можливості відповідати на всі повідомлення. Якщо буде визначено, що файл або веб-сайт шкідливий, ми додамо засоби для його виявлення до одного з наступних оновлень продукту ESET.

Вибір зразка для аналізу: підозрілий файл

Виявлені ознаки та симптоми зараження шкідливою програмою: введіть опис поведінки підозрілого файлу, виявленого на комп'ютері.

Походження файлу (URL-адреса чи постачальник) – укажіть походження файлу (джерело) і зазначте, як його було знайдено.

Примітки й додаткова інформація – тут можна ввести додаткову інформацію чи опис, які допоможуть під час обробки або виявлення підозрілого файлу.

i Лише перший параметр (**Виявлені ознаки та симптоми зараження шкідливою програмою**) потрібно вказати обов'язково, але надання додаткової інформації значно допоможе працівникам наших лабораторій у процесі ідентифікації й обробки зразків.

Вибір зразка для аналізу: підозрілий сайт

Виберіть один із наведених нижче елементів розкривного меню **Проблема із сайтом**.

- **Інфікований:** веб-сайт, що містить віруси або інше шкідливе ПЗ, поширюване різними способами.
- **Фішинговий:** часто використовується для отримання доступу до конфіденційних даних (PIN-кодів, номерів банківських рахунків тощо). Докладніше про цей тип атаки див. у [глосарії](#).
- **Шахрайський:** оманливий або зловмисний веб-сайт, часто створюваний із метою отримання швидкого прибутку.
- Виберіть **Інше**, якщо жоден із наведених вище варіантів не відповідає вашому випадку.

Примітки й додаткова інформація: тут можна ввести додаткову інформацію чи опис, які можуть бути корисними під час аналізу підозрілого веб-сайту.

Вибір зразка для аналізу: помилково розпізнаний файл

Якщо файл помилково визначено як інфікований, надішліть його нам. Це допоможе покращити роботу модулів захисту від вірусів і шпигунських програм, а також посилити безпеку інших користувачів. Помилкові результати можуть виникати, коли шаблон файлу збігається із шаблоном, збереженим в обробнику виявлення.

Назва й версія програми: назва програми та її версія (наприклад, номер або альтернативна чи кодова назва).

Походження файлу (URL-адреса чи постачальник): укажіть походження файлу (джерело) і те, яким чином його було знайдено.

Призначення програми: загальний опис програми, її тип (наприклад, веб-браузер, медіапрогравач тощо) і функції.

Примітки й додаткова інформація: тут можна вказати додаткову інформацію або опис, які допоможуть під час обробки підозрілого файлу.

i Перші три параметри необхідні для того, щоб виявити легальні програми й відрізнити їх від шкідливого коду. Надання додаткової інформації значно допоможе працівникам наших лабораторій під час ідентифікації й обробки зразків.

Вибір зразка для аналізу: помилково розпізнаний сайт

Якщо сайт помилково визначено як інфікований, шахрайський або фішинговий, повідомте про це нам. Помилкові результати можуть виникати, коли шаблон файлу збігається із шаблоном, збереженим в обробнику виявлення. Повідомляйте нам про такі випадки, щоб ми могли покращити роботу модулів захисту від вірусів і фішинг-атак, а також посилити захист інших користувачів.

Примітки й додаткова інформація: тут можна вказати додаткову інформацію або опис, які допоможуть під час обробки підозрілого веб-сайту.

Вибір зразка для аналізу: інше

Використовуйте цю форму, якщо файл не можна віднести до категорії **Підозрілий файл** або **Помилковий результат**.

Причина відправлення файлу: введіть детальний опис файлу й причину його відправлення.

Оновлення Microsoft Windows®

Служба Windows Update – важливий компонент захисту користувачів від шкідливого програмного забезпечення. Тому критично необхідно інсталиувати оновлення Microsoft Windows одразу ж, як вони стають доступними. ESET NOD32 Antivirus повідомляє про відсутні оновлення відповідно до рівня, встановленого користувачем. Для вибору доступні наведені нижче рівні.

- **Жодних оновлень:** жодні оновлення системи не пропонуватимуться для завантаження.
- **Необов'язкове оновлення:** для завантаження пропонуватимуться оновлення, позначені як низькопріоритетні, і важливіші.
- **Рекомендовані оновлення:** для завантаження пропонуватимуться оновлення, позначені як найпоширеніші, і такі, що мають пізнішу дату випуску.
- **Важливі оновлення:** для завантаження пропонуватимуться оновлення, позначені як важливіші, і такі, що мають пізнішу дату випуску.
- **Критичні оновлення:** для завантаження пропонуватимуться лише критичні оновлення.

Натисніть кнопку **ОК**, щоб зберегти зміни. Вікно "Оновлення системи" відкриється після перевірки стану на сервері оновлень. Відповідно, інформація про оновлення системи може бути доступна не відразу після збереження змін.

Діалогове вікно "Оновлення системи"

Якщо є доступні оновлення для вашої операційної системи, у головному вікні ESET NOD32 Antivirus відображаються сповіщення. Щоб відкрити вікно «Оновлення системи», натисніть **Докладніше**.

У вікні "Оновлення системи" показано список доступних оновлень, готових для завантаження та інсталяції. Тип оновлення відображається поруч із його назвою.

Двічі клацніть кнопкою миші будь-який рядок оновлення, щоб відкрити вікно [Інформація про оновлення](#) з додатковою інформацією.

Натисніть **Запустити оновлення системи**, щоб розпочати завантаження й інсталяцію оновлень системи.

Інформація про оновлення

Інформація про оновлення Windows. Назва й номер оновлення вказані у верхній частині вікна разом із пріоритетом та описом проблеми, які це оновлення усуває.

Інтерфейс користувача

Щоб налаштувати графічний інтерфейс користувача програми, у [головному вікні програми](#) натисніть **Налаштування > Додаткові параметри (F5) > Інтерфейс користувача**.

Ви можете налаштувати вигляд і візуальні ефекти програми на екрані [Елементи інтерфейсу користувача](#) на екрані додаткових параметрів.

Щоб гарантувати максимальну надійність системи безпеки, можна запобігти видаленню параметрів або внесенню будь-яких несанкціонованих змін у її параметри, установивши пароль за допомогою засобу [Параметри доступу](#).



Щоб налаштувати системні сповіщення, сигнали про виявлення та статуси програм, див. розділ [Сповіщення](#).

Елементи інтерфейсу користувача

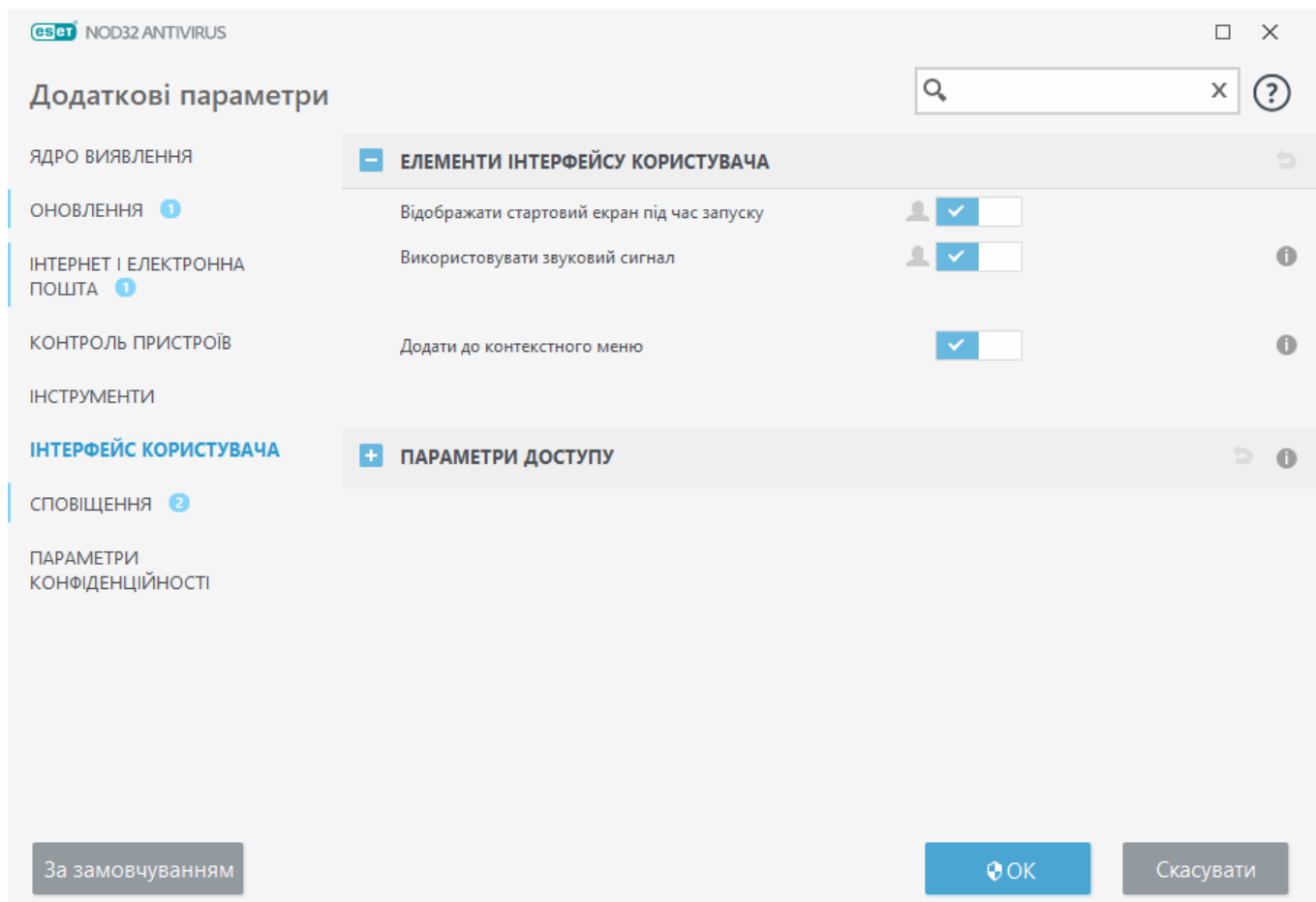
Параметри конфігурації інтерфейсу користувача в програмі ESET NOD32 Antivirus дають можливість коригувати робоче середовище відповідно до своїх потреб. Доступ до цих параметрів конфігурації можна отримати в гілці **Додаткові параметри (F5) > Інтерфейс користувача > Елементи інтерфейсу користувача**.

Щоб вимкнути стартовий екран ESET NOD32 Antivirus, зніміть прапорець **Відображати стартовий**

екран під час запуску.

Прапорець "Використовувати звуковий сигнал": установлюється, щоб під час сканування програма ESET NOD32 Antivirus відтворювала звукове попередження про важливі події (наприклад, виявлення загрози або завершення процесу).

Додати до контекстного меню: додати елементи керування ESET NOD32 Antivirus до контекстного меню.



Параметри доступу

Параметри ESET NOD32 Antivirus є критично важливою складовою вашої політики безпеки. Неавторизовані зміни можуть загрожувати стабільності й захисту системи. Щоб уникнути несанкціонованих змін, параметри налаштування й видалення ESET NOD32 Antivirus можна захистити паролем.

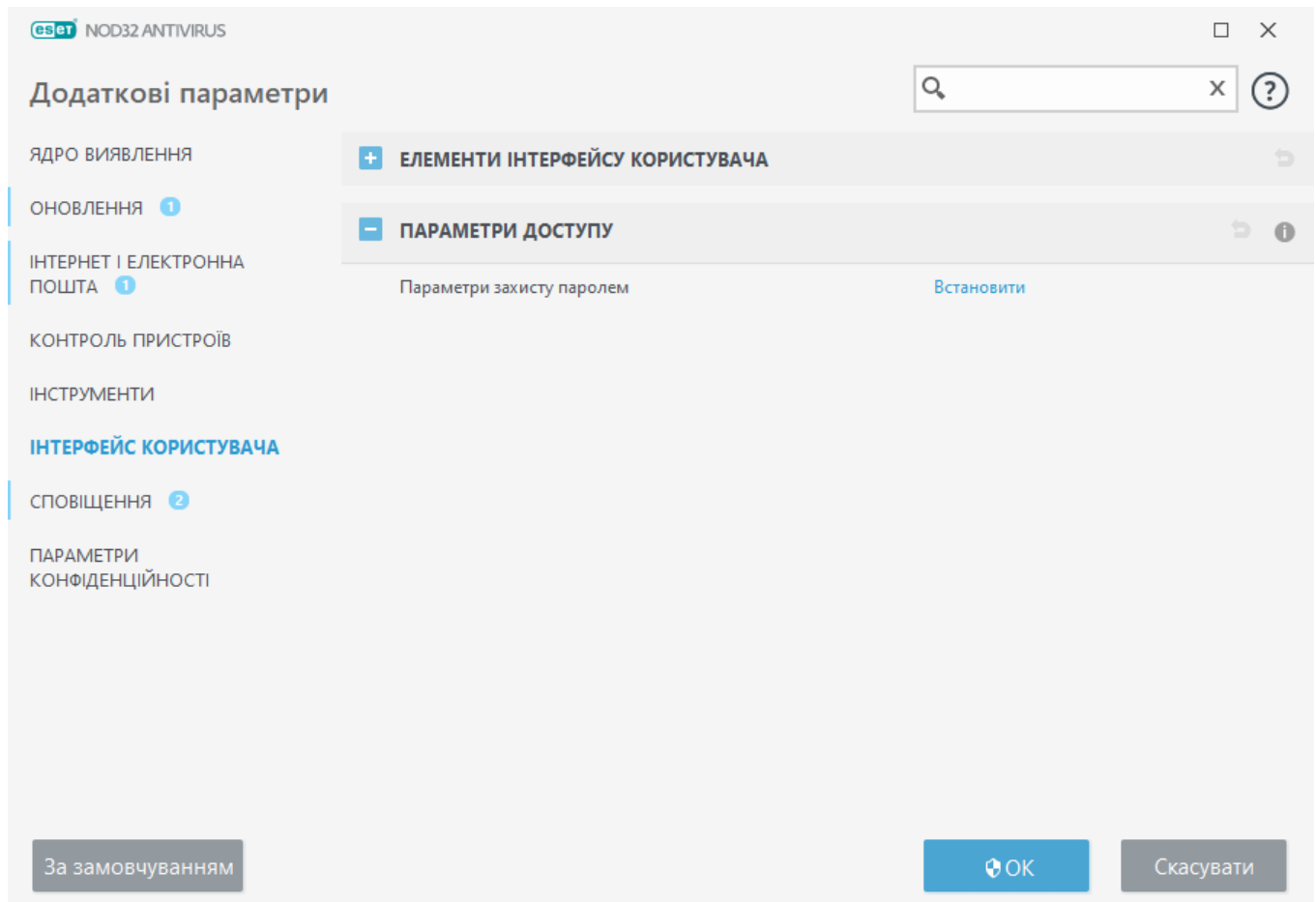
Щоб задати пароль для захисту параметрів налаштування й видалення ESET NOD32 Antivirus, клацніть **Задати** поруч із розділом **Параметри, захищені паролем**.

і Якщо потрібно отримати доступ до захищених додаткових параметрів, відобразиться вікно введення пароля. Якщо ви забули або втратили пароль, натисніть **Відновити пароль** нижче та вкажіть адресу електронної пошти, яку ви використали для реєстрації ліцензії. Ви отримаєте електронний лист від ESET із кодом підтвердження й інструкцією зі скидання пароля.

- [Як розблокувати додаткові параметри](#)

Щоб змінити пароль, клацніть **Змінити пароль** поруч із розділом **Параметри, захищені паролем**.

Щоб видалити пароль, клацніть **Видалити пароль** поруч із розділом **Параметри, захищені паролем**.



Пароль для розділу "Додаткові параметри"

Щоб захистити додаткові параметри ESET NOD32 Antivirus від несанкціонованих змін, потрібно задати новий пароль.

Порядок зміни поточного пароля

1. Уведіть поточний пароль у поле **Старий пароль**.
2. Уведіть новий пароль у поля **Новий пароль** і **Підтвердьте пароль**.
3. Клацніть **ОК**.


Цей пароль потрібно буде вводити під час кожної спроби внести зміни до параметрів ESET NOD32 Antivirus.

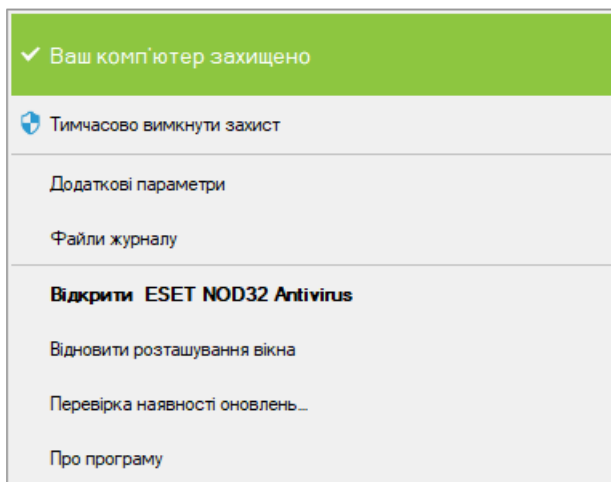
Якщо ви забули пароль, доступ до додаткових параметрів можна [відновити за допомогою методу "Відновити пароль"](#).

Якщо потрібно відновити втрачений ліцензійний ключ ESET, термін дії ліцензії або іншу

інформацію про ліцензію для ESET NOD32 Antivirus, дотримуйтеся інструкцій у статті нашої бази знань [за цим посиланням](#).

Піктограма в системному треї

Доступ до деяких найбільш важливих параметрів і функцій можна отримати, клацнувши правою кнопкою миші піктограму в системному треї .



Тимчасово вимкнути захист: відображається діалогове вікно з підтвердженням, у якому можна вимкнути [ядро виявлення](#), тобто модуль, який захищає систему від атак зловмисників, контролюючи передачу даних у файлах, через Інтернет та електронну пошту.

Розкриття меню **Проміжок часу** служить для вибору періоду, протягом якого захист залишатиметься вимкненим.



Вимкнути антивірус та антишпигун?

Якщо вимкнути антивірус та антишпигун, свою роботу припинять модулі захисту в режимі реального часу, захисту документів, захисту доступу до Інтернету, захисту поштового клієнта, а також захисту від фішинг-атак. Через це ваш комп'ютер стане вразливим до великої кількості загроз.

Тимчасово вимкнути ... ▼

Застосувати

Скасувати

Додаткові параметри: скористайтеся цією опцією, щоб відкрити дерево **Додаткові параметри**. Дерево додаткових параметрів можна відкрити й іншими способами, наприклад натиснувши клавішу F5 або перейшовши до розділу **Параметри > Додаткові параметри**.

Файли журналу: [файли журналу](#) містять інформацію про важливі програмні події та надають огляд виявлених загроз.

Відкрити ESET NOD32 Antivirus: відкриває [головне вікно програми](#) ESET NOD32 Antivirus за допомогою піктограми в системному треї.

Скинути макет вікна – відновлення стандартного розміру та розміщення вікна ESET NOD32 Antivirus.

Перевірити наявність оновлень – ініціювання оновлення обробника виявлення (попередня назва – "вірусна база даних") для забезпечення належного рівня захисту від шкідливого коду.

Про програму – вікно із системною інформацією, відомостями про інсталювану версію ESET NOD32 Antivirus та інсталюваними модулями програми. Тут також міститься інформація про термін дії ліцензії, операційну систему та її ресурси.

Підтримка програм для читання екрана

ESET NOD32 Antivirus можна використовувати разом із програмами для читання екрана, щоб дозволити користувачам ESET із вадами зору працювати з продуктом і налаштовувати його параметри. Підтримуються такі програми для читання екрана: (JAWS, NVDA, Narrator).

Щоб програма для читання екрана мала правильний доступ до GUI ESET NOD32 Antivirus, дотримуйтеся інструкцій у нашій [статті бази знань](#).

Довідка та підтримка

ESET NOD32 Antivirus містить засоби для виправлення неполадок і технічну інформацію, яка допоможе у вирішенні можливих проблем.



Ліцензія

- **Виправлення неполадок із ліцензією:** натисніть це посилання, щоб знайти рішення проблем із активацією або зміною ліцензії.
- **Змінити ліцензію** – натисніть, щоб відкрити вікно активації й активувати продукт. Якщо пристрій [підключено до ESET HOME](#), виберіть ліцензію в обліковому записі ESET HOME або додайте нову.



Інсталюваний продукт

- **Нові функції й можливості:** клацніть цей параметр, щоб відкрити вікно з інформацією про нові й удосконалені функції.
- **Про ESET NOD32 Antivirus** – відомості про вашу копію ESET NOD32 Antivirus.
- **Виправлення некоректної роботи продукту** натисніть це посилання, щоб знайти рішення найпоширеніших проблем.
- **Змінити продукт** – натисніть, щоб дізнатися, чи дає змогу поточна ліцензія ESET NOD32 Antivirus [перейти на інший продукт](#).



Сторінка довідки: натисніть це посилання, щоб відкрити довідку ESET NOD32 Antivirus.



[Служба технічної підтримки](#)

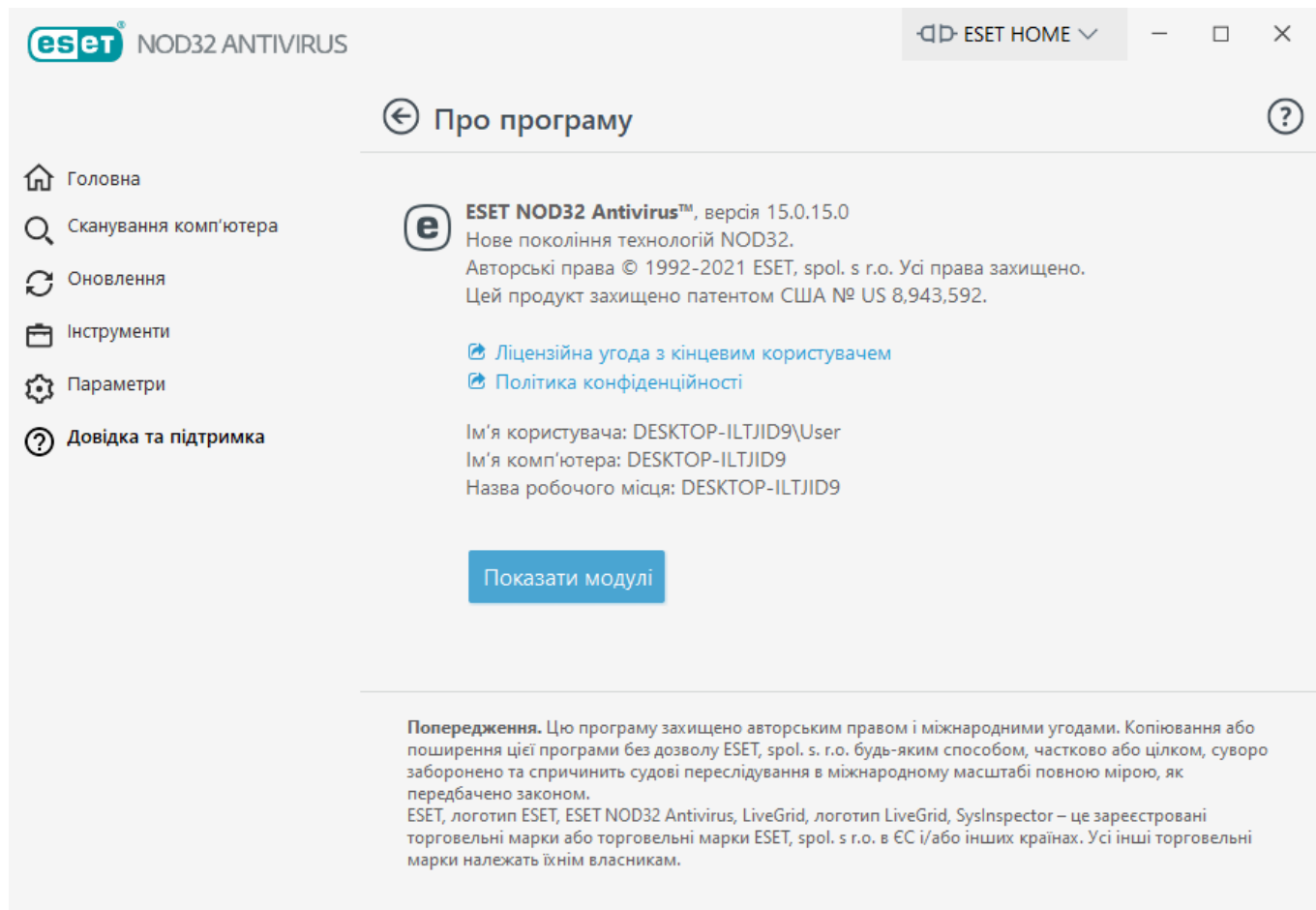


База знань – [база знань ESET](#) містить відповіді на найпоширеніші запитання, а також

рекомендовані способи вирішення різноманітних проблем. Регулярне оновлення, яке виконують технічні спеціалісти ESET, робить базу знань найефективнішим інструментом для вирішення різноманітних проблем.

Про продукт ESET NOD32 Antivirus

У цьому вікні вказуються докладні відомості про інсталювану версію продукту ESET NOD32 Antivirus і ваш комп'ютер.



Клацніть **Показати модулі**, щоб переглянути інформацію про список завантажених модулів програми.

- Інформацію про модулі можна скопіювати в буфер обміну, натиснувши **Копіювати**. Ця функція може бути корисною під час виправлення неполадок і звернення до служби технічної підтримки.
- Клацніть **Ядро виявлення** у вікні модулів, щоб відкрити вірусний радар ESET, що містить інформацію про кожну версію ядра виявлення ESET.

Новини ESET

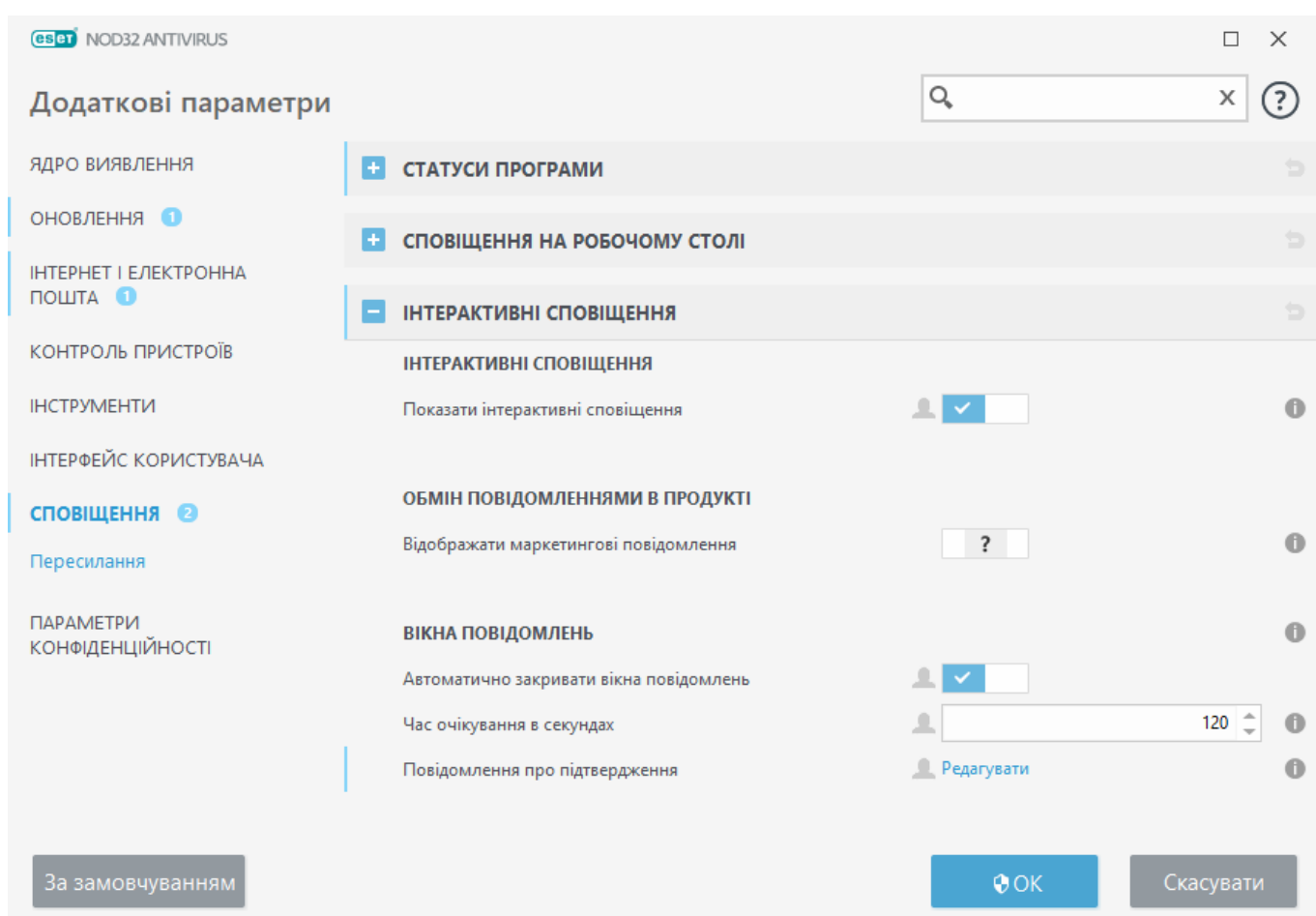
У цьому вікні програма ESET NOD32 Antivirus регулярно інформує вас про новини компанії ESET.

Обмін повідомленнями в продукті розроблено, щоб інформувати користувачів про новини ESET і

повідомляти інші корисні відомості. Для надсилання маркетингових повідомлень потрібна згода користувача. Тому маркетингові повідомлення за замовчуванням не надсилаються користувачу (відображається як знак питання). Увімкнувши цю опцію, ви погоджуєтесь отримувати маркетингові повідомлення від ESET. Якщо ви не хочете їх отримувати, вимкніть опцію **Показувати маркетингові повідомлення**.

Щоб увімкнути або вимкнути отримання маркетингових повідомлень у спливаючому вікні, виконайте наведені нижче інструкції.

1. Відкрийте головне вікно продукту ESET.
2. Натисніть клавішу **F5**, щоб відкрити меню **Додаткові параметри**.
3. Клацніть **Сповіщення** > **Інтерактивні сповіщення**.
4. Змініть опцію **Показувати маркетингові повідомлення**.



Надсилання даних про конфігурацію системи

Щоб надавати допомогу якомога швидше та якісніше, компанії ESET потрібна інформація про конфігурацію ESET NOD32 Antivirus, систему й запущені процеси ([файл журналу ESET SysInspector](#)), а також дані реєстру. Компанія ESET використовуватиме ці відомості виключно для надання технічної підтримки користувачеві.

Під час надсилання [веб-форми](#), дані про конфігурацію системи передаються компанії ESET. Установіть прапорець **Завжди надсилати ці дані**, щоб запам'ятати відповідну дію для цього процесу. Щоб надіслати форму без додаткових даних, натисніть **Не надсилати дані**. До служби технічної підтримки ESET можна звернутися за допомогою онлайн-форми.

Цей параметр також можна налаштувати в меню **Додаткові параметри > Інструменти > Діагностика > [Служба технічної підтримки](#)**.

i Якщо ви вирішили надіслати дані про систему, заповніть і надішліть веб-форму, інакше ваше звернення не буде зареєстровано, а дані про систему буде втрачено.

Технічна підтримка

У [головному вікні програми](#) виберіть пункти **Довідка та підтримка > Служба технічної підтримки**.

Зверніться до служби технічної підтримки

Надіслати запит до служби технічної підтримки: якщо вам не вдається знайти відповідь на своє запитання, скористайтесь формою на веб-сайті ESET, щоб швидко зв'язатися зі співробітниками служби технічної підтримки ESET. Залежно від налаштувань перед заповненням веб-форми вам може знадобитися [надіслати дані конфігурації системи](#).

Отримайте відомості для служби технічної підтримки

Інформація для технічної підтримки: ви можете скопіювати й надіслати інформацію (наприклад, дані ліцензій, назву продукту, версію, операційну систему та відомості про комп'ютер) в службу технічної підтримки ESET, коли відобразиться відповідний запит.

ESET Log Collector – переспрямовує на статтю [бази знань ESET Knowledgebase](#), де можна завантажити програму ESET Log Collector, яка автоматично збирає інформацію й журнали на комп'ютері для швидкого вирішення проблем. Більш докладну інформацію див. в [онлайн-посібнику користувача ESET Log Collector](#).

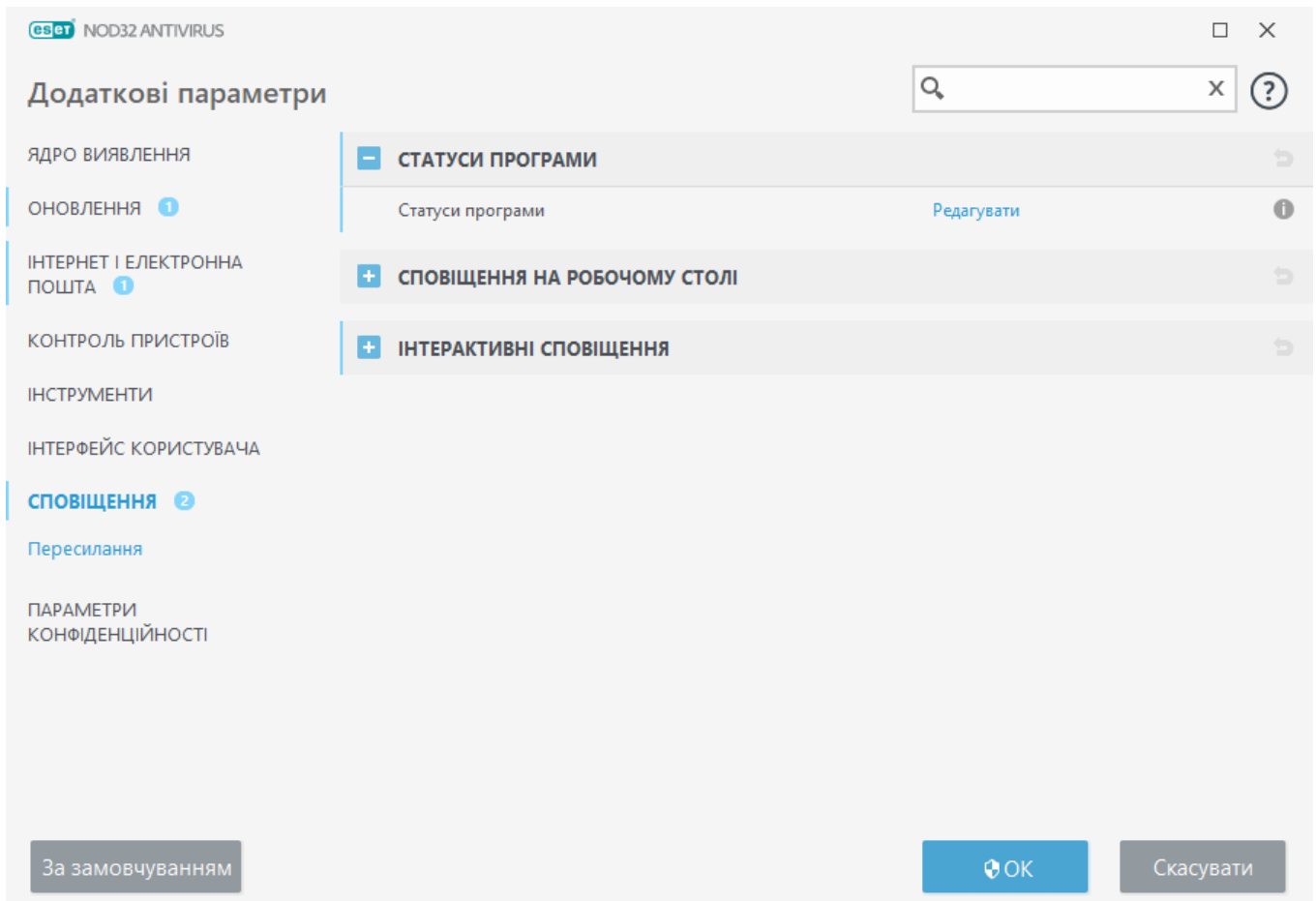
Натисніть **Розширене журналювання**, щоб створити розширені журнали для всіх доступних функцій. Це дасть змогу розробникам діагностувати й усувати проблеми. За замовчуванням задано мінімальний рівень ведення журналу — **Діагностика**. Розширене журналювання автоматично вимикається через дві години, якщо не зупинити його раніше, натиснувши **Припинити розширене журналювання**. Коли всі журнали створено, відображається вікно зі сповіщеннями, які надають прямий доступ до папки "Diagnostic" зі створеними журналами.

Сповіщення

Щоб керувати сповіщеннями ESET NOD32 Antivirus, відкрийте **Додаткові параметри (F5) > Сповіщення**. Ви можете налаштувати вказані нижче типи сповіщень.

- Статуси програм: сповіщення, що відображаються в основному розділі [головного вікна програми](#).

- [Сповіщення на робочому столі](#): невелике спливаюче вікно поруч із панеллю завдань системи.
- [Інтерактивні сповіщення](#): вікна сповіщень і вікна повідомлень, що потребують втручання користувача.
- [Пересилання](#) (Сповіщення електронною поштою): сповіщення електронною поштою надсилаються на вказану адресу електронної пошти.



– Статуси програми

Статуси програм: натисніть **Редагувати**, щоб вибрати статуси програми, що відображаються в основному розділі [головного вікна програми](#).

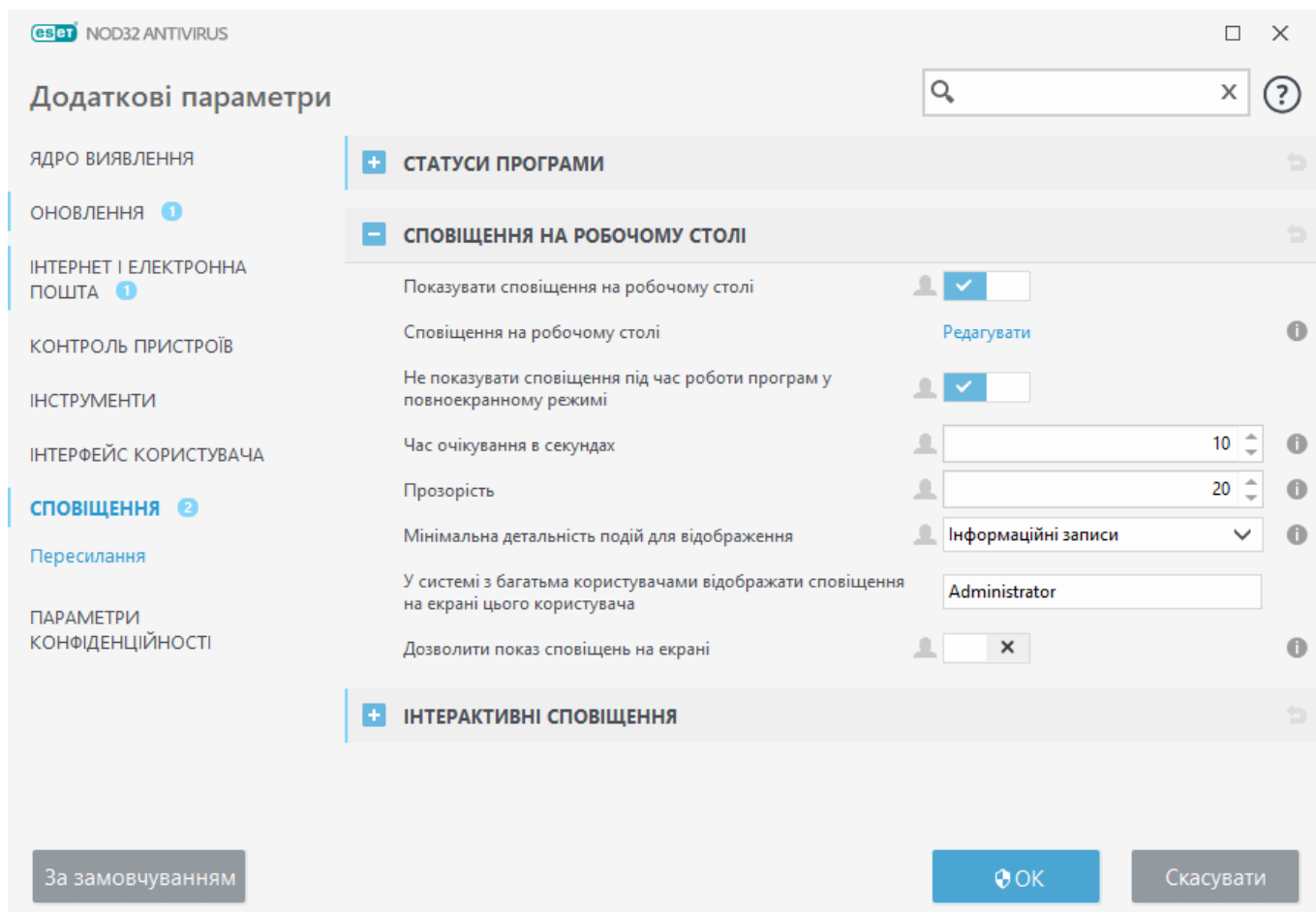
Діалогове вікно: статуси програми

У цьому діалоговому вікні можна вибирати, які відображатимуться статуси програми. Наприклад, коли ви призупиняєте роботу антивірусу й антишпигуна чи активуєте ігровий режим.

Статус програми також відображатиметься, якщо продукт не активовано або термін дії ліцензії минув.

Сповіщення на робочому столі

Сповіщення на робочому столі відображаються в маленькому спливаючому вікні поруч із панеллю завдань системи. За замовчуванням воно відображається протягом 10 секунд, а потім поступово зникає. Сповіщення містять інформацію про успішні оновлення продукту, нові підключені пристрої, завершення завдань сканування на наявність вірусів або знайдені нові загрози.



Показувати сповіщення на робочому столі. Рекомендуємо не вимикати цю опцію, щоб продукт інформував про нові події.

Сповіщення на робочому столі. Натисніть **Редагувати**, щоб увімкнути або вимкнути конкретні [сповіщення на робочому столі](#).

Не показувати сповіщення під час роботи програм у повноекранному режимі: скасовує відображення всіх неінтерактивних сповіщень, коли програми працюють у повноекранному режимі.

Час очікування в секундах: укажіть інтервал часу, протягом якого відображатиметься сповіщення. Значення має бути в діапазоні від 3 до 30 секунд.

Прозорість: укажіть ступінь прозорості сповіщень (у відсотках). Підтримується діапазон значень від 0 (зовсім непрозорі сповіщення) до 80 (сповіщення з дуже високим ступенем прозорості).

Мінімальна детальність подій для відображення: укажіть початковий рівень важливості

сповіщень, які потрібно відображати на екрані. У розкритому меню виберіть один із таких параметрів:

о**Діагностика**: запис інформації, необхідної для оптимізації програми, і всіх зазначених вище елементів.

о**Інформаційні записи**: запис інформаційних повідомлень (наприклад, про нестандартні події в мережі), включно зі сповіщеннями про успішне оновлення, і всіх зазначених вище елементів.

о**Попередження**: відображення попереджень, помилок і критичних помилок (наприклад, збій або неправильне оновлення Antist stealth).

о**Помилки**: відображення помилок (наприклад, захист документів не запущено) і критичних помилок.

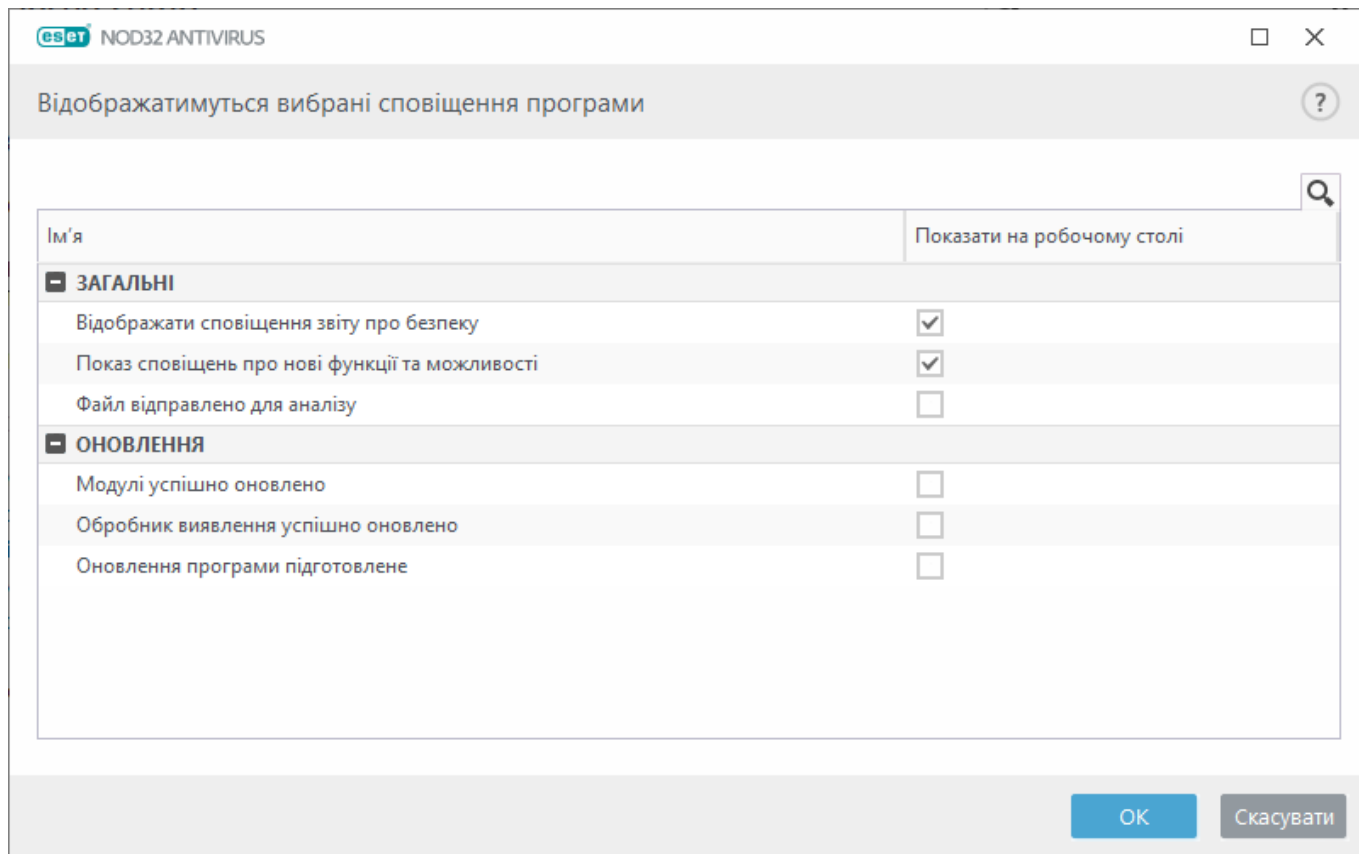
о**Критичні помилки**: відображатимуться тільки критичні помилки (помилка запуску антивірусного захисту, інфікування системи тощо).

У системі з багатьма користувачами відображати сповіщення на екрані цього користувача: для вибраних облікових записів сповіщення відображатимуться на робочому столі. Наприклад, якщо ви не використовуєте обліковий запис адміністратора, уведіть повне ім'я облікового запису. Після цього ви будете отримувати сповіщення на робочому столі. Сповіщення на робочому столі може отримувати лише один обліковий запис користувача.

Дозволити показ сповіщень на екрані: сповіщення показуватимуться на екрані; для їх перегляду потрібно буде натиснути комбінацію клавіш **ALT + Tab**.

Список сповіщень на робочому столі

Щоб налаштувати видимість сповіщень на робочому столі (які відображаються в нижньому правому куті екрана), у меню **Додаткові параметри (F5)** перейдіть у розділ **Сповіщення > Сповіщення на робочому столі**. Натисніть **Редагувати** поруч із пунктом **Сповіщення на робочому столі** й установіть прапорець **Показати**.



Загальні

Показ сповіщень щодо звіту про безпеку: отримувати сповіщення про створення нового [звіту про безпеку](#).

Показ сповіщень про нові функції та можливості: сповіщення про всі нові й удосконалені функції останньої версії продукту.

Файл відправлено для аналізу: отримувати сповіщення щоразу, коли ESET NOD32 Antivirus надсилає файл для аналізу.

Оновлення

Оновлення програми підготовлене: отримувати сповіщення, коли готове оновлення до нової версії програми ESET NOD32 Antivirus.

Обробник виявлення оновлено: отримувати сповіщення про оновлення модулів обробника виявлення.

Модулі оновлено: отримувати сповіщення про оновлення компонентів програми.

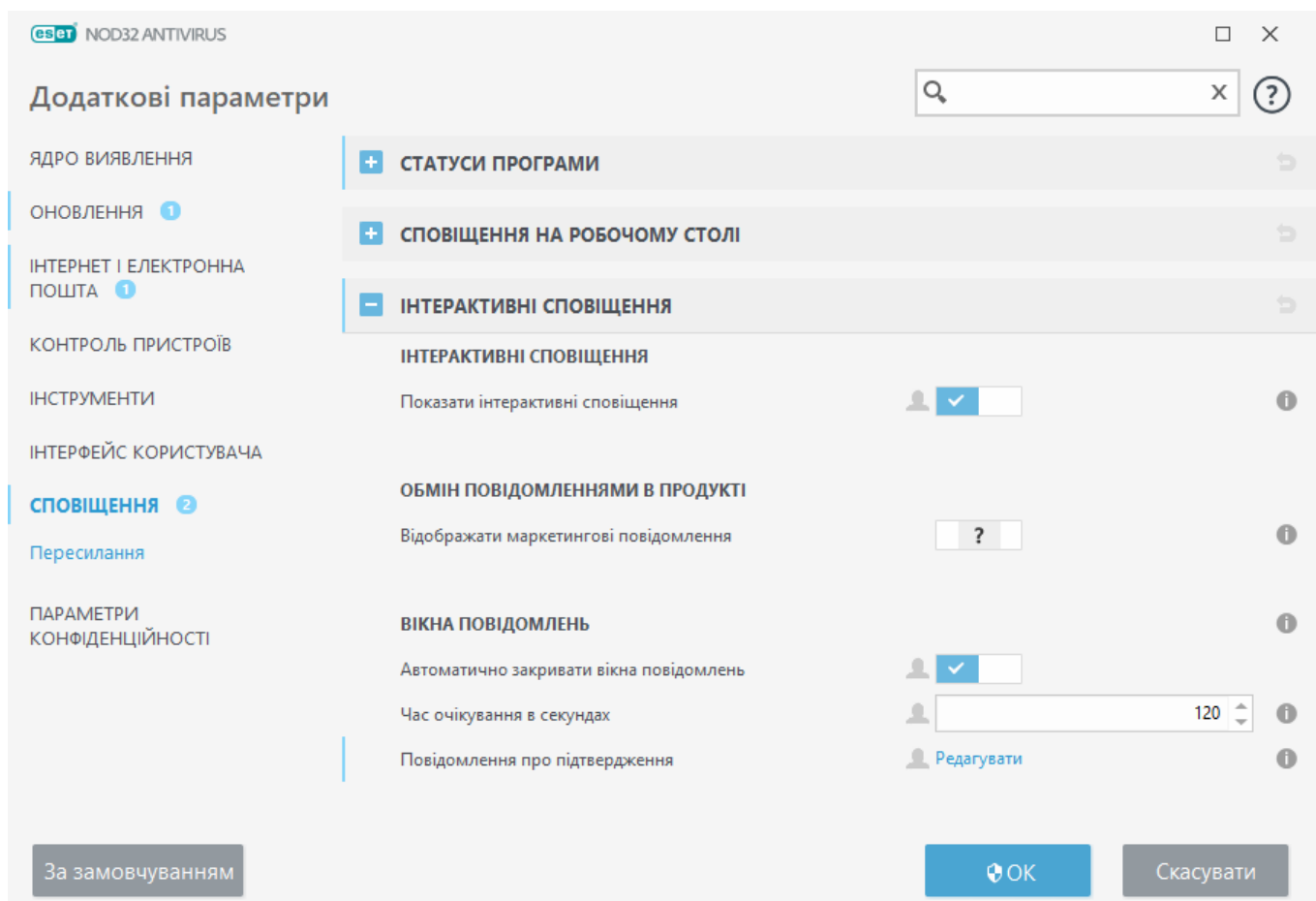
Щоб задати загальні параметри сповіщень на робочому столі, наприклад, тривалість відображення повідомлень або мінімальний рівень деталізації подій для відображення, відкрийте [Сповіщення на робочому столі](#) (**Додаткові параметри (F5) > Сповіщення**).

Інтерактивні сповіщення

Шукаєте інформацію про стандартні сигнали та сповіщення?

- [Знайдено загрозу](#)
- [Адресу заблоковано](#)
- [Продукт не активовано](#)
- [Перейти на продукт із більшою кількістю функцій](#)
- [Перехід на продукт з меншою кількістю функцій](#)
- [Доступне оновлення](#)
- [Невідповідність інформації про оновлення](#)
- [Виправлення неполадок, пов'язаних із появою повідомлення "Помилка оновлення модулів"](#)
- [Усунення помилок оновлення модулів](#)
- [Сертифікат веб-сайту відкликано](#)

У розділі **Інтерактивні сповіщення**, перейшовши в меню **Додаткові параметри** (F5) > **Сповіщення**, можна визначати, яким чином ESET NOD32 Antivirus буде обробляти вікна повідомлень та інтерактивні сповіщення для виявлених об'єктів, щодо яких має прийняти рішення користувач (наприклад, потенційні фішингові веб-сайти).



Інтерактивні сповіщення

Якщо параметр **Показати інтерактивні сповіщення** вимкнено, приховуватимуться всі вікна сповіщень і діалогові вікна браузера, що доречно лише для обмеженої кількості особливих ситуацій. Для більшості користувачів ESET рекомендує залишити цей параметр увімкненим.

Обмін повідомленнями у продукті

Обмін повідомленнями в продукті розроблено, щоб інформувати користувачів про новини ESET і повідомляти інші корисні відомості. Для надсилання маркетингових повідомлень потрібна згода користувача. Тому маркетингові повідомлення за замовчуванням не надсилаються користувачу (відображається як знак питання). Увімкнувши цю опцію, ви погоджуєтесь отримувати маркетингові повідомлення від ESET. Якщо ви не хочете їх отримувати, вимкніть опцію **Показувати маркетингові повідомлення**.

Вікна повідомлень

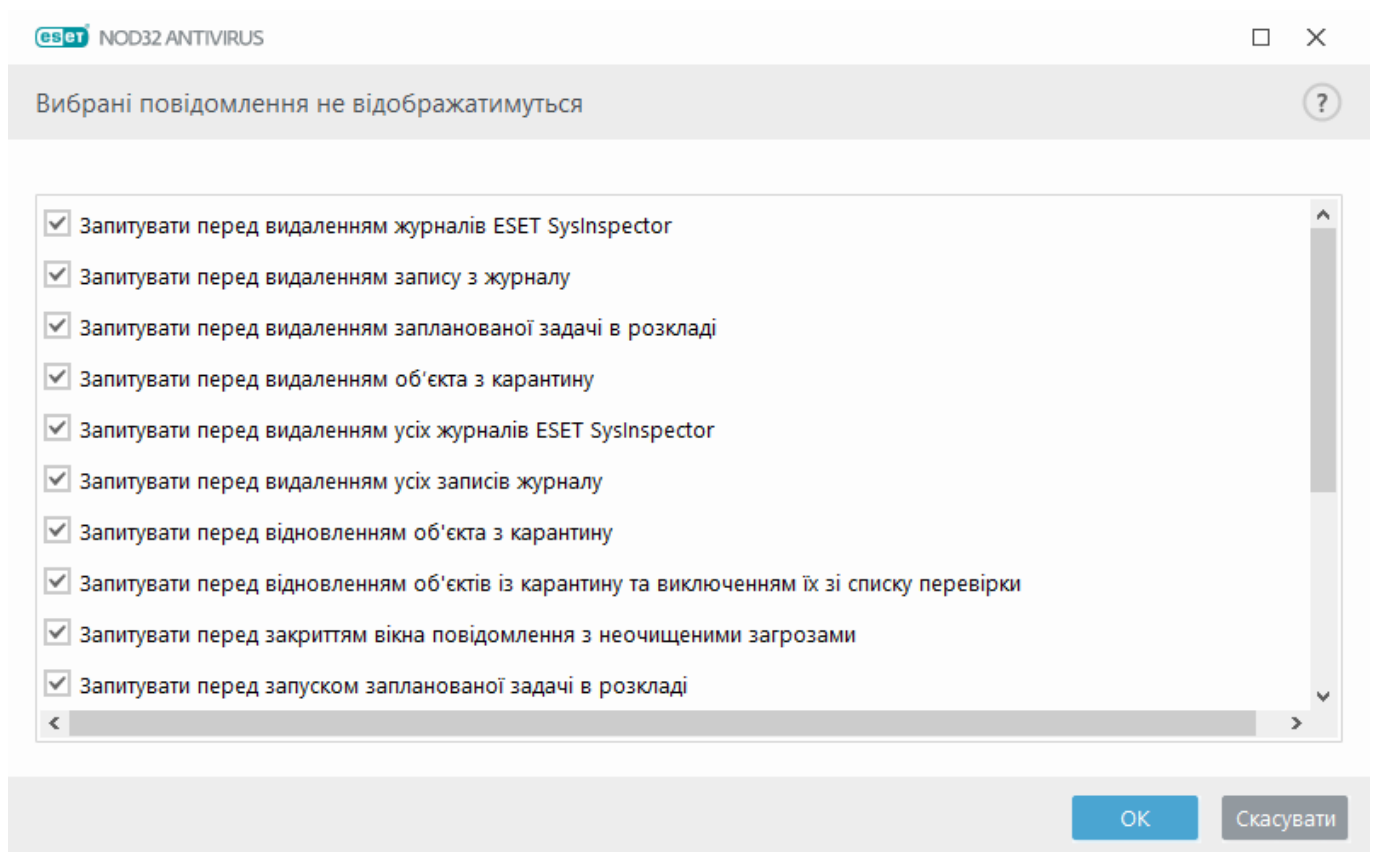
Щоб вікна повідомлень закривались автоматично через певний проміжок часу, установіть параметр **Автоматично закривати вікна повідомлень**. Якщо вікна сигналів тривоги не закрити вручну, їх буде закрито автоматично після завершення вказаного періоду часу.

Час очікування в секундах: укажіть інтервал часу, протягом якого відображатиметься сигнал. Значення має бути в діапазоні від 10 до 999 секунд.

Повідомлення про підтвердження: натисніть **Редагувати**, щоб показати [список повідомлень про підтвердження](#), де можна вибрати ті, що потрібно відображати.

Повідомлення про підтвердження

Щоб змінити повідомлення про підтвердження, перейдіть у меню **Додаткові параметри (F5) > Сповіщення > Інтерактивні сповіщення** й натисніть **Редагувати** поруч з опцією **Повідомлення з підтвердженнями**.



У цьому діалоговому вікні відображатимуться повідомлення про підтвердження від програми

ESET NOD32 Antivirus перед виконанням будь-якої дії. Установіть або зніміть прапорець біля кожного повідомлення про підтвердження, щоб увімкнути або вимкнути його.

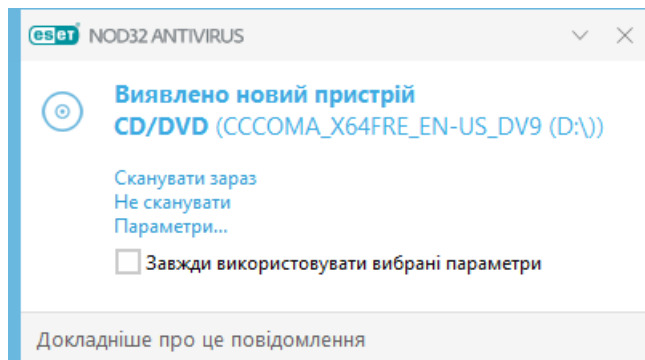
Дізнайтеся більше про функцію, пов'язану з повідомленнями з підтвердженням:

- [Запитувати перед видаленням журналів ESET SysInspector](#)
- [Запитувати перед видаленням усіх журналів ESET SysInspector](#)
- [Запитувати перед видаленням об'єкта з карантину](#)
- Запитувати перед скасуванням змін у розділі додаткових параметрів
- [Запитувати перед закриттям вікна повідомлення з неочищеними загрозами](#)
- [Запитувати перед видаленням запису з журналу](#)
- [Запитувати перед видаленням запланованої задачі в розкладі](#)
- [Запитувати перед видаленням усіх записів журналу](#)
- [Запитувати перед скиданням даних статистики](#)
- [Запитувати перед відновленням об'єкта з карантину](#)
- [Запитувати перед відновленням об'єктів із карантину та виключенням їх зі списку перевірки](#)
- [Запитувати перед запуском запланованої задачі в розкладі](#)
- [Показувати діалоги для підтвердження в продукті операцій для поштових клієнтів Outlook Express і Windows Mail](#)
- [Показувати діалоги для підтвердження в продукті операцій для Windows Live Mail](#)
- [Показувати діалоги для підтвердження в продукті операцій для поштового клієнта Outlook](#)

Знімні носії

ESET NOD32 Antivirus забезпечує автоматичне сканування змінних носіїв (компакт-/DVD-диск/USB тощо) після вставлення в комп'ютер. Це може бути корисним, якщо адміністратору комп'ютера потрібно заборонити користувачам застосовувати знімні носії з недозволим вмістом.

Якщо в ESET NOD32 Antivirus вибрано параметр **Показати параметри сканування**, після вставлення змінного носія відобразиться таке діалогове вікно:



Нижче наведено параметри, доступні в цьому діалоговому вікні.

- **Сканувати зараз:** ініціювати сканування змінного носія.
- **Не сканувати:** змінні носії не скануватимуться.
- **Параметри:** відкрити розділ **Додаткові параметри**.
- **Завжди використовувати вибрані параметри:** якщо цей прапорець встановлено, після підключення змінного носія виконуватиметься та сама дія.

Окрім цього, ESET NOD32 Antivirus має функцію контролю пристроїв, яка дає змогу визначати правила для використання зовнішніх пристроїв на певному комп'ютері. Докладнішу інформацію про контроль пристроїв можна знайти в розділі [Контроль пристроїв](#).

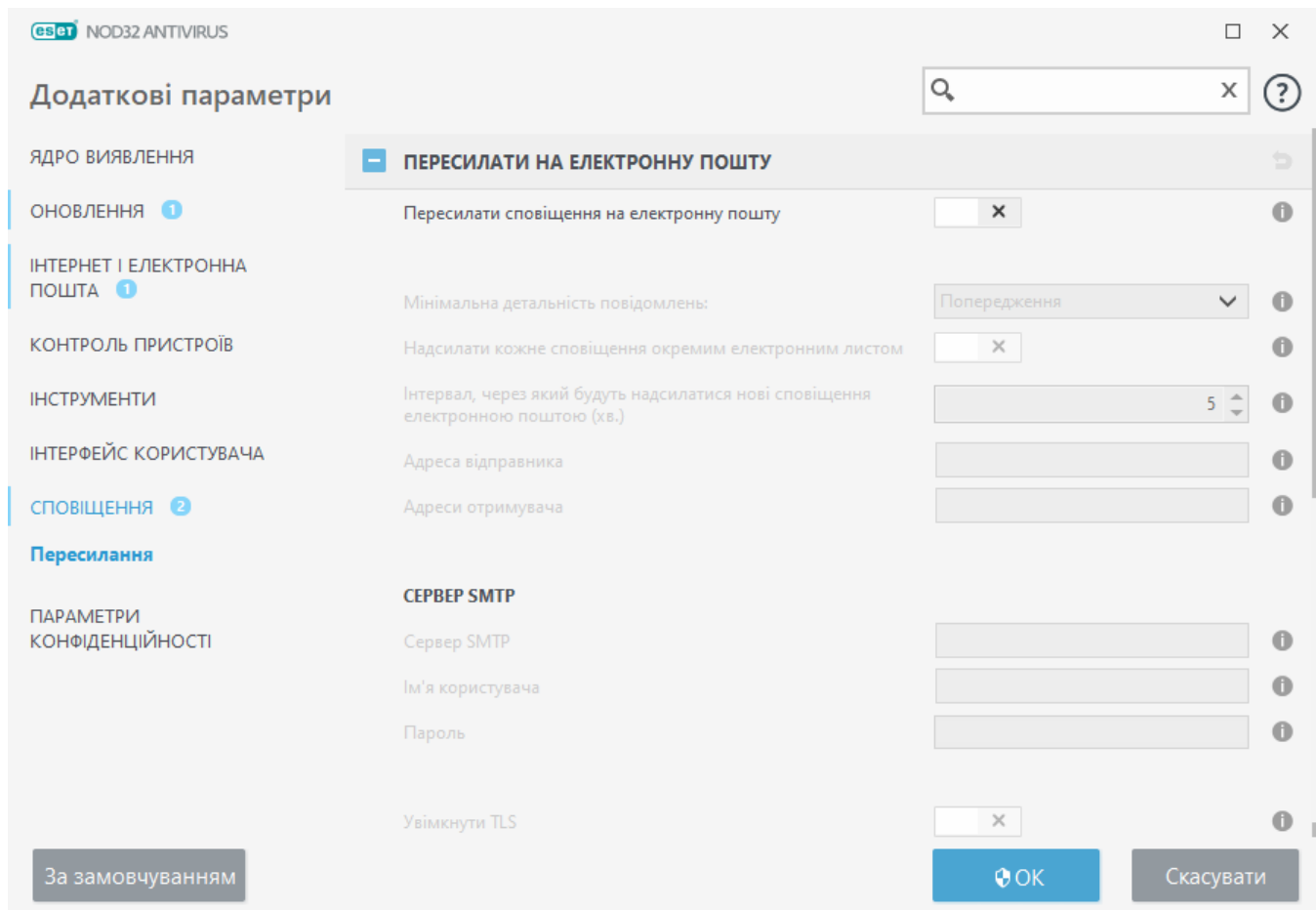
Щоб перейти до налаштувань сканування змінних носіїв, відкрийте розділ Додаткові параметри (F5) > **Ядро виявлення** > **Сканування шкідливого ПЗ** > **Змінні носії**.

Дії, які потрібно виконувати після вставлення змінного носія: виберіть дію за замовчуванням, яка виконуватиметься в разі використання на комп'ютері змінного носія (компакт-/DVD-диск/USB). Виберіть дію, яку потрібно виконувати після вставлення в комп'ютер змінного носія.

- **Не сканувати:** не виконуватиметься жодна дія, а вікно **Виявлено новий пристрій** не відображатиметься.
- **Автоматичне сканування пристроїв:** виконуватиметься сканування використовуваного змінного носія.
- **Показати параметри сканування:** відкриває розділ "Параметри змінного носія".

Пересилання

ESET NOD32 Antivirus може автоматично надсилати сповіщення електронною поштою, якщо відбуватимуться події з вибраним рівнем розголошення. Щоб активувати сповіщення електронною поштою, перейдіть у **Додаткові параметри** (F5) > **Сповіщення** > **Пересилання** та ввімкніть налаштування **Пересилати сповіщення на електронну пошту**.



У розкритому меню **Мінімальна детальність повідомлень** можна вибрати початковий рівень важливості сповіщень, які потрібно надсилати.

- **Діагностика** – запис інформації, необхідної для оптимізації програми, і всіх зазначених вище елементів.
- **Інформаційні записи**: запис інформаційних повідомлень (наприклад, про нестандартні події в мережі), включно зі сповіщеннями про успішне оновлення, і всіх зазначених вище елементів.
- **Попередження**: фіксуються всі критичні помилки й попереджувальні повідомлення (антируткіт не працює належним чином або не вдалося здійснити оновлення).
- **Помилки**: запис помилок (захист документів не запущено) і критичних помилок.
- **Критичні помилки**: запис лише критичних помилок (наприклад, помилка запуску антивірусного захисту або виявлення загрози).

Надсилати кожне сповіщення окремим електронним листом: якщо ввімкнено, кожне сповіщення надсилатиметься окремо. Їх може надійти чимало за короткий проміжок часу.


Інтервал, через який будуть надсилатися нові сповіщення електронною поштою (хв): інтервал у хвилинах, через який електронною поштою надсилатимуться нові сповіщення. Якщо вибрати 0, сповіщення надходитимуть миттєво.

Адреса відправника: у цьому полі необхідно вказати адресу відправника, що відображатиметься в заголовку надісланих електронною поштою сповіщень.

Адреса отримувача: у цьому полі необхідно вказати адресу отримувача, що відображатиметься в заголовку надісланих електронною поштою сповіщень. Якщо потрібно ввести кілька адрес. Розділяйте їх крапкою з комою.

сервер SMTP

Сервер SMTP: сервер SMTP, що використовується для надсилання сповіщень (наприклад, smtp.provider.com:587, попередньо визначений порт — 25).

 Сервери SMTP з шифруванням TLS підтримуються ESET NOD32 Antivirus.

Ім'я користувача й пароль – якщо SMTP-сервер вимагає автентифікації, у ці поля слід ввести дійсні ім'я користувача та пароль, які надають доступ до SMTP-сервера.

Увімкнути TLS: Secure Alert та сповіщення, що використовують шифрування TLS.

Перевірити підключення SMTP: тестовий електронний лист буде надіслано на адресу електронної пошти одержувача. Потрібно заповнити поля "Сервер SMTP", "Ім'я користувача", "Пароль", "Адреса відправника" й "Адреса одержувача".

Формат повідомлень

Зв'язок між програмою та віддаленим користувачем або системним адміністратором установлюється через поштові повідомлення чи повідомлення в локальній мережі (за допомогою служби обміну повідомленнями Windows). **Установлений за замовчуванням формат** сигнальних повідомлень і сповіщень оптимальний для більшості ситуацій. За деяких обставин вам, можливо, знадобиться змінити формат повідомлень про події.

Формат повідомлень про події: формат повідомлень про події, що відображаються на віддалених комп'ютерах.

Формат попереджень про загрози: визначений за замовчуванням формат повідомлень про загрози та сповіщень. ESET не рекомендує змінювати цей формат. Проте за деяких обставин (наприклад, якщо використовується автоматична система обробки електронної пошти) може виникнути необхідність змінити формат повідомлень.

Набір символів: перетворює текст повідомлення електронної пошти на кодування символів ANSI залежно від регіональних параметрів Windows (наприклад, windows-1250, Unicode (UTF-8), ACSII 7-bit або кодування для Японії (ISO-2022-JP)). У результаті "á" буде замінено на "a", а невідомі символи — на "?".

Використовувати кодування даних у формат Quoted-printable – джерело повідомлення електронної пошти буде закодовано у формат Quoted-printable (QP), який використовує символи ASCII та може правильно передати спеціальні символи національного алфавіту електронною поштою у 8-бітному форматі (áéíóú).

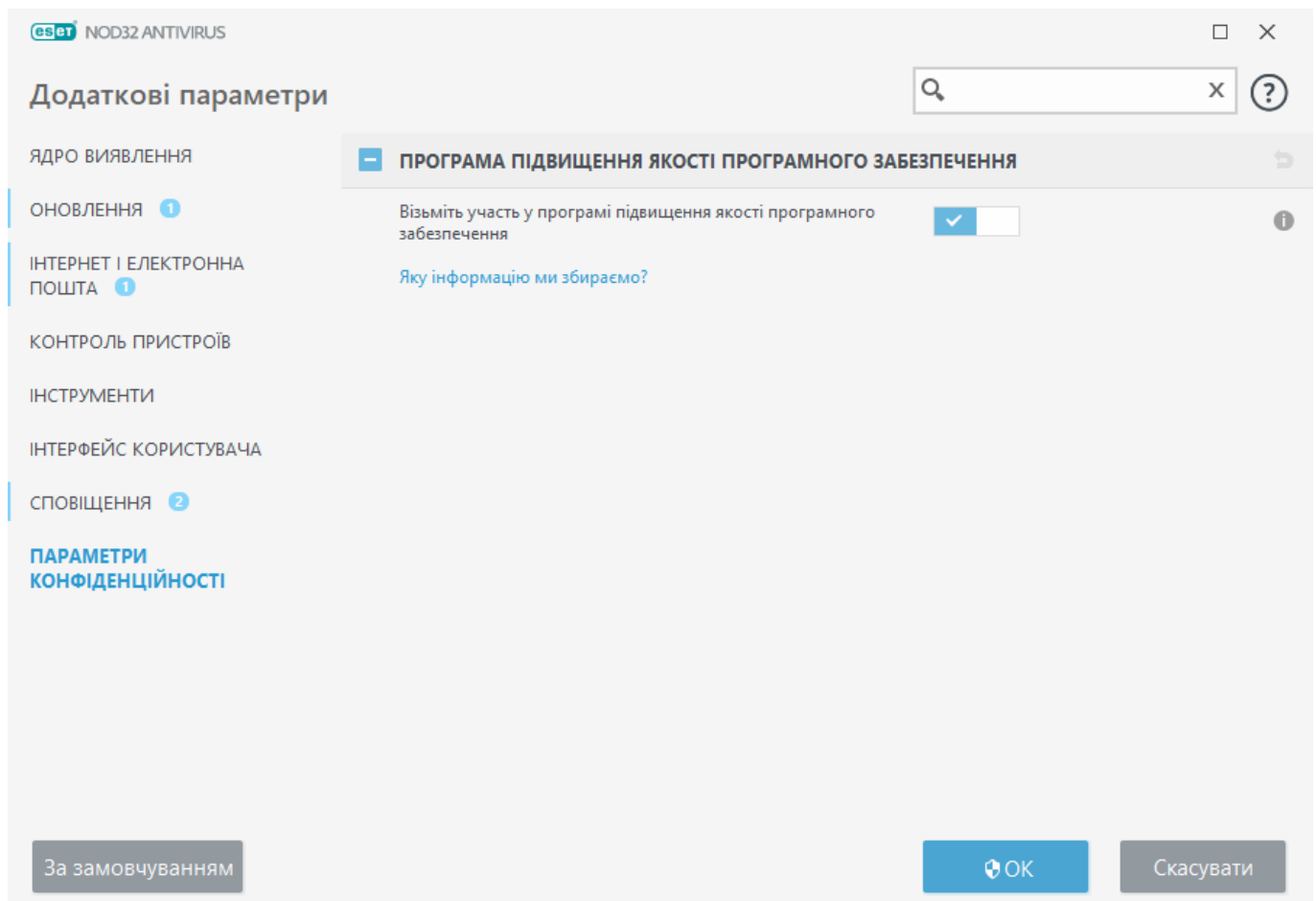
- **%TimeStamp%** – дата й час реєстрації події.
- **%Scanner%** – задіяний модуль.
- **%ComputerName%** – ім'я комп'ютера, на якому зареєстровано сигнал тривоги.

- **%ProgramName%** – програма, яка спричинила тривогу.
- **%InfectedObject%** – ім'я інфікованого файлу, повідомлення тощо.
- **%VirusName%** – ідентифікатор інфекції.
- **%Action%**: дія, виконана у відповідь на виявлення загрози.
- **%ErrorDescription%** – опис події, не пов'язаної з вірусом.

Ключові слова **%InfectedObject%** і **%VirusName%** використовуються лише в попередженнях про загрозу, а **%ErrorDescription%** – лише в повідомленнях про події.

Параметри конфіденційності

У [головному вікні програми](#) натисніть **Налаштування > Додаткові параметри (F5) > Параметри конфіденційності**.



Програма підвищення якості програмного забезпечення

Увімкніть повзунок поруч із пунктом **Узяти участь у програмі підвищення якості програмного забезпечення** для участі в програмі. Якщо ви берете участь у програмі підвищення якості програмного забезпечення, до ESET надсилаються анонімні дані про використання продуктів ESET. Зібрані дані допоможуть нам удосконалити продукт. У жодному разі ми не надаємо ці дані третім сторонам. [Яку інформацію ми збираємо?](#)

Профілі

Менеджер профілів використовується у двох розділах ESET NOD32 Antivirus: **Сканування комп'ютера за вимогою** й **Оновлення**.

Сканування комп'ютера

У ESET NOD32 Antivirus є чотири попередньо визначених профіля сканування:

- **Інтелектуальне сканування** – цей профіль розширеного сканування використовується за замовчуванням. Профіль "Інтелектуальне сканування" використовує технологію Smart-оптимізації, що виключає зі сканування файли, які в процесі попереднього сканування визначені як непошкоджені й з цього моменту не змінювалися. Це дозволяє знизити час сканування з мінімальним впливом на безпеку системи.
- **Сканування з контекстного меню** – у контекстному меню можна запустити сканування за вимогою для будь-якого файлу. Профіль сканування з контекстного меню дозволяє визначити конфігурацію сканування, яка буде використовуватися в разі запуску такого сканування.
- **Детальне сканування** – профіль детального сканування за замовчуванням не використовує технологію Smart-оптимізації, тому за умови використання цього профілю жоден файл не виключається зі сканування.
- **Сканування комп'ютера** – цей профіль використовується за замовчуванням під час стандартного сканування комп'ютера.

Потрібні параметри сканування можна зберегти для майбутнього використання. Рекомендується створити окремі профілі (з різними об'єктами сканування, способами сканування та іншими параметрами) для кожного типу сканування, які регулярно застосовуються.

Щоб створити новий профіль, відкрийте вікно додаткових параметрів (F5) і натисніть **Обробник виявлення > Сканування на шкідливе ПЗ > Сканування комп'ютера за вимогою > Список профілів**. У вікні **Менеджер профілів** міститься розкривне меню **Вибраний профіль** зі списком наявних профілів перевірки й опцією для створення нового. Щоб створити профіль, який точно відповідатиме вашим вимогам, ознайомтесь із вмістом розділу [Налаштування параметрів підсистеми ThreatSense](#), у якому окремо описуються функції кожного параметра сканування.

Припустімо, що вам потрібно створити власний профіль сканування, для якого частково підходить конфігурація функції **Сканування комп'ютера**, але ви не бажаєте сканувати [упаковані](#) або [потенційно небезпечні програми](#) й додатково хочете застосувати параметр **Завжди виправляти виявлені об'єкти**. Введіть ім'я нового профілю у вікні **Менеджер профілів** і натисніть **Додати**. Виберіть новий профіль у розкривному меню **Вибраний профіль** і відкоригуйте решту параметрів відповідно до своїх потреб. Потім натисніть **ОК**, щоб зберегти свій новий профіль.

Оновлення

Редактор профілів у розділі параметрів оновлення дає змогу користувачам створювати нові профілі оновлення. Створювати й використовувати власні спеціальні профілі (відмінні від стандартного **Мій профіль**) слід лише тоді, коли на комп'ютері застосовується кілька способів підключення до серверів оновлення.

Наприклад, портативний комп'ютер, як правило, підключається до локального сервера (дзеркала) в локальній мережі, а в разі відключення від неї (під час відрядження) завантажує оновлення безпосередньо із серверів оновлення ESET. При цьому можуть використовуватися два профілі: перший – для з'єднання з локальним сервером, другий – для підключення до серверів ESET. Налаштувавши ці профілі, перейдіть до меню **Інструменти > Завдання за розкладом** і змініть параметри завдання оновлення. Призначте один профіль первинним, а інший вторинним.

Профіль оновлення: профіль оновлення, який зараз використовується. Щоб змінити його, виберіть інший профіль із розкривного меню.

Список профілів: дає змогу створювати й видаляти профілі оновлення.

Сполучення клавіш

Між елементами інтерфейсу ESET NOD32 Antivirus можна легко переходити за допомогою наведених нижче сполучень клавіш:

Сполучення клавіш	Дія
F1	відкрити сторінку довідки
F5	відкрити додаткові параметри
Стрілка вгору / стрілка вниз	перехід між елементами розкривного меню
TAB	перейти до наступного елемента графічного інтерфейсу користувача у вікні
Shift+TAB	перейти до попереднього елемента графічного інтерфейсу користувача у вікні
ESC	закрити активне діалогове вікно
Ctrl+U	показує інформацію про ліцензію ESET і ваш комп'ютер (докладна інформація для служби технічної підтримки)
Ctrl+R	відновити стандартний розмір вікна та його розміщення на екрані
ALT + стрілка вліво	перейти назад
ALT + стрілка вправо	перейти вперед
ALT+Home	перейти на головну

Для навігації також можна використовувати кнопки для миші "назад" або "вперед".

Діагностичні дані

Модуль діагностики створює дампи робочих процесів ESET у разі збою програми (наприклад, ekrn). Якщо програма аварійно завершує роботу, створюється дамп. Це може допомогти розробникам вирішити різноманітні проблеми з програмою ESET NOD32 Antivirus і налагодити її роботу.

Клацніть розкривне меню **Тип дампу** й виберіть один із трьох доступних параметрів:

- Виберіть **Вимкнути**, щоб вимкнути цю функцію.
- **Мінімальний** (за замовчуванням) – фіксує мінімальний набір корисної інформації, яка може допомогти визначити причину неочікуваного завершення роботи програми. Дамп такого типу може знадобитися, якщо обсяг вільного місця обмежений. Проте аналіз цього файлу може не виявити помилок, які не було безпосередньо спричинено виконуваним потоком, оскільки зібрана інформація є неповною.
- **Повний** – записує весь вміст системної пам'яті в разі аварійного завершення роботи програми. Повний дамп пам'яті може містити дані про процеси, які виконувалися під час створення дампу пам'яті.

Цільовий каталог: каталог збереження файлу дампу в разі збою програми.

Відкрити папку діагностичних даних – натисніть **Відкрити**, щоб відкрити цей каталог у новому вікні Провідника *Windows*.

Створити дамп із даними діагностики – натисніть **Створити**, щоб додати відповідні файли в **Цільовий каталог**.

Розширене ведення журналів

Увімкнути розширене ведення журналів для повідомлень про актуальні пропозиції: записувати всі події, пов'язані з повідомленнями про актуальні пропозиції в продукті.

Розширене ведення журналів Scanner: записувати всі події, які виникають під час сканування файлів і папок компонентом сканування комп'ютера.

Увімкнути розширене журналювання для контролю пристроїв: записувати всі події контролю пристроїв. Це може допомогти розробникам діагностувати й усувати проблеми, пов'язані з контролем пристроїв.

Увімкнути розширене ведення журналів Direct Cloud: записувати всі події ESET LiveGrid®. Це може допомогти розробникам діагностувати й усувати проблеми, пов'язані з ESET LiveGrid®.

Увімкнути розширене ведення журналів для модуля "Захист документів": записувати всі події модуля "Захист документів" для діагностування й вирішення проблем.

Увімкнути розширене ведення журналів захисту поштового клієнта: записувати всі події модуля "Захист поштового клієнта" й плагіна поштового клієнта для діагностики й вирішення проблем.

Увімкнути розширене ведення журналів ядра: записувати всі події в ядрі ESET (ekrn).

Увімкнути розширене журналювання для процедур ліцензування: записувати всю інформацію, пов'язану з обміном даними з серверами активації ESET або серверами ESET License Manager.

Увімкнути відстеження пам'яті: записувати всі події, які допоможуть розробникам діагностувати втрати пам'яті.

Увімкнути розширене ведення журналів для операційної системи: записувати додаткову інформацію про операційну систему, зокрема про виконувані процеси, активність ЦП, операції з диском тощо. Це допоможе розробникам діагностувати й усувати проблеми з продуктом ESET у вашій операційній системі.

Увімкнути розширене журналювання для фільтрації протоколів: записувати всі дані, що проходять через підсистему фільтрації протоколів у форматі PCAP, щоб розробники могли діагностувати й усувати проблеми, пов'язані з фільтрацією протоколів.

Увімкнути розширене ведення журналів для push-повідомлень: записувати всі події, що відбуваються під час надсилання push-повідомлень.

Увімкнути розширене ведення журналів модуля "Захист файлової системи в режимі реального часу": записувати всі події, що відбуваються під час сканування файлів і папок за допомогою модуля "Захист файлової системи в режимі реального часу".

Увімкнути розширене журналювання для підсистеми оновлення: записувати всі події, що трапляються під час оновлення. Це дає розробникам змогу діагностувати й усувати проблеми, пов'язані з підсистемою оновлення.

Розташування файлів журналів: *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Технічна підтримка

Надсилаючи запит у [службу технічної підтримки ESET](#) із продукту ESET NOD32 Antivirus, ви можете відправити дані про конфігурацію системи. У спадному меню **Надіслати дані про конфігурацію системи** виберіть параметр **Завжди надсилати**, щоб відправляти дані автоматично, або натисніть **Запитувати перед надсиланням**, щоб щоразу отримувати запит на підтвердження.

Параметри імпорту та експорту

Можна імпортувати або експортувати спеціально визначений файл конфігурації ESET NOD32 Antivirus .xml із меню **Параметри**.

Ілюстровані інструкції

i У розділі [Import or export ESET configuration settings using an .xml file](#) (Імпорт або експорт параметрів конфігурації ESET за допомогою XML-файлу) є ілюстровані інструкції, доступні англійською й деякими іншими мовами.

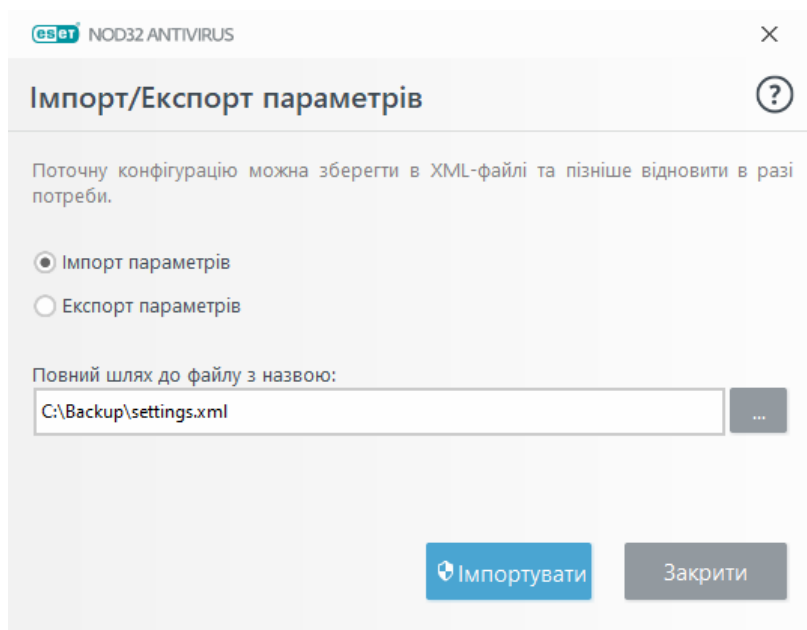
Імпортування й експортування файлів конфігурації є корисними функціями, якщо потрібно створити резервну копію поточної конфігурації ESET NOD32 Antivirus для використання в майбутньому. Окрім того, функція експорту параметрів стане в пригоді, коли потрібно буде

застосовувати власну конфігурацію на кількох комп'ютерах: для передачі параметрів потрібно буде імпортувати файл .xml.


Щоб імпортувати конфігурацію, у [головному вікні програми](#) клацніть **Параметри** > **Імпорт/Експорт параметрів** і виберіть пункт **Параметри імпорту**. Уведіть шлях до файлу конфігурації або натисніть кнопку ... й виберіть файл конфігурації для імпорту.

Щоб експортувати конфігурацію, у [головному вікні програми](#) клацніть **Параметри** > **Імпорт/Експорт параметрів**. Виберіть пункт **Експорт параметрів** і введіть повний шлях до файлу з іменем. Клацніть ... і виберіть папку, куди буде збережено файл конфігурації.

i Під час експортування параметрів може виникнути помилка, якщо ви не маєте достатньо прав для запису експортованого файлу в указаний каталог.



Відновлення всіх параметрів у поточному розділі

Клацніть круглу стрілку , щоб відновити встановлене ESET значення за замовчуванням для всіх параметрів у поточному розділі.

Зверніть увагу, що після вибору параметра **Відновити параметри за замовчуванням** усі зміни буде втрачено.

Відновити вміст таблиць: після ввімкнення цього параметра правила, завдання або профілі, додані вручну чи автоматично, буде втрачено.

Див. також розділ [Імпорт і експорт параметрів](#).

Відновити налаштування за замовчуванням

У розділі "**Додаткові параметри** (F5)" клацніть **За замовчуванням**, щоб повернути всі налаштування програми для всіх модулів до стану, який вони мали б одразу після інсталяції. За замовчуванням, щоб повернути всі налаштування програми для всіх модулів до стану, який вони мали б одразу після інсталяції.

Див. також розділ [Імпорт і експорт параметрів](#).

Помилка під час збереження конфігурації

Це повідомлення про помилку вказує на те, що через помилку параметри не було правильно збережено.

Зазвичай це означає, що користувач, який намагався змінити параметри програми:

- Не має достатніх прав доступу або прав у системі, необхідних для зміни файлів конфігурації й системного реєстру.
> Щоб вносити зміни, адміністратор системи має увійти в систему.
- Нещодавно ввімкнув режим навчання в системі запобігання вторгненням (HIPS) чи брандмауері або намагався внести зміни в розділ "Додаткові параметри".
> Щоб зберегти конфігурацію й уникнути конфлікту конфігурації, закрийте розділ "Додаткові параметри" без збереження змін і спробуйте внести бажані зміни знову.

Інша типова причина — програма не працює належним чином, пошкоджена, а тому потребує повторного встановлення.

Сканер командного рядку

Антивірусний модуль ESET NOD32 Antivirus можна запустити з командного рядка: вручну (командою `ecds`) або за допомогою пакетного файлу (`bat`).

Використання сканера командного рядка ESET

```
ecds [OPTIONS..] FILES..
```

У разі запуску антивірусного сканера з командного рядка можна використовувати наведені нижче параметри та перемикачі.

Параметри

/base-dir=ПАПКА	завантажити модулі з ПАПКИ
/quar-dir=ПАПКА	ПАПКА карантину
/exclude=МАСКА	виключити файли, що відповідають МАСЦІ, під час сканування
/subdir	сканувати підпапки (за замовчуванням)

/no-subdir	не сканувати підпапки
/max-subdir-level=PIBЕНЬ	максимальний підрівень папок, вкладених у папки для сканування
/symlink	переходити за символьними посиланнями (за замовчуванням)
/no-symlink	пропускати символьні посилання
/ads	сканувати ADS (за замовчуванням)
/no-ads	не сканувати ADS
/log-file=ФАЙЛ	виводити дані з журналу у ФАЙЛ
/log-rewrite	перезаписувати вихідний файл (за замовчуванням – дозаписувати)
/log-console	виводити дані журналу на консоль (за замовчуванням)
/no-log-console	не виводити дані журналу на консоль
/log-all	також реєструвати чисті файли
/no-log-all	не реєструвати чисті файли (за замовчуванням)
/aind	показувати індикатор активності
/auto	сканувати всі локальні диски та автоматично очищувати інфекції

Параметри сканера

/files	сканувати файли (за замовчуванням)
/no-files	не сканувати файли
/memory	сканувати пам'ять
/boots	сканувати завантажувальні сектори
/no-boots	не сканувати завантажувальні сектори (за замовчуванням)
/arch	сканувати архіви (за замовчуванням)
/no-arch	не сканувати архіви
/max-obj-size=РОЗМІР	сканувати лише файли, розмір яких не перевищує значення РОЗМІР у мегабайтах (за замовчуванням 0 = необмежено)
/max-arch-level=PIBЕНЬ	максимальний підрівень архівів в архівах (вкладених архівів) для сканування
/scan-timeout=ЛІМІТ	сканувати архіви не довше, ніж визначено значенням ЛІМІТ у секундах
/max-arch-size=РОЗМІР	сканувати лише файли в архівах, розмір яких не перевищує значення РОЗМІР (за замовчуванням 0 = необмежено)
/max-sfx-size=РОЗМІР	сканувати лише файли в саморозпакувальних архівах, якщо їх розмір не перевищує значення РОЗМІР у мегабайтах (за замовчуванням 0 = необмежено)
/mail	сканувати файли електронної пошти (за замовчуванням)
/no-mail	не сканувати файли електронної пошти
/mailbox	сканувати поштові скриньки (за замовчуванням)
/no-mailbox	не сканувати поштові скриньки
/sfx	сканувати саморозпакувальні архіви (за замовчуванням)
/no-sfx	не сканувати саморозпакувальні архіви
/rtp	сканувати упаковані файли (за замовчуванням)

/no-rtp	не сканувати програми для стиснення виконуваних файлів
/unsafe	сканувати на наявність потенційно небезпечних програм
/no-unsafe	не сканувати на наявність потенційно небезпечних програм (за замовчуванням)
/unwanted	сканувати на наявність потенційно небажаних програм
/no-unwanted	не сканувати на наявність потенційно небажаних програм (за замовчуванням)
/suspicious	перевіряти на наявність підозрілих програм (за замовчуванням)
/no-suspicious	не перевіряти на наявність підозрілих програм
/pattern	використовувати вірусні сигнатури (за замовчуванням)
/no-pattern	не використовувати вірусні сигнатури
/heur	увімкнути евристику (за замовчуванням)
/no-heur	вимкнути евристику
/adv-heur	увімкнути розширену евристику (за замовчуванням)
/no-adv-heur	вимкнути розширену евристику
/ext-exclude=РОЗШИРЕННЯ	не сканувати файли, які мають указані РОЗШИРЕННЯ, розділені двокрапкою
/clean-mode=РЕЖИМ	використовувати РЕЖИМ очищення інфікованих об'єктів Доступні наведені нижче варіанти: <ul style="list-style-type: none"> • none (за замовчуванням) – автоматичне очищення не виконується. • standard – програма ecls.exe спробує автоматично очистити або видалити інфіковані файли. • ретельно – програма ecls.exe спробує автоматично очистити або видалити інфіковані файли без втручання користувача (перед видаленням не відображатиметься запит на підтвердження дії). • суворо – програма ecls.exe видалятиме файли без спроби очищення незалежно від їх типу. • видалення – програма ecls.exe без спроби очищення видалятиме файли, оминаючи важливі (наприклад, системні файли Windows).
/quarantine	копіювати інфіковані файли (у разі очищення) до карантину (як доповнення до операції, що виконується під час чищення)
/no-quarantine	не копіювати інфіковані файли до карантину

Загальні параметри

/help	відкрити довідку та вийти
/version	показати інформацію про версію та вийти
/preserve-time	зберегти час останнього доступу

Коди завершення

0	загроз не знайдено
1	загрози знайдено й очищено
10	деякі файли не вдалося просканувати (можуть становити загрозу)

50	знайдено загрозу
100	помилка

i Коди завершення зі значенням більше 100 означають, що файл не був просканий і, відповідно, може бути інфікований.

ESET CMD

Ця функція активує додаткові команди escmd. Що дає змогу експортувати й імпортувати параметри за допомогою командного рядка (escmd.exe). До цього часу експорт та імпорт параметрів був можливий лише за допомогою [графічного інтерфейсу користувача](#). Конфігурацію ESET NOD32 Antivirus можна експортувати у файл формату *.xml*.

Якщо ESET CMD ввімкнено, доступні два методи авторизації.

- **Немає:** без авторизації. Ми не рекомендуємо цей метод, оскільки тоді можна буде імпортувати будь-яку непідписану конфігурацію, що становить потенційний ризик.
- **Пароль для додаткових параметрів:** для імпорту конфігурації з файлу *.xml* буде потрібен пароль. Цей файл має бути підписаним (див. файл конфігурації *.xml* нижче). Для імпорту нової конфігурації спочатку необхідно вказати пароль у підменю [Параметри доступу](#). Якщо параметри доступу не активовано, то пароль не збігатиметься або файл конфігурації у форматі *.xml* не підписуватиметься, тож конфігурація не імпортуватиметься.

Якщо ESET CMD ввімкнено, то для імпорту або експорту конфігурацій ESET NOD32 Antivirus можна використовувати командний рядок. Це можна зробити вручну або створити сценарій для автоматизації.



Щоб використовувати додаткові команди escmd, потрібно запустити їх із правами адміністратора або відкрити командний рядок Windows (cmd), вибравши пункт **У режимі адміністратора**. Якщо цього не зробити, з'явиться повідомлення **Error executing command**. Окрім того, щоб експортувати конфігурацію, потрібна цільова папка. Команда експорту працює, навіть якщо вимкнено параметр ESET CMD.



Команда параметрів експорту:
escmd /getcfg c:\config\settings.xml

Команда параметрів імпорту:
escmd /setcfg c:\config\settings.xml

i Розширені команди escmd можна виконати лише локально.

Підписання файлу конфігурації у форматі *.xml*

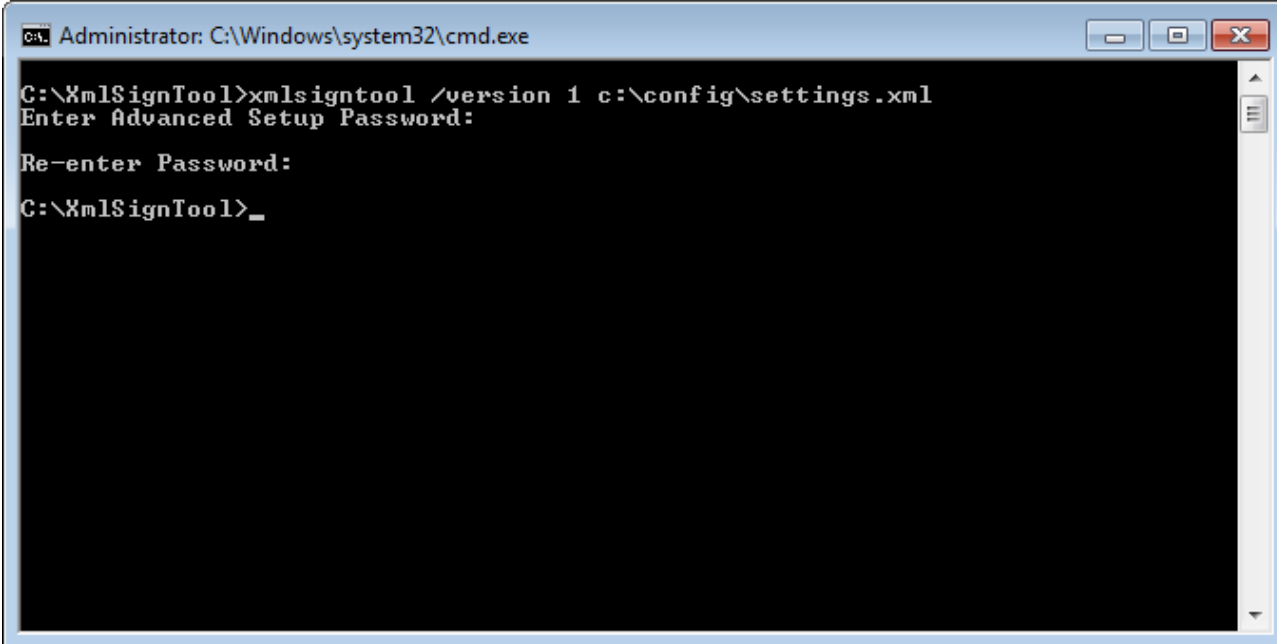
1. Завантажте виконуваний файл [XmlSignTool](#).
2. Відкрийте командний рядок Windows (cmd), вибравши параметр **У режимі адміністратора**.
3. Перейдіть до розташування, в якому збережено файл `xmlsigntool.exe`
4. Щоб підписати файл конфігурації у форматі *.xml*, виконайте таку команду: `xmlsigntool /version 1|2 <xml_file_path>`

Значення параметра `/version` залежить від версії ESET NOD32 Antivirus. Використовуйте параметр `/version 1` для версій продукту ESET NOD32 Antivirus, які передують 11.1. Використовуйте `/version 2` для поточної версії ESET NOD32 Antivirus.

5. Коли з'явиться відповідний запит XmlSignTool, введіть пароль для [додаткових параметрів](#), а потім введіть його повторно. Тепер ваш файл конфігурації у форматі `.xml` підписано, тож його можна використовувати для імпорту іншого екземпляра ESET NOD32 Antivirus за допомогою ESET CMD із використанням пароля для авторизації.

Команда для підпису експортованого файлу конфігурації

```
xmlsigntool /version 2 c:\config\settings.xml
```



Якщо пароль у підменю [Параметри доступу](#) змінено, і необхідно імпортувати файл конфігурації, раніше підписаний старим паролем, потрібно знову підписати файл конфігурації `.xml`, використовуючи поточний пароль. Це дозволяє використовувати старий файл конфігурації, не екпортуючи його на інший комп'ютер із ESET NOD32 Antivirus перед імпортом.

Ми не рекомендуємо вмикати ESET CMD без авторизації, оскільки тоді можна буде імпортувати будь-яку непідписану конфігурацію. Установіть пароль у меню **Додаткові параметри > Інтерфейс користувача > Параметри доступу**, щоб заборонити несанкціоновану зміну користувачами.

Виявлення неактивного стану

Параметри виявлення неактивного стану можна вказати в розділі **Додаткові параметри**. Для цього виберіть **Ядро виявлення > Сканування шкідливого ПЗ > Сканування в неактивному стані > Виявлення неактивного стану**. Ці параметри визначають умови ініціювання [Сканування в неактивному стані](#):

- Вимкнений екран або заставка
- блокування комп'ютера;
- Вихід користувача із системи.

Щоб активувати чи вимкнути певні умови для ініціювання виявлення неактивного стану, скористайтеся відповідними повзунками.

Поширені запитання

У цьому розділі розглянуто питання й проблеми, які виникають у користувачів найчастіше. Клацніть назву теми, щоб дізнатися, як вирішити вашу проблему:

- [Оновлення ESET NOD32 Antivirus](#)
- [Видалення вірусу з ПК](#)
- [Створення нового запланованого завдання](#)
- [Додавання до розкладу завдання сканування \(щотижня\)](#)
- [Як розблокувати додаткові параметри](#)
- [Як вирішити проблему з деактивацією продукту на порталі ESET HOME](#)

Якщо ви не знайшли потрібну проблему в списку вище, виконайте пошук в онлайн-довідці ESET NOD32 Antivirus.

Якщо ви не знайшли спосіб вирішення проблеми (відповідь на питання) в онлайн-довідці ESET NOD32 Antivirus, див. статті в [базі знань ESET](#), яка постійно оновлюється. Нижче наведено посилання на найпопулярніші статті бази знань:

- [Як оновити мою ліцензію?](#)
- [Під час інсталяції продукту ESET виникає помилка активації. Що це означає?](#)
- [Активувати домашню версію продукту ESET для ОС Windows за допомогою імені користувача, пароля або ліцензійного ключа](#)
- [Видалення або повторна інсталяція домашньої версії продукту ESET](#)
- [З'являється повідомлення про те, що інсталяцію ESET перервано.](#)
- [Що робити після оновлення ліцензії? \(Для користувачів домашньої версії.\)](#)
- [Які наслідки матиме зміна електронної адреси?](#)
- [Перенос мого продукту ESET на новий комп'ютер або пристрій](#)
- [Як запустити Windows у безпечному режимі або безпечному режимі з роботою в мережі?](#)
- [Виключення безпечного веб-сайту з блокування](#)
- [Надання доступу програмам для читання екрана до графічного інтерфейсу користувача ESET](#)

За потреби ви можете звернутися із запитаннями чи проблемами до [нашої служби технічної підтримки](#).

Оновлення ESET NOD32 Antivirus

Оновлення ESET NOD32 Antivirus можна виконати вручну або автоматично. Щоб запустити оновлення, натисніть кнопку **Оновити** у [головному вікні програми](#), потім — кнопку **Перевірка наявності оновлень**.

Під час інсталяції програми за замовчуванням створюється завдання автоматичного оновлення, яке виконується щогодини. Для зміни інтервалу оновлення перейдіть до розділу **Інструменти > Розклад**.

Видалення вірусу з ПК

Якщо комп'ютер виявляє ознаки зараження шкідливою програмою, наприклад, працює повільніше, часто "зависає" тощо, рекомендується виконати наведені нижче дії.

1. У [головному вікні програми](#) натисніть **Перевірка комп'ютера**.
2. Натисніть **Сканування комп'ютера**, щоб розпочати сканування системи.
3. Після завершення сканування перегляньте журнал, де вказана кількість просканованих, заражених і очищених файлів.
4. Щоб просканувати лише певну частину диска, натисніть опцію **Вибіркове сканування** та виберіть об'єкти для перевірки на наявність вірусів.

Додаткові відомості див. у [цьому посібнику бази знань ESET](#), вміст якого регулярно оновлюється.

Створення нового запланованого завдання

Щоб створити нове завдання, у меню **Інструменти > Інші інструменти > Планувальник** клацніть **Додати** або натисніть праву кнопку миші для виклику контекстного меню й виберіть пункт **Додати**. Запланувати можна завдання п'ятих різних типів:

- **Запуск зовнішньої програми**: планування запуску зовнішньої програми.
- **Обслуговування журналу** – окрім усього іншого, у журналах також містяться залишки видалених записів. Це завдання регулярно оптимізовує записи в журналах для підвищення ефективності роботи.
- **Перевірка файлів під час запуску системи**: перевірка файлів, що запускаються автоматично під час завантаження системи або входу до облікового запису.
- **Створити знімок стану системи**: створення знімка системи засобом ESET SysInspector, який збирає докладну інформацію про системні компоненти (наприклад, драйвери, програми) й оцінює рівень ризику для кожного з них.
- **Сканування комп'ютера за вимогою**: сканування файлів і папок на комп'ютері.

- **Оновлення** – планування завдання оновлення, у рамках якого оновлюються модулі програми.

Оскільки найчастіше використовуються завдання **Оновлення**, нижче описано, як його додати.

У розкритому меню **Заплановане завдання** виберіть пункт **Оновлення**. Заповніть поле **Ім'я завдання** й натисніть **Далі**. Виберіть періодичність виконання завдання. Доступні наведені нижче варіанти: **Одноразово**, **Багаторазово**, **Щодня**, **Щотижня** та **За умови виникнення події**. Виберіть **Не запускати завдання, якщо комп'ютер працює від батареї**, щоб зменшити використання системних ресурсів, коли портативний комп'ютер працює від батареї. Завдання буде виконуватись у вибраний день і час відповідно до параметрів розділу **Запуск завдання**. Далі слід визначити, яку дію виконувати, якщо завдання не може бути виконане або завершене в запланований час. Можна вибрати один із наведених нижче варіантів.

- **Під час наступного запланованого виконання**
- **Якомога швидше**
- **Негайно, якщо час після останнього запуску перевищує зазначений інтервал** (інтервал можна вибрати за допомогою повзунка **Минуло часу після останнього запуску (годин)**)

У наступному кроці буде показано загальні відомості про поточне заплановане завдання. Натисніть **Готово**, завершивши вносити зміни.

Відкриється діалогове вікно, де користувач може вибрати профілі, які застосовуватимуться для запланованого завдання. Тут можна визначити основний й альтернативний профілі. Альтернативний профіль застосовується, якщо завдання неможливо виконати з використанням основного профілю. Підтвердьте зміни, натиснувши **Готово**. Нове завдання буде додано до списку поточних запланованих завдань.

Додавання до розкладу завдання щотижневого сканування комп'ютера

Щоб запланувати завдання, яке має регулярно виконуватися, відкрийте [головне вікно програми](#) та натисніть **Інструменти > Розклад**. Нижче наведено короткі інструкції щодо того, як запланувати завдання зі сканування локальних дисків комп'ютера раз на тиждень. Докладніші інструкції наведено в [цій статті бази знань](#).

Щоб додати до розкладу завдання сканування, виконайте наведені нижче дії.

1. Натисніть **Додати** на головному екрані розділу "Завдання за розкладом".
2. Уведіть ім'я і в розкритому меню **Тип завдання** виберіть пункт **Сканування комп'ютера за вимогою**.
3. Виберіть параметр **Щотижня** для періодичності виконання завдання.
4. Установіть день і час виконання завдання.
5. Виберіть **Запустити завдання за першої нагоди**, щоб виконати завдання пізніше, якщо

це не вдалося зробити вчасно з якихось причин (наприклад, комп'ютер було вимкнено).

6. Перегляньте загальні відомості про заплановане завдання й клацніть **Готово**.

7. У розкритому меню **Об'єкти** виберіть опцію **Локальні диски**.

8. Натисніть **Готово**, щоб застосувати завдання.

Як розблокувати додаткові параметри, захищені паролем

Якщо потрібно отримати доступ до захищених додаткових параметрів, відобразиться вікно введення пароля. Якщо ви забули або втратили пароль, клацніть **Відновити пароль** і вкажіть адресу електронної пошти, яку ви використали для реєстрації ліцензії. Ви отримаєте електронний лист від ESET із кодом підтвердження, дійсним протягом семи днів. Уведіть цей код і підтвердьте новий пароль. Код підтвердження діє протягом семи днів.

Відновити пароль через обліковий запис ESET HOME: скористайтесь цим параметром, якщо ліцензія, яку використано для активації, пов'язана з вашим обліковим записом ESET HOME. Уведіть адресу електронної пошти для входу в обліковий запис [ESET HOME](#).

Якщо ви не запам'ятали адресу електронної пошти або стикаєтеся з труднощами під час відновлення пароля, клацніть **Зверніться до служби технічної підтримки**. Відкриється веб-сайт ESET для звернення в службу технічної підтримки.

Згенерувати код для служби технічної підтримки: цей параметр дає змогу згенерувати код для служби технічної підтримки. Скопіюйте код, наданий службою технічної підтримки, і клацніть **У мене є код підтвердження**. Уведіть цей код і підтвердьте новий пароль. Код підтвердження діє протягом семи днів.

Більш докладну інформацію див. в розділі [Розблокування пароля налаштувань у продуктах ESET для Windows для приватного використання](#).

Як вирішити проблему з деактивацією продукту на порталі ESET HOME

Продукт не активовано

Це повідомлення про помилку з'являється, коли власник ліцензії деактивує ваш продукт ESET NOD32 Antivirus на порталі ESET HOME або у вашого облікового запису ESET HOME забирають доступ до ліцензії. Щоб вирішити цю проблему, дотримуйтеся таких інструкцій:

- Натисніть **Активувати** та скористайтесь одним зі [способів активації](#) для продукту ESET NOD32 Antivirus.
- Повідомте власника ліцензії, що він деактивував ваш продукт ESET NOD32 Antivirus або у вас забрали доступ до ліцензії. Власник зможе вирішити проблему на [ESET HOME](#).

Продукт деактивовано, пристрій відключено

Це повідомлення про помилку з'являється після [видалення пристрою з облікового запису ESET HOME](#). Щоб вирішити цю проблему, дотримуйтеся таких інструкцій:

- Натисніть **Активувати** та скористайтесь одним зі [способів активації](#) для продукту ESET NOD32 Antivirus.
- Повідомте власника ліцензії, що ваш продукт ESET NOD32 Antivirus деактивовано й пристрій відключено від порталу ESET HOME.
- Якщо ви власник ліцензії та не знаєте про ці зміни, перегляньте [записи в стрічці активності на ESET HOME](#). Якщо ви знайдете записи про підозрілі дії, [змінить пароль облікового запису ESET HOME](#) і [зверніться в службу технічної підтримки ESET](#).

Продукт деактивовано, пристрій відключено

Це повідомлення про помилку з'являється після [видалення пристрою з облікового запису ESET HOME](#). Щоб вирішити цю проблему, дотримуйтеся таких інструкцій:

- Натисніть **Активувати** та скористайтесь одним зі [способів активації](#) для продукту ESET NOD32 Antivirus.
- Повідомте власника ліцензії, що ваш продукт ESET NOD32 Antivirus деактивовано й пристрій відключено від порталу ESET HOME.
- Якщо ви власник ліцензії та не знаєте про ці зміни, перегляньте [записи в стрічці активності на ESET HOME](#). Якщо ви знайдете записи про підозрілі дії, [змінить пароль облікового запису ESET HOME](#) і [зверніться в службу технічної підтримки ESET](#).

Продукт не активовано

Це повідомлення про помилку з'являється, коли власник ліцензії деактивує ваш продукт ESET NOD32 Antivirus на порталі ESET HOME або у вашого облікового запису ESET HOME забирають доступ до ліцензії. Щоб вирішити цю проблему, дотримуйтеся таких інструкцій:

- Натисніть **Активувати** та скористайтесь одним зі [способів активації](#) для продукту ESET NOD32 Antivirus.
- Повідомте власника ліцензії, що він деактивував ваш продукт ESET NOD32 Antivirus або у вас забрали доступ до ліцензії. Власник зможе вирішити проблему на [ESET HOME](#).

Програма підвищення якості програмного

забезпечення

Якщо ви берете участь у програмі підвищення якості програмного забезпечення, до ESET надсилаються анонімні дані про використання ваших продуктів. Більш докладну інформацію про обробку даних див. на сторінці Політика конфіденційності.

Ваша згода

Участь у цій програмі добровільна. Для цього потрібна ваша згода. Участь у цій програмі не вимагатиме від вас жодних дій. Згоду можна відкликати в будь-який час у параметрах продукту. Після цього ми більше не будемо обробляти анонімні дані від вас.

Згоду можна відкликати в будь-який час у параметрах продукту.

- [Зміна параметрів програми підвищення якості програмного забезпечення в домашніх версіях продуктів ESET для Windows](#)

Які типи інформації ми збираємо?

Дані про взаємодію з продуктом

Ці дані дозволяють нам дізнатися більше про те, як використовуються наші продукти. Завдяки цим даним ми знаємо, зокрема, про таке: функції, які використовуються найчастіше, параметри, які змінюють користувачі, тривалість використання продукту тощо.

Дані про пристрої

Ми збираємо ці дані, щоб розуміти, де та на яких пристроях використовуються наші продукти. Збираються, зокрема, дані про модель пристрою, країну, версію й назву операційної системи.

Дані діагностики помилок

Окрім того, збираються дані про помилки й випадки аварійного завершення роботи. Збираються, зокрема, дані про помилки, що виникли, а також про дії, які призвели до цього.

Для чого ми збираємо цю інформацію?

Ця анонімна інформація дозволяє нам удосконалювати наші продукти для вас — наших користувачів. Вона дозволяє нам забезпечити максимально можливий рівень відповідності наших продуктів потребам користувачів, зробити їх якомога зручнішими, а також максимально зменшити кількість помилок.

Хто контролює цю інформацію?

ESET, spol. s r.o. є єдиним контролером даних, зібраних у цій програмі. Ми не надаємо ці дані третім сторонам.

Ліцензійна угода з кінцевим користувачем

Набуває чинності 19 жовтня 2021 року.

УВАГА! Перш ніж завантажувати, інстальювати, копіювати або використовувати продукт, уважно ознайомтеся з наведеними нижче положеннями й умовами його застосування.

ЗАВАНТАЖИВШИ, ІНСТАЛЮВАВШИ, СКОПІЮВАВШИ АБО ЗАСТОСУВАВШИ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИ ПРИЙМАЄТЕ ЦІ ПОЛОЖЕННЯ Й УМОВИ, А ТАКОЖ ПОГОДЖУЄТЕСЯ З [ПОЛІТИКОЮ КОНФІДЕНЦІЙНОСТІ](#).

Ліцензійна угода з кінцевим користувачем

Ця ліцензійна угода з кінцевим користувачем ("Угода"), укладена між компанією ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 85101 Bratislava, Slovak Republic, унесена до комерційного реєстру окружного суду м. Братислави I. Розділ Sro, запис № 3586/B, реєстраційний номер: 31333532 ("ESET" або "Постачальник") і Вами, фізичною або юридичною особою ("Ви" або "Користувач"), надає Вам право використовувати Програмне забезпечення, визначене в статті 1 цієї Угоди. Указане Програмне забезпечення можна отримати на носії даних або електронною поштою, завантажити з Інтернету, серверів Постачальника або отримати з інших джерел відповідно до зазначених нижче умов і положень.

ЦЕ УГОДА ПРО ПРАВА КОРИСТУВАЧА, А НЕ ДОГОВІР КУПІВЛІ. Постачальник залишає за собою право власності на копію Програмного забезпечення та фізичного носія, на якому Програмне забезпечення постачається в товарній упаковці, а також усі інші копії, які Користувач має право створювати відповідно до умов цієї Угоди.

Вибравши під час завантаження, інсталяції, копіювання або використання Програмного забезпечення варіант «Прийняти», Ви засвідчуєте свою згоду дотримуватись умов і положень цієї Угоди та підтверджуєте ознайомлення з Політикою конфіденційності. Якщо Ви не погоджуєтесь з будь-якими положеннями або умовами Угоди та/або Політики конфіденційності, виберіть варіант «Закрити», скасуйте інсталяцію чи завантаження, знищте Програмне забезпечення, інсталяційний носій, супровідну документацію та товарний чек або поверніть їх Постачальнику чи в торгову точку, де Ви отримали Програмне забезпечення.

ВИ ПОГОДЖУЄТЕСЯ, ЩО ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАСВІДЧУЄ ФАКТ ПРОЧИТАННЯ ВАМИ ЦЬОЇ УГОДИ, РОЗУМІННЯ ЇЇ УМОВ І ПОЛОЖЕНЬ ТА ВАШУ ЗГОДУ НА ЇЇ ДОТРИМАННЯ.

1. Програмне забезпечення. Термін "Програмне забезпечення" в цій Угоді означає: (i) комп'ютерну програму, що супроводжується цією Угодою, включно з усіма її компонентами; (ii) увесь вміст дисків, компакт- і DVD-дисків, повідомлень електронної пошти та будь-яких вкладень або інших носіїв, з якими надається ця Угода, разом із формою об'єктного коду Програмного забезпечення, що постачається на носії даних, надається електронною поштою чи завантажується через Інтернет; (iii) усі письмові пояснення та будь-яку іншу документацію, пов'язану з Програмним забезпеченням, насамперед опис Програмного забезпечення, його характеристик, властивостей і способу використання, опис операційного середовища, у якому використовується Програмне забезпечення, інструкції із застосування або інсталяції Програмного забезпечення чи будь-який опис правил його використання ("Документація"); (iv) копії Програмного забезпечення, виправлення можливих помилок Програмного забезпечення, доповнення до нього, його розширення, змінні версії Програмного забезпечення й усі оновлення його компонентів (якщо є), право на використання яких Вам надає Постачальник

згідно з розділом 3 цієї Угоди. Програмне забезпечення постачається виключно як виконуваний об'єктний код.

2. Інсталяція, комп'ютер і ліцензійний ключ. Програмне забезпечення, яке надається на носії даних або електронною поштою, завантажується з Інтернету, серверів Постачальника або отримується з інших джерел, необхідно інсталювати. Ви маєте інсталювати Програмне забезпечення на правильно налаштованому комп'ютері відповідно до мінімальних потреб, наведених у відповідній Документації. Метод інсталяції описано в Документації. На Комп'ютері, де Ви інсталюєте Програмне забезпечення, не повинно бути жодних програм або компонентів обладнання, які можуть негативно вплинути на роботу Програмного забезпечення. Під Комп'ютером розуміється обладнання, яке включає в себе, серед іншого, персональні комп'ютери, ноутбуки, робочі станції, надолонні комп'ютери, смартфони, ручні електронні пристрої або інші електронні пристрої, для яких розроблено Програмне забезпечення, на яких воно буде інсталюватися та (або) використовуватися. Ліцензійний ключ — унікальна послідовність символів, літер, цифр або спеціальних символів, що надається Кінцевому користувачу для легального використання Програмного забезпечення, його особливих версій або продовження терміну дії Ліцензії у відповідності до умов цієї Угоди.

3. Ліцензія. Якщо Ви погоджуєтесь з положеннями цієї Угоди й дотримуетесь усіх наведених тут умов і положень, Постачальник надає Вам указані права ("Ліцензію").

а) Інсталяція та використання. Вам надається невиняткове та непередаване право інсталювати Програмне забезпечення на жорсткому диску комп'ютера або іншому носії для постійного зберігання даних, інсталяції та збереження Програмного забезпечення в пам'яті комп'ютерної системи, а також застосовувати, зберігати й відображати Програмне забезпечення.

б) Застереження щодо кількості ліцензій. Право використання Програмного забезпечення обумовлюється кількістю Користувачів. Наведена нижче інформація стосується одного Користувача: (i) інсталяція Програмного забезпечення на одній комп'ютерній системі або (ii) за умови, що обсяг ліцензії визначається кількістю поштових скриньок, один Користувач означає користувача комп'ютера, який отримує електронну пошту через користувацький поштовий агент («КПА»). Якщо КПА приймає електронну пошту, після чого автоматично розподіляє її між кількома користувачами, кількість Користувачів визначається відповідно до їх фактичного числа, серед якого розподіляється електронна пошта. Якщо поштовий сервер виконує функцію поштового шлюзу, кількість Користувачів дорівнює числу користувачів поштових серверів, яких обслуговує такий шлюз. Якщо адреси електронної пошти (наприклад, псевдоніми), точна кількість яких не визначена, належать одному користувачеві й один користувач приймає всі відповідні повідомлення, а пошта не розподіляється автоматично клієнтом між більшою кількістю користувачів, Ліцензія необхідна лише для одного комп'ютера. Забороняється одночасно використовувати одну й ту саму Ліцензію на кількох комп'ютерах. Кінцевий користувач має право вводити Ліцензійний ключ у Програмному забезпеченні виключно в межах наявних у цього користувача прав на використання Програмного забезпечення та у відповідності до обмеження кількості Ліцензій, наданих Постачальником. Ліцензійний ключ є конфіденційною інформацією. Ви не маєте права ділитися Ліцензійним ключем із третіми особами або дозволяти їм використовувати Ліцензійний ключ, якщо це не дозволено цією Угодою або Постачальником. У випадку порушення конфіденційності Ліцензійного ключа негайно повідомте про це Постачальника.

с) Home/Business Edition. Версія Програмного забезпечення Home Edition має використовуватися виключно в приватному та (або) некомерційному середовищі лише для сімейних і домашніх потреб. Для використання в комерційному середовищі та на поштових серверах, засобах

пересилання пошти, поштових або інтернет-шлюзах потрібно придбати версію Програмного забезпечення Business Edition.

г) **Термін дії ліцензії.** Право використання Програмного забезпечення обмежено в часі.

е) **ОЕМ-версія Програмного забезпечення.** OEM-версії Програмного забезпечення мають використовуватися лише на Комп'ютері, з яким постачаються. Його заборонено передавати для використання на іншому комп'ютері.

ф) **НДП та ПРОБНА ВЕРСІЯ Програмного забезпечення.** Програмне забезпечення, що визначається як «не для продажу» (НДП), або його ПРОБНА ВЕРСІЯ не підлягає оплаті та має використовуватися лише в демонстраційних цілях чи для тестування функцій Програмного забезпечення.

г) **Припинення дії ліцензії.** Дія ліцензії припиняється автоматично після закінчення періоду, на який вона надається. Якщо Ви не дотримуєтеся положень цієї Угоди, Постачальник має право скасувати Угоду без шкоди для своїх прав або судового захисту, що надається Постачальнику в таких випадках. У разі скасування Ліцензії Ви повинні негайно видалити, знищити чи повернути за власний кошт Програмне забезпечення та всі резервні копії в компанію ESET або торгову точку, де Ви отримали Програмне забезпечення. Якщо дію Ліцензії припинено, Постачальник також має право скасувати право Користувача використовувати функції Програмного забезпечення, для чого потрібне підключення до серверів Постачальника або серверів третіх осіб.

4. **Функції, для яких потрібні дозволи на збір даних та доступ до Інтернету.** Для правильної роботи Програмному забезпеченню потрібно збирати дані (у відповідності до Політики конфіденційності), підключатися до Інтернету і через рівні проміжки часу з'єднуватися з серверами Постачальника або третіх осіб. Нижче вказано функції Програмного забезпечення, для яких потрібно підключення до Інтернету до дозволи на збір даних:

а) **Оновлення Програмного забезпечення.** Постачальник може час від часу випускати оновлення Програмного забезпечення (далі «Оновлення»), але не зобов'язаний надавати їх. Цю функцію активовано у стандартних налаштуваннях Програмного забезпечення; таким чином, Оновлення інстальються автоматично, якщо Користувач не вимкнув відповідну функцію. Для надання оновлень нам необхідно перевірити автентичність Ліцензії, включаючи інформацію про комп'ютер та (або) платформу, на якій інстальовано Програмне забезпечення у відповідності до Політики конфіденційності.

На надання Оновлень може поширюватися Політика закінчення терміну служби ("Політика EOL"), доступна за адресою https://go.eset.com/eol_home. Оновлення Програмного забезпечення не надаватимуться після завершення терміну служби будь-яких його функцій, визначених у Політиці EOL.

б) **Надсилання Постачальнику Інформації про загрози.** Програмне забезпечення має функції, які збирають зразки вірусів та інших шкідливих комп'ютерних програм, а також підозрілих, проблемних, потенційно небажаних або небезпечних об'єктів: файлів, URL-адрес, IP-пакетів і Ethernet-фреймів ("Загрози"). Ці відомості ("Дані"), зокрема інформація про процес інсталяції, комп'ютер і (або) платформу, на яких інстальовано Програмне забезпечення, операції й роботу Програмного забезпечення, надсилаються Постачальнику. Інформація про Загрози та Дані можуть містити відомості про Кінцевого користувача й інших користувачів комп'ютера, на якому інстальовано Програмне забезпечення (зокрема випадково отримані особисті дані), і файли, пошкоджені внаслідок Загроз, з відповідними метаданими.

Дані та Інформацію про загрози збирають такі функції ПЗ:

i. LiveGrid Reputation System передбачає збір і надсилання Постачальнику односторонніх хешів, пов'язаних із загрозами. Ця функція активується в стандартних налаштуваннях ПЗ.

ii. LiveGrid Feedback System передбачає збір і надсилання Постачальнику Даних про загрози з відповідними метаданими та Інформації. Цю функцію активує Кінцевий користувач під час інсталяції Програмного забезпечення.

Постачальник використовує Дані й Інформацію про загрози лише для аналізу та дослідження несанкціонованого доступу, удосконалення Програмного забезпечення та перевірки автентичності Ліцензії. Потім Постачальник уживає належних заходів, щоб забезпечити конфіденційність отриманих даних. Активуючи описану вище функцію Програмного забезпечення, Ви надаєте Постачальнику право збирати і обробляти Дані й Інформацію про загрози відповідно до чинних правових норм. Ви завжди можете відключити ці функції.

З метою виконання положень цієї Угоди Постачальнику необхідно збирати, обробляти та зберігати дані, які дають змогу ідентифікувати Вас, у відповідності до Політики конфіденційності. Ви дозволяєте Постачальнику власними засобами перевіряти, чи використовуєте Ви програмне забезпечення у відповідності до положень цієї Угоди. Ви погоджуєтесь, що з метою виконання положень цієї Угоди для забезпечення функціональності Програмного забезпечення і надання авторизації на його використання, а також для захисту прав Постачальника будуть передаватися дані між Програмним забезпеченням і комп'ютерними системами Постачальника та його бізнес-партнерів, що входять до його мережі підтримки та розповсюдження.

Після укладання цієї Угоди Постачальник або його бізнес-партнери (які входять до мережі підтримки і розповсюдження Постачальника) матимуть право передавати, обробляти й зберігати важливі дані, що ідентифікують Вас, для виставлення рахунків, виконання цієї Угоди та передавання сповіщень на Ваш комп'ютер.

Докладні відомості про конфіденційність, захист персональних даних і Ваші права як суб'єкта даних можна знайти в документі "Політика конфіденційності" на веб-сайті Постачальника. Окрім того, ця інформація доступна безпосередньо в процесі інсталяції. Також можна ознайомитися з цим документом у довідці Програмного забезпечення.

5. Реалізація прав Користувача. Ви зобов'язуєтесь реалізувати права Користувача особисто або через своїх співробітників. Ви маєте право використовувати Програмне забезпечення лише для захисту безпеки своєї роботи та тих комп'ютерів і комп'ютерних систем, для яких надано Ліцензію.

6. Обмеження прав. Вам забороняється копіювати, розповсюджувати, вилучати компоненти чи створювати похідні продукти на основі цього Програмного забезпечення. Використовуючи Програмне забезпечення, Ви зобов'язуєтесь дотримуватися наведених нижче обмежень.

а) Ви можете створити одну копію Програмного забезпечення на носії для постійного збереження даних за умови, що така архівна резервна копія не буде інсталюватися та використовуватися на будь-якому іншому комп'ютері. Створення будь-яких інших копій Програмного забезпечення вважається підставою для скасування цієї Угоди.

б) Ви не маєте права використовувати, змінювати, перебудовувати Програмне забезпечення,

робити його копії або передавати право на використання Програмного забезпечення чи його копій будь-яким способом, окрім чітко передбаченого положеннями цієї Угоди.

с) Вам забороняється продавати, надавати в оренду, позичати Програмне забезпечення, передавати право на його користування чи використовувати його з комерційною метою.

д) Ви не маєте права виконувати зворотне проектування, декомпілювати або дезасемблювати Програмне забезпечення чи застосувати будь-які інші засоби виявлення його вихідного коду, крім випадків, коли таке обмеження прямо заборонене законодавством.

е) Ви погоджуєтесь використовувати Програмне забезпечення лише таким способом, що відповідає всім застосовним юридичним нормам законодавства, яке регулює його застосування, включно з відповідними обмеженнями згідно із законом про авторське право й інші права на інтелектуальну власність, але не обмежуючись цим.

ф) Ви даєте свою згоду використовувати Програмне забезпечення та його функції лише таким способом, що не обмежує можливостей доступу до них інших кінцевих користувачів. Постачальник зберігає за собою право обмежити перелік доступних послуг, що надаються окремим кінцевим користувачам, з метою надання своїх послуг максимальній кількості кінцевих користувачів. Обмеження переліку доступних послуг також передбачає повну заборону на використання будь-яких функцій Програмного забезпечення й видалення Даних та інформації із серверів Постачальника або серверів третьої сторони, пов'язаних із конкретною функцією Програмного забезпечення.

г) Ви погоджуєтесь не вчиняти будь-які дії щодо використання Ліцензійного ключа, які суперечать положенням цієї Угоди або можуть призвести до передачі Ліцензійного ключа будь-якій особі, яка не має права використовувати Програмне забезпечення. Зокрема, Ви погоджуєтесь не передавати використовуваний або невикористовуваний Ліцензійний ключ у будь-якій формі, а також утриматися від несанкціонованого відтворення або розповсюдження дублікатів Ліцензійних ключів або створених Ліцензійних ключів або від використання Програмного забезпечення з Ліцензійним ключем, отриманим із будь-якого іншого джерела, окрім Постачальника.

7. Авторське право. Програмне забезпечення та всі права, включно із правами власності та відповідними правами на інтелектуальну власність без обмежень, належать компанії ESET та/або її ліцензіарам. Ці права захищено положеннями міжнародного договірної права та всіма іншими застосовними законами країни, у якій використовується Програмне забезпечення. Структура, організація та код Програмного забезпечення є комерційною таємницею та конфіденційною інформацією компанії ESET і/або її ліцензіарів. Ви не маєте права копіювати Програмне забезпечення, за винятком визначених у розділі 6 (а) випадків. Будь-які копії, які дозволено створювати відповідно до умов цієї Угоди, мають містити такі самі позначки про право власності й авторське право, які використано у Програмному забезпеченні. Якщо Ви виконуєте зворотне проектування, декомпілюєте чи дезасемблюєте Програмне забезпечення або застосовуєте будь-які інші засоби виявлення його вихідного коду, тим самим порушуючи умови цієї Угоди, то погоджуєтесь, що будь-яка отримана таким чином інформація буде автоматично й безповоротно вважатися належною для передавання Постачальнику та цілком належатиме йому з моменту її отримання, незалежно від права Постачальника на розірвання цієї Угоди.

8. Захист прав. Постачальник залишає за собою всі права на Програмне забезпечення, за винятком тих, що чітко надані Вам як Користувачу Програмного забезпечення відповідно до умов цієї Угоди.

9. Багатомовні версії, програмне забезпечення, що постачається на носіях двох типів, кілька копій. Якщо Програмне забезпечення підтримує кілька платформ чи мов, або Ви одержали кілька копій Програмного забезпечення, Ви не маєте права інсталиювати Програмне забезпечення на більшій кількості комп'ютерних систем або інші версії ніж ті, на які розповсюджується Ліцензія. Вам забороняється продавати, надавати в оренду, позичати Програмне забезпечення, укласти договір лізингу, надавати право на користування чи передавати версії або копії Програмного забезпечення, які Ви не використовуєте.

10. Набуття Угодою чинності та припинення дії Угоди. Ця Угода набуває чинності з дати погодження з її умовами. Ви можете припинити дію цієї Угоди, остаточно видаливши, знищивши або повернувши за власний кошт Програмне забезпечення, усі резервні копії та всі пов'язані матеріали, отримані від Постачальника або його ділових партнерів. На право використання Програмного забезпечення та його функцій може поширюватися Політика EOL. Після завершення терміну служби Програмного забезпечення або будь-яких його функцій, визначених у Політиці EOL, ваше право на використання Програмного забезпечення буде скасовано. Незалежно від способу припинення дії цієї Угоди, умови розділів 7, 8, 11, 13, 19 і 21 є чинними без обмежень у часі.

11. ЗАЯВА КОРИСТУВАЧА. ЯК КОРИСТУВАЧ, ВИ ВИЗНАЄТЕ, ЩО ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАДАЄТЬСЯ «ЯК Є» БЕЗ БУДЬ-ЯКИХ СПЕЦІАЛЬНИХ АБО НЕПРЯМИХ ГАРАНТІЙ, НАСКІЛЬКИ ЦЕ ДОПУСКАЄТЬСЯ ЧИННИМ ЗАКОНОДАВСТВОМ. НІ ПОСТАЧАЛЬНИК РАЗОМ ІЗ ЙОГО ЛІЦЕНЗІАРАМИ Й ДОЧІРНІМИ КОМПАНІЯМИ, НІ ВЛАСНИКИ АВТОРСЬКОГО ПРАВА НЕ НАДАЮТЬ БУДЬ-ЯКИХ ТВЕРДЖЕНЬ АБО СПЕЦІАЛЬНИХ ЧИ НЕПРЯМИХ ГАРАНТІЙ, ЗОКРЕМА ГАРАНТІЙ ПРИДАТНОСТІ ДЛЯ ПРОДАЖУ ЧИ КОНКРЕТНОГО ЗАСТОСУВАННЯ АБО ГАРАНТІЙ ТОГО, ЩО ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НЕ ПОРУШУЄ БУДЬ-ЯКІ ПАТЕНТИ, АВТОРСЬКІ ПРАВА, ТОВАРНІ ЗНАКИ ЧИ ІНШІ ПРАВА ТРЕТІХ СТОРІН. ПОСТАЧАЛЬНИК АБО БУДЬ-ЯКА ІНША СТОРОНА НЕ НАДАЄ ЖОДНИХ ГАРАНТІЙ ТОГО, ЩО ФУНКЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІДПОВІДАТИМУТЬ ВАШИМ ВИМОГАМ АБО ВОНО ФУНКЦІОНУВАТИМЕ БЕЗПЕРЕБІЙНО ТА БЕЗ ПОМИЛОК. ВИ УСВІДОМЛЮЄТЕ РИЗИКИ, ПОВ'ЯЗАНІ З ВИБОРОМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДОСЯГНЕННЯ ПОТРІБНИХ РЕЗУЛЬТАТІВ, І БЕРЕТЕ НА СЕБЕ ПОВНУ ВІДПОВІДАЛЬНІСТЬ ЗА ЦЕ, А ТАКОЖ ЗА ІНСТАЛЯЦІЮ, ВИКОРИСТАННЯ ТА НАСЛІДКИ ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.

12. Відсутність інших зобов'язань. Ця Угода не створює жодних зобов'язань із боку Постачальника та його ліцензіарів, окрім тих, що чітко визначено в цьому документі.

13. ОБМЕЖЕННЯ ВІДПОВІДАЛЬНОСТІ. У МАКСИМАЛЬНО ДОЗВОЛЕНИХ РАМКАХ, ВИЗНАЧЕНИХ ЧИННИМ ЗАКОНОДАВСТВОМ, ЗА ЖОДНИХ ОБСТАВИН ПОСТАЧАЛЬНИК, ЙОГО СПІВРОБІТНИКИ АБО ЛІЦЕНЗІАРИ НЕ НЕСУТЬ ВІДПОВІДАЛЬНОСТІ ЗА БУДЬ-ЯКІ ВТРАЧЕНІ ПРИБУТКИ, ДОХОДИ, ЗНИЖЕННЯ ОБСЯГІВ ПРОДАЖІВ АБО ВТРАТУ ДАНИХ, А ТАКОЖ ДОДАТКОВІ ВИТРАТИ, ПОВ'ЯЗАНІ З ПРИДБАННЯМ ЗАПАСНИХ ТОВАРІВ АБО ПОСЛУГ, ЗАПОДІЯНУ МАЙНУ ШКОДУ, ОСОБИСТУ ШКОДУ, ПРИПИНЕННЯ КОМЕРЦІЙНОЇ ДІЯЛЬНОСТІ, ВТРАТУ ДІЛОВОЇ ІНФОРМАЦІЇ ЧИ БУДЬ-ЯКІ СПЕЦІАЛЬНІ, ПРЯМІ, НЕПРЯМІ, ВИПАДКОВІ, КОМЕРЦІЙНІ, ШТРАФНІ ЧИ ОПОСЕРЕДКОВАНІ ЗБИТКИ, БУДЬ-ЯКИМ ЧИНОМ ОБУМОВЛЕНІ ДІЄЮ УГОДИ, ЦИВІЛЬНЕ ПРАВОПОРУШЕННЯ, НЕДБАЛІСТЬ АБО ІНШИЙ ФАКТ, ЩО ВИМАГАЄ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ ВНАСЛІДОК ІНСТАЛЯЦІЇ, ВИКОРИСТАННЯ АБО НЕМОЖЛИВОСТІ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАВІТЬ ЯКЩО ПОСТАЧАЛЬНИКУ, ЙОГО ЛІЦЕНЗІАРАМ АБО ДОЧІРНИМ КОМПАНІЯМ ВІДОМО ПРО МОЖЛИВІСТЬ ТАКИХ ЗБИТКІВ. В ОКРЕМИХ КРАЇНАХ І ЮРИСДИКЦІЯХ НЕ ПЕРЕДБАЧЕНО ВИНЯТКИ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ, АЛЕ ЇЇ МОЖЕ БУТИ ОБМЕЖЕНО. ТОБТО ВІДПОВІДАЛЬНІСТЬ ПОСТАЧАЛЬНИКА, ЙОГО СПІВРОБІТНИКІВ, ЛІЦЕНЗІАРІВ АБО ДОЧІРНИХ КОМПАНІЙ ОБМЕЖУЄТЬСЯ СУМОЮ, ЯКУ ВИ СПЛАТИЛИ ЗА ЛІЦЕНЗІЮ.

14. Жодна умова цієї Угоди не має порушувати законні права будь-якої сторони, що виступає як

клієнт, у тих випадках, коли вони їм суперечать.

15. Технічна підтримка. Компанія ESET або вповноважені нею треті сторони надають технічну підтримку на власний розсуд без жодних гарантій або заяв. Технічна підтримка не надаватиметься після завершення терміну служби Програмного забезпечення або будь-яких його функцій, визначених у Політиці EOL. Перед наданням технічної підтримки Користувач повинен створити резервні копії всіх поточних даних, програмного забезпечення та програмних засобів. Компанія ESET або вповноважені нею треті сторони не несуть відповідальності за пошкодження або втрату даних, майна, програмного чи апаратного забезпечення, а також комерційні збитки, що виникають унаслідок надання технічної підтримки. Компанія ESET і/або вповноважені нею треті сторони залишають за собою право приймати рішення щодо того, чи належить проблема до обсягу послуг, які надаються в рамках технічної підтримки. Компанія ESET залишає за собою право на власний розсуд приймати рішення щодо відмови в наданні технічної підтримки, її призупинення чи скасування. Для забезпечення технічного обслуговування може знадобитися інформація про Ліцензію та інші дані у відповідності до Політики конфіденційності.

16. Передача Ліцензії. Програмне забезпечення може передаватися з однієї комп'ютерної системи на іншу, якщо такі дії не суперечать умовам Угоди. За умови дотримання положень Угоди Користувач має право остаточної передачі Ліцензії та всіх прав, що виникають унаслідок укладання цієї Угоди, іншому Користувачеві за згоди Постачальника, якщо (i) вихідний Користувач не зберігає жодних копій Програмного забезпечення; (ii) виконується пряма передача прав, наприклад, від вихідного Користувача до нового; (iii) новий Користувач приймає від вихідного всі права, що надаються відповідно до умов цієї Угоди; (iv) вихідний Користувач надає новому документацію, що дозволяє підтвердити автентичність Програмного забезпечення відповідно до розділу 17.

17. Підтвердження автентичності Програмного забезпечення. Кінцевий користувач може підтвердити своє право застосовувати Програмне забезпечення одним із таких способів: (i) за допомогою ліцензійного сертифіката, наданого Постачальником або вповноваженою ним третьою особою; (ii) за допомогою ліцензійної угоди в письмовій формі (якщо така укладалася); (iii) надавши надісланий Постачальником електронний лист із ліцензійними даними (ім'я користувача та пароль). Для підтвердження автентичності Програмного забезпечення може знадобитися інформація про Ліцензію та ідентифікаційні дані Кінцевого споживача у відповідності до Політики конфіденційності.

18. Надання ліцензії органам державної влади й уряду США. Програмне забезпечення надається органам державної влади, включно з урядом США, з урахуванням ліцензійних прав і обмежень, наведених у цій Угоді.

19. Дотримання процедур із контролю за торгівлею.

а) Забороняється в прямий чи непрямий спосіб експортувати, реекспортувати, передавати або іншим чином надавати програмне забезпечення будь-яким іншим особам. Ви зобов'язуєтесь утриматися від будь-яких способів використання цього програмного забезпечення й (або) не брати участь у жодних діях, які можуть призвести до проблем із дотриманням законодавства або до негативних наслідків для компанії ESET, її холдингових і дочірніх компаній або дочірніх компаній будь-яких холдингових компаній ESET, відповідно до законів із контролю за торгівлею, зокрема тих, що наведені нижче:

і. Усі закони, які регулюють, обмежують або накладають ліцензійні вимоги для експорту, реекспорту або передачі товарів, програмного забезпечення, технологій або послуг, що видані

або прийняті будь-якими органами державної влади, органами влади штату або органами регулювання США, Сінгапуру, Великої Британії, Європейського Союзу, будь-яких країн-членів ЄС, будь-яких країн, де необхідно виконувати зобов'язання згідно з цією Угодою, або будь-яких країн, де веде діяльність компанія ESET або афілійовані з нею компанії

ii. Усі економічні, фінансові, торгові або інші санкції, обмеження, ембарго, заборони експорту або імпорту, заборони передачі коштів або активів чи надання послуг або рівнозначні заходи, які запроваджуються будь-якими органами державної влади, органами влади штату або органами регулювання США, Сінгапуру, Великої Британії, Європейського Союзу, будь-яких країн-членів ЄС, будь-яких країн, де необхідно виконувати зобов'язання згідно з цією Угодою, або будь-яких країн, де веде діяльність компанія ESET або афілійовані з нею компанії.

(законні акти, зазначені в пунктах i та ii вище, разом згадуються як "Закони з контролю за торгівлею").

b) ESET має право призупинити виконання зобов'язань за цими Умовами або припинити їх дію з негайним набуттям чинності за таких умов:

i. ESET має обґрунтовані підстави вважати, що Користувачем уже порушено, або, імовірно, буде порушено умови Статті 19 а) Угоди; або

ii. Користувач i (або) Програмне забезпечення стали предметом законів із контролю за торгівлею, і через це ESET має обґрунтовані підстави вважати, що подальше виконання зобов'язань за цією Угодою може призвести до проблем із дотриманням законодавства або до негативних наслідків для компанії ESET або афілійованих із нею компаній відповідно до законів із контролю за торгівлею.

c) Жодна умова Угоди в жодному разі не має тлумачитися як така, що має на меті спонукати будь-яку зі сторін або вимагати від неї вчинити дії або утриматися від вчинення дій (чи погодитися на це) у будь-який спосіб, який буде суперечити законам із контролю за торгівлею або заборонений цими законами.

20. Примітки. Усі зауваження та запити на повернення Програмного забезпечення та Документації слід надсилати на адресу: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic без шкоди для права ESET повідомляти Вам про зміни цієї Угоди, Політики конфіденційності, Політики EOL та Документації відповідно до ст. 22 Угоди. ESET може надсилати Вам електронні листи, сповіщення в програмі через Програмне забезпечення або розмішувати повідомлення на Вашому веб-сайті. Ви погоджуєтесь отримувати сповіщення правового характеру від ESET в електронній формі, зокрема всі сповіщення про внесення змін в Умови, Спеціальні Умови або Політики конфіденційності, будь-які пропозиції укласти (прийняти) договір або запрошення до початку ділових відносин, сповіщення з правовою інформацією або будь-які інші повідомлення правового характеру. Отримання таких повідомлень в електронній формі прирівнюється до їх отримання в письмовій формі, якщо інше явно не вимагається застосовними законами.

21. Чинне законодавство. Ця Угода регулюється та тлумачиться відповідно до законодавства Словацької Республіки. Користувач i Постачальник погоджуються, що суперечливі положення регулюючого законодавства та Конвенції Організації Об'єднаних Націй щодо контрактів для міжнародної торгівлі товарами не мають застосовуватися. Ви повністю погоджуєтесь, що розгляд будь-яких заяв до Постачальника чи суперечок із ним, які викликані цією Угодою, або заяв чи суперечок, будь-яким чином пов'язаних із використанням Програмного забезпечення, i прийняття відповідних рішень здійснюється окружним судом м. Братислава I, а також

підтверджуєте виконання юрисдикції вказаним судом.

22. Загальні положення. Якщо будь-яке з положень цієї Угоди юридично не дійсне або не має позовної сили, це не повинно впливати на законність інших положень Угоди. Вони повинні залишатися чинними й такими, що мають законну силу, відповідно до передбачених тут умов. Цю Угоду укладено англійською. У разі розбіжностей між англійською й перекладеною версією Угоди (наданою для зручності або з будь-якою іншою метою) перевага надається документу англійською мовою.

Компанія ESET зберігає за собою право в будь-який час змінювати Програмне забезпечення, а також змінювати текст цієї Угоди, Додатків і Доповнень до неї, Політики конфіденційності, Політики закінчення терміну служби та документації або будь-яких їхніх складових шляхом оновлення застосовного документа (i) відповідно до змін, внесених в Програмне забезпечення або в спосіб ведення бізнесу ESET, (ii) із юридичних, регуляторних причин та з міркувань безпеки або (iii) для запобігання несанкціонованому використанню або нанесенню шкоди. Ми сповістимо Вас про будь-яке внесення змін в Угоду в електронному листі, сповіщеннях в програмі або через інші електронні способи зв'язку. Якщо Ви не згодні із запропонованими змінами в Угоді, то можете припинити її дію відповідно до ст. 10 протягом 30 днів після отримання сповіщення про зміну. Якщо Ви не припините дію Угоди протягом цього терміну, запропоновані зміни вважатимуться прийнятими й наберуть чинності з дати отримання Вами сповіщення про зміну.

Цей документ становить повну Угоду між Вами й Постачальником щодо Програмного забезпечення та цілком заміняє будь-які попередні подання, обговорення, зобов'язання, повідомлення й рекламні матеріали, пов'язані з Програмним забезпеченням.

ДОДАТОК ДО УГОДИ

Оцінка рівня захисту пристроїв, підключених до мережі. Додаткові положення застосовуються до оцінки рівня захисту пристроїв, підключених до мережі, таким чином:

Програмне забезпечення має функцію перевірки рівня захисту локальної мережі кінцевого користувача й пристроїв у ній. Для цього необхідно мати ім'я локальної мережі, а також дані про пристрій в локальній мережі, зокрема дані про наявність, тип, ім'я, IP-адресу й MAC-адресу пристрою в локальній мережі, на який розповсюджується дія ліцензії. Ці дані, поміж іншого, містять тип захисту й тип шифрування бездротової мережі для маршрутизаторів. Окрім того, ця функція може надавати інформацію щодо доступності програми захисту, що забезпечує безпеку пристроїв у локальній мережі.

Захист від незаконного використання даних. Додаткові положення застосовуються до захисту від незаконного використання даних таким чином:

Програмне забезпечення містить функцію, яка запобігає втраті або незаконному використанню критичних даних унаслідок крадіжки комп'ютера. У налаштуваннях Програмного забезпечення за замовчуванням цю функцію вимкнено. Щоб активувати її, потрібно створити Обліковий запис ESET HOME. Після цього у випадку крадіжки комп'ютера активуватиметься збирання даних. Якщо Ви активуєте цю функцію Програмного забезпечення, будуть збиратися та надсилатися Постачальнику дані про викрадений комп'ютер, які можуть містити відомості про мережу комп'ютера, вміст, який відображався на екрані, конфігурацію пристрою та дані, записані камерою, підключеною до комп'ютера (далі "Дані"). Кінцевий користувач отримує право на використання Даних, які збираються цією функцією і надаються через Обліковий запис ESET HOME, виключно для усунення негативної ситуації, спричиненої крадіжкою комп'ютера. Виключно для роботи цієї функції Постачальник оброблює Дані у відповідності до положень

документа "Політика конфіденційності" та застосовних правових норм. Постачальник надає Кінцевому користувачу доступ до Даних на період часу, необхідний для досягнення мети, з якою було запитано ці дані. Цей період часу не може перевищувати період зберігання, визначений в Політиці конфіденційності. Захист від незаконного використання даних використовується виключно для комп'ютерів та облікових записів, до яких Кінцевий користувач має законний доступ. Інформація про будь-які випадки незаконного використання буде передаватися до компетентних органів. Постачальник діє згідно з відповідним законодавством і надає допомогу правоохоронним органам у випадку незаконного використання. Ви погоджуєтесь та підтверджуєте, що несете відповідальність за захист пароля доступу до облікового запису ESET HOME, а також даєте згоду не розголошувати свій пароль третім особам. Кінцевий користувач несе відповідальність за будь-яку діяльність, пов'язану із застосуванням функції захисту від незаконного використання даних, а також облікового запису ESET HOME, незалежно від отриманих повноважень. У разі виявлення несанкціонованого доступу до облікового запису ESET HOME негайно повідомте про це Постачальника. Додаткові положення щодо захисту від незаконного використання даних застосовуються виключно до Кінцевих користувачів ESET Internet Security і ESET Smart Security Premium.

ESET Secure Data. Додаткові положення застосовуються до ESET Secure Data таким чином:

1. Визначення. У цих додаткових положеннях до ESET Secure Data використовуються такі терміни:

а) "Інформація" Будь-яка інформація й дані, які шифруються чи дешифруються за допомогою програмного забезпечення.

б) "Продукти" Програмне забезпечення ESET Secure Data й документація на нього.

с) "ESET Secure Data" Програмне забезпечення, яке використовується для шифрування й дешифрування електронних даних.

Програмне забезпечення, яке використовується для шифрування й дешифрування електронних даних. Посилання на будь-яку особу в однині або будь-якому роді також включає посилання на таку особу у множині й усіх інших родах.

2. Додаткова декларація кінцевого користувача. Ви запевняєте й підтверджуєте, що дотримуетесь таких зобов'язань:

а) Зберігати Дані, захищати їх безпеку та створювати їх резервні копії.

б) Створювати повні резервні копії всієї інформації й даних на комп'ютері (включно з критично важливими) перед інсталяцією ESET Secure Data.

с) Безпечно зберігати всі свої паролі й інші дані, потрібні для налаштування та використання ESET Secure Data, і створювати резервні копії всіх ключів шифрування, ліцензійних кодів, файлів ключів та інших даних на окремих носіях.

д) Відповідати за наслідки використання продуктів Постачальник не несе відповідальності за жодні збитки, шкоду та претензії, спричинені несанкціонованим чи помилковим шифруванням або дешифруванням інформації чи даних незалежно від місця їх збереження.

е) Не використовувати ESET Secure Data й інші пов'язані продукти в зонах, які вимагають відмовостійких захисних систем або мають високий рівень ризику (небезпеки), зокрема на атомних електростанціях і бойових комплексах, у системах управління, зв'язку, аеронавігації, оборони, життєзабезпечення та моніторингу стану хворих (незважаючи на те, що

Постачальник ужив усіх розумних заходів, щоб гарантувати цілісність і безпеку своїх продуктів).

f) Стежити за тим, щоб рівень безпеки та шифрування, забезпечуваний продуктами, відповідав Вашим вимогам.

g) Ви несете відповідальність за використання Продуктів або будь-яких їх компонентів. Зокрема, під час використання продуктів Ви повинні дотримуватись усіх чинних законів і нормативно-правових актів Словацької Республіки або іншої країни, регіону чи штату, де застосовуються продукти, попередньо переконавшись, що на ці продукти не поширюються жодні державні ембарго.

h) Програмне забезпечення ESET Secure Data періодично може підключатися до серверів Постачальника, щоб перевіряти ліцензійну інформацію й шукати виправлення, пакети оновлень тощо для покращення, обслуговування, зміни чи вдосконалення роботи ESET Secure Data. При цьому Програмне забезпечення може надсилати загальні відомості про систему, пов'язані з її роботою, у відповідності до Політики конфіденційності.

i) Звільнити Постачальника від відповідальності за будь-які збитки, витрати, шкоду та претензії, спричинені втратою, крадіжкою, пошкодженням, знищенням паролів, даних налаштування, ключів шифрування, кодів активації ліцензій та інших даних, створених або збережених під час використання програмного забезпечення, або зловживанням такими даними.

Додаткові положення до ESET Secure Data застосовуються виключно до Кінцевих користувачів ESET Smart Security Premium.

Програмне забезпечення Password Manager. Додаткові положення застосовуються до Програмного забезпечення Password Manager таким чином:

1. Додаткова декларація кінцевого користувача. Ви запевняєте й підтверджуєте, що Ви не будете вчиняти такі дії:

a) Використовувати Програмне забезпечення Password Manager для критично важливих програм, від яких залежать людські життя чи безпека власності Ви визнаєте, що Програмне забезпечення Password Manager не призначено для таких цілей, а його відмова в разі застосування з такими програмами може призвести до смерті, травми чи серйозної шкоди майну або навколишньому середовищу, і Постачальник не несе відповідальності за такі наслідки.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ PASSWORD MANAGER НЕ СТВОРЕНО, НЕ ПРИЗНАЧЕНО ТА НЕ ЛІЦЕНЗОВАНО ДЛЯ ВИКОРИСТАННЯ В НЕБЕЗПЕЧНИХ СЕРЕДОВИЩАХ, ЯКІ ВИМАГАЮТЬ ВІДМОВИСТИЙКИХ ЗАСОБІВ УПРАВЛІННЯ, ЗОКРЕМА В ГАЛУЗІ ПРОЕКТУВАННЯ, БУДІВНИЦТВА, ОБСЛУГОВУВАННЯ Й ЕКСПЛУАТАЦІЇ АТОМНИХ ЕЛЕКТРОСТАНЦІЙ, БОЙОВИХ КОМПЛЕКСІВ, А ТАКОЖ СИСТЕМ ЗВ'ЯЗКУ, АЕРОНАВІГАЦІЇ, КЕРУВАННЯ ПОВІТРЯНИМ РУХОМ І ЖИТТЄЗАБЕЗПЕЧЕННЯ. ПОСТАЧАЛЬНИК ПРЯМО ЗАЯВЛЯЄ, ЩО НЕ НАДАЄ ЖОДНИХ ЯВНИХ І ОПОСЕРЕДКОВАНИХ ГАРАНТІЙ ПРИДАТНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ТАКИХ ЦІЛЕЙ.

b) Використовувати Програмне забезпечення Password Manager способом, який порушує цю угоду або закони Словацької Республіки чи Вашої юрисдикції. Зокрема, забороняється застосовувати Програмне забезпечення Password Manager для виконання чи пропаганди незаконних дій, наприклад завантаження шкідливого вмісту, матеріалів, які можна використати для

незаконних дій, або вмісту, що будь-яким чином порушує закон або права третіх осіб (включно з правами на об'єкти інтелектуальної власності), для спроб отримати доступ до облікових записів у Системі збереження даних (у контексті цих додаткових умови до Програмного забезпечення Password Manager "Система збереження даних" визначається як середовище збереження даних, яким керує Постачальник або третя особа, через яке синхронізуються дані користувачів і в якому зберігаються резервні копії цих даних) або облікових записів та інформації інших користувачів Програмного забезпечення Password Manager або Системи збереження даних. У разі порушення Вами будь-якого з цих положень Постачальник має право негайно розірвати цю угоду, покласти на вас відповідальність за відшкодування збитків (якщо таке знадобиться) і вжити потрібних заходів для того, щоб Ви більше не змогли використовувати Програмне забезпечення Password Manager, без відшкодування вам його вартості.

2. ОБМЕЖЕННЯ ВІДПОВІДАЛЬНОСТІ. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ PASSWORD MANAGER ПОСТАЧАЄТЬСЯ НА УМОВАХ "ЯК Є", БЕЗ ЖОДНИХ ПРЯМИХ І НЕПРЯМИХ ГАРАНТІЙ. ВИ ВИЗНАЄТЕ, ЩО КОРИСТУВАТИМЕТЕСЯ НИМ НА ВЛАСНИЙ СТРАХ І РИЗИК. ВИРОБНИК НЕ НЕСЕ ВІДПОВІДАЛЬНОСТІ ЗА ОБМЕЖЕНУ ДОСТУПНІСТЬ СЛУЖБИ, УТРАТУ Й ПОШКОДЖЕННЯ ДАНИХ (ВКЛЮЧНО З ТИМИ, ЩО НАДСИЛАЮТЬСЯ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ PASSWORD MANAGER У ЗОВНІШНІ СИСТЕМИ ЗБЕРЕЖЕННЯ ДАНИХ ДЛЯ СИНХРОНІЗАЦІЇ ТА СТВОРЕННЯ РЕЗЕРВНИХ КОПІЙ). ШИФРУВАННЯ ДАНИХ ЗА ДОПОМОГОЮ PASSWORD MANAGER НЕ ОЗНАЧАЄ, ЩО ПОСТАЧАЛЬНИК НЕСЕ БУДЬ-ЯКУ ВІДПОВІДАЛЬНОСТІ ЗА БЕЗПЕКУ ЦИХ ДАНИХ. ВИ ПОГОДЖУЄТЕСЯ, ЩО ДАНІ, ЯКІ ОТРИМУЮТЬСЯ, ВИКОРИСТОВУЮТЬСЯ, ШИФРУЮТЬСЯ, ЗБЕРІГАЮТЬСЯ, СИНХРОНІЗУЮТЬСЯ ТА НАДСИЛАЮТЬСЯ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ PASSWORD MANAGER, ТАКОЖ МОЖУТЬ ЗБЕРІГАТИСЯ НА СЕРВЕРАХ ТРЕТІХ ОСІБ (ЦЕ ПОЛОЖЕННЯ СТОСУЄТЬСЯ ЛИШЕ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ PASSWORD MANAGER, У ЯКОМУ ВВІМКНЕНО СИНХРОНІЗАЦІЮ ТА РЕЗЕРВНЕ КОПІЮВАННЯ). ЯКЩО ПОСТАЧАЛЬНИК НА ВЛАСНИЙ РОЗСУД ВИРІШИТЬ ВИКОРИСТОВУВАТИ ТАКУ СТОРОННЮ СИСТЕМУ ЗБЕРЕЖЕННЯ ДАНИХ, ВЕБ-САЙТ, ВЕБ-ПОРТАЛ, СЕРВЕР АБО СЛУЖБУ, ВІН У ЖОДНОМУ РАЗІ НЕ НЕСЕ ВІДПОВІДАЛЬНОСТІ ЗА ЯКІСТЬ, БЕЗПЕКУ ТА ДОСТУПНІСТЬ ЇХ РОБОТИ, А ТАКОЖ БУДЬ-ЯКІ ПОРУШЕННЯ ТРЕТЬОЮ ОСОБОЮ СВОЇХ ДОГОВІРНИХ І ПРАВОВИХ ЗОБОВ'ЯЗАНЬ, ТАК САМО ЯК І ФІНАНСОВІ Й ІНШІ ЗБИТКИ, ШКОДУ, УТРАЧЕНУ ВИГОДУ Й БУДЬ-ЯКІ ІНШІ ВТРАТИ, ПОНЕСЕНІ ПІД ЧАС ВИКОРИСТАННЯ ЦЬОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ. ПОСТАЧАЛЬНИК НЕ НЕСЕ ВІДПОВІДАЛЬНОСТІ ЗА ВМІСТ ДАНИХ, ЯКІ ОТРИМУЮТЬСЯ, ВИКОРИСТОВУЮТЬСЯ, ШИФРУЮТЬСЯ, ЗБЕРІГАЮТЬСЯ, СИНХРОНІЗУЮТЬСЯ ТА НАДСИЛАЮТЬСЯ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ PASSWORD MANAGER АБО СИСТЕМОЮ ЗБЕРЕЖЕННЯ. ВИ ВИЗНАЄТЕ, ЩО ПОСТАЧАЛЬНИК НЕ МАЄ ДОСТУПУ ДО ВМІСТУ ЦИХ ДАНИХ І, ВІДПОВІДНО, ЗМОГИ ВІДСТЕЖУВАТИ Й ВИДАЛЯТИ НЕЗАКОННІ МАТЕРІАЛИ.

Постачальник володіє всіма правами на покращення, оновлення та виправлення Програмного забезпечення Password Manager (далі "Покращення"), навіть створені на основі ідей, пропозицій або відгуків, поданих вами в будь-якій формі, а ви при цьому не маєте права на жодну компенсацію, гонорар або відрахування.

ОРГАНІЗАЦІЇ Й ЛІЦЕНЗІАРИ ПОСТАЧАЛЬНИКА НЕ НЕСУТЬ ПЕРЕД ВАМИ ВІДПОВІДАЛЬНОСТІ ЗА ЖОДНІ ПРЕТЕНЗІЇ Й ЗОБОВ'ЯЗАННЯ (ЗАКОННІ АБО ЗАСНОВАНІ НА ПРАВІ СПРАВЕДЛИВОСТІ), ПОВ'ЯЗАНІ З ВИКОРИСТАННЯМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ PASSWORD MANAGER ВАМИ ТА ТРЕТІМИ ОСОБАМИ, КОРИСТУВАННЯМ АБО НЕКОРИСТУВАННЯМ ПОСЛУГАМИ ДИЛЕРІВ І ПОСЕРЕДНИЦЬКИХ ФІРМ, ПРОДАЖЕМ АБО ПРИДБАННЯМ БУДЬ-ЯКИХ ЗАСОБІВ ЗАХИСТУ.

ОРГАНІЗАЦІЇ Й ЛІЦЕНЗІАРИ ПОСТАЧАЛЬНИКА НЕ НЕСУТЬ ПЕРЕД ВАМИ ВІДПОВІДАЛЬНОСТІ ЗА ЖОДНІ ПРЯМІ, НЕПРЯМІ, ПОБІЧНІ, ФАКТИЧНІ ТА ВИПАДКОВІ ЗБИТКИ, ПОВ'ЯЗАНІ З БУДЬ-ЯКИМ СТОРОННІМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ, ОТРИМАНИМИ ЧИ НАДАНИМИ ЧЕРЕЗ ПРОГРАМНЕ

ЗАБЕЗПЕЧЕННЯ PASSWORD MANAGER ДАНИМИ, ВИКОРИСТАННЯМ АБО НЕМОЖЛИВІСТЮ ВИКОРИСТАННЯ PASSWORD MANAGER (А ТАКОЖ ДОСТУПОМ АБО НЕМОЖЛИВІСТЮ ДОСТУПУ ДО ЦЬОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ), НЕЗАЛЕЖНО ВІД ТОГО, ЧИ ЗАСНОВАНІ ЗАКОННІ ПРЕТЕНЗІЇ ПРО ТАКУ ШКОДУ НА ПРАВИ СПРАВЕДЛИВОСТІ. ЦЕ ПОЛОЖЕННЯ НЕ ПОШИРЮЄТЬСЯ НА ДЕЯКІ ВИДИ ЗБИТКІВ, ЗОКРЕМА ПОВ'ЯЗАНІ З УТРАЧЕНОЮ КОМЕРЦІЙНОЮ ВИГОДОЮ, ТРАВМАМИ, ПОШКОДЖЕННЯМ МАЙНА, ПРОСТОЯМИ КОМЕРЦІЙНОЇ ДІЯЛЬНОСТІ, УТРАТОЮ ДІЛОВОЇ ЧИ ОСОБИСТОЇ ІНФОРМАЦІЇ. ЯКЩО ЗАКОН ВАШОЇ ЮРИСДИКЦІЇ НЕ ДОПУСКАЄ ОБМЕЖЕННЯ ВІДПОВІДАЛЬНОСТІ ЗА НЕПРЯМІ ТА ВИПАДКОВІ ЗБИТКИ, ПОСТАЧАЛЬНИК НЕСЕ ВІДПОВІДАЛЬНІСТЬ У МІНІМАЛЬНОМУ ОБСЯЗІ, ВИЗНАЧЕНОМУ ЧИННИМ ЗАСТОСОВНИМ ЗАКОНОМ.

ВІДОМОСТІ (БІРЖОВІ ЦІНИ, ФОНДОВИЙ АНАЛІЗ, РИНКОВА ІНФОРМАЦІЯ ТА НОВИНИ, ФІНАНСОВІ ДАНІ ТОЩО), ЯКІ НАДАЮТЬСЯ ЧЕРЕЗ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ PASSWORD MANAGER, МОЖУТЬ НАДХОДИТИ НЕВЧАСНО, БУТИ НЕТОЧНИМИ, НЕПОВНИМИ ЧИ ПОМИЛКОВИМИ, І ОРГАНІЗАЦІЇ Й ЛІЦЕНЗІАРИ ПОСТАЧАЛЬНИКА НЕ НЕСУТЬ ПЕРЕД ВАМИ ЗА ЦЕ ЖОДНОЇ ВІДПОВІДАЛЬНОСТІ. ПОСТАЧАЛЬНИК МОЖЕ КОЛИ ЗАВГОДНО БЕЗ ПОПЕРЕДЖЕННЯ ЗМІНЮВАТИ Й ВИЛУЧАТИ ПАРАМЕТРИ, МОЖЛИВОСТІ Й ФУНКЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ PASSWORD MANAGER, А ТАКОЖ ВИКОРИСТОВУВАНІ В НЬОМУ ТЕХНОЛОГІЇ ТА СПОСІБ ЇХ ЗАСТОСУВАННЯ.

СТОРОНИ ПОГОДЖУЮТЬСЯ, ЩО В РАЗІ ВИЗНАННЯ ПОЛОЖЕНЬ ЦІЄЇ СТАТТІ НЕДІЙСНИМИ (НЕЗАЛЕЖНО ВІД ПРИЧИНИ) ЧИ ВИЗНАННЯ ПОСТАЧАЛЬНИКА ВІДПОВІДАЛЬНИМ ЗА ЗБИТКИ, ШКОДУ ТОЩО ЗГІДНО З ЧИННИМ ЗАСТОСОВНИМ ЗАКОНОМ ОБСЯГ ВІДПОВІДАЛЬНОСТІ ПОСТАЧАЛЬНИКА ПЕРЕД ВАМИ БУДЕ ОБМЕЖЕНО ЗАГАЛЬНОЮ СУМОЮ ЗДІЙСНЕНИХ ВАМИ ЛІЦЕНЗІЙНИХ ПЛАТЕЖІВ.

ВИ ЗОБОВ'ЯЗУЄТЕСЯ ЗАБЕЗПЕЧИТИ ПОСТАЧАЛЬНИКУ ТА ЙОГО СПІВРОБІТНИКАМ, ДОЧІРНИМ ОРГАНІЗАЦІЯМ, БРЕНДАМ, ФІЛІАЛАМ ТА ІНШИМ ПАРТНЕРАМ ПРАВОВИЙ ЗАХИСТ І ВІДШКОДУВАННЯ ЗБИТКІВ У РАЗІ БУДЬ-ЯКИХ ПРЕТЕНЗІЙ ТРЕТІХ ОСІБ (ВКЛЮЧНО З ВЛАСНИКАМИ ПРИСТРОЇВ І СТОРОНАМИ, ЧИЇ ПРАВА БУЛО ПОРУШЕНО ВИКОРИСТАННЯМ ДАНИХ У ПРОГРАМНОМУ ЗАБЕЗПЕЧЕННІ PASSWORD MANAGER АБО СИСТЕМІ ЗБЕРЕЖЕННЯ) ЩОДО ШКОДИ, ЗБИТКІВ, ВИТРАТ, ПЛАТЕЖІВ І ЗБОРІВ, ПОНЕСЕНИХ АБО ЗДІЙСНЕНИХ У РЕЗУЛЬТАТІ ВИКОРИСТАННЯ ВАМИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ PASSWORD MANAGER, І ГАРАНТУВАТИ ЗВІЛЬНЕННЯ ВІД ВІДПОВІДАЛЬНОСТІ ПЕРЕД ЦИМИ ТРЕТІМИ ОСОБАМИ.

3. Дані у Програмному забезпеченні Password Manager. Усі введені вами дані, які зберігаються в базі даних Програмного забезпечення Password Manager, за замовчуванням (якщо ви самі не зміните цей параметр) записуються на комп'ютер або вибраний вами пристрій збереження даних у зашифрованому вигляді. Ви визнаєте, що в разі видалення чи пошкодження бази даних або інших файлів Програмного забезпечення Password Manager усі збережені в них дані буде втрачено без можливості відновлення, і приймаєте цей ризик. Той факт, що ваші особисті дані зашифровано на комп'ютері, не означає, що їх не може вкрасти чи неправомірно використати особа, яка дізнається ваш головний пароль або отримує доступ до вибраного активаційного пристрою для відкривання бази даних. Ви несете відповідальність за безпеку всіх використовуваних вами методів доступу до даних.

4. Передача особистих даних Постачальнику чи в Систему збереження. Програмне забезпечення Password Manager може передавати або надсилати через Інтернет особисті дані зі своєї бази (паролі, облікові записи, дані для входу, особистості) у Систему збереження. Це робиться тільки за умови ввімкнення вами відповідного параметра й виключно з метою вчасної синхронізації та створення резервних копій даних. Дані передаються лише в зашифрованому вигляді. Використання Програмного забезпечення Password Manager для підставлення паролів, даних для входу й іншої інформації в онлайн-форми вимагає передачі таких відомостей через Інтернет на вказаний вами веб-сайт. Такі операції передачі ініціюєте саме ви, а не Програмне

забезпечення Password Manager, тому Постачальник не відповідає за їх безпеку. Передача будь-яких даних через Інтернет (незалежно від того, чи пов'язано їх із Програмним забезпеченням Password Manager) здійснюється на ваш власний розсуд і ризик, і ви несете повну відповідальність за будь-яку шкоду своїй комп'ютерній системі чи втрату інформації, спричинену завантаженням таких даних і (або) використанням веб-сайтів. Постачальник рекомендує регулярно створювати резервні копії бази даних та інших конфіденційних файлів на зовнішніх носіях, щоб мінімізувати ризик втрати цінної інформації. Постачальник не надає допомоги з відновленням утрачених або пошкоджених даних. Будь-які послуги резервного копіювання файлів користувацьких баз даних, які надаються Постачальником на випадок пошкодження чи видалення файлів на ПК користувачів, не передбачають жодних гарантій і відповідальності перед вами з боку Постачальника.

Використовуючи Програмне забезпечення Password Manager, Ви погоджуєтесь, що періодично воно може підключатися до серверів Постачальника, щоб перевіряти ліцензійну інформацію й шукати виправлення, пакети оновлень тощо для покращення, обслуговування, зміни чи вдосконалення роботи Програмного забезпечення Password Manager. При цьому Програмне забезпечення може надсилати загальні відомості про систему, пов'язані з роботою Password Manager, у відповідності до Політики конфіденційності.

5. Інформація про видалення й інструкції. Перш ніж видаляти Програмне забезпечення Password Manager, ви повинні експортувати з бази даних усі відомості, які хочете зберегти.

Додаткові положення до Програмного забезпечення Password Manager застосовуються виключно до Кінцевих користувачів ESET Smart Security Premium.

ESET LiveGuard. Додаткові положення застосовуються до ESET LiveGuard таким чином:

Програмне забезпечення підтримує функцію додаткового аналізу файлів, надісланих Кінцевим користувачем. Постачальник має використовувати файли, надіслані Кінцевим користувачем, і результати аналізу у суворій відповідності до Політики конфіденційності та чинних правових норм.

Додаткові положення до ESET LiveGuard застосовуються виключно до Кінцевих користувачів ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Політика конфіденційності

Захист персональних даних має особливо важливе значення для компанії ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 851 01 Bratislava, Slovak Republic, запис № 3586/B у комерційному реєстрі окружного суду м. Братислави I, розділ Sro, реєстраційний номер: 31333532) як Контролера даних (далі — "ESET" або "Ми"). Ми прагнемо забезпечити відповідність вимогам до прозорості, установленим у Загальному регламенті ЄС щодо захисту даних (далі — "GDPR"). З цією метою Ми публікуємо цю Політику конфіденційності, виключне призначення якої — проінформувати наших клієнтів (далі — "Кінцевий користувач" або "Ви") як суб'єктів даних про наведені нижче аспекти захисту персональних даних.

- Правові основи для обробки персональних даних.
- Обмін даними та конфіденційність.

- Безпека даних.
- Права суб'єкта даних.
- Обробка персональних даних.
- Контактна інформація.

Правові основи для обробки персональних даних

Є лише декілька законних підстав для обробки даних, які ми використовуємо відповідно до чинної законодавчої бази, пов'язаної із захистом персональних даних. Компанії ESET в основному необхідно обробляти персональні дані з метою виконання положень документа [Ліцензійна угода з кінцевим користувачем](#) (далі — "EULA") з Кінцевим користувачем (ст. 6 (1) (b) GDPR), що застосовується для надання продуктів або служб ESET, якщо явно не зазначено інше, наприклад:

- Правові підстави законних інтересів (ст. 6 (1) (f) GDPR), які дозволяють нам обробляти дані про спосіб використання Служб нашими клієнтами й про ступінь їхнього задоволення, що дає змогу надавати нашим користувачам найкращий захист і підтримку, а також забезпечувати найвищий рівень обслуговування. Навіть маркетингові комунікації згідно з чинним законодавством визнаються законним інтересом, тому ми спираємося на це, коли надсилаємо повідомлення маркетингового характеру нашим клієнтам.
- Згода (ст. 6 (1) (a) GDPR), яку Ми можемо просити Вас надати в певних випадках, коли вважатимемо таку правову підставу найбільш відповідною, або якщо це необхідно згідно із законодавством.
- Виконання правових зобов'язань (ст. 6 (1) (c) GDPR), наприклад визначення вимог до електронних комунікацій і зберігання рахунків-фактур або документів, пов'язаних із розрахунками.

Обмін даними та конфіденційність

Ми не передаємо Ваші дані третім сторонам. Однак ESET — це компанія, яка працює в усьому світі через афілійовані компанії або партнерів, які входять до нашої мережі розповсюдження, обслуговування та підтримки. Інформація про ліцензування, розрахунки й технічну підтримку, яка оброблюється ESET, може передаватись афілійованим компаніям чи партнерам або надходити від них. Це необхідно для виконання положень Ліцензійної угоди з кінцевим користувачем, таких як надання послуг або підтримки.

У компанії ESET ми віддаємо перевагу обробці даних на території Європейського Союзу (ЄС). Однак, залежно від Вашого місцезнаходження (використання наших продуктів і/або служб за межами ЄС) та (або) вибраної Вами служби, нам, можливо, доведеться передати Ваші дані в країну за межами ЄС. Наприклад, ми використовуємо служби третіх сторін для виконання обчислень у хмарі. У таких випадках Ми ретельно вибираємо наших постачальників послуг і забезпечуємо належний рівень захисту даних шляхом укладення договорів, а також за допомогою технічних та організаційних заходів. Як правило, Ми діємо згідно зі стандартними та додатковими (за потреби) договірними положеннями ЄС.

Для деяких країн за межами ЄС, наприклад Великобританії та Швейцарії, уже визначено аналогічний рівень захисту даних. Завдяки відповідному рівню захисту для передачі даних у ці

країни не потрібен спеціальний дозвіл або угода.

Безпека даних

ESET впроваджує відповідні технічні та організаційні заходи, щоб забезпечити безпеку на тому рівні, якій відповідає потенційним ризикам. Ми докладемо всіх зусиль, щоб постійно забезпечувати конфіденційність, цілісність, доступність і стійкість систем обробки і сервісів. Однак у випадку витоку конфіденційної інформації, що загрожує Вашим правам і свободам, ми готові сповістити про це відповідний наглядовий орган, а також Кінцевих користувачів як суб'єктів даних.

Права суб'єкта захисту персональних даних

Права кожного Кінцевого користувача мають велике значення, і Ми хотіли б повідомити Вам, що всі Кінцеві користувачі (з будь-якої країни ЄС або за його межами) мають наведені нижче права, гарантовані ESET. Щоб скористатися своїми правами суб'єкта даних, зв'яжіться з нами за допомогою форми служби підтримки або електронною поштою за адресою dro@eset.sk. Для ідентифікації Ми попросимо надати таку інформацію: ім'я, адресу електронної пошти та, за наявності, ліцензійний ключ або номер клієнта й місце роботи. Не надсилайте нам будь-які інші персональні дані, наприклад дату народження. Хочемо зазначити, що для обробки Вашого запиту, а також для ідентифікації Ми оброблятимемо Ваші персональні дані.

Право відкликати згоду. Право відкликати згоду застосовується до даних, які обробляються лише за згодою. Якщо Ми обробляємо персональні дані на підставі Вашої згоди, Ви маєте право відкликати її в будь-який час без пояснення причин. Відкликання згоди застосовується лише до майбутніх операцій обробки й не впливає на законність даних, оброблених до відкликання.

Право на заперечення. Право на заперечення застосовується, коли обробка даних здійснюється на основі законних інтересів компанії ESET або третьої сторони. Якщо Ми обробляємо персональні дані для захисту законного інтересу, Ви, як суб'єкт даних, маєте право в будь-який час заперечити проти зазначеного нами законного інтересу й обробки Ваших персональних даних. Заперечення застосовується лише до майбутніх операцій обробки й не впливає на законність даних, оброблених до заперечення. Якщо Ми обробляємо Ваші персональні дані в цілях прямого маркетингу, наводити причини для заперечення не потрібно. Це також стосується формування профілів, оскільки воно пов'язане з прямим маркетингом. У всіх інших випадках Ми просимо Вас коротко повідомити нам, чому Ви не згодні із законним інтересом компанії ESET до обробки Ваших персональних даних.

Зверніть увагу, що в деяких випадках, незважаючи на відкликання Вашої згоди, Ми маємо право на подальшу обробку Ваших персональних даних на іншій правовій основі, наприклад для виконання умов договору.

Право на доступ. Як суб'єкт даних Ви маєте право в будь-який час безкоштовно отримати інформацію про свої дані, що зберігаються компанією ESET.

Право на виправлення. Якщо Ваші персональні дані, які перебувають у нашому розпорядженні, містять помилку, Ви маєте право на її виправлення.

Право на видалення й обмеження обробки. Як суб'єкт даних Ви маєте право вимагати видалення чи обмеження обробки Ваших персональних даних. Якщо для обробки Ваших персональних даних не залишиться правових підстав (наприклад, договору чи Вашої згоди), ми

негайно видалимо їх. Ваші персональні дані також буде видалено в кінці терміну зберігання, щойно вони більше не будуть потрібні для вказаних для них цілей.

Якщо Ми використовуємо Ваші персональні дані виключно з метою прямого маркетингу, і Ви відкликали свою згоду або заперечили проти основного законного інтересу компанії ESET, Ми обмежимо обробку Ваших персональних даних шляхом включення Ваших контактних даних у наш внутрішній чорний список із метою уникнення небажаних контактів. Інакше Ваші персональні дані буде видалено.

Зверніть увагу, що Ми можемо бути зобов'язані дотримуватись умов і термінів зберігання даних, установлених законодавчими або наглядовими органами. Умови й терміни зберігання даних також може бути визначено в законодавстві Словаччини. Після завершення відповідного періоду часу дані видалятимуться звичайним чином.

Право забезпечити можливість переносу даних. Як суб'єкт даних Ви можете отримати Ваші персональні дані, які обробляє компанія ESET, у форматі XLS.

Право на подання скарги. Як суб'єкт даних Ви маєте право в будь-який час звертатися зі скаргою до наглядових органів влади. ESET є суб'єктом регулювання відповідно до законів Словацької Республіки. Відповідним наглядовим органом є Управління з питань захисту персональних даних Словацької Республіки, розташованим за адресою Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Обробка персональних даних

Служби компанії ESET реалізовані в нашому продукті й надаються згідно з [EULA](#), однак деякі з них потребують особливої уваги. Ми хочемо надати Вам більше відомостей про збір даних, що пов'язаний із наданням наших послуг. Ми надаємо різні служби, описані в Ліцензійній угоді та [документації](#). Щоб забезпечувати роботу всіх цих служб, нам необхідно збирати дані, які наведено нижче:

Дані про ліцензії та розрахунки. Відповідно до чинного законодавства або за Вашою згодою компанія ESET збирає й обробляє такі відомості, як ім'я, адресу електронної пошти, ліцензійний ключ і (якщо застосовно) адресу, місце роботи та платіжні дані з метою проведення таких заходів: активація ліцензії, доставка ліцензійного ключа, нагадування про закінчення терміну дії, обробка запитів на підтримку, перевірка справжності ліцензії, надання служби й надсилання сповіщень, включаючи маркетингові повідомлення. За законом компанія ESET зобов'язана зберігати платіжну інформацію протягом 10 років, проте інформацію про ліцензію буде анонімізовано не пізніше ніж через 12 місяців після закінчення терміну дії ліцензії.

Оновлення й інші статистичні дані. З метою впровадження оновлень, обслуговування, захисту безпеки та поліпшення нашої серверної інфраструктури ми обробляємо інформацію, пов'язану з процесом інсталяції й вашим комп'ютером, зокрема платформою, у якій інстальовано продукт, а також інформацію про операції й функціональність наших продуктів, зокрема відомості про операційну систему й обладнання, ідентифікатори інсталяції та ліцензії, IP-адреси, MAC-адреси та параметри конфігурації продукту.

Ця інформація зберігається окремо від ідентифікаційних даних, необхідних для цілей ліцензування та виставлення рахунків, оскільки в цьому випадку ідентифікація Кінцевого користувача не потрібна. Період зберігання: до 4 років.

Система репутації ESET LiveGrid®. Односторонні хеші, пов'язані із загрозами, обробляються для

забезпечення роботи системи репутації ESET LiveGrid®, яка підвищує ефективність рішень для захисту від шкідливого ПЗ, здійснюючи перевірку файлів за білим і чорним списками в хмарній базі даних об'єктів. Цей процес не передбачає ідентифікацію Кінцевого користувача.

Система зворотного зв'язку ESET LiveGrid®. Отримуючи підозрілі зразки та метадані від системи зворотного зв'язку ESET LiveGrid®, ми можемо миттєво реагувати на потреби користувачів і підтримувати системи ESET в актуальному стані. Якість роботи наших продуктів залежить від такої інформації, яку ми отримуємо від Вас:

- Загрози, зокрема потенційні зразки вірусів і інших шкідливих та підозрілих програм; проблемні, потенційно небажані або потенційно небезпечні об'єкти, зокрема виконувані файли, повідомлення електронної пошти, позначені Вами або нашим продуктом як спам;
- Інформація щодо використання Інтернету, зокрема IP-адреса й географічні дані, IP-пакети, URL-адреси й кадри Ethernet;
- Файли аварійного дампа з пов'язаною інформацією.

Ми не маємо наміру збирати Ваші дані, які не входять до зазначеного переліку, однак іноді цьому неможливо запобігти. Випадково зібрані дані можуть збиратися шкідливим програмним забезпеченням і надходити безпосередньо з нього (без вашого відома або згоди) або надходити в іменах файлів чи URL-адресах. Ми не маємо наміру використовувати такі дані в наших системах або оброблювати їх відповідно до умов, визначених цією Політикою конфіденційності.

Уся інформація, отримана й оброблена через систему зворотного зв'язку ESET LiveGrid®, призначена для використання без ідентифікації Кінцевого користувача.

Оцінка рівня захисту пристроїв, підключених до мережі. Щоб забезпечити роботу функції оцінки рівня захисту, Ми обробляємо дані про ім'я локальної мережі та підключені до неї пристрої, зокрема відомості про їх наявність, тип, ім'я, IP-адресу й MAC-адресу в контексті інформації про ліцензію. Ці дані, поміж іншого, містять тип захисту й тип шифрування бездротової мережі для маршрутизаторів. Інформацію про ліцензію, за якою можна ідентифікувати Кінцевого користувача, буде анонімізовано не пізніше ніж через 12 місяців після закінчення терміну дії ліцензії.

Технічна підтримка. Контактна інформація, відомості про ліцензію та дані, які містяться в запитах до служби підтримки, можуть знадобитися для надання послуг підтримки. В залежності від обраного каналу зв'язку ми можемо збирати такі дані: адреса електронної пошти, номер телефону, дані ліцензії, дані продукту і опис Вашого звернення до служби підтримки. До Вас може надійти запит щодо надання іншої інформації для прискорення обслуговування службою підтримки. Дані, що оброблялися з метою надання технічної підтримки, зберігаються протягом 4 років.

Захист від незаконного використання даних. Якщо Кінцевий користувач облікового запису ESET HOME, створеного за адресою <https://home.eset.com>, активує відповідну функцію у зв'язку з крадіжкою комп'ютера, буде зібрано й оброблено таку інформацію: дані про місцезнаходження, знімки екрана, відомості про конфігурацію комп'ютера та дані, записані камерою комп'ютера. Зібрані дані зберігаються на наших серверах або серверах наших постачальників послуг протягом 3 місяців.

Password Manager. Якщо Ви вирішите активувати функцію Password Manager, на Вашому

комп'ютері або іншому зазначеному пристрої в зашифрованому вигляді зберігатимуться Ваші дані для входу. Якщо Ви активуєте службу синхронізації, зашифровані дані зберігатимуться на наших серверах або на серверах наших постачальників послуг для забезпечення синхронізації. Ані ESET, ані постачальник послуг не мають доступу до зашифрованих даних. Тільки Ви маєте ключ для дешифрування даних. Після вимкнення функції дані буде видалено.

ESET LiveGuard. Активація функції ESET LiveGuard передбачає передачу зразків — файлів, попередньо визначених і вибраних користувачем. Зразки, вибрані для віддаленого аналізу, буде завантажено в службу ESET. Результат аналізу буде надіслано назад на Ваш комп'ютер. Будь-які підозрілі зразки обробляються у формі інформації, яку збирає система зворотного зв'язку ESET LiveGrid®.

Програма підвищення якості програмного забезпечення. Якщо Ви активуєте [Програма підвищення якості програмного забезпечення](#), анонімні дані телеметрії, пов'язані з використанням Наших продуктів, будуть збиратися й використовуватися, тільки якщо Ви надасте на це згоду.

Зверніть увагу, що якщо особа, яка використовує наші продукти та служби, не є Кінцевим користувачем, який придбав продукт або службу й уклав із Нами Ліцензійну угоду (наприклад, співробітник Кінцевого користувача, член сім'ї або інша особа, уповноважена використовувати продукт або службу Кінцевим користувачем відповідно до Ліцензійної угоди), обробка даних здійснюється в законних інтересах компанії ESET у розумінні ст. 6 (1) (f) GDPR, щоб дати змогу користувачу, уповноваженому Кінцевим користувачем, використовувати продукти та служби, що надаються Нами відповідно до Ліцензійної угоди.

Контактна інформація

Якщо Ви бажаєте скористатися Вашими правами як суб'єкта захисту даних або маєте питання чи застереження, надішліть нам повідомлення за такою адресою:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk