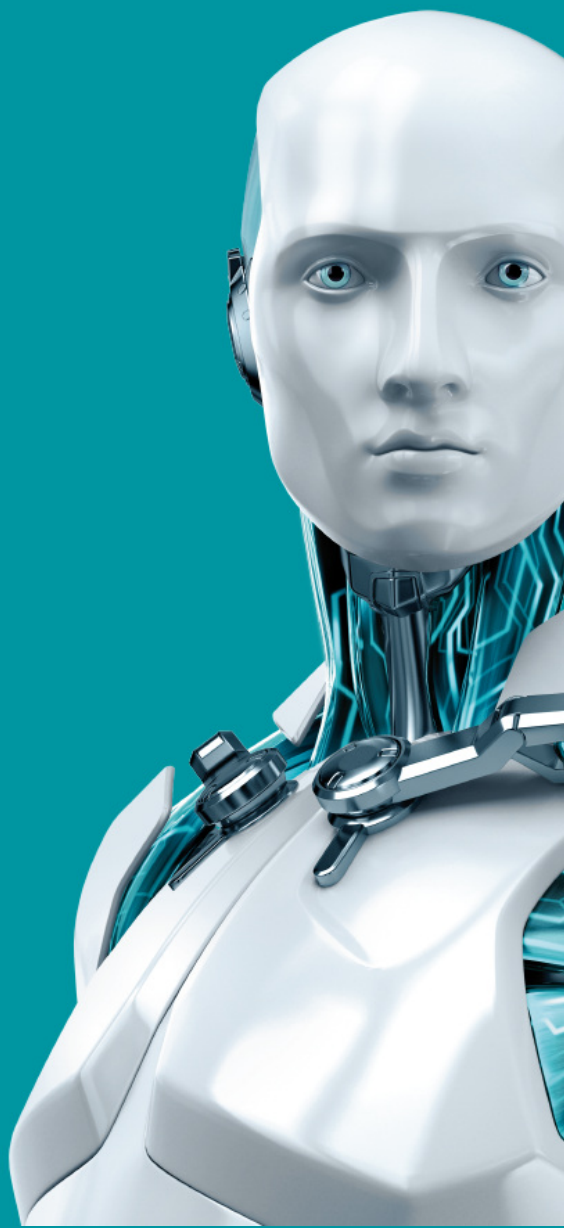
NOD32® ANTIVIRUS

Пайдаланушы нұсқаулығы

(11.0 және жоғарырақ өнім нұсқасына арналған)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / Home Server 2011

Осы құжаттың соңғы нұсқасын жүктеп алу үшін осы жерді басыңыз



ENJOY SAFER TECHNOLOGY™

ESET **NOD32 ANTIVIRUS**

Дүниежүзілік тұтынушыны қолдау орталығы: www.eset.com/support

ТҮЗЕТУ 20.10.2017

Мазмұны

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus шынымен біріктірілген компьютер қауіпсіздігіне жаңа көзқарасты білдіреді. ESET LiveGrid® қарап шығу механизмінің ең соңғы нұсқасы жылдам және дәл бола отырып, компьютеріңізді қауіпсіз сақтайды. Нәтиже – компьютерге қауіп төндіретін шабуылдар мен зиянды бағдарламаларға үнемі қырағы болатын интеллектуалдық жүйе.

ESET NOD32 Antivirus - ең жоғарғы қорғаныс біріктіретін және ең аз орын алатын толық қауіпсіздік шешімі. Біздің жаңа технологияларымыз жүйе өнімділігін кідіртусіз не компьютерге зақым келтірмей вирустартың, троялық аттың, құрттардың, жарнамалық бағдарламаның, руткиттердің және басқа қауіптердің кіруін алдын алу үшін жасанды функцияны пайдаланады.

Мүмкіндіктер мен артықшылықтар

Қайта жасақталған пайдаланушы интерфейсі	пайдаланушы интерфейсі айтарлықтай қайта жасақталды және пайдалану ыңғайлылығын сынау нәтижелерінің негізінде жеңілдетілді. Графикалық пайдаланушы интерфейсінің барлық сөздері мен хабарландырулары мұқият қарап шығылды және енді интерфейсі иврит және араб тілдері сияқты оңнан солға қарай жазылатын тілдерге қолдау көрсетеді. **Қазір Онлайн анықтама** ESET NOD32 Antivirus бағдарламасына біріктірілген және жаңартылған қолдау мазмұнын динамикалық түрде ұсынады.
Вирусқа қарсы және тыңшылыққа қарсы бағдарлама	Әлдеқайда белгілі және белгісіз вирустарды, құрттарды, троялық аттарды және руткиттерді белсенді түрде анықтайды және тазалайды. **Кеңейтілген эвристика** технологиясы белгісіз қауіптерден қорғап, олар өз зардабын тигізгенге дейін жоя отырып, тіпті бұрын-соңды көрінбеген зиянкес бағдарламаны белгілейді. **Веб қатынасты қорғау** және **Антифишинг** веб-браузерлер мен қашықтағы серверлер (SSL қамтитын) арасындағы байланысты бақылау арқылы жұмыс істейді. **Электрондық пошта клиентін қорғау** POP3(S) және IMAP(S) протоколдары арқылы алынған электрондық пошта байланысын бақылауды қамтамасыз етеді.
Тұрақты жаңартулар	Анықтау механизмін (бұрын «вирус қолтаңбаларының дерекқоры» ретінде белгілі болған) және бағдарлама модульдерін жүйелі түрде жаңарту — компьютерде ең жоғары қауіпсіздік деңгейін қамтамасыз етудің ең жақсы жолы.
ESET LiveGrid® (Деңгей бойынша іске қосылған процестерді талдау)	Сіз іске қосылған процестердің деңгейін және файлдарды тікелей ESET NOD32 Antivirus бағдарламасынан тексере аласыз.
Құрылғыны басқару	Барлық USB флэш-жадын, жад карталарын және ықшам дискілерін/DVD дискілерін автоматты түрде қарап шығады. Құралға, өндірушіге, өлшемге және басқа атрибуттарға негізделген алынбалы құралды блоктайды.
HIPS мүмкіндігі	Жүйенің қасиетін толығырақ реттеуге; жүйе тіркеуіне және белсенді процестер мен бағдарламаларға арналған ережелерді анықтауға, қауіпсіздік қатынасын реттеуге болады.
Ойыншы режимі	Ойындарға және басқа толық экранды әрекеттерге арналған жүйе ресурстарын үнемдеу үшін барлық қалқымалы терезелерді, жаңартуларды не жүйенің басқа қарқынды әрекеттерін кейінге қалдырады.

ESET NOD32 Antivirus мүмкіндіктері жарамды болу үшін лицензия белсенді болуы тиіс. ESET NOD32 Antivirus лицензиясының мерзімі аяқталмастан бірнеше апта бұрын лицензияны қайта жаңарту ұсынылады.

1.1 Осы нұсқадағы жаңа мүмкіндіктер

ESET NOD32 Antivirus бағдарламасының жаңа нұсқасында келесі жақсартулар бар:

- **Сценарийлерге негізделген шабуылдаудан қорғау** — Сізді сценарийлерге негізделген шабуылдардан және дәстүрлі емес шабуыл векторларынан пробелсенді түрде қорғайды. Қосымша ақпаратты осында қараңыз
- **Жоғары өнімділік және жүйеге төмен әсер** – Бұл нұсқа жүйе ресурстарын тиімді пайдалануға арналған, осылайша қауіптердің жаңа түрлерінен қорғай отырып, компьютердің өнімділігін пайдалануға қамтамасыз етеді.
- **Windows 10 жүйесімен үйлесімділік** — ESET бағдарламасы Microsoft Windows 10 жүйесін толығымен қолдайды.
- **JAWS** — ESET NOD32 Antivirus бағдарламасы JAWS атты ең танымал экранды оқу құралын қолдайды.
- **Сүйреп апарып тастау арқылы файлдарды қарап шығу** – Файлды немесе қалтаны жай сол файлды немесе қалтаны белгіленген аумаққа жылжыту арқылы қолмен қарап шыға аласыз.
- ESET NOD32 Antivirus сіз қорғалмаған сымсыз желіге немесе қорғауы әлсіз желіге қосылғанда хабарлайды.

ESET NOD32 Antivirus бағдарламасындағы жаңа мүмкіндіктер туралы қосымша мәліметтерді келесі ESET білім қоры мақаласында оқыңыз:
ESET үйге арналған өнімдерінің осы нұсқасындағы жаңа мүмкіндіктер

1.2 Мендегі өнім қандай?

ESET жаңа өнімдерде бірнеше қауіпсіздік деңгейін ұсынады: қуатты және жылдам антивирус шешімінен жүйеде ең аз іздер қалдыратын барлығы-біреуде қауіпсіздік шешіміне дейін.

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

Қай өнімді орнатқаныңызды анықтау үшін бағдарламаның негізгі терезесін ашыңыз (Білім қорының мақаласын қараңыз), сонда терезенің жоғарғы жағында (тақырып) өнім атауын көресіз.

Төмендегі кестеде әрбір өнімде қолжетімді мүмкіндіктер берілген.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Антивирус	✔	✔	✔
Антишпион	✔	✔	✔
Бүлдіруді блоктаушы	✔	✔	✔
Сценарийлерге негізделген шабуылдаудан қорғау	✔	✔	✔
Антифишинг	✔	✔	✔
Вебке қатынасуды қорғау	✔	✔	✔
HIPS (**Зиянкес хакерлік бағдарламалардан қорғауды** қамтиды)	✔	✔	✔
Антиспам		✔	✔
Брандмауэр		✔	✔
Қосылған үй мониторы		✔	✔
Веб-камераны қорғау		✔	✔
Желілік шабуылдан қорғау		✔	✔
Ботнеттен қорғау		✔	✔
Банкингті және төлемдерді қорғау		✔	✔

Ата-ана бақылауы		✔	✔
Ұрлыққа қарсы		✔	✔
ESET Password Manager			✔
ESET Secure Data			✔

ЕСКЕРТПЕ
Жоғарыдағы кейбір өнімдер сіздің тіл/аймақ үшін қолжетімді болмауы мүмкін.

1.3 Жүйе талаптары

ESET NOD32 Antivirus оңтайлы жұмыс істеуі үшін жүйе келесі жабдыққа және бағдарламалық құралға қойылатын талаптарды орындауы керек:

Қолдау көрсетілетін процессорлар

Intel® немесе AMD x86-x64

Қолдау көрсетілетін операциялық жүйелер

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7
Microsoft® Windows® Vista
Microsoft® Windows® Home Server 2011 64-биттік

1.4 Алдын алу

Компьютермен жұмыс істеген кезде, әсіресе интернетті шолғанда дүниеде ешқандай антивирус жүйесінің инфильтрациялардың қаупін толығымен жоя алмайтынын есте ұстаңыз және шабуылдар. Қауіпсіздіктің жоғары деңгейі мен қолайлылықпен қамтамасыз ету үшін антивирус шешімін дұрыс пайдаланып, бірнеше пайдалы ережелерді сақтау маңызды:

Тұрақты түрде жаңарту

ThreatSense статистикасына сәйкес, мыңдаған жаңа, бірегей инфильтрациялар қолданыстағы қауіпсіздік шараларын айналып өтіп, авторларға пайда әкелу үшін барлығы пайдаланушылардың есебінен жасалады. ESET вирус зертханасының мамандары осы қауіптерді күн сайын талдап, пайдаланушыларымызға қорғау деңгейін үзіліссіз жақсартып отыру үшін жаңартуларды дайындап шығарады. Осы жаңартулардың ең жоғарғы тиімділігін тексеру үшін жаңартулар жүйеде дұрыс конфигурациялануы маңызды. Жаңартуларды конфигурациялау әдістері туралы толық ақпарат алу үшін Жаңарту параметрлері тармағын қараңыз.

Қауіпсіздік түзетулерін жүктеу

Зиянды бағдарламалық құралдың авторлары зиянды кодтың таралу тиімділігін арттыру үшін әр түрлі жүйенің осал тұстарын жиі қолданады. Сол себептен, бағдарламалық құрал компаниялары қауіпсіздік жаңартуларын жасап шығару үшін бағдарламаларынан кез келген осал тұстарын мұқият бақылап, ықтимал қауіптерді тұрақты түрде жойып отырады. Бұл қауіпсіздік жаңартуларын шығысымен жүктеп алу маңызды. Microsoft Windows және Internet Explorer секілді веб-шолғыштар тұрақты кезеңде шығатын қауіпсіз жаңартуларына арналған бағдарламалардың екі үлгісі болып табылады.

Маңызды деректердің сақтық көшірмесін жасау

Зиянкес бағдарламаны жазушылар әдетте пайдаланушылардың қажеттіліктерін ойламайды, сондықтан зиянды бағдарламалардың белсенділігі операциялық жүйенің толық жұмыс істемеуіне және маңызды деректердің жоғалуына жиі алып келеді. Маңызды әрі әлсіз деректердің DVD сияқты сыртқы құралда немесе сыртқы қатты дискіде сақтық көшірмесін үнемі жасап отыру маңызды. Бұл жүйеде ақау болған кезде деректерді жеңілірек әрі жылдамырақ қалпына келтіреді.

Компьютердің вирустарын үнемі қарап шығу

Нақты уақыттағы файл жүйесін қорғау модулі қолданатын белгілі және белгісіз вирустарды, құрттарды, трояндарды және руткиттерді анықтайды. Бұл кез келген уақытта файлға кіруді не ашуды білдіреді, ол зиянды әрекеттерге тексеріледі. Біз компьютерді толық қарап шығуды кемінде айына бір рет орындауды ұсынамыз, өйткені зиянкес бағдарламалардың қолтаңбалары өзгеріп отыруы мүмкін және анықтау механизмін өзін күнде жаңартады.

Негізгі қауіпсіздік ережелерін орындау

Бұл барлығының ішінен ең пайдалы әрі тиімді ереже болып саналады – әрқашан сақ болыңыз. Бүгінде көптеген инфильтрациялар орындалу және таратылу үшін пайдаланушының араласуын қажет етеді. Егер жаңа файлдар ашудан сақтансаңыз, инфильтрацияларды жоюға жұмсалатын уақыт пен күш-жігеріңізді үнемдейсіз. Мына жерде кейбір пайдалы нұсқаулар бар:

- Қалқымалы терезелері мен жыпылықтаған жарнамалары көп күдікті веб-тораптарға кірмеңіз.
- Тегін бағдарламаларды, кодек пакеттерін, т.б. орнатқан кезде сақ болыңыз. Тек қауіпсіз бағдарламаларды пайдаланып, интернеттегі қауіпсіз веб-тораптарқа кіріңіз.
- Электрондық пошта тіркемелерін, әсіресе көп пайдаланушыға жіберілген хабарлардағылар мен белгісіз жіберушілерден келген хабарлардағы тіркемелерді ашқан кезде сақ болыңыз.
- Компьютерде күнделікті жұмыс істегенде Әкімшінің есептік жазбасын пайдаланбаңыз.

2. Орнату

Компьютеріңізде ESET NOD32 Antivirus орнатудың бірнеше әдістері бар. Орнату әдістері еліне және тарату жолдарына байланысты әр түрлі болуы мүмкін:

- Live орнатушысын ESET веб-сайтынан жүктеп алуға болады. Орнату бумасы барлық тілдер үшін әмбебап (қажетті тілді таңдаңыз). Live орнатушысы кішкентай файл; ESET NOD32 Antivirus орнатуға қажетті қосымша файлдар автоматты түрде жүктеледі.

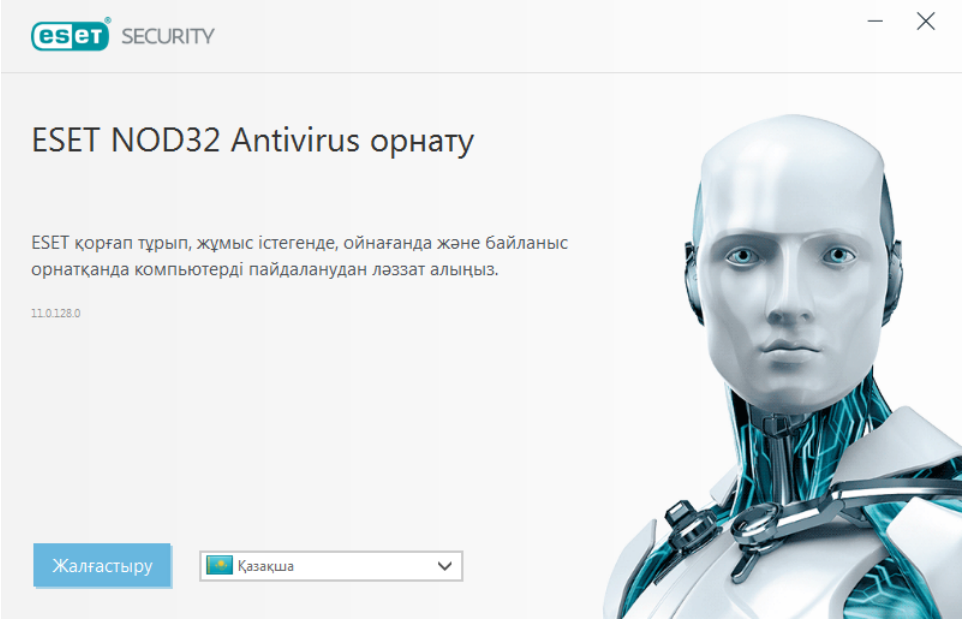
- Оффлайн орнату – Орнатудың бұл түрі ықшам дискіден/DVD дискінен орнатқанда пайдаланылады. Бұл Live орнатушысының файлынан үлкенірек *.exe* файлын пайдаланады және орнатуды орындау үшін интернет қосылымын немесе қосымша файлдарды қажет етпейді.

МАҢЫЗДЫ
ESET NOD32 Antivirus бағдарламасын орнату алдында компьютерде басқа антивирустық бағдарламалар орнатылмағанын тексеріңіз. Егер бір компьютерде екі немесе одан көп антивирустық шешімдер орнатылған болса, олардың арасында қайшылықтар болуы мүмкін. Жүйеден басқа антивирустық бағдарламаларды жою ұсынылады. Жалпы антивирустық бағдарламаны құралдар тізімінен жою үшін ESET білім қоры мақаласын (ағылшын және бірнеше басқа тілдерде қол жетімді) қараңыз.

2.1 Live орнатушысы

Live орнатушысы орнату бумасын жүктеп алғаннан кейін орнату файлын екі рет басып, орнатушы терезесіндегі нұсқауларды қадамдары бойынша орындаңыз.

МАҢЫЗДЫ
Орнатудың бұл түрін жүзеге асыру үшін интернетке қосылуыңыз қажет.



Ашылмалы мәзірден қажетті тілді таңдап, **Жалғастыру** түймешігін басыңыз. Орнату файлдарының жүктелуіне біраз уақыт беріңіз.

Соңғы пайдаланушының лицензиялық келісімін қабылдағаннан кейін сізден **ESET LiveGrid®** және **ықтимал қалаусыз қолданбаларды анықтауды** конфигурациялау сұралады. **ESET LiveGrid®** Тұтынушыларымызды қорғау үшін ESET жаңа қауіптер туралы бірден және үздіксіз хабардар болып отыруын қамтамасыз етеді. Бұл жүйе жаңа қауіптерді ESET зертханасына жіберуге мүмкіндік береді. Бұл зертханада олар талданады, өңделеді және анықтау механизміне қосылады.

Әдепкі бойынша, **ESET LiveGrid® кері байланыс жүйесін қосу (ұсынылады)** опциясы таңдалған. Ол осы мүмкіндікті іске қосады.

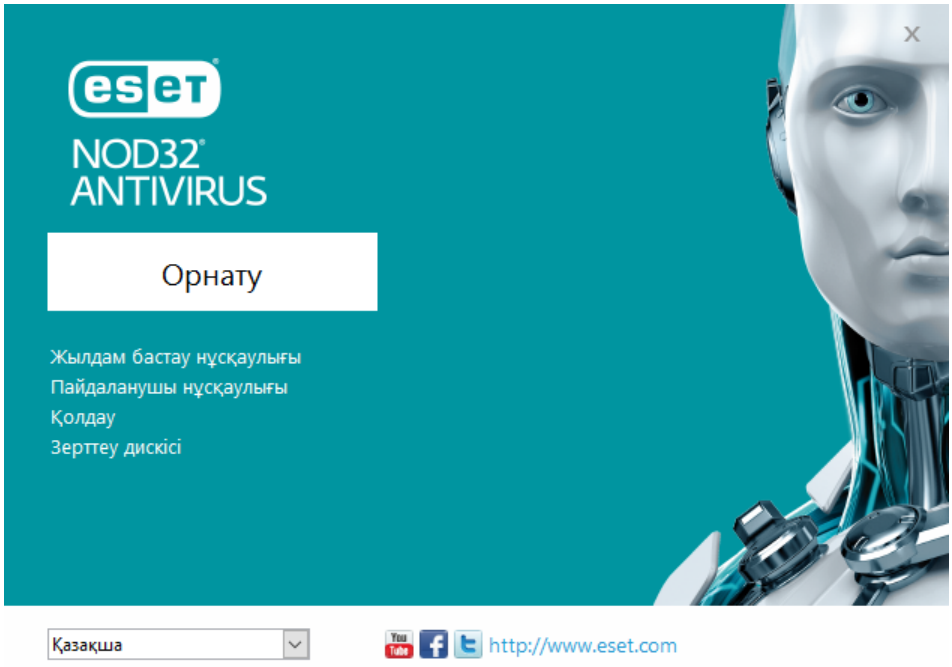
Орнату процесіндегі келесі қадам – ықтимал қалаусыз бағдарламаларды анықтауды конфигурациялау. Қажетсіздігі ықтимал бағдарламалар міндетті түрде зиянды емес, бірақ жиі операциялық жүйенің әрекетіне теріс әсер етеді. Қосымша мәліметтерді алу үшін Қажетсіздігі ықтимал бағдарламалар тарауын қараңыз.

Орнату процесін іске қосу үшін **Орнату** түймесін басыңыз. Бұл біраз уақыт алуы мүмкін. Өнімді орнатуды аяқтау және белсендіру процесін бастау үшін **Дайын** түймесін басыңыз.

ЕСКЕРТПЕ
Сізде өнімнің басқа нұсқаларын орнатуға рұқсат ететін лицензия бар болса, қалауыңызға сай өнімді таңдаңыз. Әрбір өнімдегі мүмкіндіктер туралы қосымша ақпарат алу үшін осы жерді басыңыз.

2.2 Автономды режимде орнату

Оффлайн режимде орнатуды (.exe) іске қосқаннан кейін орнату шебері орнатудан қадамдарынан өткізеді.



Ашылмалы мәзірден қажетті тілді таңдап, **Жалғастыру** түймешігін басыңыз. Орнату файлдарының жүктеп алынуын біраз күтіңіз.

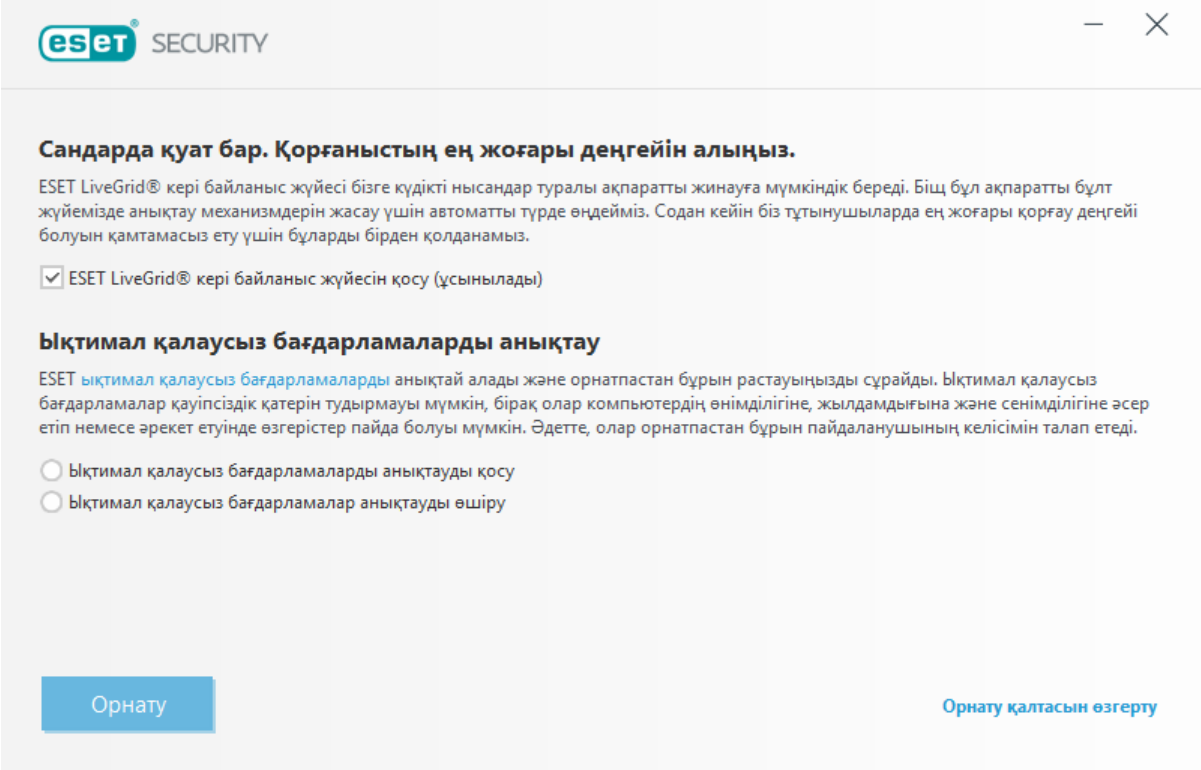
Соңғы пайдаланушының лицензиялық келісімін қабылдағаннан кейін сізден **Лицензиялық кілтті енгізу** немесе **Лицензиялар реттеушісін пайдалану** сұралады.

Сізде лицензия әлі жоқ болса, ESET өнімін шектеулі уақыт бойы сынау үшін **Тегін сынақ** пәрменін таңдаңыз немесе **Лицензияны сатып алу** пәрменін таңдаңыз. Я болмаса, орнатуды белсендірусіз жалғастыру үшін **Белсендіруді өткізіп жіберу** пәрменін таңдауға болады. Лицензиялық кілт кейінірек сұралады.

2.2.1 Лицензиялық кілтті енгізу

Орнату шебері лицензиялық кілтіңізге сай орнататын өнімді таңдайды және орнату кезінде өнім атауын көрсетеді. Лицензияңызбен белсендіруге болатын өнімдердің тізімін көру үшін **Өнімді өзгерту** пәрменін басыңыз. Әрбір нақты өнімдегі мүмкіндіктер туралы қосымша ақпарат алу үшін осы жерді басыңыз.

Жалғастыру түймесін басыңыз, **ESET LiveGrid®** және **ықтимал қалаусыз қолданбаларды анықтау** үшін таңдаулы параметрлерді таңдаңыз. **ESET LiveGrid®** Тұтынушыларымызды қорғау үшін ESET жаңа қауіптер туралы бірден және үздіксіз хабардар болып отыруын қамтамасыз етеді. Бұл жүйе жаңа қауіптерді ESET зертханасына жіберуге мүмкіндік береді. Бұл зертханада олар талданады, өңделеді және анықтау механизміне қосылады. **Ықтимал қалаусыз қолданбалар** міндетті түрде зиянкес болып табылмайды, бірақ операциялық жүйенің әрекетіне теріс әсер етуі мүмкін. Қосымша мәліметтерді Ықтимал қалаусыз қолданбалар тарауында қараңыз.



Орнату процесін бастау үшін **Орнату** түймесін басыңыз. Бұл біраз уақыт алуы мүмкін. Өнімді орнатуды аяқтау және белсендіру процесін бастау үшін **Дайын** түймесін басыңыз.

ЕСКЕРТПЕ
Өнімдер арасында таңдауға мүмкіндік беретін лицензияңыз болса, өнімді жеке параметрлерге сай орната аласыз. Әрбір нақты өнімдегі мүмкіндіктер туралы қосымша ақпарат алу үшін осы жерді басыңыз.

Орнату қадамдары, **ESET LiveGrid®** және **Ықтимал қалаусыз қолданбаларды анықтау** туралы қосымша нұсқауларды «Live орнатушысы» бөлімінде қараңыз.

2.2.2 Лицензиялар реттеушісін пайдалану

Лицензия реттеушісін пайдалану параметрін таңдағаннан кейін сізден жаңа терезеде my.eset.com тіркелгі деректері сұралады. Лицензия реттеушісіндегі лицензияны пайдалану үшін my.eset.com тіркелгі деректерін енгізіңіз және **Кіру** түйсін басыңыз. Белсендіретін лицензияны таңдаңыз, **Жалғастыру** түймесін басыңыз, содан кейін ESET NOD32 Antivirus белсендіріледі.

ЕСКЕРТПЕ
Сізде my.eset.com есептік жазбасы әлі жоқ болса, **Есептік жазба жасау** түймесін басу арқылы тіркеңіз.

ЕСКЕРТПЕ
Құпиясөзіңізді ұмытып қалсаңыз, **Құпиясөзімді ұмытып қалдым** пәрменін басыңыз және сіз қайта бағытталатын веб-беттегі қадамдарды орындаңыз.

ESET License Manager сізге барлық ESET лицензияларыңызды басқаруға көмектеседі. Лицензияны оңай мерзімін ұзартуға, жаңартуға немесе ұзартуға және маңызды лицензия мәліметтерін көруге болады. Алдымен лицензиялық кілтті енгізіңіз. Содан кейін сіз өнімді, байланысты құрылғыны, қолжетімді орындар санын және мерзімі біту күнін көресіз. Белгілі бір құрылғыларды ажыратуға немесе қайта атауға болады. **Ұзарту** пәрменін басқанда сіз сатып алуды растауға және мерзімді ұзартуды сатып алуға болатын онлайн дүкенге қайта бағытталасыз.

Лицензияңызды жаңартқыңыз келсе (мысалы, ESET NOD32 Antivirus дегеннен ESET Smart Security Premium дегенге) немесе ESET қауіпсіздік өнімін басқа құрылғыда орнатқыңыз келсе, сіз сатып алуды орындау үшін онлайн дүкенге қайта бағытталасыз.

Сондай-ақ ESET License Manager ішінде әртүрлі лицензияларды қосуға, құрылғыларыңызға өнімдерді жүктеп алуға немесе лицензияларды электрондық пошта арқылы бөлісуге болады.

2.2.3 Қосымша параметрлер

Орнату қалтасын өзгерту пәрменін таңдағаннан кейін орнату орнын таңдау сұралады. Әдепкі бойынша бағдарлама келесі каталогқа орнатылады:

C:\Program Files\ESET\ESET NOD32 Antivirus

Бұл орынды өзгерту үшін **Шолу** түймешігін басыңыз (ұсынылмайды).

Келесі орнату қадамдарын (**ESET LiveGrid®** және **Ықтимал қалаусыз қолданбаларды анықтау**) орындау үшін «Live орнатқышы» бөліміндегі нұсқауларды қараңыз («Live орнатқышы» бөлімін қараңыз).

Орнатуды аяқтау үшін **Жалғастыру** түймешігін, содан кейін **Орнату** түймешігін басыңыз.

2.3 Жиі кездесетін орнату мәселелері

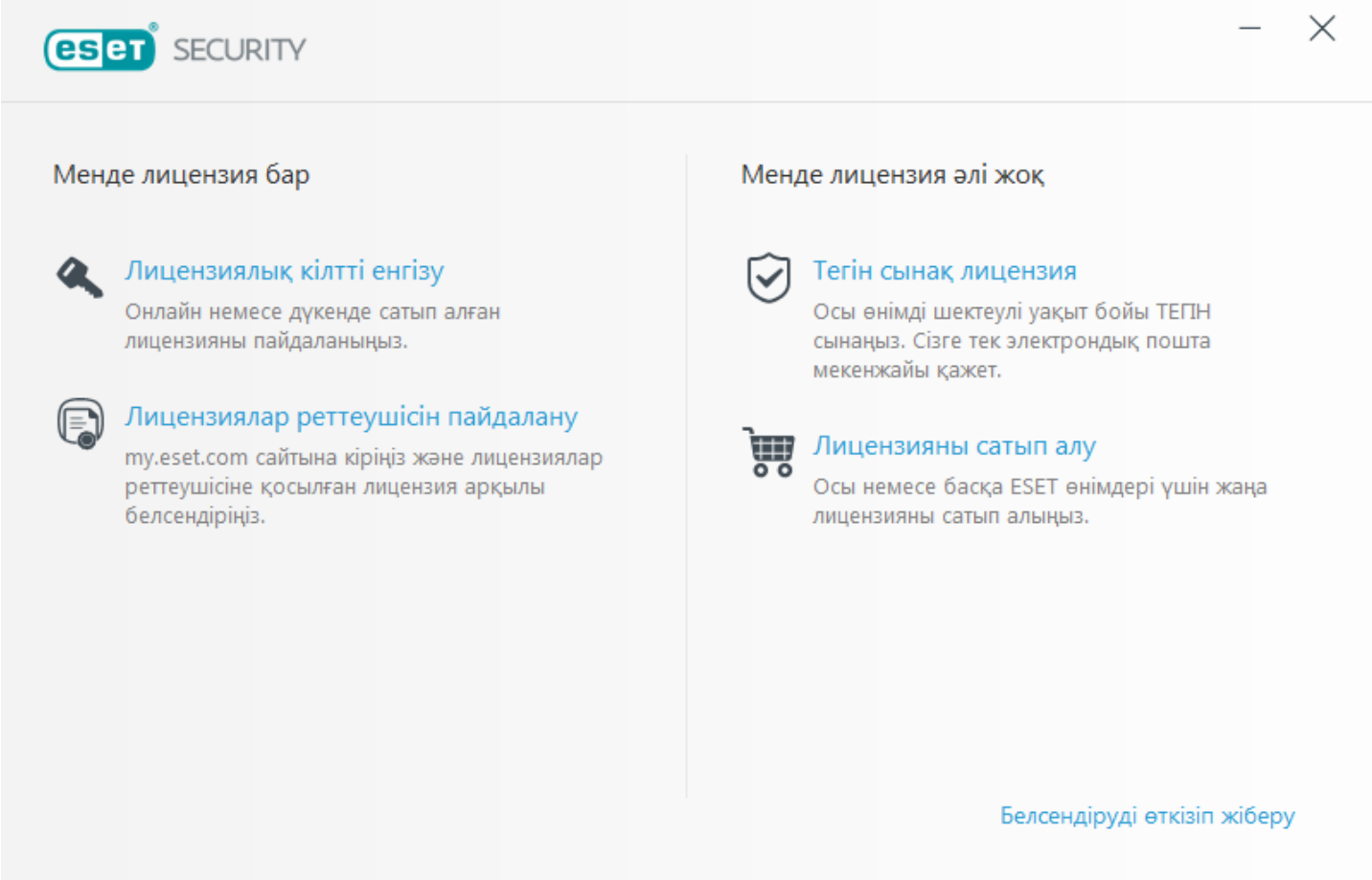
Орнату кезінде мәселелер орын алса, мәселенің шешімін табу үшін жиі кездесетін орнату қателері және шешімдер тізімін қараңыз.

2.4 Өнімді іске қосу

Кейін орнату аяқталды, өнімді белсендіру сұралады.

Өнімді іске қосудың бірнеше әдісі бар. Елге байланысты іске қосу терезесінде нақты іске қосу сценарийінің және тарату жолдарының (ықшам диск/DVD, ESET веб-беті, т.б.) қол жетімділігі өзгеріп отыруы мүмкін:

- Егер өнімнің бөлшектеп сатылатын қораптағы нұсқасын сатып алсаңыз, **Лицензиялық кілтті** пайдалана отырып өнімді іске қосыңыз. Лицензиялық кілт әдетте өнім қаптамасының ішінде немесе артында орналасады. Лицензиялық кілт іске қосу сәтті болуы үшін берілгендей енгізілуі керек. Лицензиялық кілт – лицензия иесін идентификациялау және лицензияны іске қосу үшін пайдаланылатын XXXX-XXXX-XXXX-XXXX-XXXX or XXXX-XXXXXXXX пішіміндегі бірегей жол.
- Егер сатып алу алдында ESET NOD32 Antivirus бағдарламасын бағалау керек болса, **Тегін сынақ нұсқасының лицензиясы** параметрін таңдаңыз. ESET NOD32 Antivirus бағдарламасын шектеулі уақытқа іске қосу үшін электрондық пошта мекенжайыңыз бен еліңізді енгізіңіз. Сынақ лицензияңыз электрондық поштаңызға жіберіледі. Сынақ лицензияларын әр тұтынушы үшін тек бір рет іске қосуға болады.
- Егер лицензияңыз жоқ болса және оны сатып алғыңыз келсе, Лицензияны сатып алу опциясын басыңыз. Бұл сізді жергілікті ESET таратушысының веб-сайтына қайта бағыттайды.



2.5 Лицензиялық кілтті енгізу

Автоматты жаңартулар қауіпсіздік үшін маңызды. ESET NOD32 Antivirus бағдарламасы жаңартуларды **Лицензиялық кілтті** пайдаланып белсендіргеннен кейін ғана алады.

Орнатудан кейін лицензиялық кілтті енгізбесеңіз, өнім белсендірілмейді. Лицензияны бағдарламаның негізгі терезесінде өзгертуге болады. Мұны істеу үшін **Анықтама және қолдау** > **Лицензияны іске қосу** тармағын басыңыз және «Өнімді іске қосу» терезесінде ESET қауіпсіздік өнімімен бірге алған лицензия деректерін енгізіңіз.

Лицензиялық кілтті енгізгенде оны дәл жазылғандай теру маңызды:

- Лицензия кілті - лицензия иесін идентификациялау және лицензияны іске қосу үшін пайдаланылатын XXXX-XXXX-XXXX-XXXX-XXXX пішіміндегі бірегей жол.

Дәлдікті қамтамасыз ету үшін лицензиялық кілтті тіркеу электрондық хабарынан көшіріп, қою ұсынылады.

2.6 Ең соңғы нұсқасына дейін жаңарту

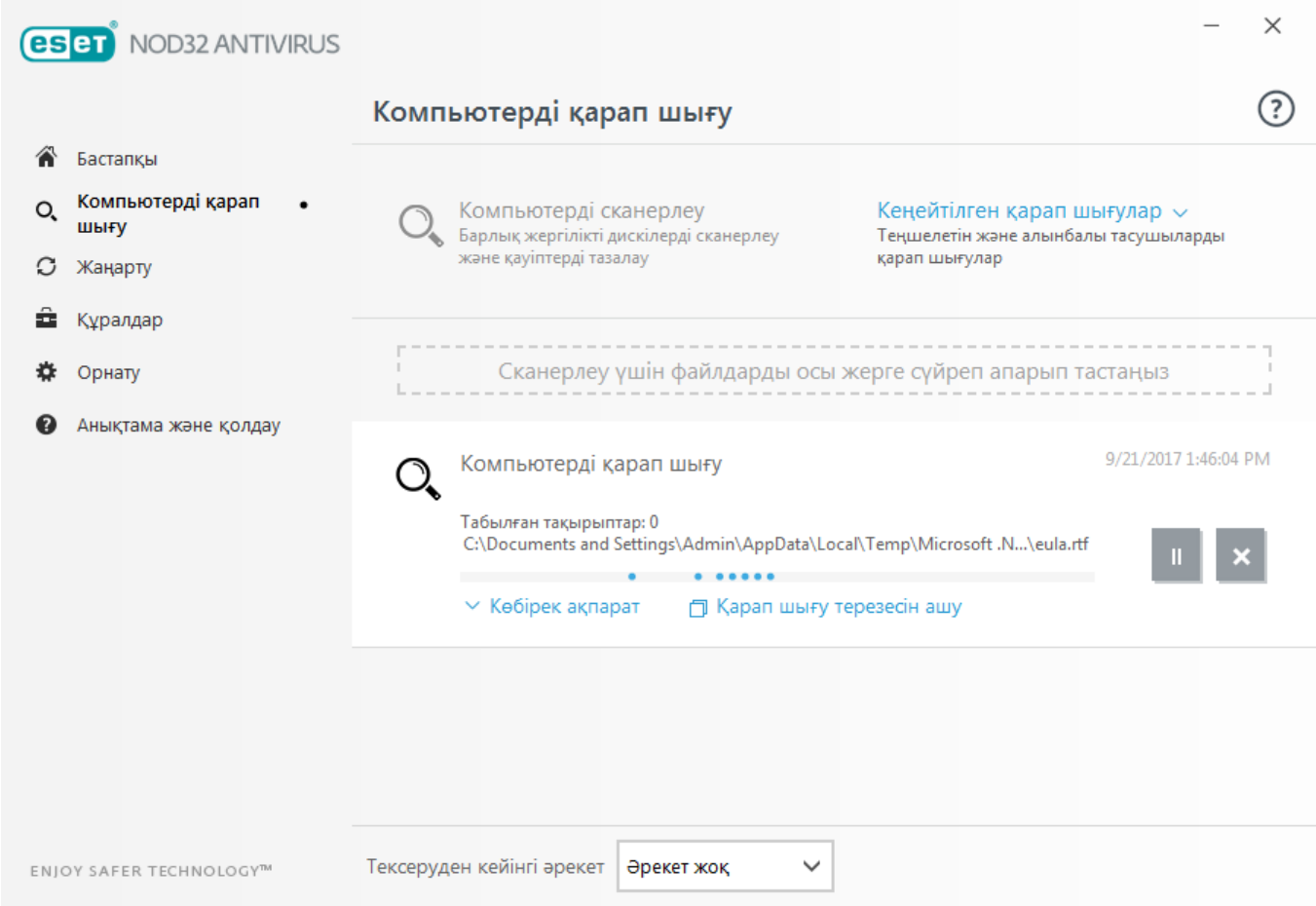
Жақсартуларды қосу немесе бағдарлама модульдерін автоматты түрде жаңарту арқылы түзету мүмкін емес мәселелерді шешу үшін ESET NOD32 Antivirus бағдарламасының жаңа нұсқалары шығарылады. Ең соңғы нұсқаға жаңартуды бірнеше жолмен орындауға болады:

1. Автоматты түрде, бағдарламаны жаңарту арқылы.
   Бағдарлама жаңартуы барлық пайдаланушыларға таратылатындықтан және белгілі бір жүйе конфигурацияларына әсер ете алатындықтан, ол барлық мүмкін жүйе конфигурацияларымен бірге қызмет ете алуына көз жеткізу үшін ұзақ тексеруден кейін шығарылады. Егер жаңа нұсқасына шығарылғаннан кейін дереу өту керек болса, төменде кқрсетілген әдістердік біреуін пайдаланыңыз.
2. Қолмен, негізгі бағдарлама терезесінде **Жаңартулар бар-жоғын тексеру** тармағын **Жаңарту** бөлімінде басу арқылы.
3. Қолмен, ең соңғы нұсқаны жүктеу және алдыңғысының үстінен орнату арқылы.

2.7 Орнатудан кейінгі бірінші қарап шығу

ESET NOD32 Antivirus орнатқаннан кейін зиянкес кодты тексеру үшін бірінші сәтті жаңартудан кейін компьютерді қарап шығу автоматты түрде іске қосылады.

Компьютерді қарап шығу > **Компьютерді қарап шығу** тармағын таңдау арқылы негізгі бағдарлама терезесінен де компьютерді қарап шығуды қолмен іске қосуға болады. Шығу туралы қосымша ақпарат алу үшін Шығу бөлімін қараңыз.



3. Жаңадан пайдаланушыларға арналған нұсқаулық

Бұл бөлімде ESET NOD32 Antivirus бағдарламасының бастапқы шолуы және оның негізгі параметрлері берілген.

3.1 Негізгі бағдарлама терезесі

ESET NOD32 Antivirus бағдарламасының негізгі терезесі екі негізгі бөлімге бөлінген. Оң жақтағы негізгі терезеде сол жақтағы негізгі мәзірден таңдалған опцияға сай ақпарат көрсетіледі.

Төменде негізгі мәзір опцияларының сипаттамасы берілген:

Басты – ESET NOD32 Antivirus бағдарламасының қорғау күйі туралы ақпаратты қамтамасыз етеді.

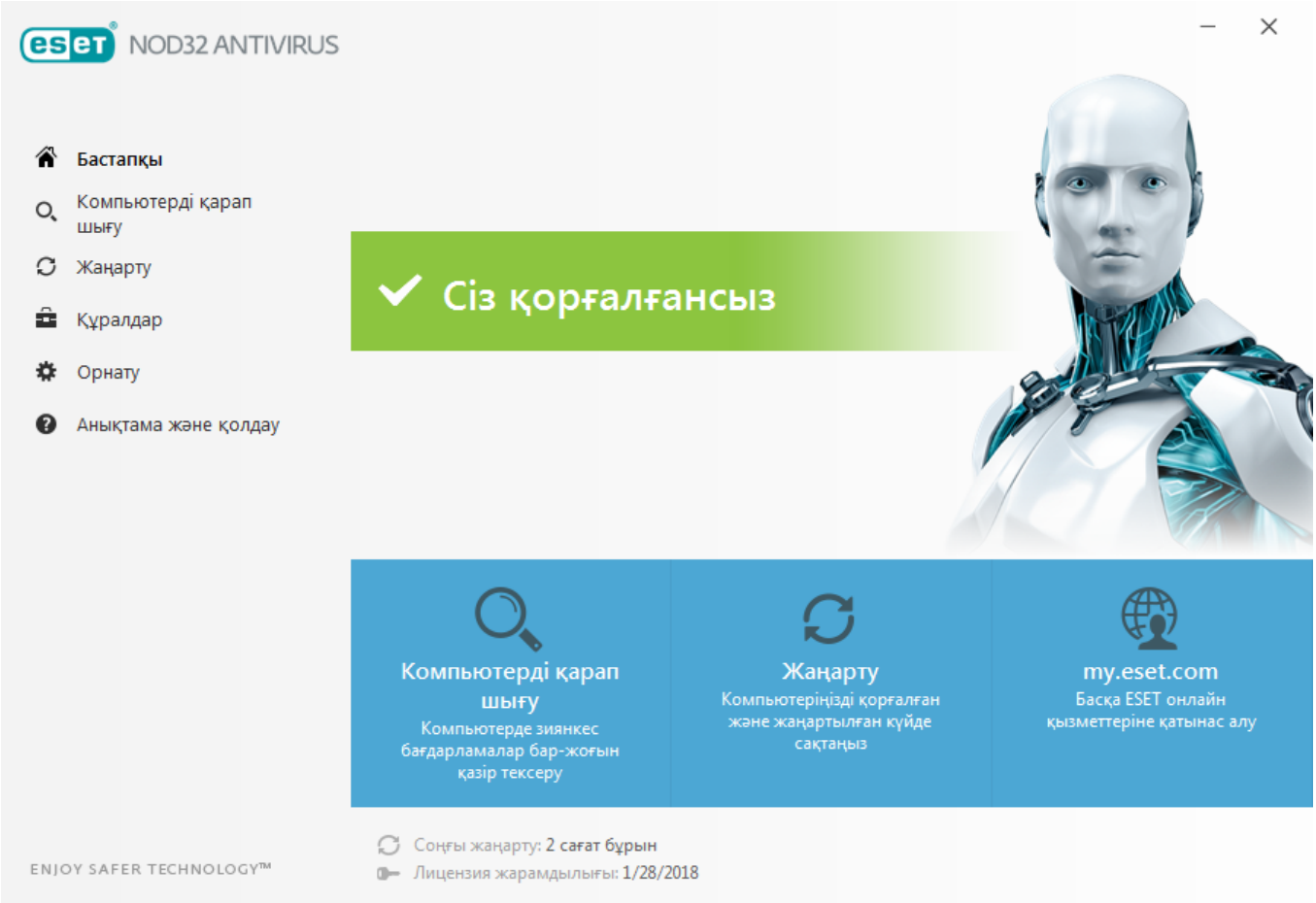
Компьютерді қарап шығу — компьютерді қарап шығуды конфигурациялау және іске қосу немесе таңдамалы қарап шығуды жасау.

Жаңарту – Анықтау механизмін жаңартулар туралы ақпаратты көрсетеді.

Құралдар - журнал файлдарына, қорғау статистикасына, көру әрекетіне, іске қосылған процестерге қатынасуды қамтамасыз етеді, Жоспарлағыш, ESET SysInspector және ESET SysRescue.

Реттеу – Бұл опцияны компьютер, интернет үшін қауіпсіздік деңгейін реттеу үшін таңдаңыз.

Анықтама және қолдау - анықтама файлдарына, ESET білім қорына, ESET веб-сайтына және тұтынушыларды қолдау қызметінен қолдау сұрауды сілтемелеріне қатынасуды қамтамасыз етеді.

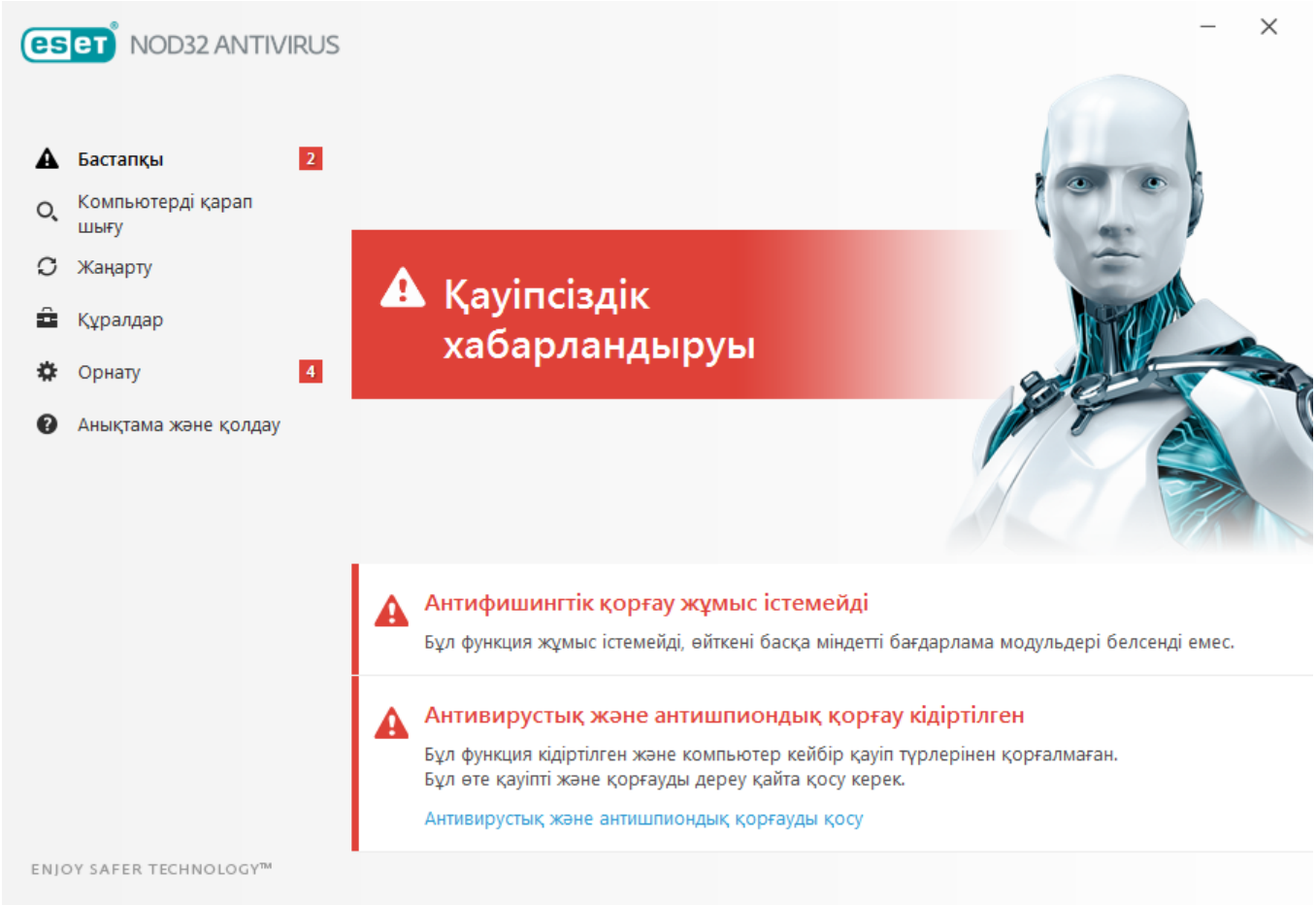


Бастапқы экраны компьютердің ағымдағы қорғау деңгейі туралы маңызды ақпаратты қамтиды. Күй терезесі ESET NOD32 Antivirus бағдарламасының жиі пайдаланылатын мүмкіндіктерін көрсетеді. Сондай-ақ, мұнда соңғы жаңарту және бағдарламаның мерзімі біту күні туралы ақпаратты табуға болады.

Жасыл белгіше мен жасыл **Ең жоғарғы қорғау** күйі ең жоғары қорғау қамтамасыз етілгенін көрсетеді.

Бағдарлама тиісті түрде жұмыс істемесе не істеу керек?

Егер белсенді қорғау модулі дұрыс жұмыс істеп жатса, оның қорғау күйінің белгішесі жасыл болады. Қызыл леп белгісі не қызғылт сары хабарландыру ең жоғарғы қорғаныс қамтамасыз етілмейтінін білдіреді. Толық қорғанысты қалпына келтіруге арналған ұсынылатын шешімдер секілді әр модульдің қорғаныс күйі туралы қосымша мәліметтер **Бастапқы** тармағында көрсетіледі. Жеке модульдердің күйін өзгерту үшін **Орнату** түймесін басып, қажетті модульді таңдаңыз.



Қызыл белгіше мен қызыл Ең жоғарғы қорғау қамтамасыз етілмейді күйі маңызды мәселелерді білдіреді. Осы күйдің көрсетілуінің бірнеше себептері бар, мысалы:

- **Өнім белсендірілмеген** – ESET NOD32 Antivirus бағдарламасын **Басты** тармағында «Қорғау күйі» астында **Өнімді белсендіру** немесе **Қазір сатып алу** пәрменін басу арқылы белсендіруге болады.
- **Анықтау механизмі ескірген** – Бұл қате вирус қолтаңбасының дерекқорын жаңартуға бірнеше сәтсіз әрекет жасалғаннан кейін шығады. Жаңарту параметрлерін тексеру ұсынылады. Бұл қатенің ең жиі себебі – дұрыс емес енгізілген түпнұсқалықты растау деректері немесе қате конфигурацияланған қосылым параметрлері.
- **Антивирустық және антишпиондық қорғау өшірілген** – Антивирустық және антишпиондық қорғауды **Антивирустық және антишпиондық қорғауды қосу** пәрменін басу арқылы қайта қосуға болады.
- **Лицензия мерзімі біткен** – Мұны қызыл қорғау күйінің белгішесі көрсетеді. Лицензияның мерзімі біткеннен кейін бағдарламаны жаңарту мүмкін емес. Лицензияны жаңарту үшін ескерту терезесіндегі нұсқауларды орындаңыз.

Сарғылт белгіше шектеулі қорғауды көрсетеді. Мысалы, бағдарламаны жаңартуда мәселе болуы немесе лицензияңыздың мерзімі аяқталуға жақын болуы мүмкін.
Осы күйдің көрсетілуінің бірнеше себептері бар, мысалы:

- **Ойыншы режимі белсенді** – Ойыншы режимін қосу ықтимал қауіпсіздік қаупі болып табылады. Бұл мүмкіндікті қосу барлық қалқымалы терезелерді өшіреді және барлық жоспарланған тапсырмаларды тоқтатады.
- **Лицензияңыздың мерзімі жақын арада бітеді** – Мұны жүйе құлпы жанында леп белгісі бар қорғау

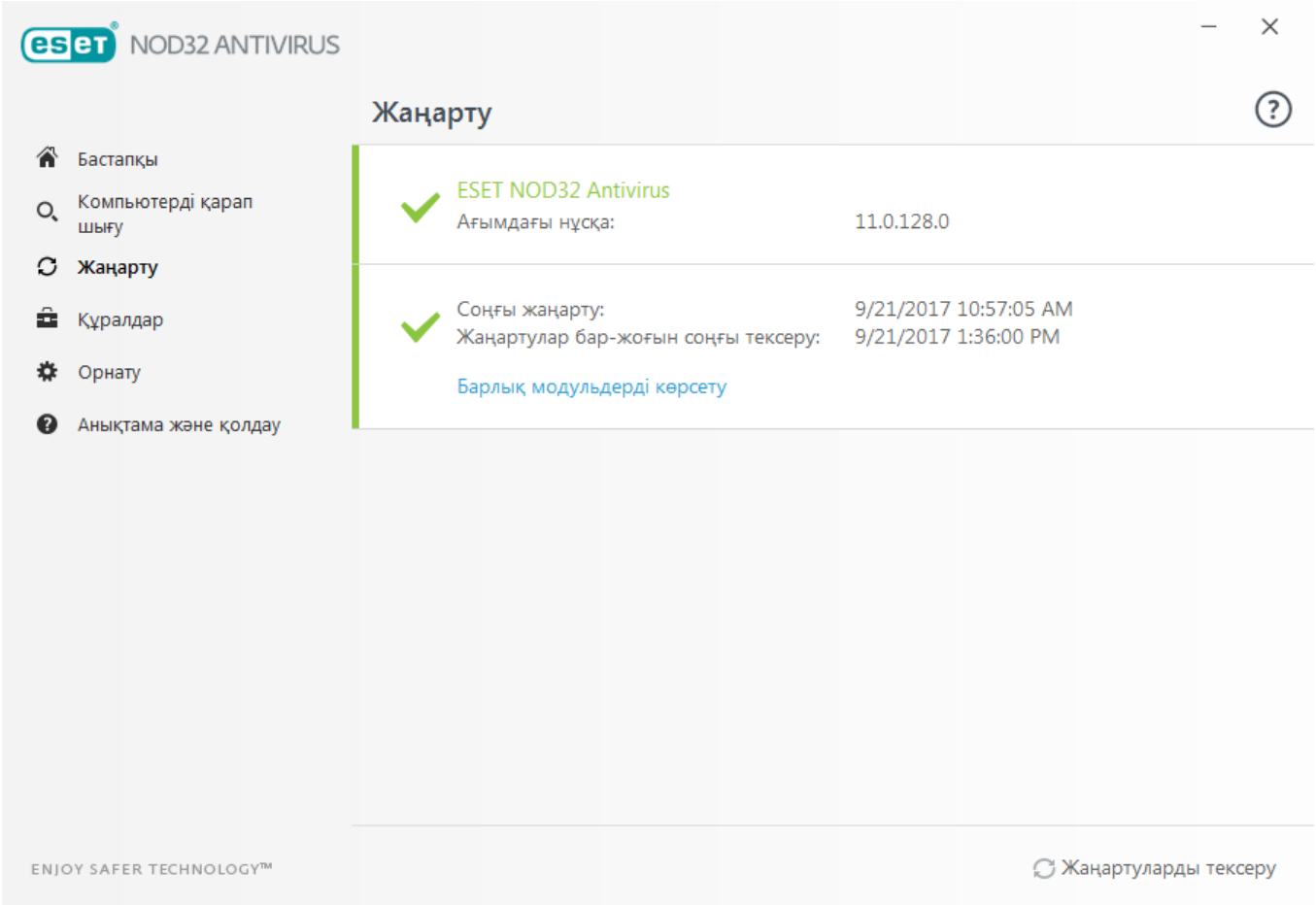
күйінің белгішесі көрсетеді. Лицензияның мерзімі аяқталғаннан кейін бағдарламаны жаңарту мүмкін болмайды және Қорғаныс күйінің белгішесі қызыл жанады.

Ұсынылған шешімдерді пайдаланып мәселені шешу мүмкін болмаса, **Анықтама және қолдау** түймесін басып анықтама файлдарын ашыңыз немесе ESET білім базасында іздеңіз. Егер әлі де көмек керек болса, қолдау сұрауын жібере аласыз. «ESET» компаниясының тұтынушыларды қолдау бөлімі сұрақтарыңызға тез жауап береді және шешімді табуға көмектеседі.

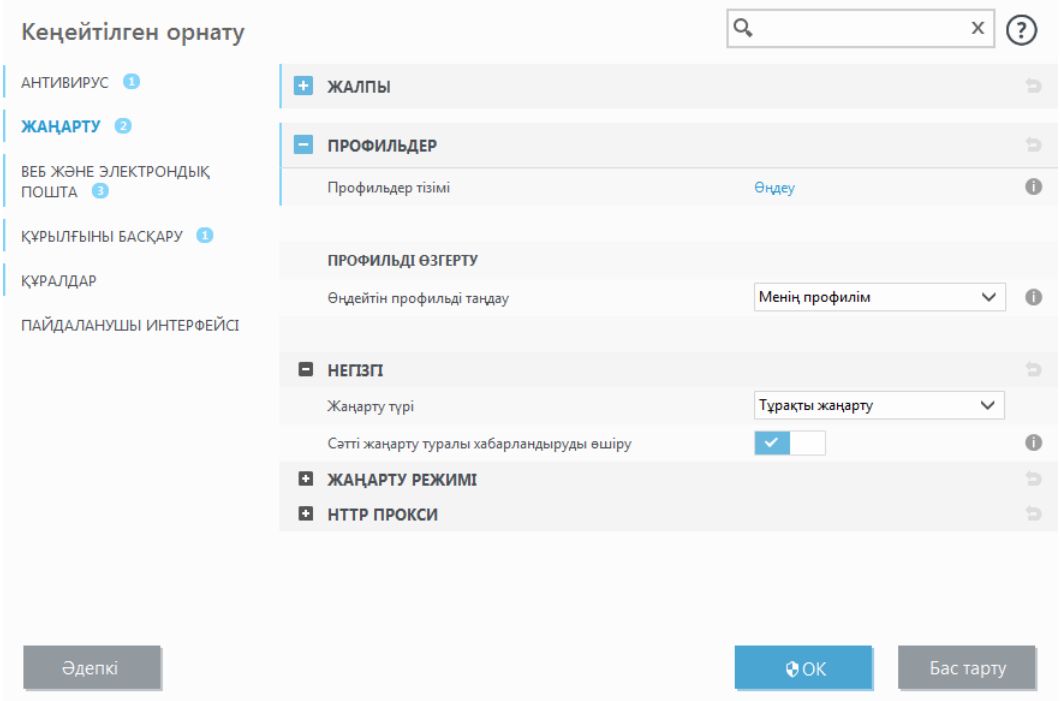
3.2 Жаңартулар

Анықтау механизмін жаңарту және бағдарлама құрамдастарын жаңарту жүйені зиянкес кодтан қорғаудың маңызды бөлігі болып табылады. Оның конфигурациясы мен операциясына аса назар аударыңыз. Басты мәзірде **Жаңарту** пәрменін басыңыз, содан кейін анықтау механизмін жаңарту бар-жоғын тексеру үшін **Қазір жаңарту** пәрменін басыңыз.

ESET NOD32 Antivirus бағдарламасын іске қосу кезінде лицензиялық кілт енгізілмесе, ол осы кезде сұралады.

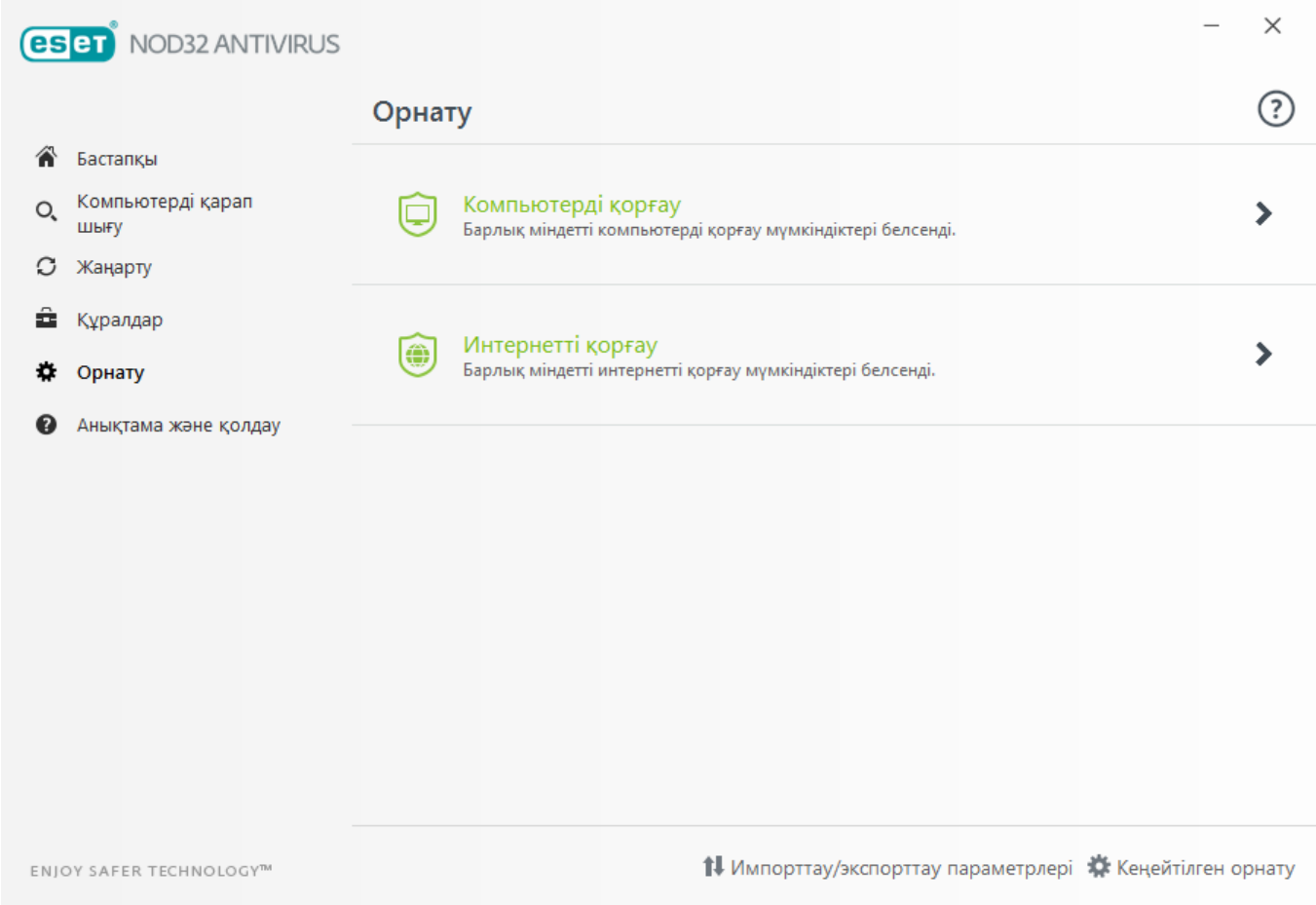


«Кеңейтілген орнату» терезесі (негізгі мәзірде **Орнату** пәрменін, содан кейін **Кеңейтілген орнату** пәрменін басыңыз немесе пернетақтада **F5** пернесін басыңыз) қосымша жаңарту опцияларын қамтиды. Жаңарту режимі, прокси серверге қатынасу және LAN қосылымдары сияқты кеңейтілген жаңарту опцияларын конфигурациялау үшін **Жаңарту** терезесінде нақты қойындыны басыңыз.



4. ESET NOD32 Antivirus бағдарламасымен жұмыс істеу

ESET NOD32 Antivirus параметрлерін орнату опциялары компьютердің қорғау деңгейлерін реттеуге мүмкіндік береді.



Орнату мәзірі келесі бөлімдерге бөлінген:

Компьютерді қорғау

Интернетті қорғау

Тиісті қорғау модулінің кеңейтілген параметрлерін реттеу үшін құрамдасты басыңыз.

Компьютер қорғаныс параметрлерін орнату келесі компоненттерді қосуға немесе ажыратуға мүмкіндік береді:

- **Файлдық жүйені нақты уақытта қорғау** - Барлық файлдарда ашылғанда, жасалғанда немесе компьютерде іске қосылғанда зиянкес код бар-жоғы қарап шығылады.
- **HIPS** - HIPS жүйесі операциялық жүйедегі оқиғаларды бақылайды және оларға теңшелген ережелер жиынына сай жауап береді.
- **Ойыншы режимі** - Ойыншы режимін қосады немесе өшіреді. Ойыншы режимін қосқаннан кейін сіз ескерту хабарын (ықтимал қауіпсіздік қаупі) аласыз және негізгі терезе қызғылт сары түске боялады.

Интернетті қорғау параметрлерін орнату келесі компоненттерді қосуға немесе ажыратуға мүмкіндік береді:

- **Веб-қатынасты қорғау** — Қосылған болса, HTTP немесе HTTPS арқылы өтетін бүкіл трафикте зиянды бағдарлама бар-жоғы қарап шығылады.
- **Электрондық пошта клиентін қорғау** — POP3 және IMAP протоколдары бойынша алынатын байланысын бақылайды.
- **Антифишингтік қорғау** — Пайдаланушыларды құпия мәліметтерді жіберуде басқаруға арналған таратылатын күмәнді мазмұны бар веб-сайттарды тексереді.

Өшірілген қауіпсіздік компонентін қайта қосу үшін жүгірткіні басып, жасыл құсбелгіні көрсетіңіз.

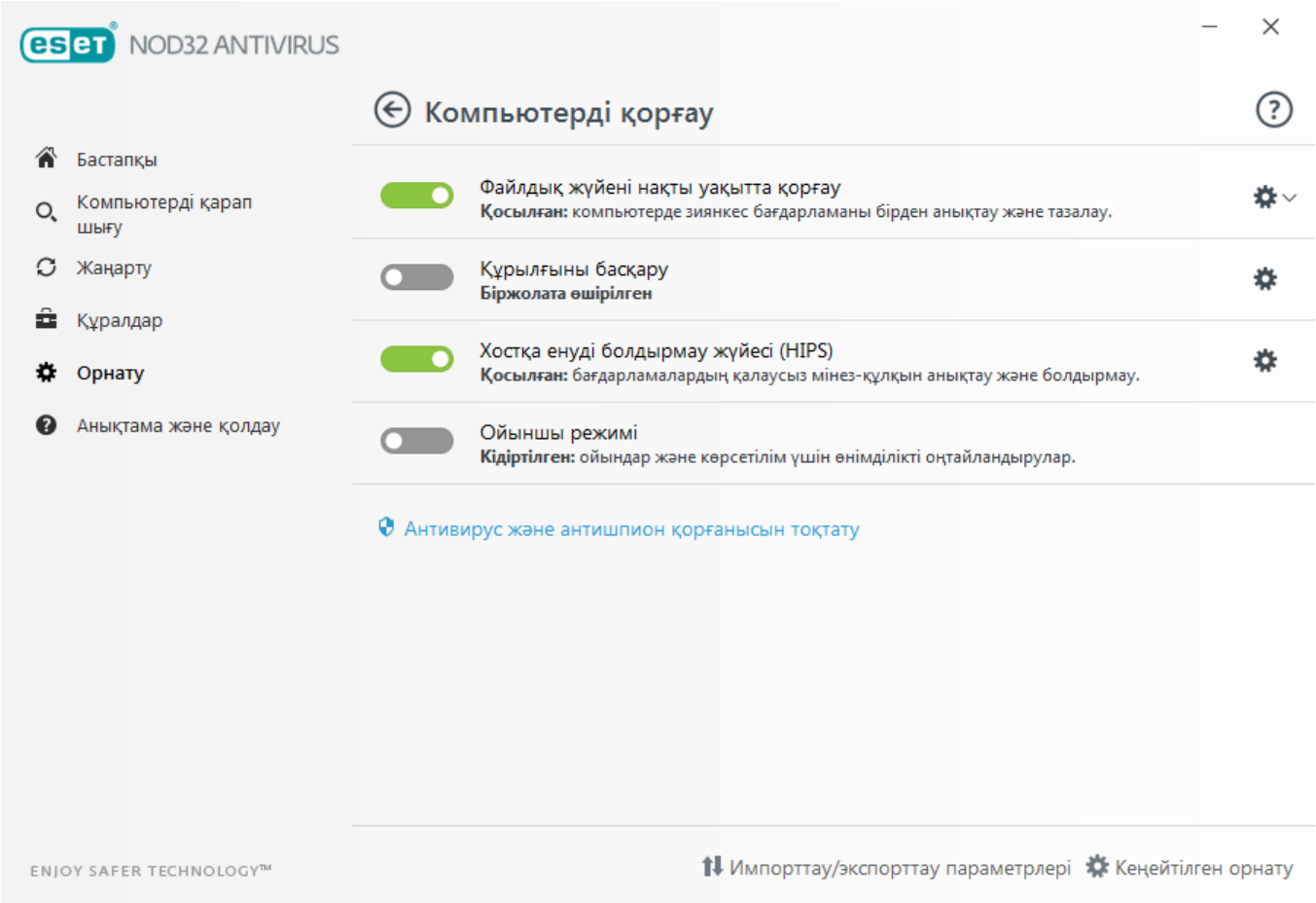
ЕСКЕРТПЕ
Осы әдісті пайдаланып қорғауды өшіргенде, қорғаудың барлық өшірілген модульдері компьютерді қайта іске қосқаннан кейін қосылады.

Орнату терезесінің төменгі жағында қосымша опциялар қол жетімді. **Кеңейтілген орнату** сілтемесін әрбір модуль үшін егжей-тегжейлі параметрлерді орнату үшін пайдаланыңыз. **Импорттау/экспорттау параметрлері** тармағын *.xml* конфигурация файлын пайдаланып орнату параметрлерін жүктеу немесе ағымдағы орнату параметрлерін конфигурация файлына сақтау үшін пайдаланыңыз.

4.1 Компьютерді қорғау

Барлық қорғау модульдеріне шолуды көру үшін «Орнату» терезесінде «Компьютерді қорғау» тармағын басыңыз. Жекелеген модульдерді уақытша өшіру үшін  түймешігін басыңыз. Оның компьютер қорғанышын деңгейін төмендететінін ескеріңіз. Модульдің кеңейтілген параметрлеріне қатынасу үшін қорғау модулінің жанында түймешігін басыңыз.

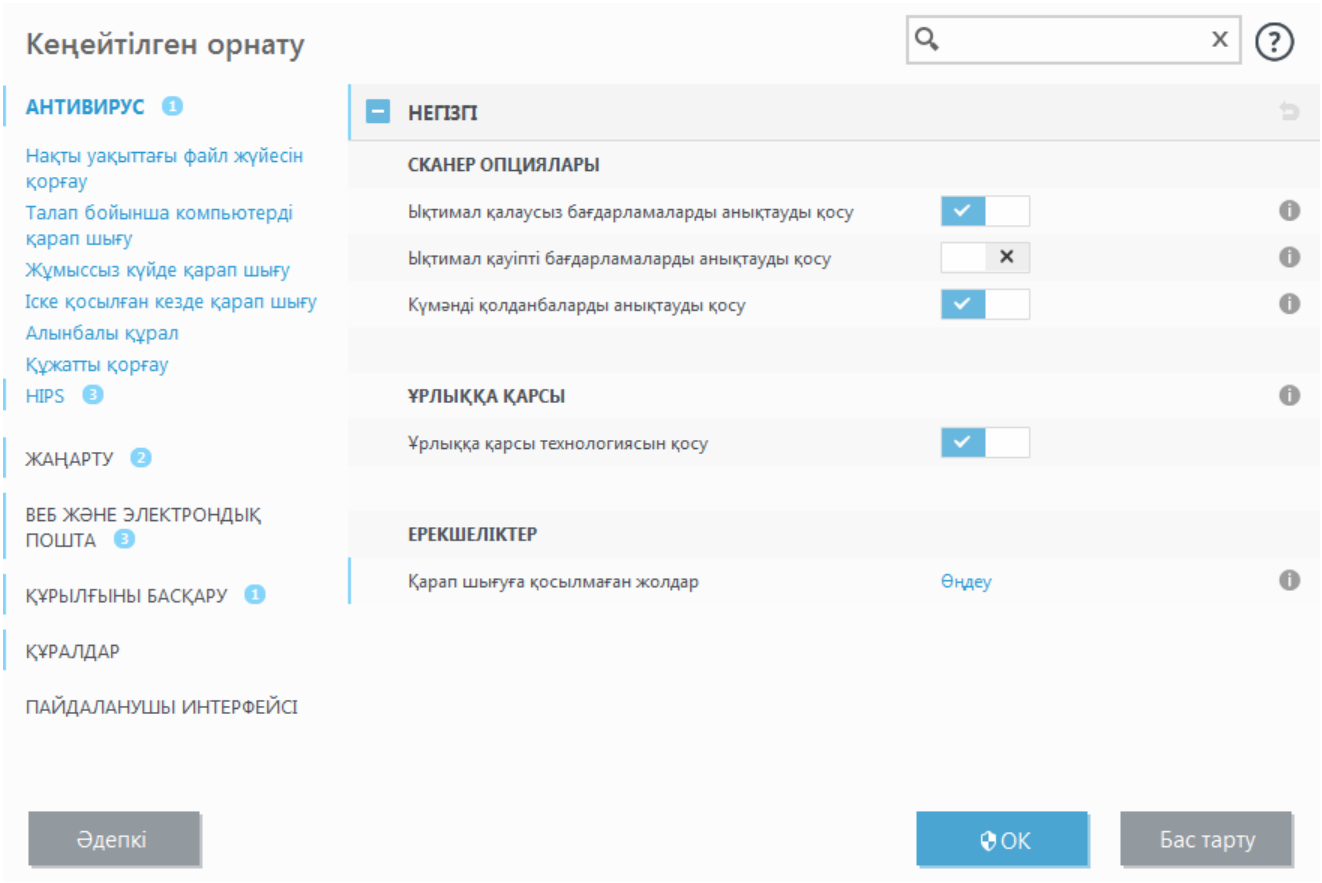
Басу  > **Ерекшеліктерді өңдеу** тармағын **Файлдық жүйені нақты уақытта қорғау** жанында басыңыз.



Антивирустық және антишпиондық қорғауды кідірту — Антивирустық және антишпиондық қорғау модульдерінің барлығын өшіреді. Қорғауды өшіргенде **Уақыт аралығы** ашылмалы мәзірін пайдаланып қорғау қанша уақыт бойы өшірулі болатынын анықтауға болатын терезе ашылады. Растау үшін **Қолдану** түймешігін басыңыз.

4.1.1 Антивирус

Антивирустық қорғау файлдарды, электрондық поштаны және интернет байланысын бақылау арқылы зиянды жүйелік шабуылдардан қорғайды. Егер зиянды коды бар қауіп анықталса, Антивирус модулі оны алдымен блоктау арқылы, ал содан кейін тазалау, жою немесе карантинге орналастыру арқылы шеттете алады.



Барлық қорғаныс модульдеріне арналған **Сканер опциялары** (мысалы, Нақты уақыттағы файл жүйесін қорғау, Веб-қатынасты қорғау,...) мыналардың анықталуын қосуға не ажыратуға мүмкіндік береді:

- **Қажетсіздігі ықтимал бағдарламалар** (PUAs) міндетті түрде зиянды болуға қажетінше арналмаған, бірақ компьютеріңіздің жұмысына кері әсерін тигізуі мүмкін.
  Глоссарий бөлімінен бағдарламалардың осы түрлері жөніндегі толығырақ ақпаратты оқыңыз.
- **Ықтимал қауіпті бағдарламалар** зиянды мақсатқа қарсы қолдануға болатын заңды коммерциялық бағдарламаға жатады. Ықтимал қауіпті бағдарламаларға қашықтан қатынасу құралдары, құпиясөздерді бұзатын бағдарламалар және пернетақталық шпиондарды (пайдаланушы басқан әрбір пернені жазып отыратын бағдарламалар) сияқты бағдарламалар кіреді. Бұл опция әдепкі мәні бойынша өшірілген.
  Глоссарий бөлімінен бағдарламалардың осы түрлері жөніндегі толығырақ ақпаратты оқыңыз.
- **Күмәнді қолданбалар** бумалаушылар не қорғаушы арқылы сығылған бағдарламаларды қамтиды. Қорғаушылардың осы түрлерін анықтаудан жасыру үшін зиянкес авторлар жиі пайдаланады.

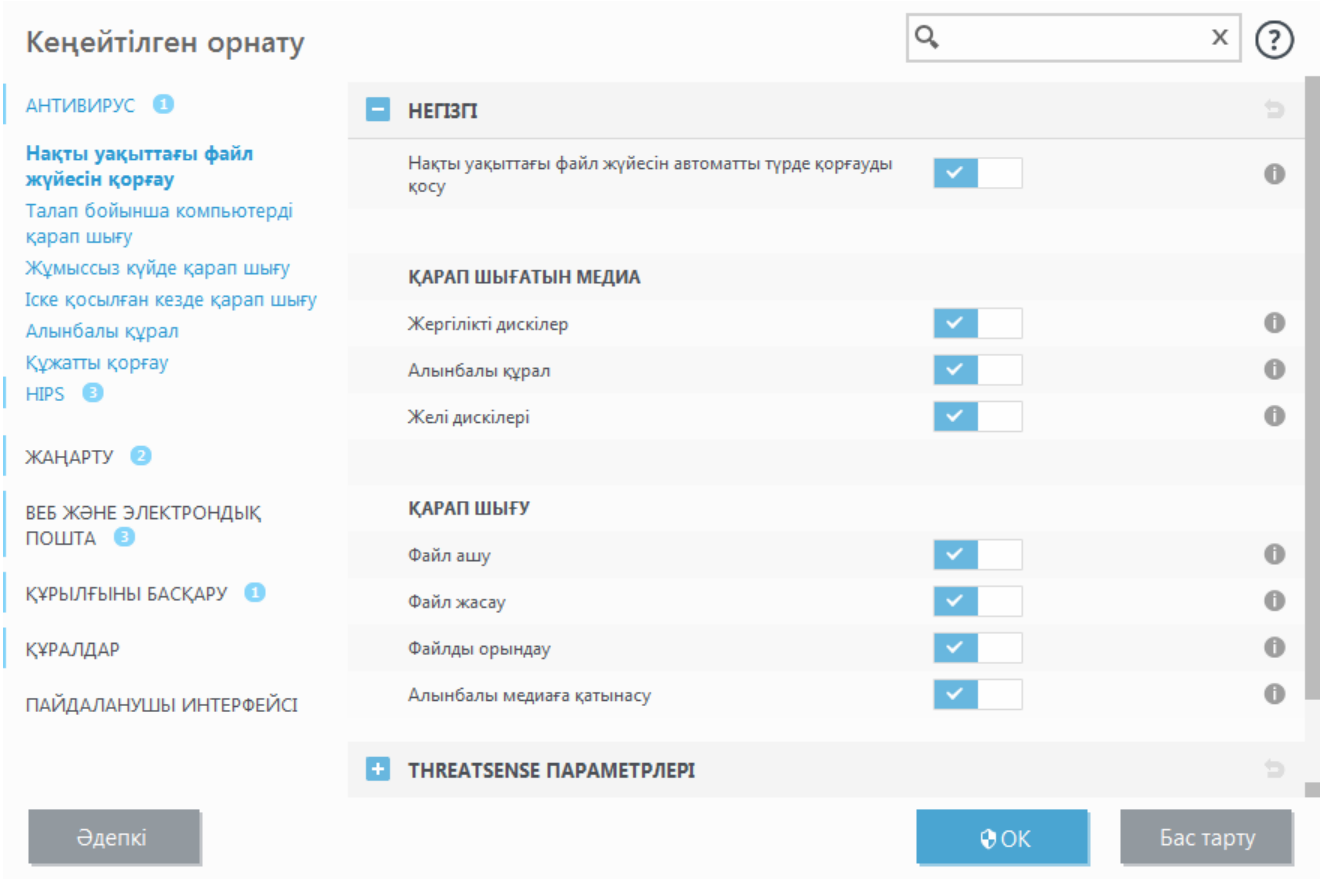
Ұрлыққа қарсы технология дегеніміз операциялық жүйеден өздерін жасыратын руткиттер сияқты қауіпті бағдарламаларды анықтауға мүмкіндік беретін күрделі жүйе. Бұл оларды қарапайым сынақ әдістерін пайдалана отырып, оларды анықтау мүмкін еместігін білдіреді.

Ерекшеліктер файлдар мен қалталарды қарап шығудан шығаруға мүмкіндік береді. Барлық нысандарда қауіптердің бар-жоқ екені тексерілгеніне көз жеткізу үшін шеттеулерді тек шынында қажет болғанда жасау ұсынылады. Нысанды шығаруды қажет етуі мүмкін жағдайлар сканерлеу кезінде компьютер жұмысын баяулататын үлкен дерекқор жазбаларын немесе қарап шығуда болатын қайшылықтарды қамтуы мүмкін. Нысанды қарап шығудан шығару үшін Ерекшеліктер бөлімін қараңыз.

AMSI арқылы кеңейтілген қарап шығуды қосу – қолданба әзірлеушілеріне зиянкес бағдарламалардан қорғаудың жаңа әдістерін беретін Microsoft Antimalware Scan Interface құралы (тек Windows 10).

4.1.1.1 Файлдық жүйені нақты уақытта қорғау

Нақты уақыттағы файл жүйесін қорғау жүйедегі барлық антивирусқа қатысты оқиғаларды басқарады. Барлық файлдарда ашылғанда, жасалғанда немесе компьютерде іске қосылғанда зиянкес код бар-жоғы қарап шығылады. Нақты уақыттағы файл жүйесін қорғау жүйе іске қосылғанда ашылады.



Әдепкі бойынша, «Нақты уақыттағы файлдық жүйені қорғау» жүйе іске қосылғанда іске қосылады және үздіксіз қарап шығуды қамтамасыз етеді. Ерекше жағдайларда (мысалы, басқа нақты уақыттағы қарап шығу құралымен қайшылық бар болса), нақты уақыттағы қорғауды **Кеңейтілген орнатуда**, **Нақты уақытта файлдық жүйені қорғау** > **Негізгі** бөліміндегі **Нақты уақытта файлдық жүйені қорғауды автоматты түрде іске қосу** құсбелгісін алу арқылы өшіруге болады.

Қарап шығатын құрал

Әдепкі бойынша, құралдардың барлық түрлерінде ықтимал қауіпті қарап шығады:

Жергілікті дискілер – Барлық жүйелік қатты дискілерді басқарады.
Алынбалы тасушы – Ықшам дискілерді/DVD дискілерін, USB қоймасын, Bluetooth құрылғыларын, т.с.с. басқарады.
Желілік дискілер – Барлық салыстырылған дискілерді қарап шығады.

Әдепкі параметрлерді пайдалану және оларды белгілі бір құралды қарап шығу деректерді тасымалдауларды айтарлықтай баяулататын сияқты ерекше жағдайларда ғана өзгерту ұсынылады.

Қарап шығу

Әдепкі бойынша, барлық файлдар ашқанда, жасағанда немесе орындағанда қарап шығылады. Осы әдепкі параметрлерді сақтау ұсынылады, өйткені олар компьютер үшін нақты уақыттағы қорғаудың ең жоғары деңгейін қамтамасыз етеді:

- **Файл ашық** – Файлдар ашық кезде қарап шығуды қосады немесе өшіреді.
- **Файл жасау** – Файлдарды жасап жатқанда қарап шығуды қосады немесе өшіреді.
- **Файлды орындау** – Файлдар орындалып жатқанда қарап шығуды қосады немесе өшіреді.
- **Алынбалы тасушыға қатынасу** – Қойма кеңістігі бар нақты алынбалы тасушыға қатынасу іске қосатын қарап шығуды қосады немесе өшіреді.
- **Компьютерді өшіру** – Компьютерді өшіру іске қосатын қарап шығуды қосады немесе өшіреді.

Нақты уақыттағы файл жүйесін қорғау барлық құрал түрлерін тексереді және файлға кіру секілді әр түрлі жүйе оқиғалары арқылы басталады. ThreatSense технологиясының анықтау әдістерін пайдалану (ThreatSense механизм параметрлерін орнату бөлімінде сипатталғандай), нақты уақыттағы файлдық жүйені қорғау бұрыннан бар файлдардан өзгеше жаңадан жасалған файлдарды қарастыру үшін конфигурацияланады. Мысалы, нақты уақыттағы файл жүйесін қорғауды жаңадан жасалған файлдарды жақынырақ бақылау үшін конфигурациялай аласыз.

Нақты уақытта қорғауды пайдалану кезінде ең кіші жүйе іздерін тексеру үшін қаралған файлдар қайта қаралмайды (файлдар өзгертілмейінше). Анықтау механизмін әрбір жаңартудан кейін файлдар бірден қайтадан қарап шығылады. Бұл әрекет **Зерделі оңтайландыру** функциясын пайдаланып басқарылады. Егер **Зерделі оңтайландыру** өшірілген болса, барлық файлдар қатынасқан сайын қарап шығылады. Бұл параметрді өзгерту үшін **F5** пернесін басып **Кеңейтілген орнату** тармағын ашыңыз және **Антивирус** > **Нақты уақытта файлдық жүйені қорғау** тармағын кеңейтіңіз. **ThreatSense параметрлері** > **Басқа** тармағын басып, **Зерделі оңтайландыруды қосу** опциясын таңдаңыз немесе одан таңдауды алыңыз.

4.1.1.1.1 Қосымша ThreatSense параметрлері

Жаңадан жасалған және өзгертілген файлдар үшін қосымша ThreatSense параметрлері

Жаңадан жасалған немесе өзгертілген файлдардағы жұқу ықтималдығы бар файлдардан салыстырмалы түрде жоғарырақ. Осы себепті бағдарлама бұл файлдарды қосымша сканерлеу параметрлері арқылы тексереді. ESET NOD32 Antivirus қолтаңбаларға негізделген қарап шығу әдістерімен бірге анықтау механизмін жаңарту шығарылмай тұрып жаңа қауіптерді анықтай алатын кеңейтілген эвристиканы пайдаланады. Жаңадан жасалған файлдарға қоса, қарап шығу, сонымен бірге, **Өздігінен ашылатын мұрағаттарда** (.sfx) және **Бумалаушының жұмыс уақыты файлдарында** (іштей сығылған орындалатын файлдар) орындалады. Әдепкі бойынша, мұрағаттарды 10-шы енгізу деңгейіне дейін қарап шығылып, іс жүзіндегі өлшеміне қарамастан тексеріледі. Мұрағатты қарап шығу параметрлерін өзгерту үшін **Әдепкі мұрағатты қарап шығу параметрлері** ұяшығынан белгіні алыңыз.

Орындалатын файлдарға арналған қосымша ThreatSense параметрлері

Файлды орындау кезіндегі кеңейтілген эвристика – Әдепкі бойынша, Кеңейтілген эвристика файлдар орындалған кезде пайдаланылады. Қосылған болса, жүйе өнімділігіне әсерді азайту үшін Зерделі оңтайландыру опциясын және ESET LiveGrid® қосылған күйде сақтау ұсынылады.

Алынбалы тасушыдан файлдарды орындау кезіндегі кеңейтілген эвристика – Кеңейтілген эвристика кодты виртуалдық ортада эмуляциялайды және кодқа алынбалы тасушыдан орындалуға рұқсат ету алдында оның әрекетін бағалайды.

4.1.1.1.2 Тазалау деңгейлері

Нақты уақыттағы қорғаныс үш тазалау деңгейіне ие (тазалау деңгейі параметрлерін ашу үшін **Нақты уақытта файлдық жүйені қорғау** бөлімінде **ThreatSense механизмінің параметрлерін орнату** тармағын басыңыз, содан кейін **Тазалау** түймесін басыңыз).

Тазаламау – Вирус жұққан файлдар автоматты түрде тазартылмайды. Бағдарлама ескерту терезесін көрсетіп, пайдаланушының әрекетті таңдауына мүмкіндік береді. Бұл деңгей инфильтрация жағдайында қандай қадамдар жасау керектігін білетін әлдеқайда тәжірибелі пайдаланушыларға арналған.

Қалыпты тазалау – Бағдарлама алдын ала анықталған әрекет негізінде вирус жұққан файлды автоматты түрде тазалауға емесе жоюға әрекет жасайды. Вирус жұққан файлдың табылуы және жойылуы туралы экранның төменгі оң жақ бұрышындағы хабарландырумен белгі беріледі. Дұрыс әрекетті автоматты түрде таңдау мүмкін болмаса, бағдарлама басқа қосымша әрекетті ұсынады. Алдын ала анықталған әрекетті орындау мүмкін болмаған кезде, бірдей жағдай орын алады.

Қатаң тазалау – Бағдарлама барлық вирус жұққан файлдарды тазалайды немесе жояды. Бұл тек жүйелік файлдарға қатысты орындалмайды. Егер оларды тазалау мүмкін болмаса, пайдаланушыдан ескерту терезесінің көмегімен әрекетті таңдау сұралады.

ЕСКЕРТУ

Егер мұрағатта вирус жұққан файл не файлдар болған жағдайда мұрағатпен жұмыс істейтін екі параметр беріледі. Стандартты режимде (қалыпты тазалау) ішіндегі барлық файлдарға вирус жұққан мұрағат толығымен жойылады. **Қатаң тазалау** режимінде мұрағат вирус жұққан кемінде бір файлды қамтитын жағдайда ондағы басқа файлдардың күйіне қарамастан бұл мұрағат жойылады.

4.1.1.1.3 Нақты уақыттағы қорғау конфигурациясын қашан өзгерту керек

Нақты уақыттағы қорғау – жүйені қауіпсіз сақтаудың ең маңызды компоненті. Оның параметрлерін өзгерткенде үнемі абай болыңыз. Оның параметрлерін ерекше жағдайларда ғана өзгерту ұсынылады.

ESET NOD32 Antivirus бағдарламасын орнатқаннан кейін барлық параметрлер пайдаланушылар үшін жүйе қауіпсіздігінің ең жоғары деңгейін қамтамасыз ету үшін оңтайландырылады. Әдепкі параметрлерді қалпына келтіру үшін терезедегі әр қойынды жанында ↩ түймесін басыңыз (**Кеңейтілген орнату** > **Антивирус** > **Нақты уақытта файлдық жүйені қорғау**).

4.1.1.1.4 Нақты уақыттағы қорғауды тексеру

Нақты уақыттағы қорғаудың жұмыс істеп жатқанын және вирустарды анықтағанын тексеру үшін eicar.com торабынан алынған тексеру файлын пайдаланыңыз. Бұл тексеру файлы – барлық антивирустық бағдарламалар анықтай алатын зиянсыз файл. Бұл файлды антивирустық бағдарламалардың жұмыс істеуін тексеру үшін EICAR компаниясы (Еуропалық Компьютерлік Антивирустық Зерттеулер институты) жасаған. Файлды http://www.eicar.org/download/eicar.com сайтынан жүктеуге болады

4.1.1.1.5 Нақты уақыттағы қорғау жұмыс істемей жатса не істеу керек

Бұл бөлімде нақты уақыттағы қорғауды пайдаланғанда пайда болуы мүмкін мәселелер және оларды шешу жолдары сипатталады.

Нақты уақыттағы қорғау өшірілген

Егер нақты уақыттағы қорғауды пайдаланушы байқаусызда өшірсе, оны қайтадан іске қосу керек. Нақты уақыттағы қорғанысты қайта іске қосу үшін негізгі бағдарлама терезесінде **Орнату** тармағына өтіп, **Компьютерді қорғау** > **Файлдық жүйені нақты уақытта қорғау** бөлімін басыңыз.

Егер нақты уақыттағы қорғаныс жүйені іске қосуда басталмаса, бұл әдетте **Нақты уақыттағы файл жүйесін қорғауды автоматты түрде іске қосу** опциясын өшіргендіктен болады. Бұл опция қосулы екенін тексеру үшін **Кеңейтілген орнату** (**F5**) тармағына өтіп, **Антивирус** > **Файлдық жүйені нақты уақытта қорғау** тармағын басыңыз.

Егер нақты уақыттағы қорғау инфильтрацияларды таппаса және тазаламаса

Компьютерде басқа антивирустық бағдарламалардың орнатылмағанына көз жеткізіңіз. Егер бір уақытта екі антивирустық бағдарлама қосылған болса, оларда бір бірінің арасында қайшылық болуы мүмкін. ESET бағдарламасын орнатпас бұрын жүйеден басқа антивирустық бағдарламаларды жою ұсынылады.

Нақты уақыттағы қорғау іске қосылмайды

Егер нақты уақыттағы қорғау жүйе іске қосылғанда қосылмаса (және **Нақты уақыттағы файл жүйесін қорғауды автоматты түрде іске қосу** қосылса), ол басқа бағдарламалармен қиындық туындағандықтан болуы мүмкін. Осы мәселені шешуге көмек алу үшін ESET тұтынушыларды қолдау орталығына хабарласыңыз.

4.1.1.2 Шығу

Талап бойынша қарап шығу құралы антивирустық шешіміңіздің маңызды бөлігі болып табылады. Ол компьютеріңіздегі файлдар мен қалталарды қарап шығу үшін пайдаланылады. Қауіпсіздік тұрғысынан компьютерді қарап шығуларды тек вирус жұғы күдігі болғанда ғана емес, әдеттегі қауіпсіздік шараларының бір бөлігі ретінде орындау маңызды. Дискіге жазылғанында Нақты уақытта файлдық жүйені қорғау анықтамаған вирустарды анықтау үшін жүйелі түрде жүйені терең қарап шығуларды орындап тұру ұсынылады. Бұл сол кезде Нақты уақытта файлдық жүйені қорғау өшірілген болса, вирустар дерекқоры ескіріп кеткен болса немесе дискіге сақталғанда файл вирус ретінде анықталмаса орын алуы мүмкін.

Екі **Шығу** түрі қол жетімді. **Компьютерді қарап шығу** қарап шығу параметрлерін көрсетусіз жүйені жылдам қарап шығады. **Теңшелетін қарап шығу** белгілі бір орындарды көздеуге арналған алдын-ала анықталған қарап шығу профильдерінен таңдауға, сонымен бірге белгілі бір қарап шығу нысаналарын таңдауға мүмкіндік береді.

Компьютерді қарап шығу

Компьютерді қарап шығу компьютерді қарап шығуды тез қосуға және пайдаланушы араласуынсыз вирус жұққан файлдарды тазалауға мүмкіндік береді. Компьютерді қарап шығу артықшылығы – онымен жұмыс істеудің жеңілдігі

және оның егжей-тегжейлі қарап шығу конфигурациясын қажет етпейтіні. Бұл қарап шығу жергілікті дискілердегі барлық файлдарды тексеріп, табылған инфильтрацияларды автоматты түрде тазалайды немесе жояды. Тазалау деңгейі автоматты түрде әдепкі мәнге орнатылады. Тазалау түрлері туралы қосымша ақпарат алу үшін Тазалау тармағын қараңыз.

Сондай-ақ файлды немесе қалтаны басу, тінтуір меңзерін тінтуір түймешігін басып тұрып белгіленген аумаққа жылжыту, содан кейін жіберу арқылы **Сүйреп апарып тастау арқылы қарап шығу** мүмкіндігін пайдалануға болады.

Кеңейтілген қарап шығулар атсында келесі қарап шығу опциялары қолжетімді:

Таңдамалы қарап шығу

Таңдамалы қарап шығу функциясы қарап шығу мақсаттары мен әдістері секілді параметрлерді анықтауға мүмкіндік береді. Таңдамалы қарап шығудың артықшылығы – параметрлерді егжей-тегжейлі конфигурациялау мүмкіндігі. Конфигурацияларды пайдаланушылық қарап шығу профильдеріне сақтауға болады және олар қарап шығу бірдей параметрлермен қайта-қайта орындалса пайдалы.

Алынбалы құралды қарап шығу

Компьютерді қарап шығу функциясына ұқсас — компьютерге қазір қосылған алынбалы құралды (мысалы, ықшам дискі/DVD/USB) қарап шығуды жедел іске қосады. Бұл USB флэш-жадын компьютерге қосып, зиянкес бағдарламалар және басқа ықтимал қауіптер оның мазмұнында бар-жоғын қарап шығу кезінде пайдалы болуы мүмкін.

Сондай-ақ, қарап шығудың бұл түрін **Таңдамалы қарап шығу** тармағын басу, **Алынбалы құрал** тармағын **Қарап шығу нысандары** ашылмалы мәзірінен таңдау және **Қарап шығу** түймешігін басу арқылы бастауға болады.

Соңғы қарап шығуды қайталау

Іске қосылған параметрлерін пайдаланып бұрын орындалған қарап шығуды жылдам іске қосуға мүмкіндік береді.

Қарап шығу процесі туралы қосымша ақпарат алу үшін Қарап шығудың орындалуы тармағын қараңыз.

ЕСКЕРТПЕ
Шығуды кемінде айына бір рет орындау ұсынылады. Қарап шығуды **Құралдар** > **Жоспарлағыш** тармағында жоспарланған тапсырма ретінде теңшеуге болады. Апта сайын компьютерді қарап шығуды жоспарлау әдісі

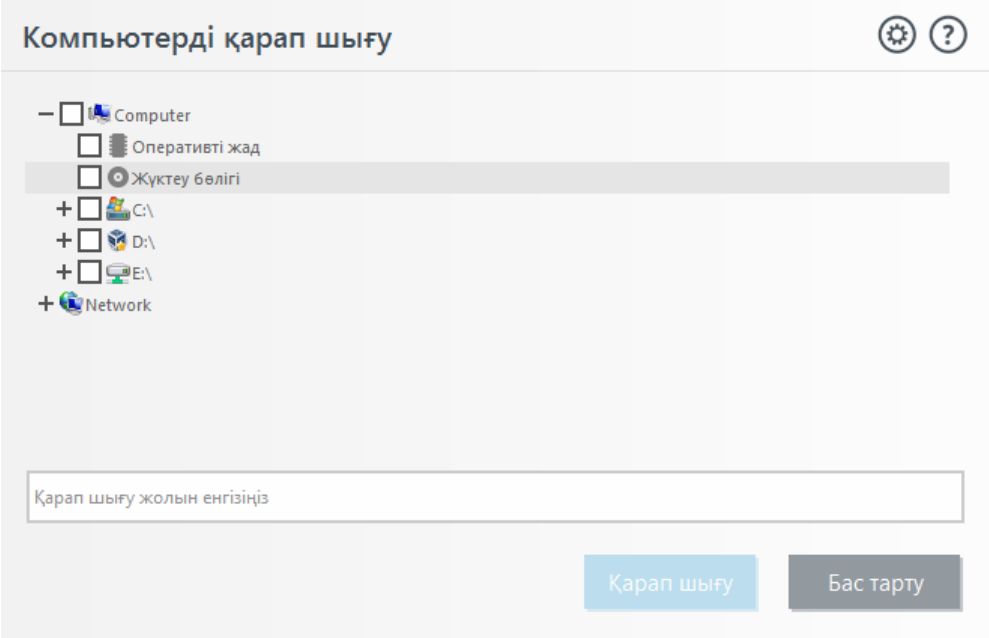
4.1.1.2.1 Таңдаулы ретпен қарап шығуды іске қосушы

Таңдаулы ретпен қарап шығуды бүкіл дискіні емес, дискінің нақты бөліктерін қарап шығу үшін пайдалануға болады. Мұны істеу үшін үшін **Компьютерді қарап шығу** > **Таңдаулы ретпен қарап шығу** тармағына басып, **Қарап шығу нысандары** ашылмалы мәзірінен опцияны таңдаңыз немесе қалта (тармақ) құрылымынан нақты нысандарды таңдаңыз.

Қарап шығу нысандары ашылмалы мәзірі алдын ала анықталған қарап шығу нысандарын таңдауға мүмкіндік береді.

- **Профиль параметрлері бойынша** — Таңдалған қарап шығу профилінде көрсетілген нысандарды таңдайды.
- **Алынбалы құрал** — Дискеталарды, USB сақтау құрылғыларын, CD/DVD дискілерді таңдайды.
- **Жергілікті дискілер** – Жүйелік қатты дискілердің барлығын таңдайды.
- **Желі дискілері** – Барлық көрсетілген желі дискілерін таңдайды.
- **Таңдау жоқ** – Барлық таңдаулардан бас тартады.

Қарап шығу нысанына жылдам өту немесе мақсатты қалтаны немесе файл(дар)ды қосу үшін қалталар тізімінің төменгі жағындағы бос өрісте мақсатты каталогты енгізіңіз. Бұл тармақ құрылымында ешбір нысан таңдалмаған және **Қарап шығу нысандары** мәзірі **Таңдау жоқ** деп орнатылған болса ғана мүмкін.



Қарап шығу үшін тазалау параметрлерін **Кеңейтілген реттеу** > **Антивирус** > **Талап бойынша компьютерді қарап шығу** > **ThreatSense параметрлері** > **Тазалау тармағында конфигурациялауға болады.** Қарап шығуды тазалау әрекетінсіз орындау үшін **Тазаламай қарап шығу** опциясын таңдаңыз. Қарап шығу журналы қарап шығу журналына сақталады.

Қиыс жағдайларды елемеу таңдалған болса, бұрын қарап шығуға қосылмаған кеңейтімдері бар файлдар ерекшеліксіз қарап шығылады.

Нақты нысандарды қарап шығу кезінде **Қарап шығу профилі** ашылмалы мәзірінен профильді таңдауға болады. Әдепкі профиль **Зерделі қарап шығу** болып табылады. **Терең қарап шығу** және **Контекстік мәзірді қарап шығу** аталатын тағы екі алдын ала анықталған қарап шығу профильдері бар. Бұл қарап шығу профильдері әр түрлі ThreatSense параметрлерін пайдаланады. Теңшелген қарап шығу профилін реттеу үшін **Реттеу...** пәрменін басыңыз. Қарап шығу профилінің опциялары ThreatSense параметрлері бөлімінде **Басқа** тармағында сипатталған.

Орнатылған таңдамалы параметрлермен қарап шығуды орындау үшін **Қарап шығу** түймесін басыңыз.

Әкімші ретінде қарап шығу түймесі қарап шығуды Әкімші есептік жазбасымен орындауға мүмкіндік береді. Ағымдағы пайдаланушының қарап шығу керек файлдарға қатынасу артықшылықтары болмаса, осыны пайдаланыңыз. Бұл түймешік ағымдағы пайдаланушы UAC әрекеттерін әкімші ретінде шақыра алмайтын кезде қолжетімді болмайды.

ЕСКЕРТПЕ
Компьютерді қарап шығу журналын қарап шығу аяқталғанда **Журналды көрсету** пәрменін басу арқылы көруге болады.

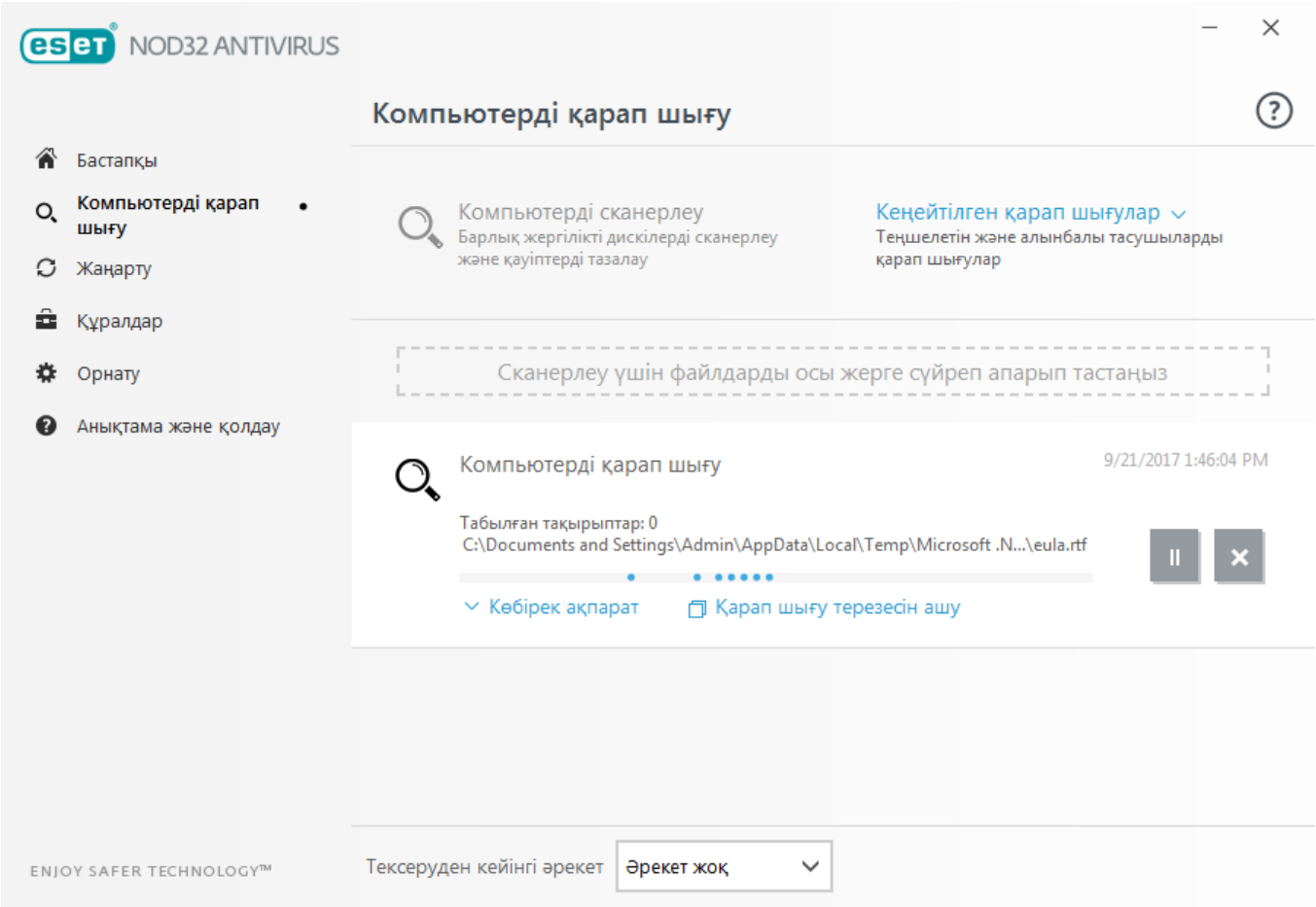
4.1.1.2.2 Қарап шығудың орындалуы

Қарап шығудың орындалу барысының терезесі қарап шығудың ағымдағы күйін және зиянды код бар екені анықталған файлдар саны туралы ақпаратты көрсетеді.

ЕСКЕРТПЕ
Құпиясөзбен қорғалған немесе жүйе ғана пайдаланатын файлдар (әдетте *pagefile.sys* және белгілі бір жұрнал файлдары) сияқты файлдарды қарап шығудың мүмкін болмауы қалыпты жағдай.

Қарап шығудың орындалу барысы – орындалу барысы жолағы әлі қарап шығуды күтіп жатқан нысандармен салыстырғандағы қарап шығылған нысандардың күйін көрсетеді. Қарап шығудың орындалу барысының күйі қарап шығуға қосылған нысандардың жалпы санынан алынады.
Нысан – Қазіргі уақытта қарап шығып жатқан нысан атауы және оның орны.
Табылған қауіптер — Қарап шыққан файлдардың, қарап шығу барысында табылған қауіптердің және тазартылған қауіптердің жалпы санын көрсетеді.
Кідірту – Қарап шығуды кідіртеді.
Жалғастыру – Бұл опция қарап шығу кідіртілгенде көрінеді. Қарап шығуды жалғастыру үшін **Жалғастыру** түймесін басыңыз.
Тоқтату – Қарап шығуды тоқтатады.
Қарап шығу журналын айналдыру – Қосылған болса, жаңа жазбалар қосылғанда соңғы жазбалар көрінуі үшін қарап шығу журналы автоматты түрде төмен айналдырылады.

ЕСКЕРТПЕ
Ағымдағы іске қосылған қарап шығу туралы егжей-тегжейлі мәліметтерді көрсету үшін ұлғайтқышты немесе көрсеткіні басыңыз. **Компьютерді қарап шығу** немесе **Таңдаулы ретпен қарап шығу** тармақтарын басу арқылы басқа қарап шығуды қатар іске қосуыңызға болады.



Қарап шығудан кейінгі әрекет – Компьютерді қарап шығу аяқталғанда жоспарланған өшіруді, қайта жүктеуді немесе ұйықтау режиміне өткізуді іске қосады. Қарап шығу аяқталған кезде өшіруді растау диалогтық терезесі 60 секундқа шығады.

4.1.1.2.3 Қарап шығу профильдері

Таңдаулы қарап шығу параметрлерін болашақ қарап шығу үшін сақтауға болады. Әр тұрақты түрде пайдаланылатын қарап шығу үшін басқа профильді (әр түрлі қарап шығу нысандары, қарап шығу әдістері және басқа параметрлер бар) жасау ұсынылады.

Жаңа профиль жасау үшін «Кеңейтілген орнату» терезесін ашып (F5), **Антивирус** > **Талап бойынша компьютерді қарап шығу** > **Негізгі** > **Профильдер тізімі** тармағын басыңыз. **Профиль реттегіші** терезесі бар қарап шығу профильдері және жаңасын жасау опциясы берілген **Таңдалған профиль** ашылмалы мәзірін қамтиды. Қажеттіліктеріңізге сай қарап шығу профилін жасауда көмек алу үшін ThreatSense механизмінің параметрлерін орнату бөлімінде қарап шығуды реттеудің әр параметрінің сипаттамасын қараңыз.

ЕСКЕРТПЕ
Жеке қарап шығу профилін жасау керек және **Компьютерді қарап шығу** конфигурациясы ішінара қолайлы, бірақ орындау уақыты бумалаушыларын немесе ықтимал қауіпті бағдарламаларды қарап шығу керек емес және **Қатаң тазалау** опциясын қолдану керек делік. Жаңа профиль атауын **Профильдер реттегіші** терезесінде енгізіп, **Қосу** түймесін басыңыз. Жаңа профильді **Таңдалған профиль** ашылмалы мәзірінен таңдаңыз және қалған параметрлерді талаптарға сай реттеңіз және жаңа профильді сақтау үшін **OK** түймесін басыңыз.

4.1.1.2.4 Компьютерді сканерлеу журналы

Компьютерді қарап шығу журналы қарап шығу туралы келесі сияқты жалпы ақпаратты береді:

- Аяқталу уақыты
- Жалпы қарап шығу уақыты
- Табылған қауіптер саны
- Қаралған нысандар саны
- Қаралған дискілер, қалталар мен файлдар
- Қарап шығу күні мен уақыты
- Анықтау механизмінің нұсқасы

4.1.1.3 Өнімділік күйде қарап шығу

Компьютер пайдаланылып жатпағанда жүйені автоматты түрде қарап шығуларға рұқсат ету үшін **Кеңейтілген онату** > **Антивирус** > **Жұмыссыз күйде қарап шығуды** > **Негізгі** тармағында **Жұмыссыз күйде қарап шығуды қосу** жанындағы қосқышты басыңыз.

Әдепкі бойынша, компьютер (ноутбук) батарея қуатымен жұмыс істеген кезде өнімділік күйіндегі сканер іске қосылмайды. Бұл параметрді **Компьютер батареямен істеп тұрса да іске қосу** мүмкіндігі арқылы қайта анықтауға болады.

Журналға тіркеуді қосу қосқышын компьютерді қарап шығу нәтижесін Журнал файлдары бөлімінде жазу үшін қосыңыз (бағдарламаның негізгі терезесінде **Құралдар** > **Журнал файлдары** тармағын басыңыз, содан кейін **Журнал** ашылмалы мәзірінде **Компьютерді қарап шығу** пәрменін таңдаңыз).

Жұмыссыз күйді анықтау компьютер келесі күйлерде болғанда іске қосылады:

- Экрандық сақтағыш
- Компьютерді құлыптау
- Пайдаланушыны жүйеден шығару

Жұмыссыз күйде қарап шығу құралы үшін қарап шығу параметрлерін (мысалы, анықтау әдістері) өзгерту үшін ThreatSense параметрлері тармағын басыңыз.

4.1.1.4 Іске қосылған кезде қарап шығу

Әдепкі бойынша, жүйе іске қосылғанда немесе анықтау механизмін жаңартулар кезінде автоматты түрде файлдарды тексеру орындалады. Бұл қарап шығу Жоспарлағыш конфигурациясы және тапсырмалар параметріне байланысты болады.

Қарап шығуды іске қосу опциясы **Жүйені іске қосу файлын тексеру** жоспарлағыш тапсырмаларының бөлігі болып табылады. Оның параметрлерін өзгерту үшін **Құралдар** > **Жоспарлағыш** тармағына өтіп, **Файлдарды тексеруді автоматты түрде іске** тармағын басыңыз да, **Өңдеу** түймешігін басыңыз. Соңғы кадамда Іске қосылған кездегі файлдарды автоматты түрде тексеру терезесі шығады (толық мәлімет алу үшін келесі тарауды қараңыз).

Жоспарлаушы тапсырмасын жасау және басқару туралы егжей-тегжейлі нұсқауларды Жаңа тапсырмаларды ашу бөлімін қараңыз.

4.1.1.4.1 Файлдарды тексеруді автоматты түрде іске қосу

Жүйелік іске қосу файлын тексеру бойынша жоспарланған тапсырманы жасау кезінде келесі параметрлерді реттеу үшін бірнеше параметр беріледі:

Жиі пайдаланылатын файлдар ашылмалы мәзірінде құпия күрделі алгоритм негізінде жүйені іске қосу кезінде орындалатын файлдар үшін қарап шығу тереңдігі көрсетіледі. Файлдар келесі шарттарға сәйкес кему ретімен қойылады:

- **Барлық тіркелген файлдар** (ең көп қарап шығарылатын файлдар)
- **Сирек пайдаланылатын файлдар**
- **Жиі пайдаланылатын файлдар**
- **Жиі пайдаланылатын файлдар**
- **Тек ең жиі пайдаланылатын файлдар** (азырақ файлдар қарап шығылады)

Сондай-ақ, екі нақты топ қосылады:

- **Пайдаланушының кіруі алдында орындалатын файлдар** – Пайдаланушы кірместен қатынасуға болатын орындардағы файлдарды қамтиды (қызметтер, браузердің көмекші нысандары, жүйеге кіру туралы хабарлау, Windows жоспарлағыш жазбалары, белгілі dll файлдары, т.с.с. сияқты барлық дерлік іске қосу орындарын қамтиды).
- **Пайдаланушы кіргеннен кейін іске қосылатын файлдар** - пайдаланушы жүйеге кіргеннен кейін кіре алатын файлдарды қамтиды (белгілі бір пайдаланушы арқылы іске қосылатын файлдарды қамтиды, әдетте бұл *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* ішіндегі файлдар).

Қарап шыққан файлдардың тізімі жоғарыда айтылған әр топқа бекітіледі.

Қарап шығу басымдығы – Қарап шығу қашан басталатынын анықтау үшін пайдаланылатын басымдық деңгейі:

- **Бос кезде** – тапсырма тек жүйе бос кезде орындалады,
- **Ең төмен** – жүйе жүктемесі ең төмен мүмкін деңгейде болғанда,
- **Төменірек** – жүйе жүктемесі төмен кезде,
- **Қалыпты** – орташа жүйе жүктемесінде.

4.1.1.5 Ерекшеліктер

Ерекшеліктер файлдар мен қалталарды қарап шығудан шығаруға мүмкіндік береді. Барлық нысандарда қауіптердің бар-жоқ екені тексерілгеніне көз жеткізу үшін шеттеулерді тек шынында қажет болғанда жасау ұсынылады. Алайда, нысанды шығаруды қажет етуі мүмкін жағдайлар бар, мысалы, сканерлеу кезінде компьютер жұмысын баяулататын үлкен дерекқор жазбалары немесе сканерлеумен болатын қайшылықтары.

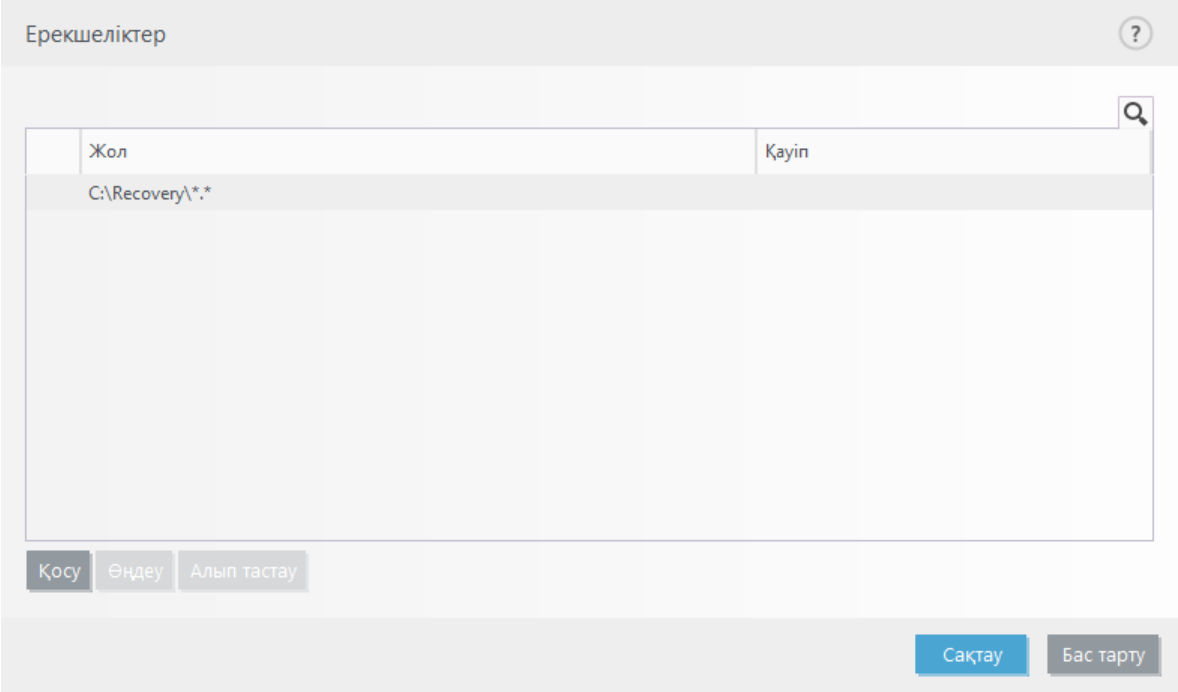
Нысанды қарап шығудан шығару үшін:

1. **Қосу** түймесін басыңыз,
2. Нысанға жолды енгізіңіз немесе оны армақ құрылымынан таңдаңыз.

Бір топ файлдарды қамту үшін арнайы таңбаларды пайдалануыңызға болады. Сұрақ белгісі (?) бір айнымалы таңбаны, ал жұлдызша (*) нөл немесе одан көп таңбадан тұратын айнымалы жолды білдіреді.

Мысалдар

- Қалтадағы барлық файлдарды қоспауды қаласаңыз, қалтаның жолын теріңіз және «*.*» бүркенішін пайдаланыңыз.
- Барлық файлдар және ішкі қалталармен бірге дискіні толығымен алып тастау үшін "D:*" бүркенішін пайдаланыңыз.
- Тек doc файлдарын қоспауды қаласаңыз, «*.doc» бүркенішін пайдаланыңыз.
- Орындалатын файлдың атауында таңбалардың белгілі бір саны болса (және таңбалар өзгеріп отырса) және тек біріншісін дәл білсеңіз (мысалы, «D») келесі пішімді пайдаланыңыз: «D????.exe». Сұрақ белгілері жоқ (белгісіз) таңбаларды алмастырады.



ЕСКЕРТПЕ
Файл сканерлеу ерекшелігіне арналған шарттарға сай келсе, файлдағы қауіп Нақты уақыттағы файл жүйесін қорғау модулі немесе компьютерді сканерлеу модулі арқылы анықталмайды.

Бағандар

Жол – Шығарылған файлдар мен қалталарға жол.

Қауіп - Егер шығарылған файлдың жанынан қауіп атауы шықса, бұл файлдың толығымен емес, тек берілген қауіп бойынша шығарылғанын білдіреді. Егер файлға басқа зиянды бағдарламадан кейінірек вирус жұққан жағдайда, оны антивирус модулі анықтайды. Бұл қоспау түрін инфильтрациялардың тек белгілі бір түрлері үшін пайдалануға болады және оны инфильтрация туралы есеп беретін қауіп туралы ескерту терезесінде (**Кеңейтілген опцияларды көрсету** тармағын басып, **Анықтауға қоспау** параметрін таңдаңыз) немесе **Құралдар** > **Карантин** тармағын басу, содан кейін карантинге қойылған файлды тінтуірдің оң жақ түймешігімен басу және контексттік мәзірден **Қалпына келтіру және анықтаудан шығару** пәрменін таңдау арқылы жасауға болады.

Басқару элементтері

Қосу – нысандарды анықтаудан шығарады.

Өңдеу – таңдалған жазбаларды өңдеу мүмкіндігін береді.

Алып тастау – Таңдалған жазбаларды алып тастайды.

4.1.1.6 ThreatSense параметрлері

ThreatSense – көп кешенді қауіпті анықтау әдістерінен тұрады. Бұл технология проактивті, яғни ол жаңа қауіптің тарауының бастапқы таралымында қорғауды да қамтамасыз етеді дегенді білдіреді. Бұл технология өзара әрекеттесу кезінде жүйе қауіпсіздігін айтарлықтай жақсартатын кодты талдау, кодты эмуляциялау, жалпы қолтаңбалар, вирус қолтаңбалары тіркесімін пайдаланады. Қарап шығу механизмі бір уақытта бірнеше деректер ағындарын бақылап, тиімділік және анықтау деңгейін жоғарылатады. Сондай-ақ, ThreatSense технологиясы руткиттерді сәтті жояды.

ThreatSense механизмін реттеу опциялары сізге бірнеше қарап шығу параметрлерін көрсетуге мүмкіндік береді:

- Қаралып шығуға тиісті файл түрлері мен кеңейтімдері
- Әр түрлі анықтау әдістерінің тіркесімі
- Тазалау деңгейлері, т.б.

Орнату терезесіне кіру үшін ThreatSense технологиясын пайдаланатын кез келген модульге арналған Кеңейтілген орнату терезесіндегі **ThreatSense параметрлері** тармағын басыңыз (төменде қараңыз). Әр түрлі қауіпсіздік сценарийлері әр түрлі конфигурацияларды қажет етуі мүмкін. Осыны ескере отырып, ThreatSense технологиясын төмендегі қорғау модульдері үшін жеке конфигурациялауға болады:

- Файлдық жүйені нақты уақытта қорғау
- Жұмыссыз күйде қарап шығу
- Іске қосылған кезде қарап шығу
- Құжатты қорғау
- Электрондық пошта клиентін қорғау
- Веб қатынасты қорғау
- Компьютерді қарап шығу

ThreatSense параметрлері әрбір модуль үшін жоғары деңгейде оңтайландырылған және оларды өзгерту жүйенің жұмысына айтарлықтай әсер етуі мүмкін. Мысалы, параметрлерді орындалу уақытының бумалаушыларын әрқашан қарап шығатындай өзгерту және «Нақты уақыттағы файл жүйесін қорғау» модулінде кеңейтілген эвристиканы қосу жүйенің баяулауына әкелуі мүмкін (әдетте, жаңадан жасалған файлдар ғана осы әдістер арқылы қарап шығылады). Біз "Шығу" модулінен басқа барлық модульдер үшін әдепкі ThreatSense параметрлерін өзгеріссіз қалдыру ұсынылады.

Қарап шығатын нысандар

Бұл бөлім қай компьютер компоненттерінде және файлдарда инфильтрациялар бар-жоғы қарап шығылатынын анықтауға мүмкіндік береді.

Оперативті жад – Жүйенің оперативті жадын шабуылдайтын қауіптерді қарап шығады.

Жүктеу бөліктері – Жүктеу бөліктерінде негізгі жүктеу жазбасында вирустар бар-жоғын қарап шығады.

Электрондық пошта файлдары – Бағдарлама келесі кеңейтімдерді қолдайды: DBX (Outlook Express) және EML.

Мұрағаттар – Бағдарлама келесі кеңейтімдерді қолдайды: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE және басқа көптеген кеңейтімдер.

Өздігінен ашылатын мұрағаттар - Өздігінен ашылатын мұрағаттар (SFX) — өздерін шығарып ала алатын мұрағаттар.

Орындау уақытындағы бумалаушылар – орындаудан кейін орындау уақытындағы бумалаушылар (стандартты мұрағат түрлерінен өзгеше) жадта сығымдаудан шығарылады. Стандартты тұрақты бумалаушыларға (UPX, yoda, ASPack, FSG, т.б.) қосымша ретінде қарап шығу құралы кодты эмуляциялау арқылы бумалаушылардың бірнеше қосымша түрін тани алады.

Қарап шығу опциялары

Жүйеде инфильтрациялар бар-жоғын қарап шығу кезінде пайдаланылатын әдістерді таңдаңыз. Мына опциялар қол жетімді:

Эвристика – эвристика – бағдарламалардың (зиянкес) белсенділігін талдайтын алгоритм. Осы технологияның басты артықшылығы — бұрын болмаған немесе бұрынғы вирус қолтаңбаларының дерекқорында қамтылмаған зиянкес бағдарламаларды анықтау қабілеті. Кемшілігі – жалған ескертулердің болу ықтималдығы (өте аз).

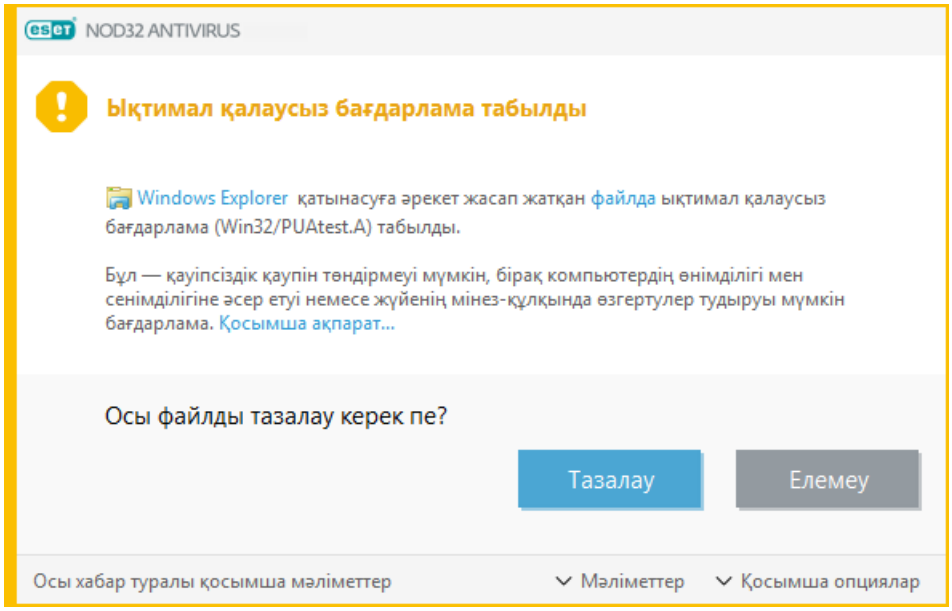
Кеңейтілген эвристика/DNA қолтаңбалары - кеңейтілген эвристика ESET компаниясы жасаған, компьютер құрттары мен троялық аттарды табу үшін оңтайландырылған және жоғары деңгейлі бағдарламалау тілдерінде жазылған бірегей эвристикалық алгоритм. Кеңейтілген эвристиканы пайдалану ESET өнімдерінің қауіптерді анықтау мүмкіндіктерін айтарлықтай арттырады. Қолтаңбалар вирустарды сенімді түрде табады және анықтайды. Автоматты жаңарту жүйесін пайдаланып, жаңа қолтаңбалар қауіп табылғаннан кейін бірнеше сағат ішінде қол жетімді болады. Қолтаңбалардың кемшілігі — олар тек өздері білетін вирустарды (немесе осы вирустардың аздап өзгертілген нұсқаларын) анықтайды.

Ықтимал қалаусыз қолданба — жарнамалық бағдарламаны қамтитын, құралдар тақталарын орнататын немесе басқа анық емес мақсатары бар бағдарлама. Пайдаланушы ықтимал қалаусыз қолданбаның артықшылықтары қауіптерден асып түсетінін сезуі мүмкін кейбір жағдайлар бар. Осы себепті ESET мұндай қолданбаларға трояндық аттар немесе құрттар сияқты зиянкес бағдарламалардың басқа түрлерімен салыстырғанда төменірек қауіп санатын тағайындайды.

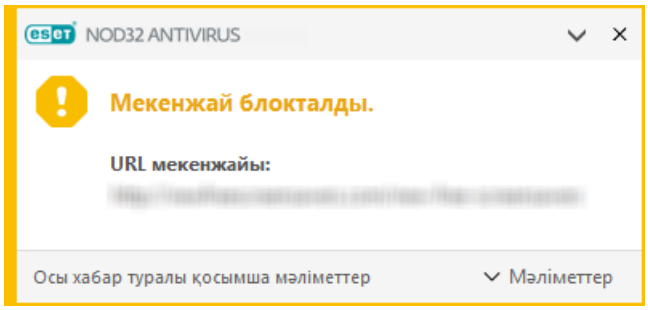
Ескерту - Ықтимал қауіп табылды

Ықтимал қалаусыз қолданба анықталғанда сіз қай әрекетті орындау керектігі туралы шешім қабылдай аласыз:

1. **Тазалау**/**Ажырату**: бұл опция әрекетті аяқтайды және ықтимал қауіптің жүйеге кіруін болдырмайды.
2. **Елемеу**: бұл опция ықтимал қауіпке жүйеге кіруге рұқсат етеді.
3. Қолданбаға болашақта үзіліссіз компьютерде жұмыс істеуге рұқсат ету үшін **Кеңейтілген опциялар** тармағын басыңыз, содан кейін **Анықтауға қоспау** жанында құсбелгі қойыңыз.

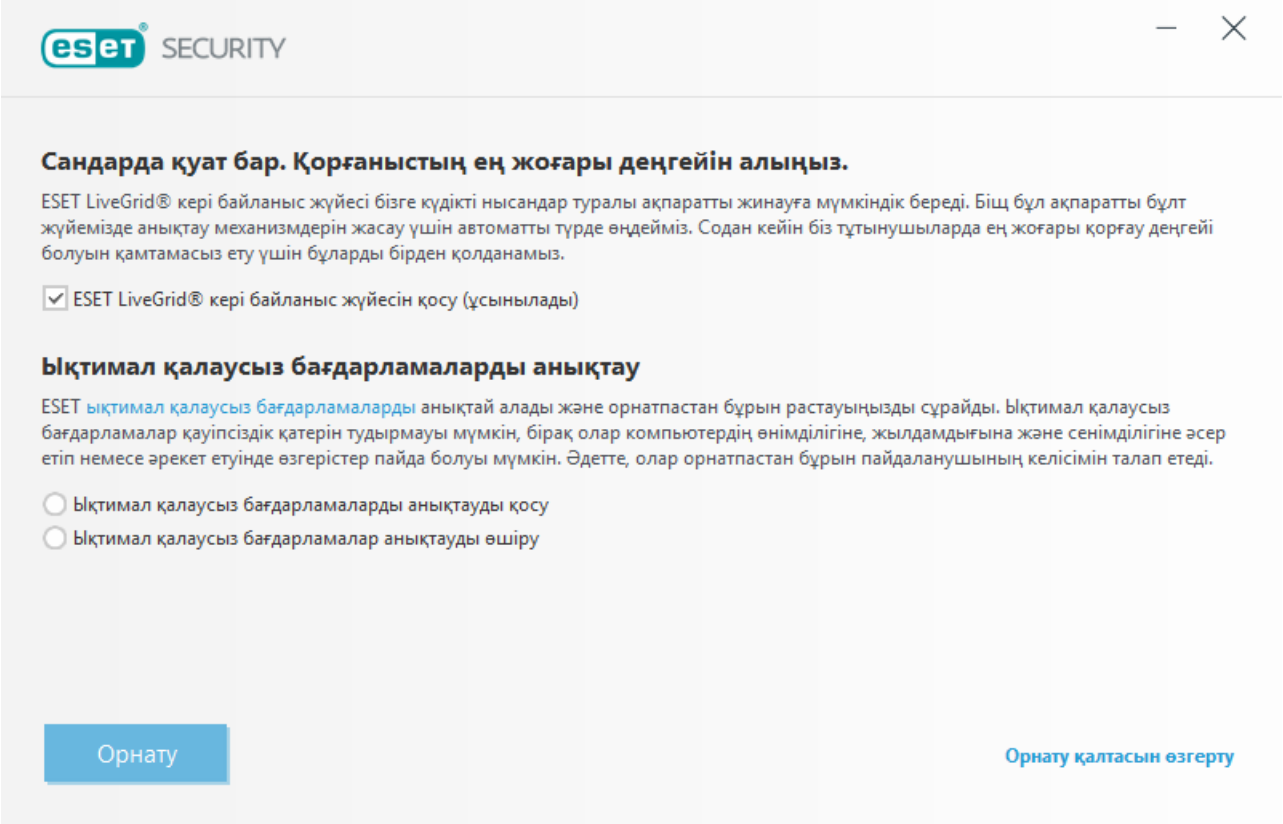


Ықтимал қалаусыз қолданба анықталса және оны тазалау мүмкін болмаса, **Мекенжай блокталды** хабарландыруы көрсетіледі. Бұл оқиға туралы қосымша ақпарат алу үшін негізгі мәзірде **Құралдар** > **Журналд файлдары** > **Сүзілген веб-сайттар** тармағына өтіңіз.



Ықтимал қалаусыз қолданбалар - Параметрлер

ESET өнімін орнатып жатқанда төменде көрсетілгендей ықтимал қалаусыз қолданбаларды анықтауды қосу-қоспау туралы шешім қабылдай аласыз:

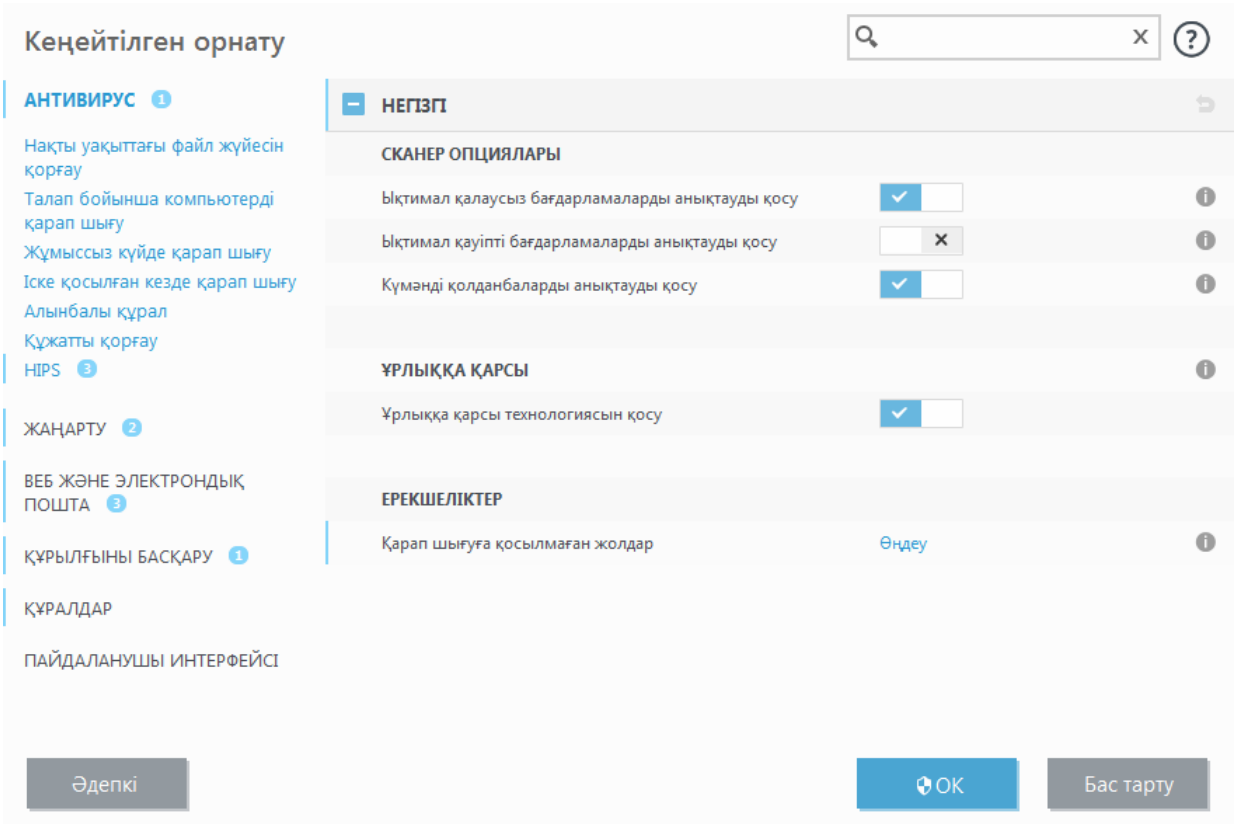


ЕСКЕРТУ

Ықтимал қалаусыз қолданбалар жарнамалық бағдарламаларды, құралдар тақталарын орнатуы немесе басқа қалаусыз және қауіпті бағдарлама мүмкіндіктерін қамтуы мүмкін.

Бұл параметрлерді бағдарлама параметрлерінде кез келген уақытта өзгертуге болады. Ықтимал қалаусыз, қауіпті немесе күдікті қолданбаларды анықтауды қосу немесе өшіру үшін мына нұсқауларды орындаңыз:

1. ESET өнімін ашыңыз. ESET өнімін қалай ашуға болады?
2. **F5** пернесін басып, **Кеңейтілген орнату** тармағын ашыңыз.
3. **Антивитус** тармағын басыңыз және таңдауыңызға сай **Ықтимал қалаусыз қолданбаларды анықтауды қосу**, **Ықтимал қалаусыз қолданбаларды анықтауды қосу** және **Күдікті қолданбаларды анықтауды қосу** опцияларын қосыңыз немесе өшіріңіз. **OK** түймесін басу арқылы растаңыз.



Ықтимал қалаусыз қолданбалар - Бағдарлама орау құралдары

Бағдарламаны орау құралы — кейбір файл-хостинг веб-сайттары пайдаланатын қолданбаны өзгертудің арнайы түрі. Бұл — сіз жүктегіңіз келген бағдарламаны орнататын, бірақ құралдар тақталары немесе жарнамалық бағдарлама сияқты қосымша бағдарламаны қосатын бағдарлама. Сондай-ақ қосымша бағдарламалық құрал веб-браузердің басты бетіне және іздеу параметрлеріне өзгертулер енгізуі мүмкін. Сондай-ақ, файл-хостинг веб-сайттары көбінесе бағдарламалық құрал жеткізушісіне немесе жүктеуді алушыға өзгертулер жасалғаны туралы хабарламайды және көбінесе өзгертуден бас тарту опцияларын жасырады. Осы себептермен ESET бағдарлама орау құралдарын пайдаланушыларға жүктеуді қабылдамау немесе қабылдамауға рұқсат ету үшін ықтимал қалаусыз қолданбаның түрі ретінде жіктейді.

Осы анықтама бетінің жаңартылған нұсқасын алу үшін осы ESET білім қоры мақаласы бөлімін қараңыз.

Ықтимал қауіпті қолданбалар – Ықтимал қауіпті қолданбалар — қашықтан қатынасу құралдары, құпия сөзді бұзу құралдары және кейлоггерлер (пайдаланушы терген әр перне басуды жазатан бағдарламалар) үшін пайдаланылатын сыныптама. Бұл опция әдепкі мәні бойынша өшірілген.

Тазалау параметрлері вирус жұққан файлдарды тазалау кезіндегі қарап шығу құралының әрекетін анықтайды. 3 тазалау деңгейі бар.

Ерекшеліктер

Кеңейтім – файл атауының нүктемен бөлінген бөлігі. Кеңейтім файлдың түрі мен мазмұнын анықтайды. ThreatSense параметрлерін реттеудің бұл бөлімі тексерілетін файл түрлерін анықтауға мүмкіндік береді.

Басқа

ThreatSense механизмінің параметрлерін талап бойынша компьютерді қарап шығу үшін конфигурациялағанда, сонымен бірге, **Басқа** бөлімінде келесі опциялар қол жетімді:

Баламалы деректер ағындарын қарап шығу (ADS) – NTFS файлдық жүйесі пайдаланатын баламалы деректер ағындары – әдеттегі қарап шығу әдістеріне көрінбейтін файл және қалта байланыстары. Көптеген инфильтрациялар өздерін балама деректер ағындары ретінде жасыру арқылы табуға жол бермеуге тырысады.

Басымдығы төмен артқы фонда қарап шығуды іске қосу – Әрбір қарап шығу тіркесімі жүйе ресурстарының белгілі бір мөлшерін тұтынады. Егер сіз жүйелік ресурстарға жоғары жүктеме түсіретін бағдарламалармен жұмыс істейтін болсаңыз, басымдығы төмен фондық қарап шығуды іске қосып бағдарламаларыңыз үшін ресурстарды сақтауға болады.

Барлық нысандарды тіркеу – егер осы опция таңдалса, журнал файлы барлық қарап шығылған файлдарды, тіпті вирус жұқпағандарын көрсетеді. Мысалы, мұрағатта инфильтрация табылса, журнал мұрағатта бар таза файлдарды да тізеді.

Зерделі оңтайландыруды қосу – зерделі оңтайландыру қосулы болғанда, ең жоғары қарап шығу жылдамдығын сақтай отырып, ең тиімді қарап шығу деңгейін қамтамасыз ету үшін ең оңтайлы параметрлер пайдаланылады. Түрлі қорғау модульдері әртүрлі қарап шығу әдістерін нақты файл түрлеріне қолдана отырып, зерделі түрде қарап шығады. Егер зерделі оңтайландыру қызметі өшірілсе, тек белгілі бір модульдердің ThreatSense негізіндегі пайдаланушылық параметрлер ғана қарап шығу барысында қолданылады.

Соңғы кіру уақыт белгісін сақтау – тексерілген файлдардың бастапқы кіру уақытын жаңартудың орнына сақтау үшін (мысалы, деректердің сақтық көшірмесін жасау жүйелерімен пайдалану үшін) осы опция ұяшығына белгі қойыңыз.

Шектеулер

Шектеулер бөлімі нысандардың ең үлкен өлшемін және қарап шығатын енгізілген мұрағаттар деңгейлерін көрсету мүмкіндігін береді:

Нысан параметрлері

Нысанның ең үлкен өлшемі – Қарап шығатын нысандардың ең үлкен өлшемін анықтайды. Берілген антивирустық модуль көрсетілген өлшемнен кішірек нысандарды қарап шығатын болады. Бұл параметр үлкенірек нысандарды қарап шығудан шығару үшін белгілі бір себептері бар алдыңғы қатарлы пайдаланушылармен ғана өзгертілуі керек. Әдепкі мәні: *шексіз*.

Нысанды қарап шығудың ең ұзақ уақыты (сек.) – Нысанды қарап шығу үшін ең көп уақыт мәнін анықтайды. Егер пайдаланушылық мән осында енгізілген болса, антивирустық модуль қарап шығудың бітуіне не бітпеуіне қарамастан, уақыт аяқталған кезде қарап шығуды тоқтатады. Әдепкі мәні: *шексіз*.

Мұрағаттарды қарап шығуды орнату

Мұрағат енгізу деңгейі – Мұрағатты қарап шығудың ең үлкен тереңдігін көрсетеді. Әдепкі мәні: *10*.

Мұрағаттағы файлдың ең үлкен өлшемі – Бұл опция қарап шығылуы қажет мұрағаттарда (бөлініп алынған кезде) қамтылған файлдар үшін ең үлкен өлшемді көрсету мүмкіндігін береді. Әдепкі мәні: *шексіз*.

ЕСКЕРТПЕ
Біз әдепкі мәндерді өзгертуді ұсынбаймыз; қалыпты жағдайда оларды өзгертудің еш негізі жоқ.

4.1.1.6.1 Тазалау

Тазалау параметрлері вирус жұққан файлдарды тазалау кезіндегі қарап шығу құралының әрекетін анықтайды. 3 тазалау деңгейі бар.

4.1.1.6.2 Қарап шығуға қосылмаған файл кеңейтімдері

Кеңейтім – файл атауының нүктемен бөлінген бөлігі. Кеңейтім файлдың түрі мен мазмұнын анықтайды. ThreatSense параметрлерін реттеудің бұл бөлімі тексерілетін файл түрлерін анықтауға мүмкіндік береді.

Әдепкі мәні бойынша, кеңейтіміне қарамастан барлық файлдар тексеріледі. Қарап шығуға қосылмаған файлдар тізіміне кез келген кеңейтімді қосуға болады.

Кейде белгілі бір файл түрлерін қарап шығу кеңейтімдерді пайдаланатын бағдарламаның дұрыс емес әрекетін тудырған жағдайда файлдарды қарап шығуға қоспаған дұрыс. Мысалы, Microsoft Exchange серверін пайдаланғанда .edb, .eml және .tmp кеңейтімдерін қоспауға кеңес беруге болады.

Қосу және **Жою** түймелерін пайдаланып белгілі бір файл кеңейтімдерін қарап шығуға рұқсат етуге немесе тыйым салуға болады. Тізімге жаңа кеңейтім қосу үшін **Бос өріске кеңейтім түрін қосу** түймесін басып, **OK** түймесін басыңыз. **Бірнеше мәнді енгізу** пәрменін таңдасаңыз, жолдармен, үтірлермен немесе нүктелі үтірлермен бөлінген бірнеше файл кеңейтімін қосуға болады. Бірнеше таңдау қосылған болса, кеңейтімдер тізімде көрсетіледі. Тізімде кеңейтімді таңдаңыз, сөйтіп бұл кеңейтімді тізімнен жою үшін **Жою** түймесін басыңыз. Таңдалған кеңейтімді өңдеу керек болса, **Өңдеу** түймесін басыңыз.

Арнайы таңбалар ? (сұрақ белгісі) арнайы таңбаларын пайдалануға болады. Бірінші сұрақ белгісі кез келген таңбаны білдіреді.

ЕСКЕРТПЕ
Windows операциялық жүйесінде файлдың дәл кеңейтімін (бар болса) көру үшін **Басқару панелі** > **Қалта опциялары** > **Көрініс** (қойынды) тармағында **Белгілі файл түрлерінің кеңейтімдерін жасыру** опциясынан құсбелгіні алу және осы өзгертуді қолдану керек.

4.1.1.7 Инфильтрация анықталды

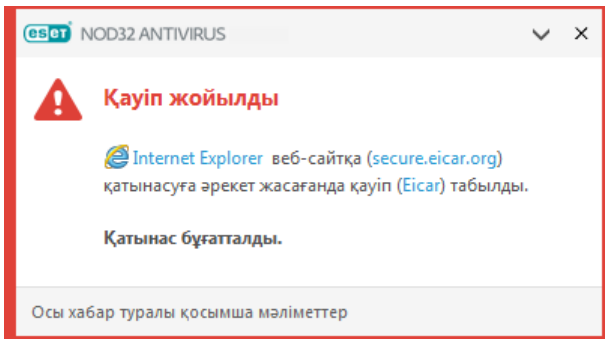
Инфильтрацияларға жүйеге әр түрлі ену нүктелерінен, мысалы, веб-беттерден, ортақ қалталардан, электрондық пошта арқылы немесе алынбалы құрылғыларынан (USB, сыртқы дискілер, ықшам дискілер, DVD дискілері, дискеталар, т.б.) қол жеткізуге болады.

Стандартты тәртіп

Инфильтрациялардың ESET NOD32 Antivirus арқылы қалай өңделетіні туралы жалпы мысалы ретінде инфильтрацияларды келесілер арқылы анықтауға болады:

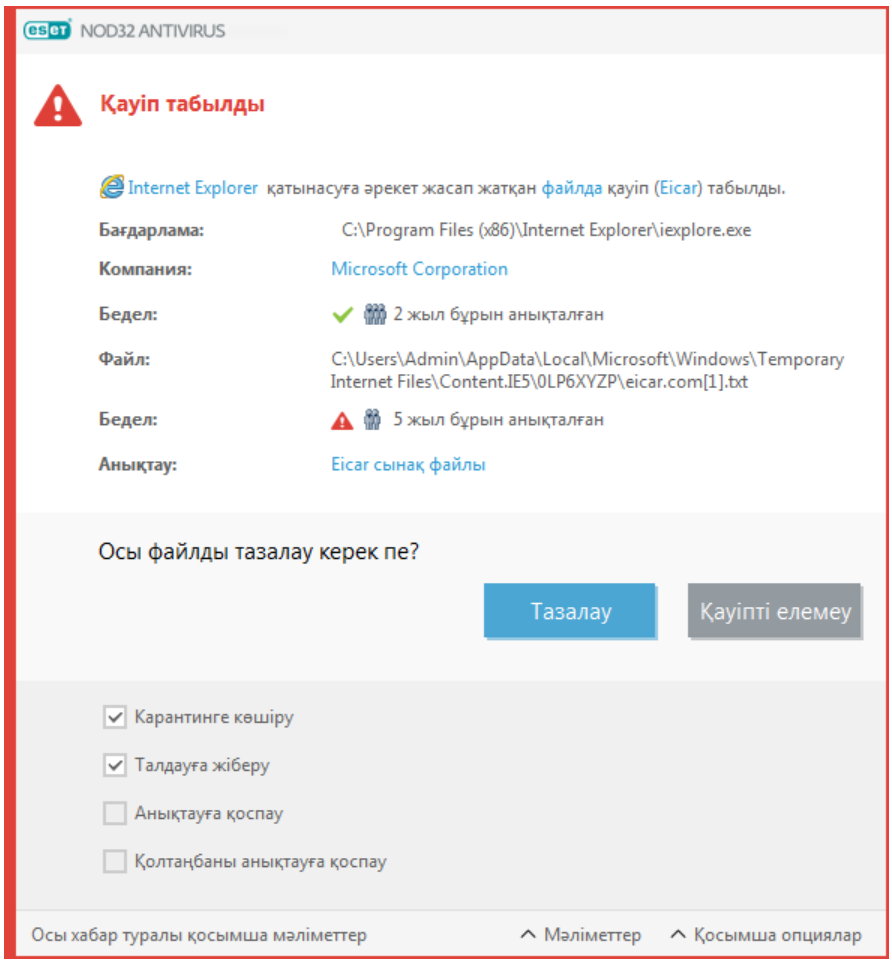
- Файлдық жүйені нақты уақытта қорғау
- Веб қатынасты қорғау
- Электрондық пошта клиентін қорғау
- Талап бойынша компьютерді қарап шығу

Әрқайсысы стандартты тазалау деңгейін пайдаланады және файлды тазалап, оны Карантин қалтасына көшіруге немесе байланысты тоқтатуға әрекет етеді. Хабарландыру терезесі экранның төменгі оң жақ бұрышындағы хабарландыру аумағында көрсетіледі. Тазалау деңгейлері мен тәртібі туралы қосымша ақпарат алу үшін Тазалау бөлімін қараңыз.



Тазалау және жою

Егер Нақты уақыттағы файл жүйесін қорғау үшін орындалатын алдын ала анықталған әрекет болмаса, сізден ескерту терезесінде опцияны таңдау сұралады. Әдетте **Тазалау**, **Жою** және **Әрекетсіз** опциялары қол жетімді. Вирус жұққан файлдарды тазаламай қалдыратындықтан, **Әрекетсіз** опциясын таңдау ұсынылмайды. Бұл тек файлдың зиянсыз екеніне және қателесіп табылғанына сенімді болатын жағдайға қатысты емес.



Файлға зиянды кодты тіркеген вирус шабуылдаған жағдайда тазалауды қолданыңыз. Мұндай жағдайда алдымен вирус жұққан файлды тазалап, бастапқы күйіне келтіруге әрекет жасаңыз. Егер файл тек зиянды кодтан тұратын болса, ол жойылады.

Егер вирус жұққан файл «құлыпталған» немесе жүйелік үрдісте пайдаланылып жатса, әдетте ол босаған кезде (әдетте жүйені қосқаннан кейін) ғана жойылады.

Бірнеше қауіп

Шығу кезінде қандай вирус жұққан файлдар тазаланбаса (немесе Тазалау деңгейі **Тазаламау** деп орнатылса), сол файлдар үшін әрекеттерді таңдауды ұсынатын ескерту терезесі көрсетіледі. Файлдар үшін әрекеттерді таңдаңыз (әрекеттер тізімдегі әр файл үшін жеке-жеке орнатылады), содан кейін **Дайын** түймешігін басыңыз.

Мұрағаттардағы файлдарды жою

Әдепкі тазалау режимінде тек вирус жұққан файлдар қамтылып мен таза файлдар болмаған жағдайда ғана мұрағат жойылады. Басқаша айтқанда, сонымен бірге зиянсыз таза файлдар бар болса, мұрағаттар жойылмайды. Қатаң тазалап қарап шығу орындалғанда мұқият болыңыз, қосылған қатаң тазалау кезінде оның құрамында кемінде бір вирусы бар файл болса, мұрағаттағы басқа файлдардың күйіне қарамастан мұрағат жойылады.

Егер компьютеріңіз зиянды жұқтыру белгілерін көрсетсе, мысалы ол баяулап қалса, жиі қатып қалса, т.б. мына әрекеттерді орындау ұсынылады:

- ESET NOD32 Antivirus бағдарламасын ашып, «Шығу» басыңыз
- **Компьютерді қарап шығу** тармағын басыңыз (қосымша ақпарат алу үшін Компьютерді қарап шығу бөлімін қараңыз)
- Қарап шығу аяқталғаннан кейін журналдан тексерілген, вирус жұққан және тазаланған файлдардың санын қарап шығыңыз

Егер дискінің белгілі бір бөлігін ғана қарап шығуды қаласаңыз, **Таңдамалы қарап шығу** пәрменін таңдап, вирустардан тексерілетін нысандарды таңдаңыз.

4.1.1.8 Құжатты қорғау

Құжатты қорғау мүмкіндігі ашу алдында Microsoft Office құжаттарын, сонымен бірге, Microsoft ActiveX элементтері сияқты Internet Explorer бағдарламасы автоматты түрде жүктеген файлдарды қарап шығады. Құжатты қорғау Нақты уақыттағы файл жүйесін қорғауға қосымша қорғаныс қабатын қамтамасыз етеді және оны Microsoft Office құжаттарының көп санын өңдемейтін жүйеде өнімділікті жақсарту үшін өшіруге болады.

Құжатты қорғауды іске қосу үшін **Кеңейтілген орнату** терезесі (F5 пернесін басыңыз) > **Антивирус** > **Құжатты қорғау** тармағын ашып, **Жүйеге біріктіру** қосқышын басыңыз.

ЕСКЕРТПЕ
Бұл мүмкіндікті Microsoft Antivirus API (мысалы, Microsoft Office 2000 және одан кейінгі нұсқалар немесе Microsoft Internet Explorer 5.0 және одан кейінгі нұсқалар) пайдаланатын қолданбалар іске қосады.

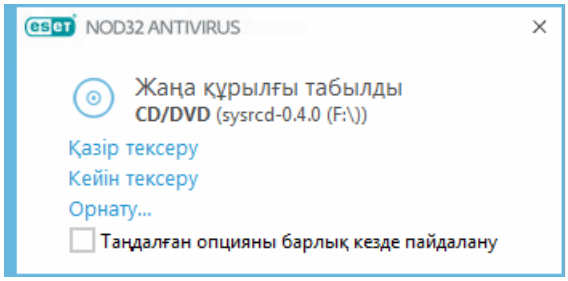
4.1.2 Алынбалы құрал

ESET NOD32 Antivirus алынбалы құралдарды (CD/DVD/USB/...) автоматты түрде қарап шығумен қамтамасыз етеді. Бұл модуль салынған медианы қарап шығуға рұқсат береді. Бұл компьютер әкімшісі пайдаланушылардың қалаусыз мазмұны бар алынбалы құралды пайдалануына жол бермеуді қалаған жағдайда пайдалы болуы мүмкін.

Алынбалы құралды қосқаннан кейін орындалатын әрекет - Компьютерге алынбалы құрал (CD/DVD/USB) қосылғанда орындалатын әдепкі әрекетті таңдаңыз. **Қарап шығу опцияларын көрсету** опциясы таңдалса, қажет әрекетті таңдауға мүмкіндік беретін хабарландыру көрсетіледі:

- **Қарап шықпау** – ешбір әрекет орындалмайды және **Жаңа құрылғы табылды** терезесі жабылады.
- **Құрылғыны автоматты түрде қарап шығу** – салынған алынбалы құрылғыда талап бойынша компьютерді қарап шығу орындалады.
- **Қарап шығу опцияларын көрсету** – «Алынбалы құралды реттеу» бөлімін ашады.

Алынбалы құрал қосылғанда келесі диалогтық терезе көрсетіледі:



Қазір қарап шығу – бұл алынбалы құралды қарап шығуды іске қосады.

Кейінірек қарап шығу – алынбалы медиа қарап шығу кейінге қалдырылады.

Орнату – «Кеңейтілген орнату» терезесін ашады.

Әрқашан таңдалған опцияны пайдалану – таңдалған болса, бірдей әрекет алынбалы құрал келесі рет қосылғанда орындалады.

Бұған қоса, ESET NOD32 Antivirus бағдарламасында берілген компьютерде сыртқы құрылғыларды пайдалану ережелерін анықтауға мүмкіндік беретін «Құрылғыны басқару» функциясы бар. Құрылғыны басқару туралы толық мәліметтерді Құрылғыны басқару бөлімінен табуға болады.

4.1.3 Құрылғыны басқару

Құрылғыны басқару

ESET NOD32 Antivirus автоматты құрылғы (CD/DVD/USB/...) басқару элементімен қамтамасыз етеді. Бұл модуль кеңейтілген сүзгілерді/рұқсаттарды бұғаттауға немесе реттеуге және пайдаланушылардың осы құрылғыға қатынасу және онымен жұмыс істеу мүмкіндігін анықтайды. Бұл компьютер әкімшісі пайдаланушылардың қалаусыз мазмұны бар құрылғыларды пайдалануға жол бермеуді қалаған жағдайда пайдалы болуы мүмкін.

Қолдау көрсетілген сыртқы құрылғылар:

- Диск сақтау құралы (HDD, USB алынбалы дискі)
- CD/DVD
- USB-принтер
- FireWire сақтау құралы
- Bluetooth құрылғысы
- Смарт карта оқушы
- Кескін құрушы құрылғы
- Модем
- LPT/COM порты
- Тасымалданатын құрылғы
- Микрофон
- Барлық құрылғы түрлері

«Құрылғы басқаруды орнату» опцияларын **Кеңейтілген орнату** (F5) > **Құрылғыны басқару** тармағында өзгертуге болады.

Жүйеге біріктіру жанындағы қосқышты қосу ESET NOD32 Antivirus өніміндегі Құрылғыны басқару мүмкіндігін іске қосады; осы өзгертудің күшіне енуі үшін компьютерді қайта іске қосуыңыз қажет. Құрылғыны басқару қосылған кезде **Ережелер** іске қосылып, Ережелерді өңдеуші терезесін ашуға мүмкіндік береді.

ЕСКЕРТПЕ
Сіз әр түрлі ережелер қоладнылатын әр түрлі құрылғылар топтарын жасай аласыз. Сондай-ақ, **Оқу/жазу** немесе **Тек оқу** әрекеті бар ереже қолданылатын құрылғылардың тек бір тобын жасай аласыз. Бұл компьютерге қосылғанда «Құрылғыны басқару» арқылы танылмаған құрылғыларды блоктауды қамтамасыз етеді.

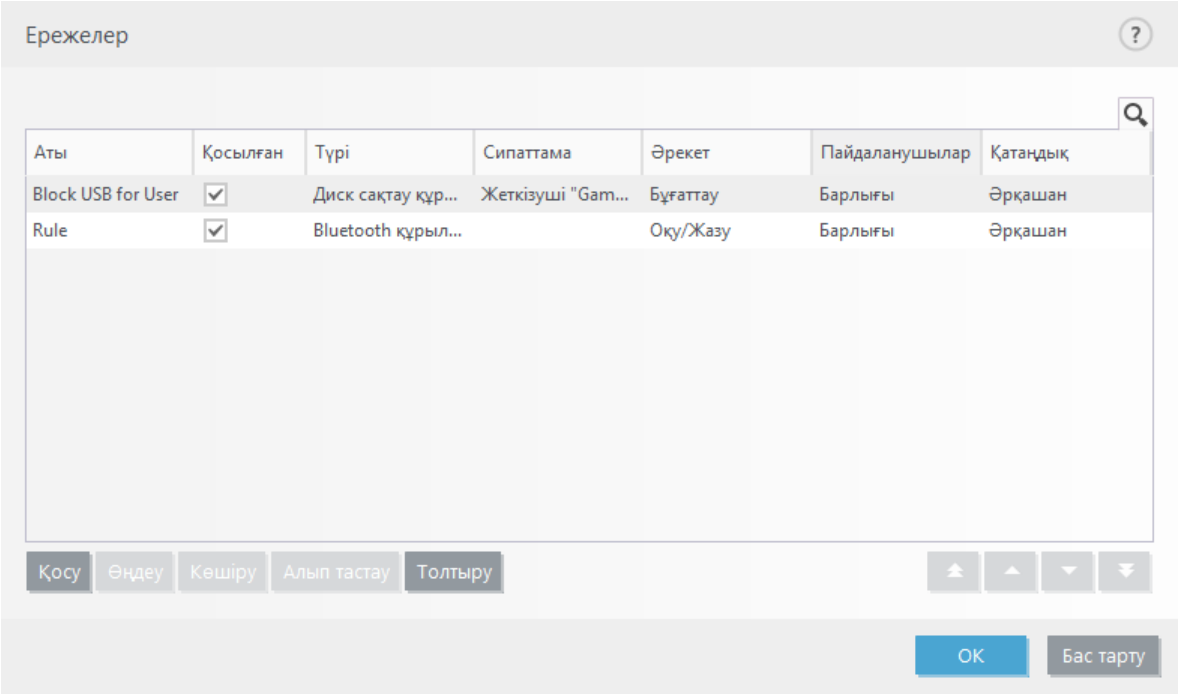
Егер бар ережемен блокталған құрылғы салынса, хабарландыру терезесі көрсетіледі және құрылғыға қатынас берілмейді.

Веб-камераны қорғау

Жүйеге біріктіру жанындағы қосқышты қосу ESET NOD32 Antivirus ішіндегі веб-камераны қорғау мүмкіндігін іске қосады. Веб-камераны қорғау қосылған кезде **Ережелер** белсенді болып, Ережелерді өңдеуші терезесін ашуға мүмкіндік береді.

4.1.3.1 Құрылғы басқару ережелерін өңдеуші

Құрылғыны басқару ережелерін өңдеуші терезесі қолданыстағы ережелерді көрсетеді және пайдаланушылар компьютерге қосатын сыртқы құрылғылардың дәл басқарылуына рұқсат береді.



Ерекше құрылғыларға пайдаланушы немесе пайдаланушылар тобы тарапынан және және ереже конфигурацияларында көрсетілуі мүмкін қосымша құрылғы параметрлерінің негізінде рұқсат беріледі немесе блокталады. Ережелер тізімі журнал қатаңдығы және атауы, сыртқы құрылғы түрі, сыртқы құрылғылар компьютеріңізге енгізілгеннен кейін орындалатын әрекеті және тіркеу қатаңдығы сияқты ережелердің бірнеше сипаттамасын қамтиды.

Ережені басқару үшін **Қосу** немесе **Өңдеу** түймесін басыңыз. Басқа таңдалған ереже үшін алдын ала анықталған параметрлерді пайдаланып жаңа ереже жасау үшін **Көшіру** түймесін басыңыз. Ережені басқан кезде көрсетілетін XML жолдарын жүйелік әкімшілерінің осы деректерді экспорттау/импорттау және пайдалануына көмектесу үшін, мысалы, ESET Remote Administrator бағдарламасында аралық сақтағышқа көшіруге болады.

CTRL түймесін түртіп және басқан кезде бірнеше ережелерді таңдауға және әрекеттерді қолдануға, мысалы барлық таңдалған ережелер үшін оларды жоюға немесе тізімде жоғары немесе төмен жылжытуға болады. **Қосылған** ұяшығы ережені қосады немесе ажыратады; егер оны болашақта пайдаланғыңыз келсе, ережені мүлде жойғыңыз келмегенде пайдалы болуы мүмкін.

Басқару элементі жоғары басымдылыққа ие ережелер ең басына қойыла отырып, өз басымдылықтарының анықталу ретімен сұрыпталатын ережелер арқылы орындалады.

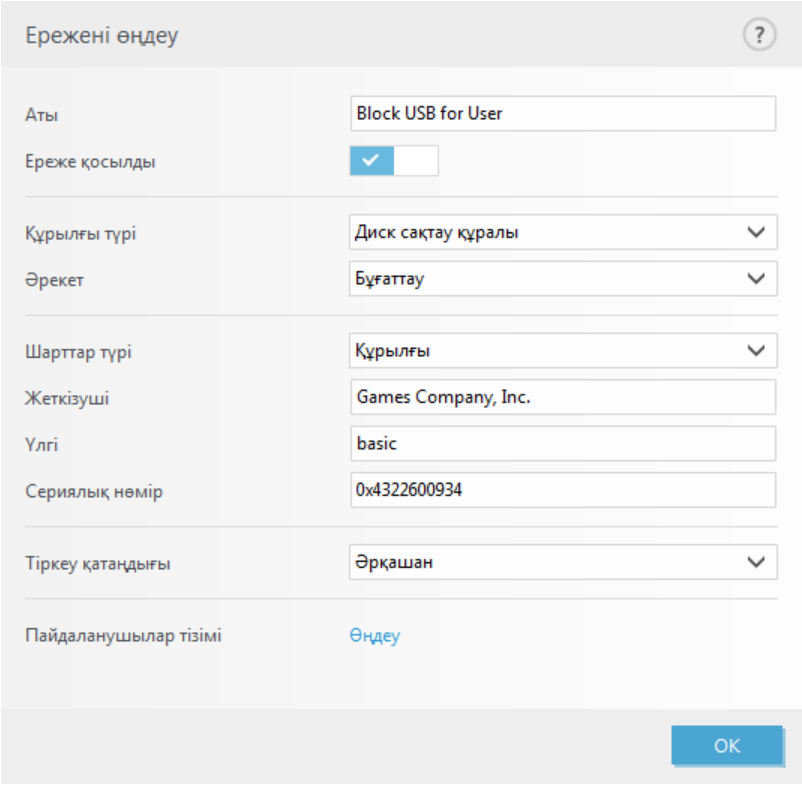
Журнал жазбаларын ESET NOD32 Antivirus бағдарламасының негізгі терезесінде **Құралдар** > **Журнал файлдары** тармағында көруге болады.

Құрылғыны басқару журналы құрылғыны басқару іске қосылған барлық жағдайларды жазады.

Компьютерге қосылған құрылғылар үшін алынбалы медиа құрылғы параметрлерін автоматты толтыру үшін **Толтыру** түймесін басыңыз.

4.1.3.2 Құрылғы басқару ережелерін қосу

Құрылғыны басқару ережесі ереже шартына сәйкес келетін құрылғы компьютерге қосылған кезде орындалатын әрекетті анықтайды.



Анықтауды жақсарту үшін **Аты** өрісіне ереже сипаттамасын енгізіңіз. Осы ережені өшіру немесе қосу үшін **Ереже қосылған** жанындағы қосқышты басыңыз; бұл ережені біржола жойғыңыз келмегенде пайдалы болуы мүмкін.

Құрылғы түрі

Ашылмалы мәзірден сыртқы құрылғының түрін таңдаңыз (диск сақтау құрылғысы/жылжымалы құрылғы/Bluetooth/FireWire/...). Құрылғы түрі туралы ақпарат операциялық жүйеден жиналады және құрылғы компьютерге қосылған болса, жүйенің құрылғы реттегіші ішінде көруге болады. Сақтау құрылғыларына USB немесе FireWire арқылы қосылатын сыртқы дискілер немесе қалыпты жад картасын оқу құралдары кіреді. Смарт картаны оқу құралдары смарт карталарды SIM картасы немесе түпнұсқалықты растау карталары сияқты кірістірілген интегралдық схемасы бар барлық смарт карталарды оқу құралдарын қамтиды. Кескін құрушы құрылғылар мысалына сканерлер немесе камералар жатады. Тек өздерінің әрекеттері туралы ақпаратты қамтамасыз ететіндіктен және пайдаланушылар туралы ақпаратты қамтамасыз етпейтіндіктен, бұл құрылғыларды ғаламдық деңгейде ғана блоктауға болады.

Әрекет

Сақтамайтын құрылғыларға қатынасуға рұқсат беруге немесе блоктауға болады. Бұған кері сінше, сақтау құрылғыларының ережелері төмендегі құқықтар параметрлерінің біреуін таңдауға мүмкіндік береді:

- **Жазу** – Құрылғыға толық кіруге рұқсат берілген.
- **Блоктау** – Құрылғыға қатынас блокталады.
- **Тек оқу** – Құрылғыға тек оқу үшін қатынасуға рұқсат беріледі.
- **Ескерту** – құрылғы қосылған сайын пайдаланушыға оған рұқсат етілгені/блокталғаны туралы хабарланады және журнал жазбасы жасалады. Құрылғылар есте сақталмайды, бірдей құрылғының келесі қосылымдарында хабарландыру бәрібір көрсетіледі.

Барлық құрылғы түрлері үшін кейбір әрекеттер (рұқсаттар) қол жетімді болмайтынын ескеріңіз. Бұл — қойма түріне жататын құрылғы, төрт әрекеттің барлығы қол жетімді. Сақтамайтын құрылғылар үшін тек қана үш әрекет қол жетімді (мысалы, Bluetooth үшін **Тек оқу** әрекеті қол жетімді емес, сондықтан Bluetooth құрылғыларына рұқсат беруге, блоктауға немесе олар туралы ескертуге болады).

Шарттар түрі – **Құрылғылар тобы** немесе **Құрылғы параметрін таңдаңыз.**

Төменде көрсетілген қосымша параметрлерді ережелерді дәл реттеу және құрылғыларға ыңғайлау үшін пайдалануға болады. Барлық параметрлер регистрге тәуелді емес:

- **Жеткізуші** – Жеткізуші аты немесе идентификаторы бойынша сүзу.
- **Модель** – Құрылғының аты.
- **Сериялық нөмір** – Сыртқы құрылғылардың әдетте өз сериялық нөмірлері болады. CD/DVD дискі болған жағдайда бұл CD дискінің емес, құралдың сериялық нөмірі болады.

ЕСКЕРТПЕ
бұл параметрлер анықталмаған болса, ереже сәйкестікті анықтау кезінде осы өрістерді елемейді. Барлық мәтіндік өрістердегі сүзу параметрлері регистрді ескереді және арнайы таңбаларға (*, ?) қолдау көрсетілмейді.

ЕСКЕРТПЕ
құрылғы туралы ақпаратты көру үшін сол құрылғы түрі үшін ережені жасаңыз, құрылғыны компьютергеқосыңыз, содан кейін Құрылғыны басқару журналы бөлімінде құрылғы мәліметтерін тексеріңіз.

Тіркеу қатаңдығы

ESET NOD32 Antivirus барлық маңызды оқиғаларды журнал файлына сақтайды. Оны негізгі мәзірден тікелей көруге болады. **Құралдар** > **Журнал файлдары** тармағын басыңыз, содан кейін **Журнал** ашылмалы мәзірінде **Құрылғыны басқару** тармағын таңдаңыз.

- **Әрқашан** – барлық оқиғаларды журналға тіркейді.
- **Диагностика** – бағдарламаны дәл реттеу үшін қажет ақпаратты журналға тіркейді.
- **Ақпарат** – ақпараттық хабарларды, соның ішінде сәтті жаңарту хабарларын, сондай-ақ, барлық жоғарыдағы жазбаларды жазады.
- **Ескерту** – маңызды қателерді және ескерту хабарларын жазады.
- **Жоқ** – Журналдар жазылмайды.

Ережелер **Пайдаланушылар тізімі** ішіне белгілі бір пайдаланушыларды немесе пайдаланушылар тобын қосылу арқылы шектеледі:

- **Қосу** – Келесіні ашады: **Нысан түрлері: Пайдаланушылар немесе топтар** қалаған пайдаланушыларды таңдауға мүмкіндік беретін диалогтық терезені ашады.
- **Жою** – таңдалған пайдаланушыны сүзгіден жояды.

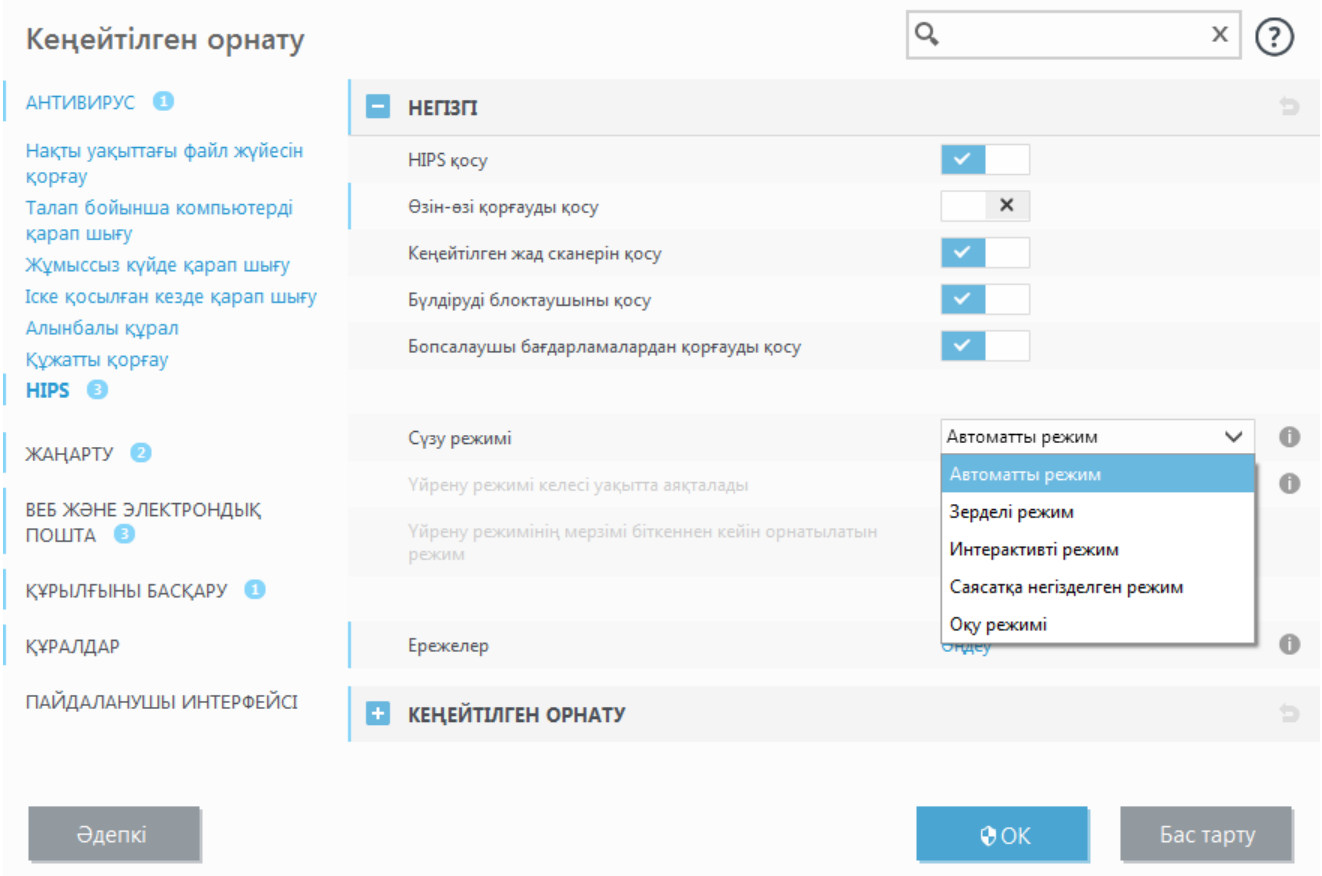
ЕСКЕРТПЕ
Барлық құрылғыларды пайдаланушылық ережелер арқылы сүзуге болады (мысалы, кескіндерді өңдеу құрылғылары пайдаланушылар туралы емес, тек әрекеттер туралы ақпаратты ұсынады).

4.1.4 Басты компьютерге басып кіруді болдырмау жүйесі (HIPS)

ЕСКЕРТУ
HIPS параметріне өзгертулерді тек тәжірибелі пайдаланушы енгізуі керек. HIPS параметрлерін дұрыс емес теңшеу жүйенің тұрақсыздығына әкелуі мүмкін.

Басты компьютерге басып кіруді болдырмау жүйесі (HIPS) жүйеңізді зиянкес бағдарламалар мен компьютерге теріс әсерін тигізетін кез келген қалаусыз әрекеттерден қорғайды. HIPS жүйесі іске қосылған процесстерді, файлдарды және тіркеу кілттерін қадағалау үшін кеңейтілген қасиет талдауын желілік сүзгінің анықтау мүмкіндігін қатар пайдаланады. HIPS Нақты уақыттағы файлдық жүйені қорғау мүмкіндігінен бөлек және брандмауэр емес, ол операциялық жүйеде ғана іске қосылған процесстерді бақылайды.

HIPS параметрлерін **Кеңейтілген орнату** (F5) > **Антивирус** > **HIPS** > **Негізгі** тармағында табуға болады. HIPS күйі (қосылған/өшірілген) ESET NOD32 Antivirus негізгі бағдарлама терезесінде **Орнату** > **Компьютерді қорғау** тармағында көрсетіледі.



ESET NOD32 Antivirus бағдарламасында кірістірілген **Өзін өзі қорғау** технологиясы пайдаланылады. Ол зиянкес бағдарламаның антивирустық және антишпиондық қорғауын бүлдіруін немесе өшіруін болдырмайды. Осылайша жүйенің әрқашан қорғалған екеніне сенімді бола аласыз. HIPS немесе Өзін-өзі қорғауды өшіру үшін Windows жүйесін қайта іске қосу керек.

Қорғалған қызмет – Ядроны қорғауды қосады (Windows 8.1, 10).

Кеңейтілген жад сканері шатастыру немесе шифрлау әрекетін пайдалану арқылы антивирустық өнімдердің анықтауын болдырмау үшін жасалған зиянкес бағдарламалардан қорғануды күшейту үшін «Бүлдіруді блоктаушы» құралымен бірге жұмыс істейді. Кеңейтілген жад сканері әдепкі бойынша қосылған. Глоссарий бөлімінде қорғаудың осы түрі туралы көбірек оқыңыз.

Бүлдіруді блоктаушы веб-браузерлер, PDF оқу құралдары, электрондық пошта клиенттері мен MS Office компоненттері сияқты әдетте пайдаланатын бағдарлама түрлерін жақсарту үшін жасалған. Бүлдіруді блоктаушы әдепкі бойынша қосылған. Глоссарий бөлімінде қорғаудың осы түрі жөніндегі толығырақ ақпаратты оқыңыз.

Зиянкес хакерлік бағдарламалардан қорғау — HIPS мүмкіндіктің бір бөлігі ретінде жұмыс істейтін тағы бір қорғау қабаты. Зиянкес хакерлік бағдарламалардан қорғау жұмыс істеуі үшін LiveGrid репутация жүйесі қосылған болуы керек. Қорғаудың осы түрі туралы осы жерде көбірек оқыңыз.

Сүзуді төрт режимнің бірінде орындауға болады:

Автоматты режим - Жүйені қорғайтын алдын ала анықталған ережелер блоктағандарды қоспағанда, әрекеттер қосылады.

Зерделі режим - пайдаланушыға тек өте күдікті оқиғалар туралы хабарланады.

Интерактивті режим - Пайдаланушыға әрекеттерді растау ұсынылады.

Саясатқа негізделген режим - Әрекеттер бұғатталады.

Үйрену режимі - Әрекеттер қосылады және әр әрекеттен кейін ереже жасалады. Бұл режимде жасалған ережелерде ережелер өңдегішінде қарауға болады, бірақ олардың басымдығы қолмен жасалған ережелерден немесе автоматты режимде жасалған ережелерден төменірек болады. HIPS «Сүзу режимі» ашылмалы мәзірінде «Үйрену режимін» таңдасаңыз, **Үйрену режимінің аяқталу уақыты** параметрі қол жетімді болады. Үйрену режимін қосу ұзақтығын таңдаңыз, ең көп ұзақтық — 14 күн. Көрсетілген ұзақтық өткенде сізге HIPS үйрену режимінде

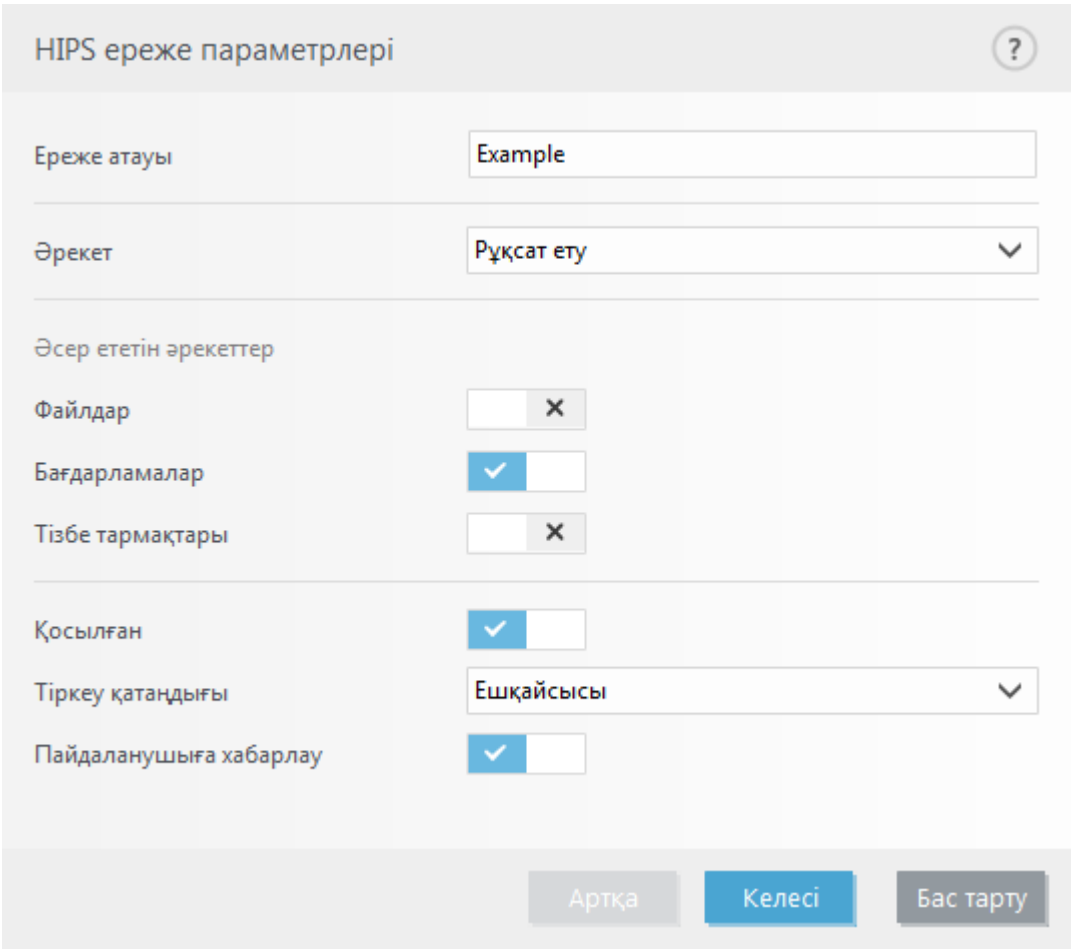
болғанда жасаған ережелерді өңдеу ұсынылады. Сондай-ақ, басқа сүзу режимін таңдауға немесе шешімді кейінге қалдыруға және үйрену режимін пайдалануды жалғастыруға болады.

Үйрену режимінің мерзімі біткеннен кейін орнатылатын режим – Үйрену режимінің мерзімі біткеннен кейін пайдаланылатын сүзу режимін таңдаңыз.

HIPS жүйесі операциялық жүйе ішіндегі оқиғаларды бақылайды және оларға брандмауэр ережелеріне ұқсас сәйкесінше әрекет етеді. HIPS ережелерін басқару терезесін ашу үшін «Ережелер» жанында **Өңдеу** пәрменін басыңыз. HIPS ережелері терезесінде ережелерді қосуға, өңдеуге немесе жоюға болады.

Келесі мысалда бағдарламалардың қалаусыз әрекетін шектеу әдісі көрсетілген:

1. Ережеге ат беріп және **Блоктау** пәрменін **Әрекет** ашылмалы мәзірінде таңдаңыз.
2. **Пайдаланушыға хабарлау** белгісін ереже қолданылатын кез келген уақытта хабарландыруды көрсету үшін қойыңыз.
3. Ереже қолданылатын кемінде бір әрекетті таңдаңыз. **Көз қолданбалар** терезесінде жаңа ережені сіз көрсеткен қолданбаларға қатысты таңдалған қолданба әрекеттерінің кез келгенін орындауға әрекет жасайтын барлы қолданбаларға қолдану үшін ашылмалы мәзірде **Барлық қолданбалар** параметрін таңдаңыз.
4. Таңдау **Басқа қолданбаның күйін өзгерту** (барлық әрекеттер F1 пернесін басу арқылы қатынасуға болатын өнім анықтамасында сипатталған).
5. Ашылмалы мәзірде **Нақты қолданбалар** параметрін таңдаңыз және қорғау керек бір немесе бірнеше қолданбаны **Қосу** әрекетін орындаңыз.
6. Жаңа ережені сақтау үшін **Аяқтау** түймесін басыңыз.



4.1.4.1 Кеңейтілген орнату

Келесі опциялар бағдарламаның әрекетінде ақауларды жою және талдау үшін пайдалы:

Драйверлерді жүктеуге әрқашан рұқсат етіледі – Пайдаланушылық ереже анық түрде блоктаған болмаса, конфигурацияланған сүзу режиміне қарамастан таңдалған драйверлердің жүктелуіне әрқашан рұқсат етіледі.

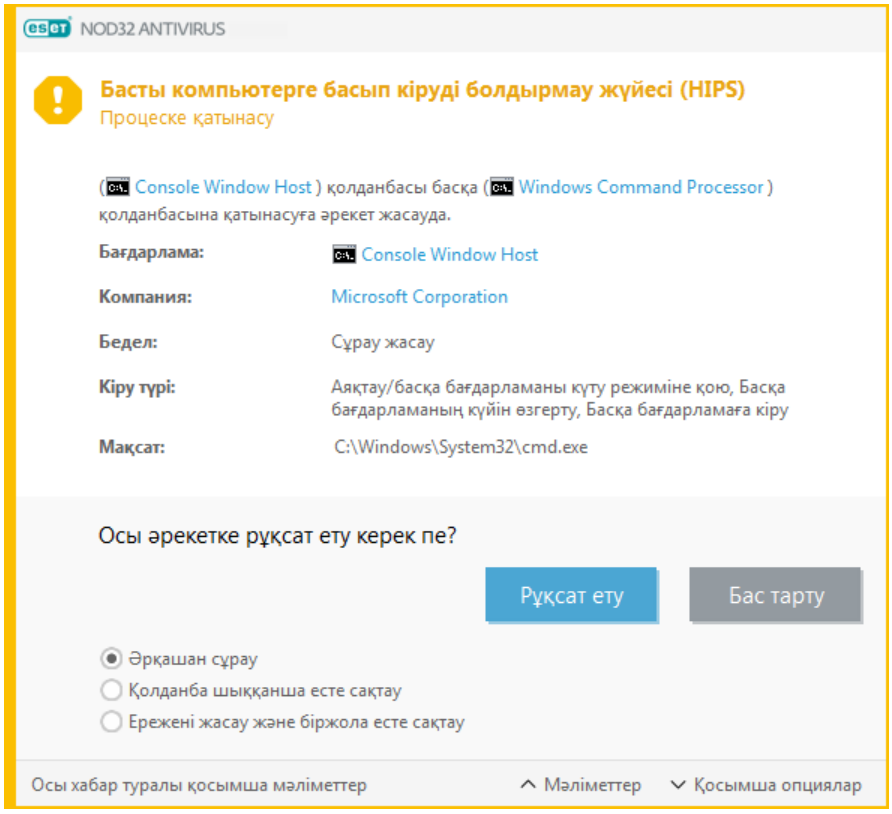
Барлық блокталған әрекеттерді тіркеу – Барлық блокталған әрекеттер HIPS журналына жазылады.

Іске қосу кезіндегі бағдарламаларда өзгерістер орын алғанда хабарландыру – Бағдарлама іске қосу жүйесінен әр қосылған немесе жойылған кезде жұмыс үстелінде хабарландыру көрсетіледі.

Осы анықтама бетінің жаңартылған нұсқасын алу үшін Білім қоры мақаласын қараңыз.

4.1.4.2 HIPS интерактивті терезесі

Егер ереже үшін әдепкі әрекет **Сұрау** деп орнатылған болса, диалогтық терезе сол ереже іске қосылған сайын көрсетіледі. Әрекетті **Қабылдамауды** немесе оған **Рұқсат етуді** таңдауға болады. Осы кезде әрекетті таңдамасаңыз, жаңа әрекет ережелерге негізделіп таңдалады.

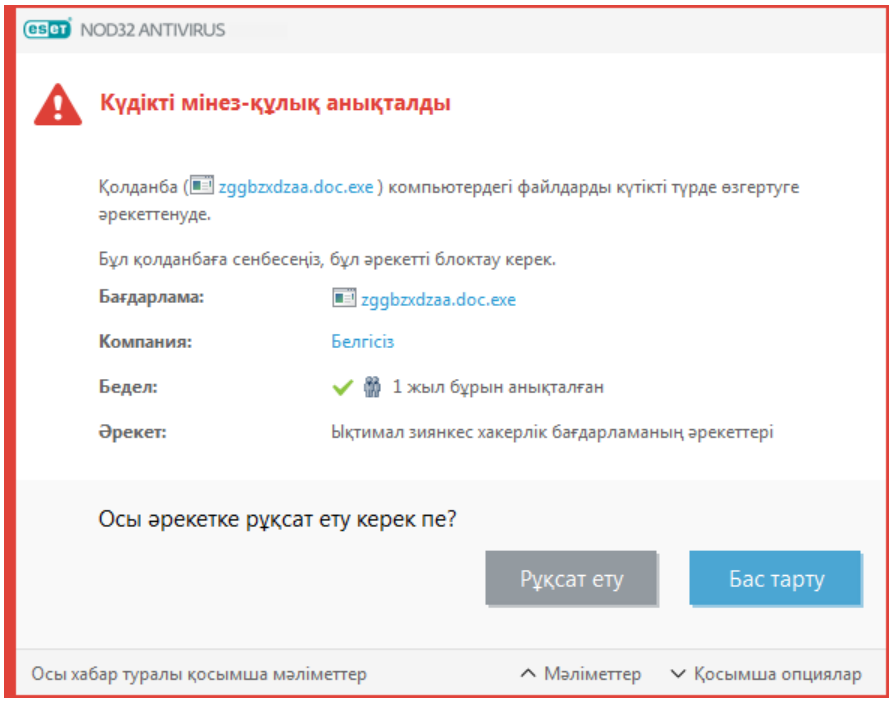


Диалогтық терезе HIPS анықтайтын кез келген жаңа әрекетке негізделген ережені жасап, сол әрекетке рұқсат ететін не тыйым салатын шарттарды анықтауға мүмкіндік береді. Нақты параметрлерге **Мәліметтер** түймесін басу арқылы қатынасуға болады. Осылай жасалған ережелер қолмен жасалған ережелерге тең деп саналады, осылайша диалогтық терезеде жасалған ереженің нақтылығы диалогтық терезені шақырған ережеден азырақ болады. Яғни, мұндай ережені жасағаннан кейін дәл сол әрекет дәл сол терезені шақыруы мүмкін.

Бағдарлама шыққанша есте сақтау ережелердің немесе сүзу режимінің өзгеруіне, HIPS модулінің жаңартылуына немесе жүйе қайта іске қосылғанға дейін қолданылатын әрекетке (**Рұқсат ету**/**Тыйым салу**) әкеледі. Осы үш әрекеттердің бірінен соң, уақытша ережелер өшіріледі.

4.1.4.3 Ықтимал зиянкес хакерлік бағдарламаның әрекеттері анықталды

Бұл интерактивті терезе ықтимал зиянкес хакерлік бағдарламаның әрекеттері анықталғанда пайда болады. Әрекетті **Қабылдамауды** немесе оған **Рұқсат етуді** таңдауға болады.



Бұл диалогтық терезе **файлды талдауға жіберуге** немесе **анықтауға қоспауға** мүмкіндік береді. Арнайы анықтау параметрлерін көру үшін **Мәліметтер** түймешігін басыңыз.

МАҢЫЗДЫ
Зиянкес хакерлік бағдарламалардан қорғау тиісті түрде жұмыс істеуі үшін ESET Live Grid мүмкіндігін қосу керек.

4.1.5 Ойыншы режимі

Ойыншы режимі - бағдарламалық жасақтаманы кедергісіз пайдалануды қажет ететін, қалқымалы терезелердің мазалауын қаламайтын және процессорды пайдалануды барынша азайтқысы келетін пайдаланушыларға арналған мүмкіндік. Сондай-ақ, ойыншы режимі антивирустық әрекеті үзуге мүмкін болмайтын көрсетулер кезінде пайдаланыла алады. Бұл мүмкіндікті қосқанда, барлық қалқымалы терезелер өшіріледі және жоспарлағыш әрекеті толығымен тоқтатылады. Жүйені қорғау әлі де фонда орындалады, бірақ ешбір пайдаланушының араласуын қажет етпейді.

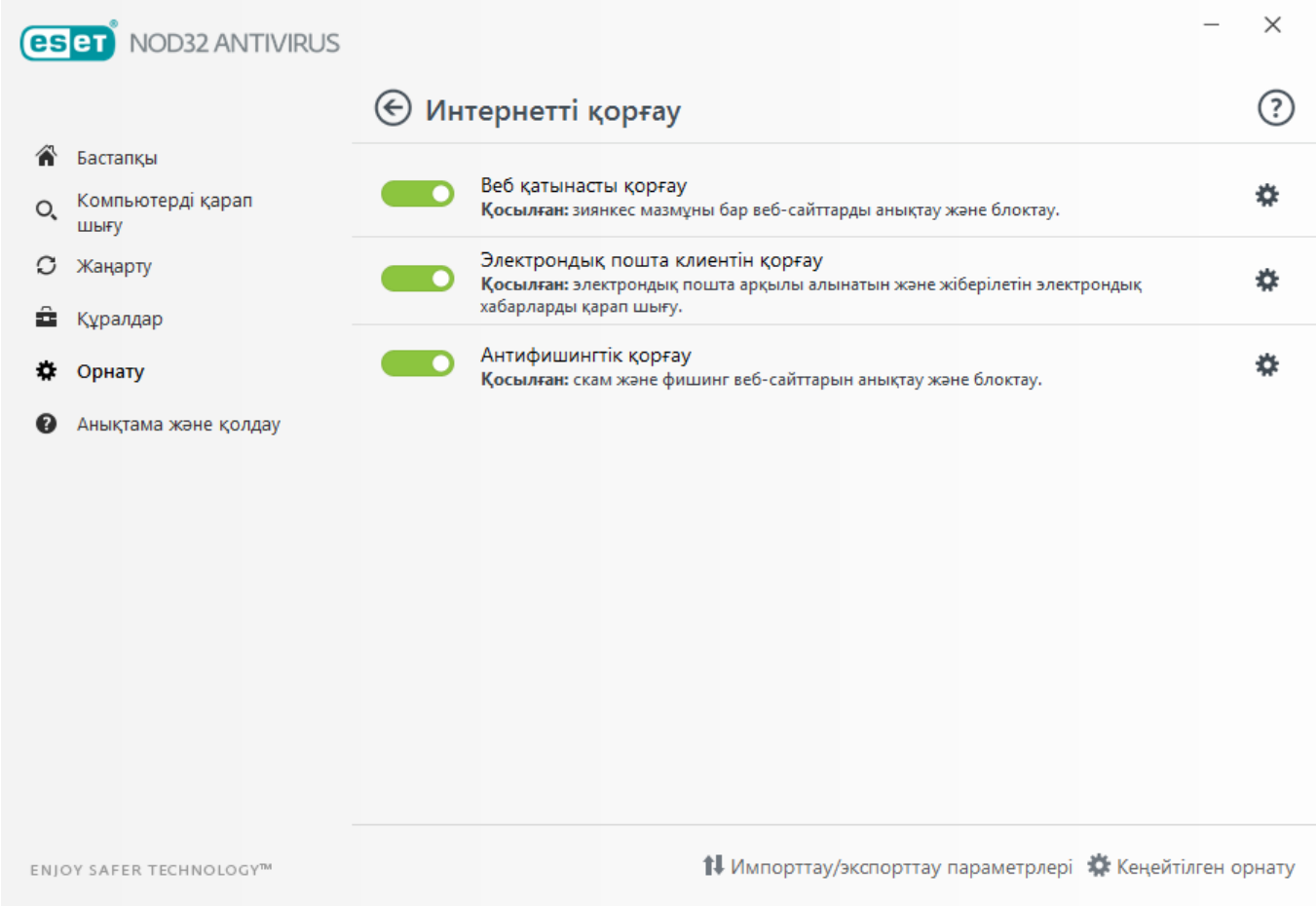
Ойыншы режимін негізгі бағдарлама терезесінде **Орнату** > **Компьютерді қорғау** тармағында немесе параметрін **Ойыншы режимі** жанында басу арқылы қосуға немесе өшіруге болады. Ойыншы режимін қосу қауіпсіздікке ықтимал қауіп болып табылады, сондықтан тапсырмалар тақтасындағы қорғау күйінің белгішесі қызғылт сарыға айналады және ескертуді көрсетеді. Сондай-ақ, бұл ескертуді бағдарламаның негізгі терезесінде көресіз, онда **Ойыншы режимі белсенді** сарғылт түсте көрсетіледі.

Толық экрандық қолданбаны іске қосқанда және қолданбадан шыққаннан кейін тоқтатқанда ойыншы режимі басталуы үшін **Кеңейтілген орнату** (F5) > **Құралдар** тармағында **Қолданбалар толық экранды режимде жұмыс істеп тұрғанда Ойыншы режимінің автоматты түрде қосылуы** параметрін таңдаңыз.

Ойыншы режимі қанша уақыттан кейін автоматты түрде өшірілетінін анықтау үшін **Ойыншы режимін X минуттан кейін автоматты түрде өшіру** опциясын іске қосыңыз.

4.2 Интернетті қорғау

Веб және электрондық пошта конфигурациясын **Орнату** аумағында **Интернетті қорғау** тармағын басу арқылы табуға болады. Осы жерден бағдарламаның егжей-тегжейлі параметрлерін ашуға болады.



Интернетке қосылу мүмкіндігі – жеке компьютерлердегі стандартты мүмкіндік. Өкінішке орай, интернет зиянды кодты тасымалдаудың негізгі құралына айналды. Осыған байланысты, **Веб-қатынасты қорғау** параметрлерін мұқият қарастыру маңызды.

Вебті/электрондық поштаны/антифишингті ашу үшін ⚙ түймесін басыңыз. Кеңейтілген орнатудағы қорғау параметрлері.

Электрондық пошта клиентін қорғау POP3 және IMAP протоколдары арқылы алынатын электрондық пошта байланыстарын бақылауды қамтамасыз етеді. Электрондық пошта клиенті үшін қосылмалы модульді пайдаланып, ESET NOD32 Antivirus электрондық пошта клиентіне немесе электрондық пошта клиенттінен барлық байланыстарын (POP3, MAPI, IMAP, HTTP) бақылауды қамтамасыз етеді.

Антифишингтік қорғау фишинг мазмұнын тарату үшін белгілі веб-беттерді блоктауға мүмкіндік береді. Антифишингті қосылған күйінде қалдыру ұсынылады.

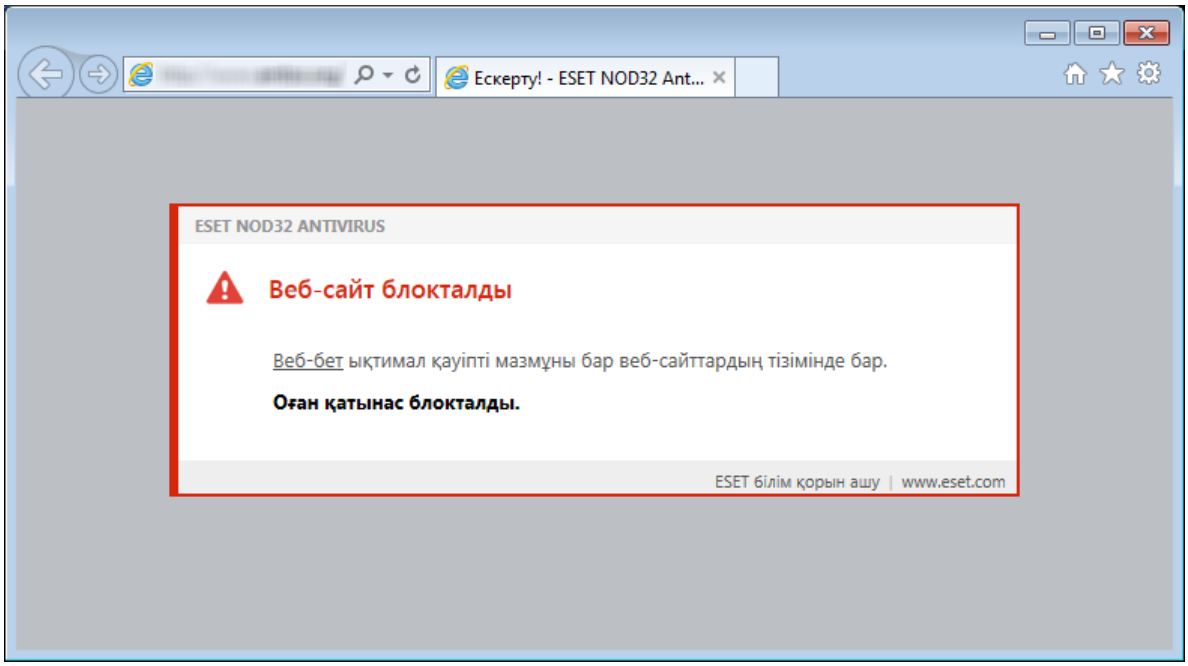
Вебті/электрондық поштаны/антифишингті өшіруге болады  түймесін басу арқылы ажыратуға болады.

4.2.1 Веб қатынасты қорғау

Интернетке қосылу мүмкіндігі – жеке компьютердегі стандартты мүмкіндік. Өкінішке орай, ол, сонымен бірге, зиянды кодты тасымалдаудың негізгі құралына айналды. «Веб-қатынасты қорғау» опциясы веб-браузерлері мен қашықтағы серверлердің арасындағы байланысты қадағалау арқылы жұмыс істеп, «HTTP» (Гипермәтінді беру протоколы) және «HTTPS» (шифрланған байланыс) ережелеріне бағынады.

Зиянкес мазмұн бар екені белгілі веб-беттерге қатынас мазмұн жүктелмей тұрып блокталады. Барлық басқа веб-беттерді жүктелгенде ThreatSense қарап шығу механизмі қарап шығады және зиянкес мазмұн анықталса блокталады. Веб қатынасты қорғау екі қорғау деңгейін ұсынады: қара тізім бойынша блоктау және мазмұн бойынша блоктау.

«Веб-қатынасты қорғау» опциясын қосу қатаң ұсынылады. Бұл опцияға **Орнату** > **Интернетті қорғау** > **Веб-қатынасты қорғау** тармағына өту арқылы ESET NOD32 Antivirus бағдарламасының негізгі терезесінен кіруге болады.



Кеңейтілген орнату (F5) > **Веб және электрондық пошта** > **Веб-қатынасты қорғау** тармағында келесі опциялар қол жетімді:

- **Веб-протоколдар** – интернет браузерлерінің көпшілігі пайдаланатын осы стандартты протоколдар үшін бақылауды конфигурациялауға мүмкіндік береді.
- **URL мекенжайларын басқару** – блоктау, рұқсат ету немесе тексеруге қоспау керек HTTP мекенжайларын көрсетуге мүмкіндік береді.
- **ThreatSense параметрлер** – Вирусты қарап шығу құралын кеңейтілген реттеу – қарап шығатын нысандардың түрлері (электрондық хабарлар, мұрағаттар, т.б.), интернетке қатынасты қорғауға арналған анықтау әдістері, т.б. сияқты параметрлерді конфигурациялауға мүмкіндік береді.

4.2.1.1 Негізгі

Веб-қатынасты қорғауды қосу - өшірілген болса, веб-қатынасты қорғау және антифишингілік қорғау жұмыс істемейді.

Браузер сценарийлерін кеңейтілген қарап шығуды қосу - Қосылған болса, антивирустың қарап шығу құралы интернет браузерлері орындайтын барлық JavaScript бағдарламаларын тексереді.

ЕСКЕРТПЕ
«Веб қатынасты қорғау» опциясын қосылған күйде қалдыру қатаң ұсынылады.

4.2.1.2 Веб-протоколдар

Әдепкі бойынша, ESET NOD32 Antivirus интернет браузерлерінің көпшілігі пайдаланатын HTTP протоколын бақылауға конфигурацияланған.

HTTP сканерін орнату

Windows Vista және одан кейінгі нұсқаларда HTTP трафигі әрқашан барлық бағдарламалар үшін барлық порттарда бақыланады. Windows XP жүйесінде **HTTP протоколы пайдаланатын порттарды Кеңейтілген орнату** (F5) > **Веб және электрондық пошта** > **Веб-қатынасты қорғау** > **Веб-протоколдар** тармағында өзгертуге болады. HTTP трафигі көрсетілген порттарда барлық бағдарламалар үшін және Веб және электрондық пошта клиенттері ретінде белгіленген бағдарламалар үшін барлық порттарда бақыланады.

HTTP сканерін орнату

Сондай-ақ, ESET NOD32 Antivirus бағдарламасы HTTPS протоколын тексеруді қолдайды. HTTPS байланысы ақпаратты сервер мен клиент арасында тасымалдау үшін шифрланған арнаны пайдаланады. ESET NOD32 Antivirus бағдарламасы SSL және TLS шифрлау протоколдарын пайдаланып байланысты тексереді. Бағдарлама операциялық жүйенің нұсқасына қарамастан тек **HTTPS протоколы пайдаланатын порттарда** анықталған порттардағы трафикті қарап шығады.

Шифрланған байланыс қарап шығылмайды. Шифрланған байланысты қарап шығуды қосу және қарап шығу құралының параметрлерін көру үшін «Кеңейтілген орнату» бөлімінде SSL/TLS тармағына өтіңіз де, **Веб және электрондық пошта** > **SSL/TLS** тармағын басып, **SSL/TLS протоколын сүзуді қосу** опциясын қосыңыз.

4.2.1.3 URL мекенжайын басқару

URL мекенжайын басқару бөлімі бұғаттайтын, рқсат ететін немесе тексеруге қоспайтын HTTP мекенжайларын көрсетуге мүмкіндік береді.

Рұқсат етілген мекенжайлар тізіміне қосылмаған болса, **Блокталған мекенжайлар тізіміндегі** веб-сайттарға қатынасу мүмкін болмайды. **Тексеруге қосылмаған мекенжайлар тізіміндегі** веб-сайттарда қатынасқан кезде зиянкес кодтың бар-жоғы қарап шығылмайды.

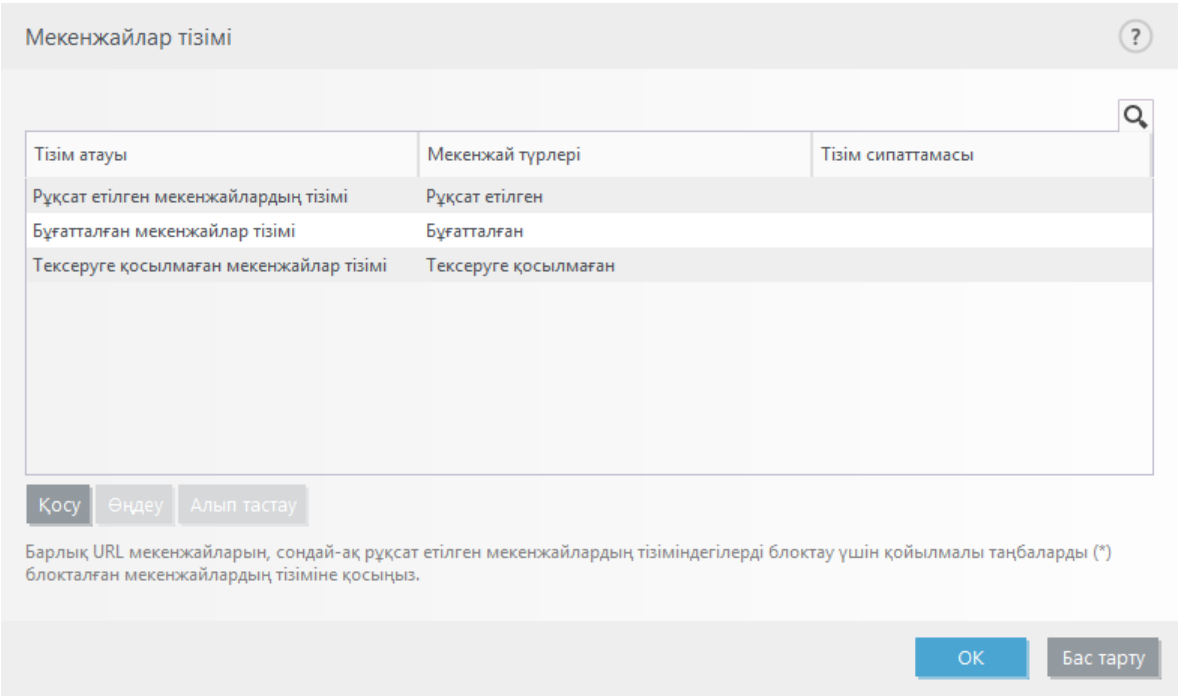
SSL/TLS протоколын сүзуді қосу опциясын HTTP веб-беттеріне қоса HTTPS мекенжайларын сүзу қажет болса таңдау керек. Әйтпесе, сіз кірген HTTPS сайттарының толық URL мекенжайы емес, тек домендері қосылады.

URL мекенжайды **Сүзуден шығарылған мекенжайлар тізімі** ішіне қоссаңыз, мекенжай қарап шығуға қосылмайды. Сондай-ақ, **Рұқсат етілген мекенжайлар тізімі** немесе **Блокталған мекенжайлар тізімі** ішіне қосу арқылы белгілі бір мекенжайларға рұқсат етуге немесе блоктауға болады.

Егер белсенді **Рұқсат етілген мекенжайлар тізімі** ішінде бар мекенжайлардан басқа барлық HTTP мекенжайларын блоктау қажет болса, белсенді **Блокталған мекенжайлар тізіміне** * таңбасын қосыңыз.

* (жұлдызша) және ? арнайы таңбаларын (сұрақ белгісі) арнайы таңбаларын пайдалануға болады. Жұлдызша кез келген таңбалық жолды, ал сұрақ белгісі кез келген таңбаны алмастырады. Қоспаған мекенжайларды көрсеткенде ерекше көңіл бөлу керек, өйткені тізімде тек сенімді және қауіпсіз мекенжайлар болуы керек. Осы сияқты, * және ? таңбаларының осы тізімде дұрыс пайдаланылғанына кепілдік беру керек. Бүкіл доменді, соның ішінде, барлық домендерді қауіпсіз сәйкестендіру әдісін HTTP мекенжайын/домен бүркенішін қосу бөлімінен қараңыз. Тізімді іске қосу үшін **Белсенді тізім** опциясын таңдаңыз. Егер сіз ағымдағы тізімнен мекенжайды енгізгенде хабардар болуды қаласаңыз, **Қолданғанда хабарлау** опциясын қосыңыз.

ЕСКЕРТПЕ
URL мекенжайларын басқару сонымен бірге интернетті шолу кезінде белгілі бір файл түрлерін ашуды блоктауға немесе оған рұқсат етуге мүмкіндік береді. Мысалы, орындалатын файлдардың ашылуын қаламаасңыз, ашылмалы мәзірде осы файлдарды блоктау керек тізімді таңдаңыз да, «**.exe» бүркенішін енгізіңіз.



Басқару элементтері

Қосу – алдын ала анықталғандарына қоса жаңа тізімді жасайды. Бұл әр түрлі мекенжайлар топтарын логикалық түрде бөлу қажет болса пайдалы болуы мүмкін. Мысалы, блокталған мекенжайлардың бір тізімі сыртқы жалпы қара тізімдегі мекенжайларды қамтуы мүмкін, ал екіншісі жеке қара тізімді қамтуы мүмкін. Бұл өзіңіздікіне тимей, сыртқы тізімді жаңартуды оңайырақ етеді.

Өңдеу – бар тізімдерді өзгертеді. Мұны мекенжайларды қосу немесе жою үшін пайдаланыңыз.

Жою – бар тізімді жояды. Әдепкі тізімдер емес, тек **Қосу** көмегімен жасалған тізімдер үшін қол жетімді.

4.2.2 Электрондық пошта клиентін қорғау

4.2.2.1 Электрондық пошта клиенттері

ESET NOD32 Antivirus бағдарламасын электрондық пошта клиентімен біріктіру электрондық пошта хабарларындағы зиянкес кодтан белсенді қорғаудың деңгейін жоғарылатады. Егер электрондық пошта клиентіне қолдау көрсетілсе, біріктіруді ESET NOD32 Antivirus бағдарламасында қосуға болады. Электрондық пошта клиентіне біріктірілген болса, ESET NOD32 Antivirus құралдар тақтасы тікелей электрондық пошта клиентіне кірістіріліп (жаңарақ Windows Live Mail нұсқаларының құралдар тақтасы кірістірілмейді), электрондық поштаны тиімдірек қорғауға мүмкіндік береді. Біріктіру параметрлері **Кеңейтілген орнату** (F5) > **Веб және электрондық пошта** > **Электрондық пошта клиентін қорғау** > **Электрондық пошта клиенттері** тармағында орналасқан.

Электрондық пошта клиентін біріктіру

Қазіргі уақытта қолдау көрсетілетін электрондық пошта клиенттеріне Microsoft Outlook, Outlook Express, Windows Mail және Windows Live Mail кіреді. Электрондық поштаны қорғау осы бағдарламаларға қосылмалы модуль ретінде жұмыс істейді. Қосылмалы модульдің басты артықшылығы – оның пайдаланылатын протоколды талғамайтыны. Электрондық пошта клиенті шифрланған хабарламаны алған кезде, оның шифры шешіледі және вирусты қарап шығу құралына жіберіледі. Қолдау көрсетілетін электрондық пошта клиенттерін және олардың нұсқаларының толық тізімін көру үшін, төмендегі ESET білім қоры мақаласын қараңыз.

Егер біріктіру қосылмаған болса да, Электрондық пошта клиентін қорғау модулі (POP3, IMAP) арқылы электрондық пошта байланысы әлі де қорғалған.

MS Outlook бағдарламасымен жұмыс істегенде жүйе баяуласа, **Кіріс мазмұнын өзгерткеннен кейін тексеруді өшіру** опциясын қосыңыз. Бұл «Kerio Outlook Connector» қорынан электрондық пошта деректерін алу кезінде пайда болуы мүмкін.

Қарап шығарылатын электрондық пошта

Клиенттік қондырмалардың электрондық поштаны қорғауын қосу – Электрондық пошта клиентінің электрондық пошта клиентін қорғауы өшірілген болса, протоколды сүзу арқылы электрондық пошта клиентін қорғау қосулы қалады.
Алынған электрондық пошта – Алынған хабарларды тексеруді ажырата-қосады.
Жіберілген электрондық пошта – Жіберілген хабарларды тексеруді ажырата-қосады.
Оқылған электрондық пошта – Оқылған хабарларды тексеруді ажырата-қосады.

Вирус жұққан электрондық поштаға қатысты орындалатын әрекет

Әрекет жоқ – Қосылған болса, бағдарлама вирус жұққан тіркемелерді анықтайды, бірақ электрондық хабарларды ешбір әрекет орындамай қалдырады.
Электрондық поштаны жою – Бағдарлама пайдаланушыға инфильтрациялар туралы хабарлайды және хабарды жояды.
Электрондық поштаны «Жойылған элементтер» қалтасына жылжыту – Вирус жұққан электрондық хабарлар «Жойылған элементтер» қалтасына автоматты түрде жылжытылады.
Электрондық поштаны қалтаға жылжыту – Вирус жұққан электрондық хабарлар көрсетілген қалтаға автоматты түрде жылжытылады.

Қалта – Анықталған кезінде вирус жұққан электрондық хабарларды жылжытқыңыз келетін теңшелетін қалтаны көрсетіңіз.

Жаңартудан кейін қарап шығуды қайталау – Анықтау механизмін жаңартудан кейін қайта қарап шығуды ажырата-қосады.

Басқа модульдерден қарап шығу нәтижелерін қабылдау – Бұл параметр таңдалған болса, электрондық поштаны қорғау модулі басқа қорғау модульдерінің (POP3, IMAP протоколдарын қарап шығу) қарап шығу нәтижелерін қабылдайды.

ЕСКЕРТПЕ
Клиенттік плагиндер арқылы электрондық поштаны қорғауды қосу және **Протоколды сүзу арқылы электрондық поштаны қорғауды қосу** опцияларын қосу ұсынылады. Бұл параметрлері Кеңейтілген орнату (F5) > Веб және электрондық пошта > Электрондық пошта клиентін қорғау > Электрондық пошта протоколдары тармағында орналасқан.

4.2.2.2 Электрондық пошта протоколдары

IMAP және POP3 протоколдары — электрондық пошта клиенті бағдарламасында электрондық хабарларды алу үшін пайдаланылатын ең кең тараған протоколдар. «Интернет Хабарына Кіру Протоколы» (IMAP) протоколы – электрондық поштаны алуға арналған тағы бір «Интернет протоколы». IMAP протоколында POP3 протоколына қарағанда кейбір артықшылықтары бар, мысалы, бірнеше клиент бір уақытта бір пошта жәшігіне қосылып, хабар оқылғаны, оған жауап берілгені немесе жойылғаны сияқты хабар күйі туралы ақпаратты сақтай алады. ESET NOD32 Antivirus бағдарламасы пайдаланылатын электрондық пошта клиентіне қарамастан және электрондық пошта клиентін қайта конфигурациялауды қажет етпестен осы протоколдар үшін қорғауды қамтамасыз етеді.

Бұл басқаруды қамтамасыз ететін қорғау модулі жүйе іске қосылғанда қосылады, содан кейін жадта белсенді болады. IMAP протоколын бақылау электрондық пошта клиентін қайта конфигурациялаусыз автоматты орындалады. Әдепкі мәні бойынша, 143-порттағы барлық байланыс тексеріледі, бірақ қажет болған жағдайда басқа байланыс порттарын қосуға болады. Бірнеше порт нөмірлерін үтірмен бөлу керек.

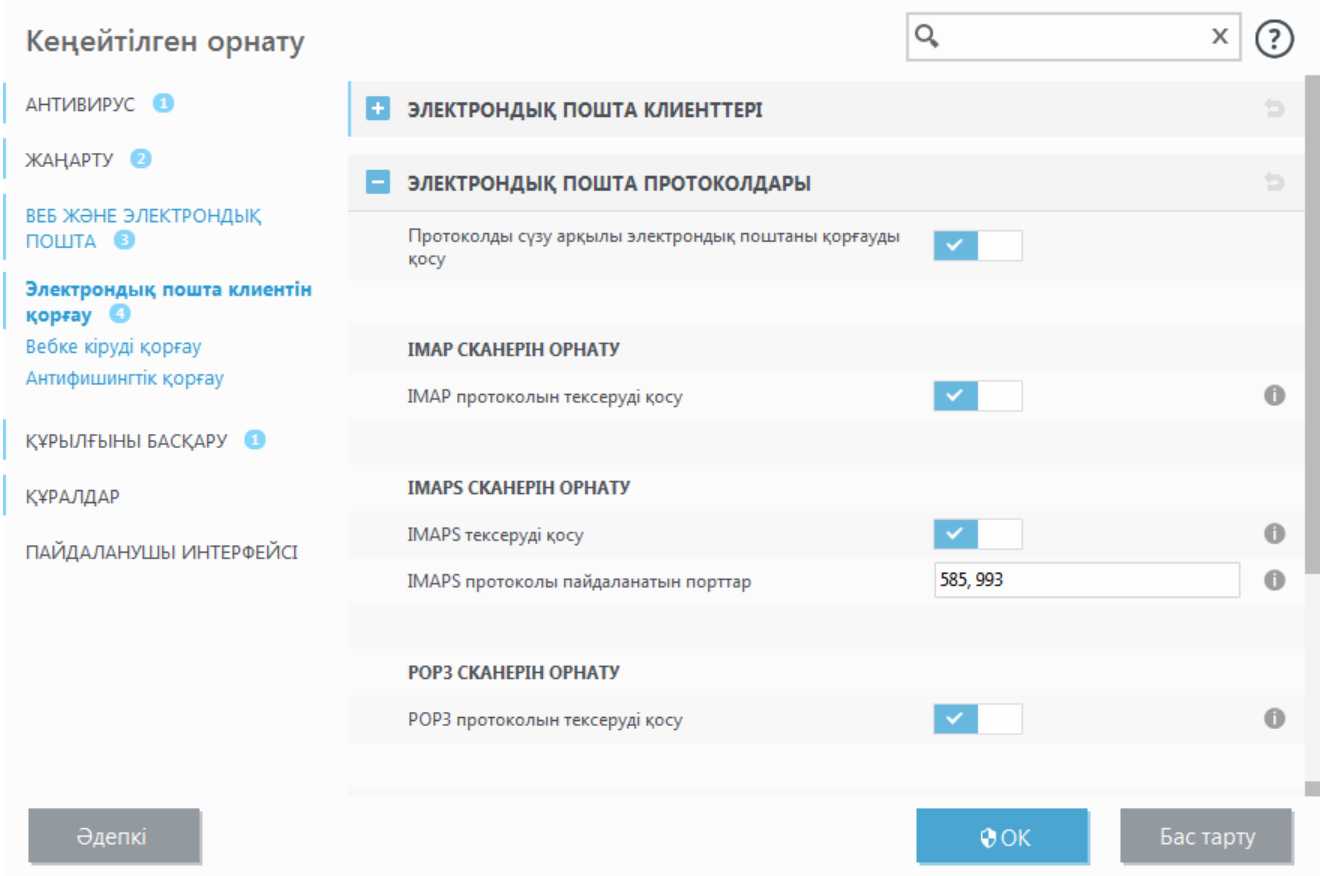
IMAP/IMAPS және POP3/POP3S протоколдарын тексеруді «Кеңейтілген орнату» тармағында конфигурациялауға болады. Бұл параметрге қатынасу үшін **Веб және электрондық пошта** > **Электрондық пошта клиентін қорғау** > **Электрондық пошта протоколдары** тармағын жайыңыз.

Протоколды сүзу арқылы электрондық поштаны қорғауды қосу – Электрондық пошта протоколдарын тексеруді қосады.

Windows Vista және одан кейінгі нұсқаларда IMAP және POP3 протоколдары автоматты түрде анықталады және барлық порттарда қарап шығылады. Windows XP жүйесінде **IMAP/POP3 протоколы пайдаланатын порттар** барлық бағдарламалар үшін қарап шығылады және барлық порттар **Веб және электрондық пошта клиенттері** ретінде белгіленген бағдарламалар үшін қарап шығылады.

ESET NOD32 Antivirus сонымен бірге IMAPS және POP3S протоколдарын қарап шығуды қолдайды. Бұл протоколдар сервер мен клиент арасында ақпаратты тасымалдау үшін шифрланған арнаны пайдаланады. ESET NOD32 Antivirus байланысты SSL және TLS протоколдарын пайдаланып тексереді. Бағдарлама операциялық жүйенің нұсқасына қарамастан тек **IMAPS/POP3S протоколы пайдаланатын порттарда** анықталған порттардағы трафикті қарап шығады.

Шифрланған байланыс қарап шығылмайды. Шифрланған байланысты қарап шығуды қосу және қарап шығу құралының параметрлерін көру үшін «Кеңейтілген орнату» бөлімінде SSL/TLS тармағына өтіңіз де, **Веб және электрондық пошта** > **SSL/TLS** тармағын басып, **SSL/TLS протоколын сүзуді қосу** опциясын қосыңыз.



4.2.2.3 Ескертулер мен хабарландырулар

Электрондық поштаны қорғау POP3 және IMAP протоколдары арқылы алынатын электрондық пошта байланысын бақылауды қамтамасыз етеді. Microsoft Outlook және басқа электрондық пошта клиенттерінің қосылатын модулін пайдаланып, ESET NOD32 Antivirus бағдарламасы электрондық пошта клиентінің барлық қосылымдарын (POP3, MAPI, IMAP, HTTP) басқаруды қамтамасыз етеді. Кіріс хабарларды қарастырғанда, бағдарлама ThreatSense қарап шығу жүйесінде қамтылған кеңейтілген қарап шығу әдістерінің барлығын пайдаланады. Бұл зиянкес бағдарламаларды анықтау тіпті анықтау механизміне қатысты салыстыру алдында орын алатынын білдіреді. POP3 және IMAP протоколдарының байланыстарын қарап шығу пайдаланылатын электрондық пошта клиентіне тәуелсіз.

Бұл функцияның опциялары **Кеңейтілген орнату** ішінде > **Веб және электрондық пошта** > **Электрондық пошта клиентін қорғау** > **Ескертулер мен хабарландырулар** тармағында қол жетімді.

Электрондық пошта тексерілгеннен кейін қарап шығу нәтижелері бар хабарландыруды хабарға бекітуге болады. **Алынған және оқылған вирус жұққан электрондық поштаның тақырыбына жазба бекіту**, **Алынған және оқылған вирус жұққан электрондық поштаның тақырыбына жазба бекіту** немесе **Жіберілген поштаға тег хабарларын бекіту** опциясын таңдауға болады. Сирек жағдайларда тег хабарлары мәселелі HTML хабарларында немесе хабарларды зиянкес бағдарлама жасалған болса өткізіп жіберілуі мүмкін. Тег хабарларын алынған және оқылған электрондық поштаға, жіберілген электрондық поштаға немесе екеуіне де қосуға болады. Мына опциялар қол жетімді:

- **Ешқашан** - Тег хабарлары қосылмайды.
- **Тек вирус жұққан электрондық поштаға** – Тек зиянды бағдарламасы бар хабарлар ғана тексерілген ретінде белгіленеді (әдепкі).
- **Қарап шыққан барлық электрондық поштаға** – Бағдарлама хабарларды бүкіл қарап шыққан электрондық поштаға қосады.

Жіберілген вирус жұққан электрондық поштаның тақырыбына жазба бекіту – электрондық поштаны қорғау вирус жұққан электрондық пошта хабарының тақырыбында вирус туралы ескертуді қамтымауы керек болса, осы құсбелгіні қоймаңыз. Бұл мүмкіндік вирус жұққан электрондық пошта хабарларын қарапайым, тақырыпқа негізделген сүзуге мүмкіндік береді (егер электрондық пошта бағдарламасы қолдаса). Сондай-ақ, ол алушы үшін сенімділік деңгейін жоғарылатады. Инфильтрация анықталса, ол электрондық хабардың немесе жіберушінің қауіп деңгейі туралы құнды ақпаратты қамтамасыз етеді.

Вирус жұққан электрондық поштаның тақырыбына қосылған үлгі – Вирус жұққан электрондық пошта хабарының тақырып префиксінің пішімін өзгерту керек болса, осы үлгіні өзгертіңіз. Бұл функция *"[virus]"* префикс мәні бар *"Hello"* хабар тақырыбын келесі пішімге өзгертеді: *"[вирус] Сәлем"*. *%VIRUSNAME%* айнымалысы анықталған қауіпті білдіреді.

4.2.2.4 Электрондық пошта клиенттерімен біріктіру

ESET NOD32 Antivirus бағдарламасын электрондық пошта клиенттерімен біріктіру электрондық пошта хабарларындағы зиянды кодтан белсенді қорғаудың деңгейін жоғарылатады. Егер электрондық пошта клиентіне қолдау көрсетілсе, біріктіруді ESET NOD32 Antivirus бағдарламасында қосуға болады. Біріктіру іске қосылған кезде ESET NOD32 Antivirus құралдар тақтасы тікелей электрондық пошта клиентіне кірістіріледі. Бұл электрондық поштаны тиімдірек қорғауға мүмкіндік береді. Біріктіру параметрлері **Орнату** > **Кеңейтілген орнату** > **Веб және электрондық пошта** > **Электрондық пошта клиентін қорғау** > **Электрондық пошта клиенттері** тармағында қол жетімді.

Қазіргі уақытта қолдау көрсетілетін электрондық пошта клиенттеріне Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail кіреді. Қолдау көрсетілетін электрондық пошта клиенттерін және олардың нұсқаларының толық тізімін көру үшін, төмендегі ESET білім қоры мақаласын қараңыз.

Электрондық пошта клиентімен жұмыс істегенде жүйе баяуласа, **Кіріс мазмұнын өзгерткеннен кейін тексеруді өшіру** опциясының жанындағы ұяшыққа белгі қойыңыз. Бұл "Kerio Outlook Connector" қорынан электрондық пошта деректерін алу кезінде пайда болуы мүмкін.

Егер біріктіру қосылмаған болса да, Электрондық пошта клиентін қорғау модулі (POP3, IMAP) арқылы электрондық пошта байланысы әлі де қорғалған.

4.2.2.4.1 Электрондық пошта клиентін қорғау конфигурациясы

Электрондық пошта клиентін қорғау модулі келесі электрондық пошта клиенттерін қолдайды: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. Электрондық поштаны қорғау осы бағдарламаларға қосылмалы модуль ретінде жұмыс істейді. Қосылмалы модульдің басты артықшылығы – оның пайдаланылатын протоколды талғамайтыны. Электрондық пошта клиенті шифрланған хабарламаны алған кезде, оның шифры шешіледі және вирусты қарап шығу құралына жіберіледі.

4.2.2.5 POP3, POP3S сүзгісі

POP3 протоколы – электрондық пошта клиенті бағдарламаларында электрондық пошта байланысын алу үшін пайдаланылатын ең кең тараған протокол. ESET NOD32 Antivirus бағдарламасы пайдаланылатын электрондық пошта клиентіне қарамастан осы протокол үшін қорғауды қамтамасыз етеді.

Бұл басқаруды қамтамасыз ететін қорғау модулі жүйе іске қосылғанда қосылады, содан кейін жадта белсенді болады. Модуль дұрыс жұмыс істеу үшін ол қосылғандығын тексеріңіз — POP3 протоколын тексеру электрондық пошта клиентін қайда конфигурациялауды сұрамай-ақ автоматты түрде орындалады. Әдепкі мәні бойынша, 110-порттағы барлық байланыс тексеріледі, бірақ қажет болған жағдайда басқа байланыс порттарын қосуға болады. Бірнеше порт нөмірлерін үтірмен бөлу керек.

Шифрланған байланыс қарап шығылмайды. Шифрланған байланысты қарап шығуды қосу және қарап шығу құралының параметрлерін көру үшін «Кеңейтілген орнату» бөлімінде SSL/TLS тармағына өтіңіз де, **Веб және электрондық пошта** > **SSL/TLS** тармағын басып, **SSL/TLS протоколын сүзуді қосу** опциясын қосыңыз.

Бұл бөлімде POP3 және POP3S хаттамаларын тексеруді қайта конфигурациялауға болады.

POP3 протоколын тексеруді қосу - Егер қосылған болса, POP3 хаттамасы арқылы өтетін трафик зиянкес бағдарламалардың болуына тексеріледі.

POP3 протоколы пайдаланатын порттар - POP3 протоколы пайдаланатын порттар тізімі (әдепкі мәні бойынша 110).

ESET NOD32 Antivirus бағдарламасы, сондай-ақ «POP3S» протоколын тексеруді қолдайды. Бұл байланыс түрі ақпаратты сервер мен клиент арасында беру үшін шифрланған арнаны пайдаланады. ESET NOD32 Antivirus бағдарламасы SSL (Қорғалған ұяшықтар протоколы) және TLS (Тасымалдау қауіпсіздігі) шифрлау әдістерін пайдалана отырып, байланысты тексереді.

POP3S протоколын тексеруді пайдаланбау - Шифрланған байланыс тексерілмейді.

Таңдалған порттар үшін POP3S протоколын тексеруді пайдалану — POP3S протоколы пайдаланатын порттар ішінде анықталған порттар үшін ғана POP3S протоколын тексеруді қосу үшін осы опцияға құсбелгі қойыңыз.

POP3S протоколы пайдаланатын порттар - Тексерілетін POP3S порттарының тізімі (әдепкі мәні бойынша 995).

4.2.3 Протоколды сүзу

Бағдарлама протоколдарына арналған антивирус қорғауы барлық зиянды бағдарламаларды қарап шығудың кеңейтілген әдістерін біркелкі біріктіретін ThreatSense қарап шығу механизмі арқылы қамтамасыз етіледі. Протоколды сүзу пайдаланылатын интернет браузеріне немесе электрондық пошта клиентіне қарамастан автоматты түрде жұмыс істейді. Шифрланған (SSL/TLS) параметрлерді өңдеу үшін **Веб және электрондық пошта** > **SSL/TLS** тармағына өтіңіз.

Бағдарламалық протокол мазмұнын сүзуді қосу – протоколды сүзуді өшіру үшін пайдалануға болады. Көп ESET NOD32 Antivirus компоненттері (Веб-қатынасты қорғау, Электрондық пошта протоколдарын қорғау, Антифишинг, Веб-басқару) осыған тәуелді екенін және онсыз қызмет етпейтінін ескеріңіз.

Қосылмаған қолданбалар – белгілі бір қолданбаларды протоколды сүзуге қоспауға мүмкіндік береді. Протоколды сүзу үйлесімділік мәселелерін тудырғанда пайдалы.

Қосылмаған IP мекенжайлары – белгілі бір қашықтағы мекенжайларды протоколды сүзуге қоспауға мүмкіндік береді. Протоколды сүзу үйлесімділік мәселелерін тудырғанда пайдалы.

Веб және электрондық пошта клиенттері – тек Windows XP операциялық жүйелерінде пайдаланылады, пайдаланылатын порттарға қарамастан протоколды сүзу бүкіл трафикті сүзетін бағдарламаларды таңдауға мүмкіндік береді.

4.2.3.1 Веб және электрондық пошта клиенттері

ЕСКЕРТПЕ
Windows Vista 1-жаңарту бумасымен және Windows Server 2008 бағдарламасымен іске қосылатын жаңа Windows сүзу платформасы (WFP) желі байланысын тексеру үшін пайдаланылады. WFP технологиясы арнайы басқару әдістерін пайдаланатындықтан, **Веб және электрондық пошта клиенттері** бөлімі қол жетімді емес.

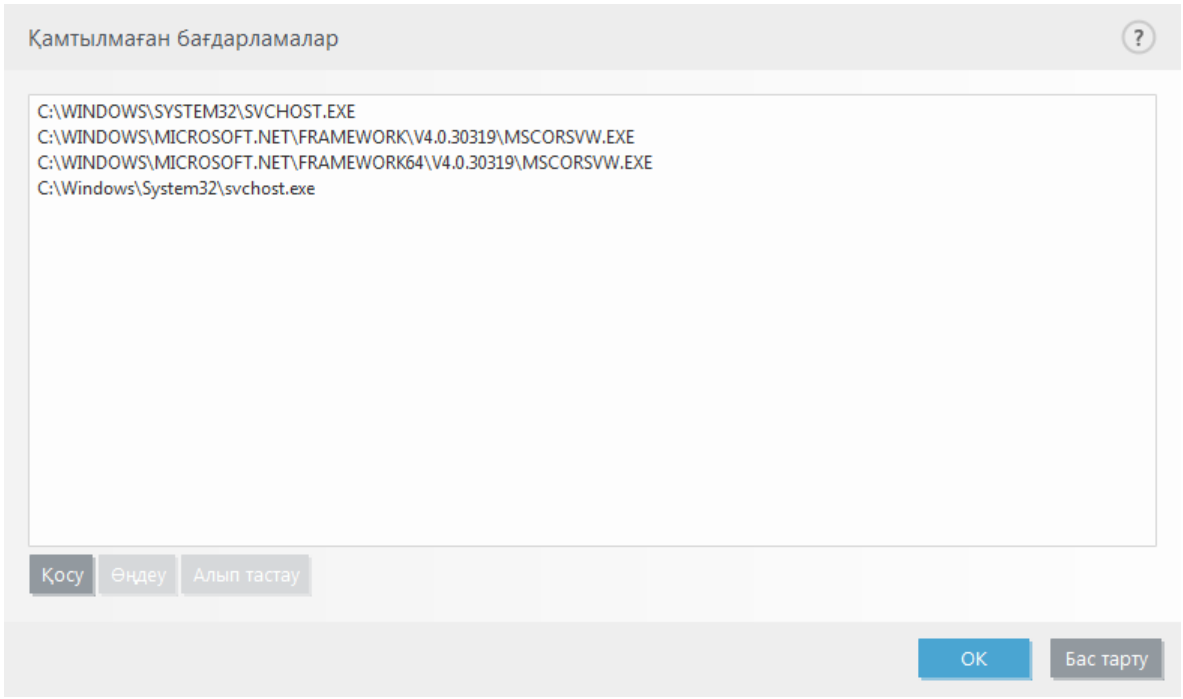
Интернетте сансыз көп зиянды кодтар таралғандықтан, қауіпсіз интернет шолу әрекеті компьютерді қорғау тұрғысынан аса маңызды болып табылады. Веб-браузердің сезімталдығы мен жалған сілтемелер зиянды кодтың жүйеге білдіртпей кіруіне септігін тигізеді, осы себепті ESET NOD32 Antivirus бағдарламасы веб-браузердің қауіпсіздігіне баса назар аударады. Желіге қатынайтын әрбір бағдарлама интернет браузері ретінде белгілене алады. Ұяшыққа белгі қоюдың екі күйі бар:

- **Таңдау алынып тасталған** — Бағдарламалардың байланысы тек көрсетілген порттарға сүзіледі.
- **Таңдалған** — Байланыс әрқашан (тіпті әр түрлі порт орнатылса да) сүзіледі.

4.2.3.2 Қамтылмаған бағдарламалар

Белгілі бір желіні пайдаланатын бағдарламалардың қосылымын мазмұнды сүзуге қоспау үшін оларды тізімде таңдаңыз. Таңдалған бағдарламалардың HTTP/POP3/IMAP байланысында қауіптердің бар-жоғы тексерілмейді. Бұл опцияны тек тексерілетін байланысымен тиісті түрде жұмыс істемейтін бағдарламалар үшін ғана пайдалану ұсынылады.

Орындалып жатқан бағдарламалар мен қызметтер мұнда автоматты түрде қол жетімді болады. Протоколды сүзу тізімінде көрсетілмеген бағдарламаны қолмен қосу үшін **Қосу** түймесін басыңыз.

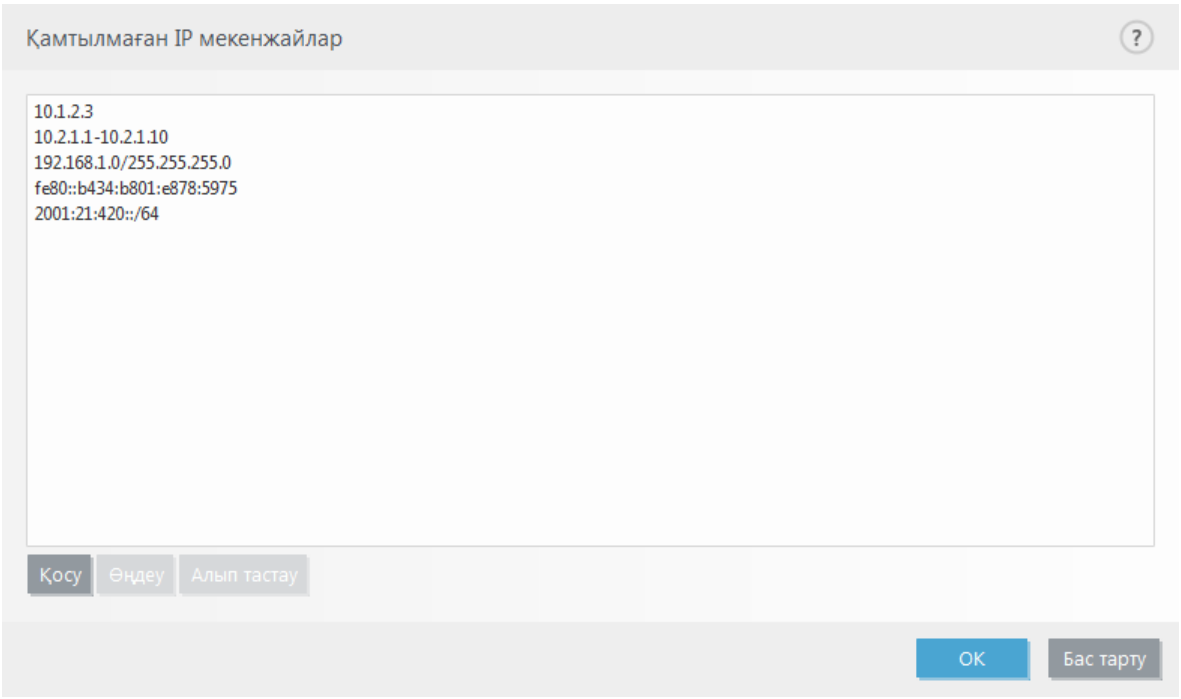


4.2.3.3 Қамтылмаған IP мекенжайлар

Тізімдегі жазбалар протокол мазмұнын сүзуден шектеледі. Таңдалған мекенжайлардың HTTP/POP3/IMAP байланысында қауіптер бар-жоғы тексерілмейді. Осы опцияны тек сенімді мекенжайларға ғана пайдалануды ұсынамыз.

Протокол сүзу тізімінде көрсетілмеген қашықтағы нүктенің IP мекенжайын/мекенжайлар ауқымын/ішкі желісін шығару үшін **Қосу** түймесін басыңыз.

Таңдалған жазбаларды тізімінен жою үшін **Жою** түймесін басыңыз.



4.2.3.3.1 IPv4 мекенжайын қосу

Бұл ереже қолданылатын қашықтағы нүктенің IP мекенжайын/мекенжай ауқымын/ішкі желісін қосуға мүмкіндік береді. Internet Protocol протоколының 4-нұсқасы ескірген, бірақ әлі де неғұрлым кеңінен қолданылатын нұсқа болып табылады.

Бір мекенжай - Ереже қолданылатын жеке бір компьютердің IP мекенжайын қосады (мысалы, *192.168.0.10*).

Мекенжайлар ауқымы - Ереже қолданылатын IP ауқымын (бірнеше компьютердің) көрсету үшін бірінші және соңғы IP мекенжайын енгізіңіз (мысалы, *192.168.0.1* және *192.168.0.99* аралығы).

Ішкі желі - Ішкі желі (компьютерлер тобы) IP мекенжайы мен бүркеніш бойынша анықталады.

Мысалы, *255.255.255.0 – 192.168.1.1* және *192.168.1.254* мекенжайлар ауқымын білдіретін *192.168.1.0/24* префиксі үшін желілік бүркеніш.

4.2.3.3.2 IPv6 мекенжайын қосу

Бұл ереже қолданылатын қашықтағы нүктенің IPv6 мекенжайын/ішкі желісін қосуға мүмкіндік береді. Бұл Интернет хаттамасының ең жаңа нұсқасы және алдыңғы 4-нұсқаның орнын басады.

Бір мекенжай - Ереже қолданылатын жеке бір компьютердің IP мекенжайын қосады (мысалы, *2001:718:1c01:16:214:22ff:fec9:ca5*).

Ішкі желі - Ішкі желі (компьютерлер тобы) IP мекенжайы мен бүркеніш бойынша анықталады (мысалы: *2002:c0a8:6301:1::1/64*).

4.2.3.4 SSL/TLS

ESET NOD32 Antivirus SSL протоколын пайдаланатын байланыстарды қауіптер бар-жоғын тексере алады. Сенімді куәліктер, белгісіз куәліктер немесе SSL арқылы қорғалған байланыстарды тексеруден шығарылған куәліктерді пайдаланатын SSL арқылы қорғалған байланыстар үшін түрлі қарап шығу режимдерін пайдалануыңызға болады.

SSL/TLS протоколын сүзуді қосу – егер протоколды сүзу өшірілсе, бағдарлама SSL арқылы болатын байланыстарды қарап шықпайды.

SSL/TLS протоколын сүзу режимі келесі опцияларда қол жетімді:

Автоматты режим - әдепкі режим тек веб-шолғыштар және электрондық пошта клиенттері сияқты тиісті қолданбаларды қарап шығады. Мұны байланыстар қарап шығылатын қолданбаларды таңдау арқылы қайта анықтауға болады.

Интерактивті режим – егер жаңа SSL арқылы қорғалған сайтқа (белгісіз куәлігі бар) кірсеңіз, әрекет таңдау диалогтық терезесі көрсетіледі. Бұл режим қарап шығуға қосылмайтын SSL куәліктерінің/қолданбалардың тізімін жасауға мүмкіндік береді.

Саясат режимі – тексеруге қосылмаған куәліктермен қорғалған байланыстардан басқа барлық SSL арқылы қорғалған байланыстарды қарап шығу үшін осы опцияны таңдаңыз. Егер белгісіз, қол қойылған куәлікті пайдаланатын жаңа қосылым орнатылса, сізге хабарландыру берілмейді және қосылым автоматты түрде сүзіледі. Сенімді деп белгіленген (ол сенімді куәліктер тізімінде) сенімсіз куәлік бар серверге қатынасқанда сервермен байланысқа рұқсат етіледі және байланыс арнасының мазмұны сүзіледі.

SSL сүзілетін қолданбалардың тізімі - белгілі бір қолданбалар үшін ESET NOD32 Antivirus мінез-құлқын теңшеуге мүмкіндік береді.

Белгілі куәліктер тізімі — ESET NOD32 Antivirus мінез-құлқын белгілі бір SSL куәліктері үшін теңшеуге мүмкіндік береді.

Кеңейтілген тексеру сертификаттарымен (EV) қорғалған байланысты қоспау — қосылған болса, SSL куәлігінің осы түрі бар байланыс тексеруге қосылмайды. Кеңейтілген тексеру SSL куәліктері сіздікі сияқты көрінетін жалған сайт (фишингілік сайттарға тән) емес, шынымен өз веб-сайтыңызды көріп жатқаныңызды қамтамасыз етеді.

Шифрланған байланысты ескірген SSL v2 протоколы арқылы блоктау – SSL протоколының ертерек нұсқасын пайдаланатын байланыс автоматты түрде блокталады.

Түбірлік куәлік

Түбірлік куәлікті белгілі шолғыштарға қосу — SSL байланысы браузерде/электрондық пошта клиенттерінде дұрыс жұмыс істеуі үшін ESET жүйесіне арналған түбірлік куәлікті белгілі түбірлік куәліктер (жариялаушылар) тізіміне қосу маңызды болып табылады. Қосылған болса, ESET NOD32 Antivirus ESET түбірлік куәлігін белгілі браузерлерге (мысалы, Opera және Firefox) автоматты түрде қосады. Жүйелік куәліктер қорын пайдаланатын браузерлерде куәлік автоматты түрде қосылады (мысалы, Internet Explorer).

Куәлікті қолдау көрсетілмейтін браузерлерге қолдану үшін **Куәлікті көру** > **Мәліметтер** > **Файлға көшіру...** тармағын таңдаңыз және оны браузерге қолмен импорттаңыз.

Куәлік жарамдылығы

Егер куәлікті TRCA куәліктер қоймасын пайдаланып тексеру мүмкін болмаса – кейбір жағдайларда, веб-сайттың куәлігін Trusted Root Certification Authorities (TRCA) қоймасын пайдаланып тексеру мүмкін емес. Яғни, куәлікке біреу (мысалы, веб-сервердің әкімшісі немесе шағын компания) өзі қол қойған және бұл куәлікті сенімді деп есептеу кейде қауіпті болып табылмайды. Үлкен компаниялардың көпшілігі (мысалы, банктер) «TRCA» қол қойған куәлікті пайдаланады. **Куәліктің заңдық күші туралы сұрау** таңдалса (әдепкіше таңдалса), пайдаланушыға шифрланған байланыс орнатылғанда орындау керек әрекетті таңдау ұсынылады. Куәліктері тексерілмеген сайттармен шифрланған байланыстарды әрқашан тоқтату үшін **Осы куәлікті пайдаланатын байланысты блоктау** опциясын таңдауға болады.

Егер куәлік жарамсыз немесе бүлінген болса – бұл куәлік мерзімі біткенін немесе дұрыс емес қол қойылғанын білдіреді. Бұл жағдайда, **Осы куәлікті пайдаланатын байланысты блоктау** опциясын таңдалған күйде қалдыру ұсынылады.

4.2.3.4.1 Куәліктер

«SSL» байланысының браузерінде/электрондық пошта клиентінде дұрыс жұмыс істеу үшін ESET жүйесіне арналған түбір куәлікті белгілі түбір куәліктер (жариялаушылар) тізіміне қосу маңызды болып табылады. **Түбір куәлікті белгілі браузерлерге қосу** опциясын қосу керек. ESET түбір куәлігін белгілі браузерлерге (мысалы, Opera және Firefox) автоматты түрде қосу үшін осы параметрді таңдаңыз. Жүйелік куәліктер қорын пайдаланатын браузерлерге куәлік автоматты түрде қосылады (мысалы, Internet Explorer). Куәлікті қолданылмайтын браузерлерге қолдану үшін **Куәлікті көру** > **Егжей-тегжейлі мәліметтер** > **Файлға көшіру...** түймесін таңдаңыз және оны браузерге қолмен импорттаңыз.

Кейбір жағдайларда, куәліктерді Сертификаттау жөніндегі сенімді түбір орталықтарының қорын (мысалы, VeriSign) пайдалана отырып, тексеру мүмкін емес. Яғни, куәлікке біреу (мысалы, веб-сервердің әкімшісі немесе шағын бизнес компаниясы) өзі қол қойған және бұл куәлікті сенімді деп есептеу әрқашан қауіпті болып табылмайды. Үлкен бизнес компанияларының көпшілігі (мысалы, банктер) «TRCA» қол қойған куәлікті пайдаланады. **Куәліктің заңдық күші туралы сұрау** таңдалса (әдепкіше таңдалса), пайдаланушыға шифрланған байланыс орнатылғанда орындау керек әрекетті таңдау ұсынылады. Әрекетті таңдау диалогтық терезесі көрсетіледі. Онда куәлікті сенімді немесе қосылмаған ретінде белгілеуді таңдауға болады. Куәлік TRCA тізімінде болмаса, терезе *қызыл* болады. Куәлік TRCA тізімінде болса, терезе *жасыл* болады.

Тексерілмеген куәлікті пайдаланатын сайтқа шифрланған қосылымды әрқашан тоқтату үшін **Куәлікті пайдаланатын байланысты блоктау** опциясын таңдауға болады.

Егер куәлік жарамсыз немесе бүлінген болса, куәліктің мерзімі біткен немесе дұрыс емес өзіндік қол қойылған. Бұл жағдайда, куәлікті пайдаланатын қосылымды бұғаттау ұсынылады.

4.2.3.4.1.1 Шифрланған желі трафигі

Егер компьютер SSL протоколын қарап шығатын етіп конфигурацияланса, шифрланған байланыс орнатуға (белгісіз куәлікті пайдалана отырып) әрекет жасалғанда, бір әрекетті таңдауыңызды сұрайтын диалогтық терезе ашылуы мүмкін.

Диалогтық терезеде мынадай ақпарат болады:

- байланысты бастаған қолданбаның атауы
- пайдаланылған куәліктің атауы
- орындалатын әрекет - шифрланған байланысты қарап шығу-шықпау және қолданба/куәлік үшін әрекетті есте сақтау-сақтамау

Егер куәлік сенімді түбірлік куәліктендіру органдарының қоймасында (TRCA) болмаса, ол сенімсіз деп есептеледі.

4.2.3.4.2 Белгілі куәліктердің тізімі

Белгілі куәліктердің тізімін белгілі бір SSL куәліктері үшін ESET NOD32 Antivirus мінез-құлқын теңшеу және **SSL/TLS протоколын сүзу режимінде Интерактивті режим** таңдалса, таңдалған әрекеттерді есте сақтау үшін пайдалануға болады. Бұл тізімді **Кеңейтілген орнату** (F5) > **Веб және электрондық пошта** > **SSL/TLS** > **Белгілі куәліктердің тізімі** тармағында көруге және өңдеуге болады.

Белгілі куәліктердің тізімі терезесі мыналардан тұрады:

Бағандар

Атау – куәліктің атауы.

Куәлікті шығарушы – куәлік жасаушының аты.

Куәлік тақырыбы – тақырып өрісі тақырып жалпы кілт өрісінде сақталған жалпы кілтпен байланысты мекемені анықтайды.

Қатынасу – сенімділігіне қарамастан осы куәлікпен қорғалған байланысқа рұқсат ету/оны блоктау үшін **Рұқсат ету** немесе **Блоктау** пәрменін **Қатынасу әрекеті** ретінде таңдаңыз. Сенімді куәліктерге рұқсат ету және сенімді еместері үшін сұрау үшін **Автоматты** опциясын таңдаңыз. Әрқашан пайдаланушыдан не істеу керек екенін сұрау үшін **Сұрау** опциясын таңдаңыз.

Қарап шығу – осы куәлікпен қорғалған байланысты қарап шығу немесе елемеу үшін **Қарап шығу** немесе **Елемеу** пәрменін **Қарап шығу әрекеті** ретінде таңдаңыз. Автоматты режимде қарап шығу және интерактивті

режимде сұрау үшін **Автоматты** опциясын таңдаңыз. Әрқашан пайдаланушыдан не істеу керек екенін сұрау үшін **Сұрау** опциясын таңдаңыз.

Басқару элементтері

Қосу – Жаңа сертификатты қосу және оның қатынасу және қарап шығу опцияларына қатысты параметрлерін реттеу.

Өңдеу – конфигурациялау керек куәлікті таңдап, **Өңдеу** түймесін басыңыз.

Жою – жою керек куәлікті таңдап, **Жою** түймесін басыңыз.

OK/бас тарту – өзгертулерді сақтау керек болса, **OK** түймесін немесе сақтаусыз шығу керек болса, **Бас тарту** түймесін басыңыз.

4.2.3.4.3 SSL/TLS сүзілетін қолданбалардың тізімі

SSL/TLS сүзілетін қолданбалардың тізімін белгілі бір қолданбалар үшін ESET NOD32 Antivirus мінез-құлқын теңшеу және **SSL/TLS протоколын сүзу режимінде Интерактивті режим** таңдалса, таңдалған әрекеттерді есте сақтау үшін пайдалануға болады. Бұл тізімді **Кеңейтілген орнату** (F5) > **Веб және электрондық пошта** > **SSL/TLS** > **SSL/TLS сүзілетін қолданбалардың тізімі** тармағында көруге және өңдеуге болады.

SSL/TLS сүзілетін қолданбалардың тізімі терезесі мыналардан тұрады:

Бағандар

Қолданба – қолданбаның атауы.

Қарап шығу әрекеті – Байланысты қарап шығу немесе елемеу үшін **Қарап шығу** немесе **Елемеу** пәрменін таңдаңыз. Автоматты режимде қарап шығу және интерактивті режимде сұрау үшін **Автоматты** опциясын таңдаңыз. Әрқашан пайдаланушыдан не істеу керек екенін сұрау үшін **Сұрау** опциясын таңдаңыз.

Басқару элементтері

Қосу – сүзілетін қолданбаны қосу.

Өңдеу – конфигурациялау керек куәлікті таңдап, **Өңдеу** түймесін басыңыз.

Жою – жою керек куәлікті таңдап, **Жою** түймесін басыңыз.

OK/бас тарту – өзгертулерді сақтау керек болса, **OK** түймесін немесе сақтаусыз шығу керек болса, **Бас тарту** түймесін басыңыз.

4.2.4 Антифишингтік қорғау

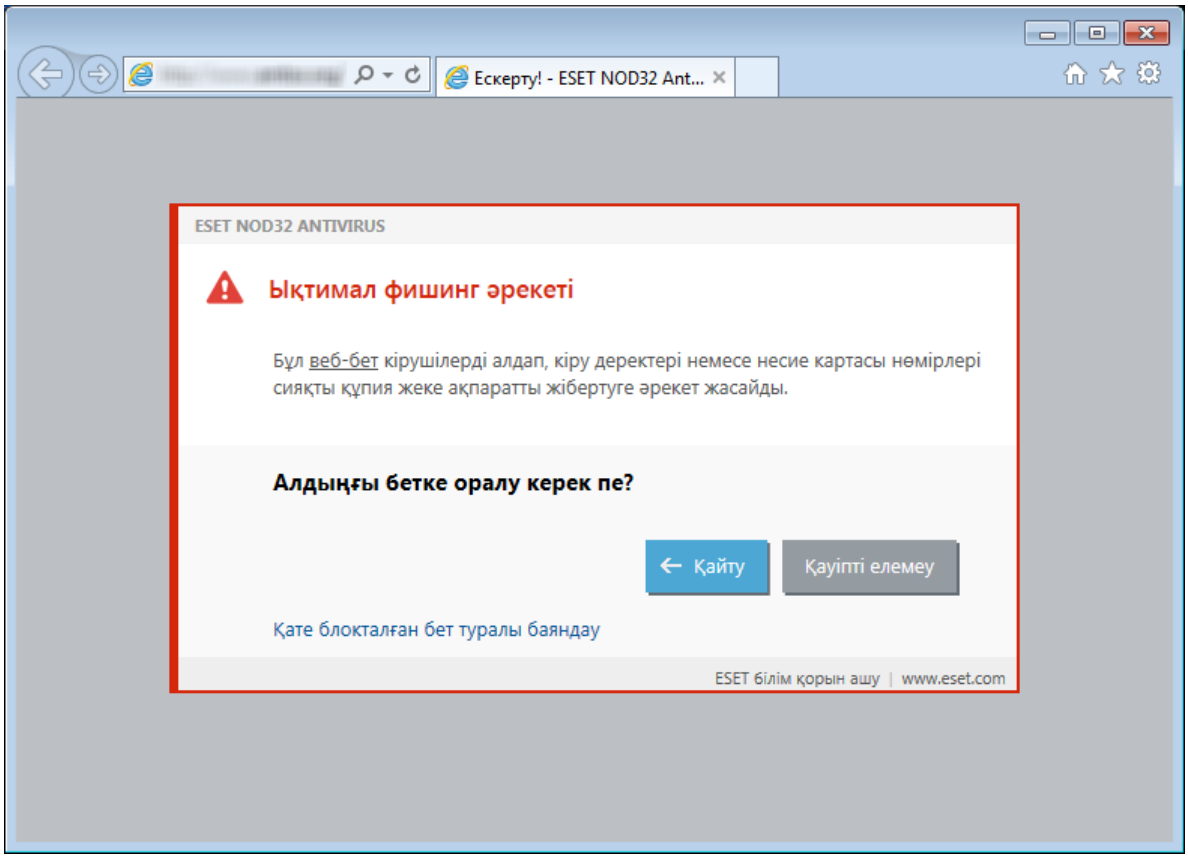
Фишинг термині қоғамдық техниканы (құпия ақпаратты алу үшін пайдаланушылардың әрекеті) пайдаланатын қылмыстық әрекетті білдіреді. Фишинг банктік есеп-шот нөмірлері, PIN-коды нөмірлері және басқалары секілді құпия деректерге кіру үшін жиі қолданылады. Осы әрекет туралы қосымша мәлімет үшін глоссарийді қараңыз. ESET NOD32 Antivirus бағдарламасы фишингке қарсы қорғанысты қамтамасыз етеді және осы мазмұнды тарататын белгілі веб-сайттарды блоктайды.

ESET NOD32 Antivirus бағдарламасында фишингке қарсы мүмкіндікті қосуды ұсынамыз. Бұлай істеу үшін **Кеңейтілген орнату** (F5) тармағын ашып, **Веб және электрондық пошта** > **Антифишингтік қорғау** тармағына өтіңіз.

ESET NOD32 Antivirus бағдарламасындағы Антифишингтік қорғау туралы қосымша ақпарат алу үшін Білім қорының мақаласына кіріңіз.

Фишингті веб-сайтқа кіру

Танылған фишингтік веб-сайтқа кіргенде веб-браузерде келесі диалогтық терезе көрсетіледі. Веб-сайтқа бәрібір кіргіңіз келсе, **Қауіпті елемеу** сілтемесін басыңыз *(ұсынылмайды)*.



ЕСКЕРТПЕ

Ақ тізімге қосылған ықтимал фишингті веб-сайттарға кіру, әдепкіге сай, бірнеше сағаттан соң аяқталады. Веб-сайтқа ұзақ уақытқа рұқсат беру үшін URL мекенжайын басқару құралын пайдаланыңыз. **Кеңейтілен орнату** (F5) тармағында **Веб және электрондық пошта** > **Веб-қатынасты қорғау** > **URL мекенжайын басқару** > **Мекенжайлар тізімі** тармағын кеңейтіп, **Өңдеу** түймешігін басыңыз, содан кейін қажет веб-сайтты тізімге қосыңыз.

Фишингті сайтты хабарлау

Есеп беру сілтемесі талдау үшін ESET компаниясына фишингтік/зиянкес веб-сайт туралы есеп беруге мүмкіндік береді.

ЕСКЕРТПЕ

ESET компаниясына жібермес бұрын мына шарттартын біріне не бірнешеуіне сай екендігін тексеріңіз:

- тіпті веб-сайт ашылмады,
- веб-сайт қауіп түрінде қате ашылды. Бұл жағдайда Қате блокталған бет туралы есеп беру әрекетін орындауға болады.

Сондай-ақ, веб-сайтты электрондық пошта арқылы жібере аласыз. Электрондық пошта хабарын samples@eset.com мекенжайына жіберіңіз. Сипаттағыш тақырыпты пайдаланыңыз және мүмкіндігінше веб-сайт туралы толығырақ ақпарат (мысалы, веб-сайт мына мекенжайдан жіберілді, бұл веб-сайт туралы қайдан білдіңіз...) енгізіңіз.

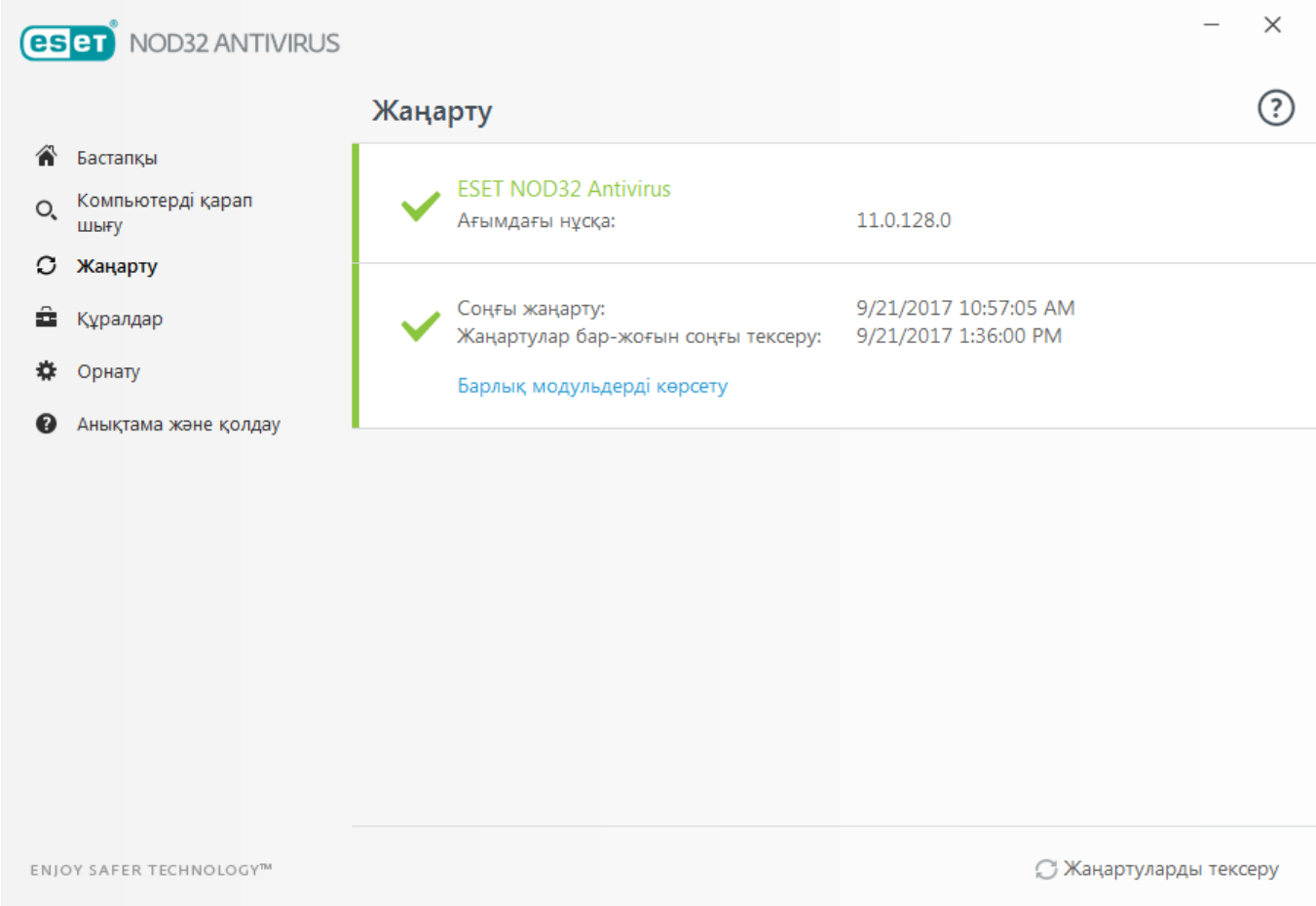
4.3 Бағдарламаны жаңарту

ESET NOD32 Antivirus бағдарламасын тұрақты түрде жаңарту – компьютерде қауіпсіздіктің ең жоғары деңгейін тексерудің ең жақсы әдісі. Жаңарту модулі бағдарлама модульдерінің де, жүйе құрамдастарының да әрдайым жаңартылған күйде болуын қамтамасыз етеді.

Негізгі бағдарлама терезесінде **Жаңарту** командасын таңдау арқылы ағымдағы жаңарту күйін, соның ішінде соңғы сәтті жаңартудың күні мен уақытын көруге және жаңарту керектігін не керек еместігін анықтауға болады.

Автоматты жаңартуларға қоса, қолмен жаңартуды іске қосу үшін **Жаңартулар бар-жоғын тексеру** пәрменін басуға болады. Бағдарлама модульдері мен құрамдастарын жүйелі түрде жаңартып тұру зиянкес кодтан толық қорғауды сақтаудың маңызды аспектісі болып табылады. Олардың конфигурациясына және әрекетіне назар аударыңыз. Жаңартуларды алу үшін лицензиялық кілтті пайдаланып өнімді белсендіру керек. Егер орнату кезінде мұны істемесеңіз, ESET жаңарту серверлеріне қатынасу үшін жаңартып жатқанда өнімді белсендіру үшін лицензиялық кілтті енгізуге болады.

ЕСКЕРТПЕ
Лицензиялық кілт ESET NOD32 Antivirus бағдарламасын сатып алудан кейін ESET компаниясының электрондық хабарында қамтамасыз етіледі.



Ағымдағы нұсқа – Сіз орнатқан ағымдағы өнім нұсқасының нұсқа нөмірін көрсетеді.

Соңғы жаңарту – Соңғы жаңартудың күнін көрсетеді. Соңғы жаңартуды көрмесеңіз, өнім модульдері ағымдағы болмауы мүмкін.

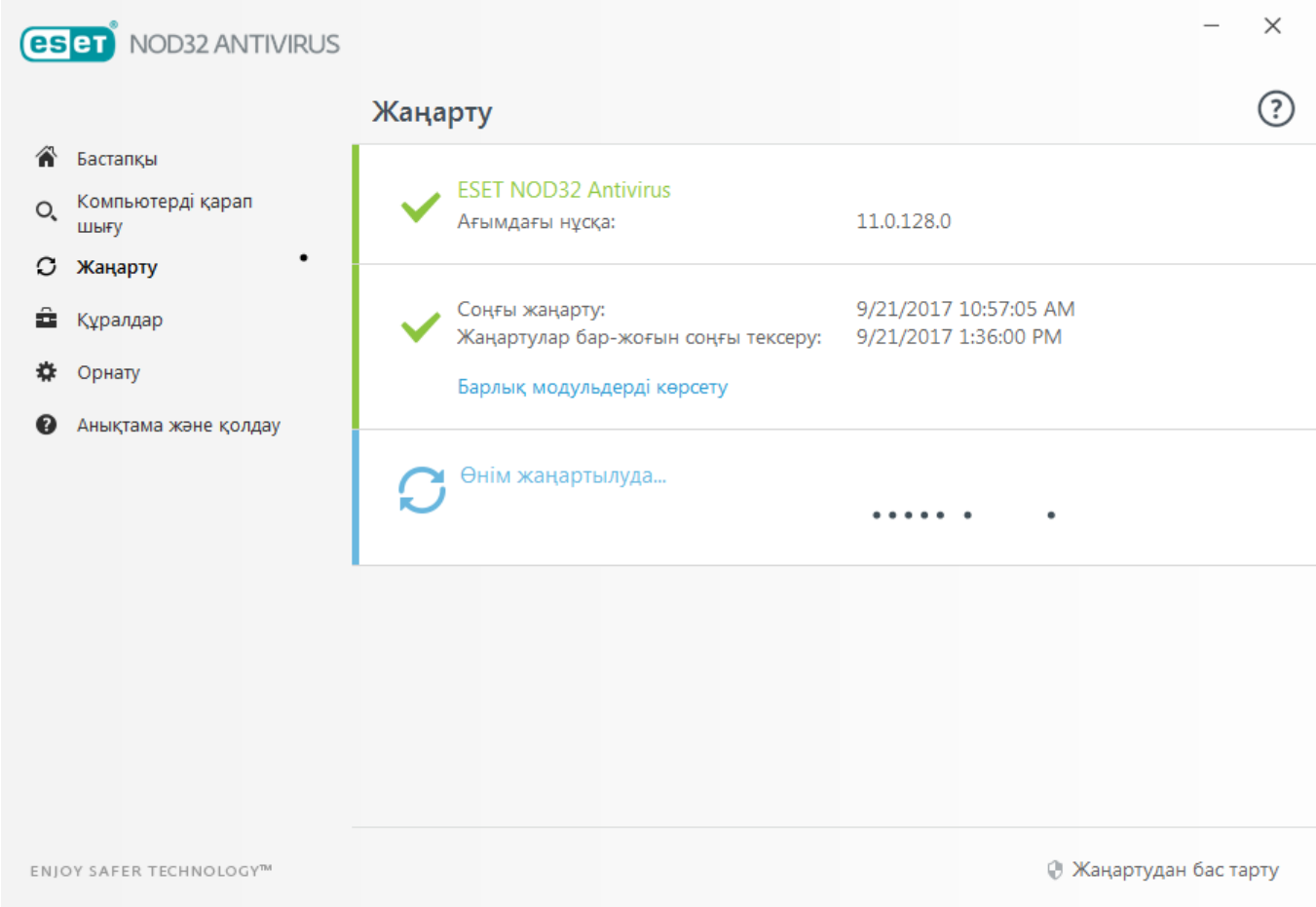
Жаңартуларды соңғы тексеру – Жаңартуларды соңғы тексерудің күнін көрсетеді.

Барлық модульдерді көрсету – Орнатылған бағдарлама модульдерінің тізімін көрсетеді.

Ең соңғы ESET NOD32 Antivirus қол жетімді нұсқасын анықтау үшін **Жаңартуларды тексеру** пәрменін басыңыз.

Жаңарту үрдісі

Жаңартулар бар-жоғын тексеру пәрменін басқаннан кейін жүктеп алу басталады. Жүктеудің орындалу жолағы мен жүктеуге дейін қалған уақыт көрсетіледі. Жаңартуды үзу үшін **Жаңартуды доғару** түймесін басыңыз.

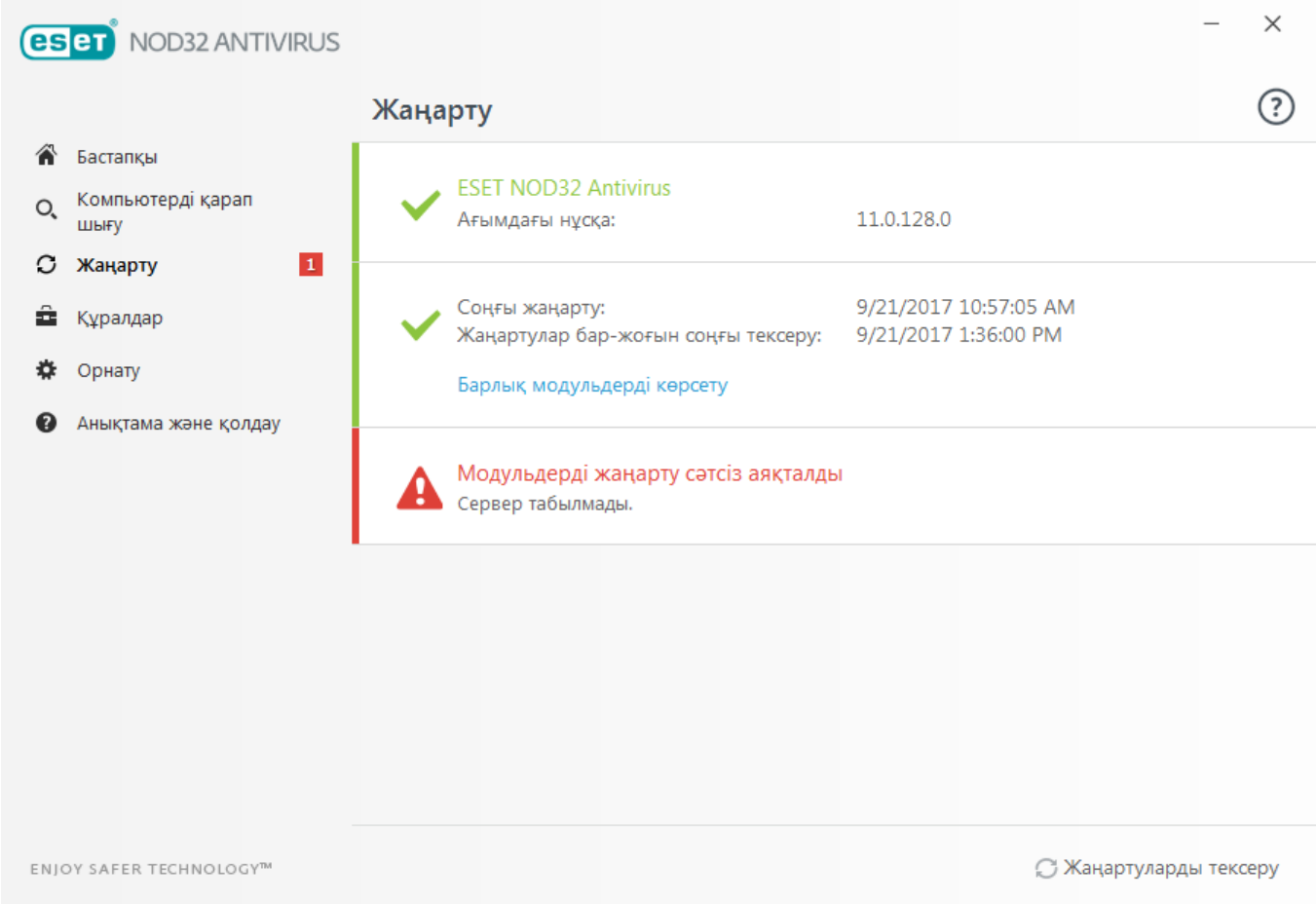


МАҢЫЗДЫ

Қалыпты жағдайларда сіз **Жаңарту** терезесінде бағдарлама жаңартылғанын көрсететін жасыл құсбелгіні көресіз. Олай болмаса, бағдарлама ескірген және жұғуға осалдығы жоғарырақ. Модульдерді мүмкіндігінше тез жаңартыңыз.

Алдыңғы хабарландыру сәтсіз жаңартулар туралы төмендегі екі хабарға қатысты:

1. **Жарамсыз лицензия** – Жаңартуды орнату кезінде лицензиялық кілт дұрыс емес енгізілген. Аутентификациялау деректерін тексеру ұсынылады. «Кеңейтілген реттеу» терезесі (негізгі мәзірде **Реттеу** тармағын басыңыз, содан кейін **Кеңейтілген реттеу** тармағын басыңыз немесе пернетақтада **F5** пернесін басыңыз) қосымша жаңарту опцияларын қамтиды. Жаңа лицензиялық кілтті енгізу үшін негізгі мәзірде **Анықтама және қолдау** > **Лицензияны өзгерту** тармағын басыңыз.
2. **Жаңарту файлдарын жүктеп алу кезінде қате орын алды** – Мұны интернет байланысының дұрыс емес параметрлері тудыруы мүмкін. Интернетке қосылу мүмкіндігін (веб-браузердегі кез келген веб-торапты ашу арқылы) тексеру ұсынылады. Егер веб-торап ашылмаса, Интернет қосылымы орнатылмаған болуы немесе компьютермен байланыс мәселелері бар болуы мүмкін. Белсенді Интернет қосылымыңыз болмаса, интернет провайдеріңізден (ISP) тексеріңіз.



ЕСКЕРТПЕ
Қосымша ақпарат алу үшін осы ESET білім қоры мақаласына кіріңіз.

4.3.1 Параметрлерді жаңарту

Жаңарту параметрлерінің опциялары **Кеңейтілген орнату** ағашында (F5), **Жаңарту** > **Негізгі** астында қол жетімді. Осы бөлімде пайдаланылатын жаңарту серверлері және осы сервер үшін түпнұсқалық растама деректері сияқты жаңарту көзі туралы ақпарат көрсетілген.

Жалпы

Қазіргі уақытта пайдаланылып жатқан жаңарту профилі **Жаңарту** профилі ашылмалы мәзірінде көрсетіледі. Жаңа профиль жасау үшін **Профильдер тізімі** жанында **Өңдеу** түймесін басыңыз, содан кейін **Қосу** түймесін басып, жеке **Профиль атауы** енгізілуі керек.

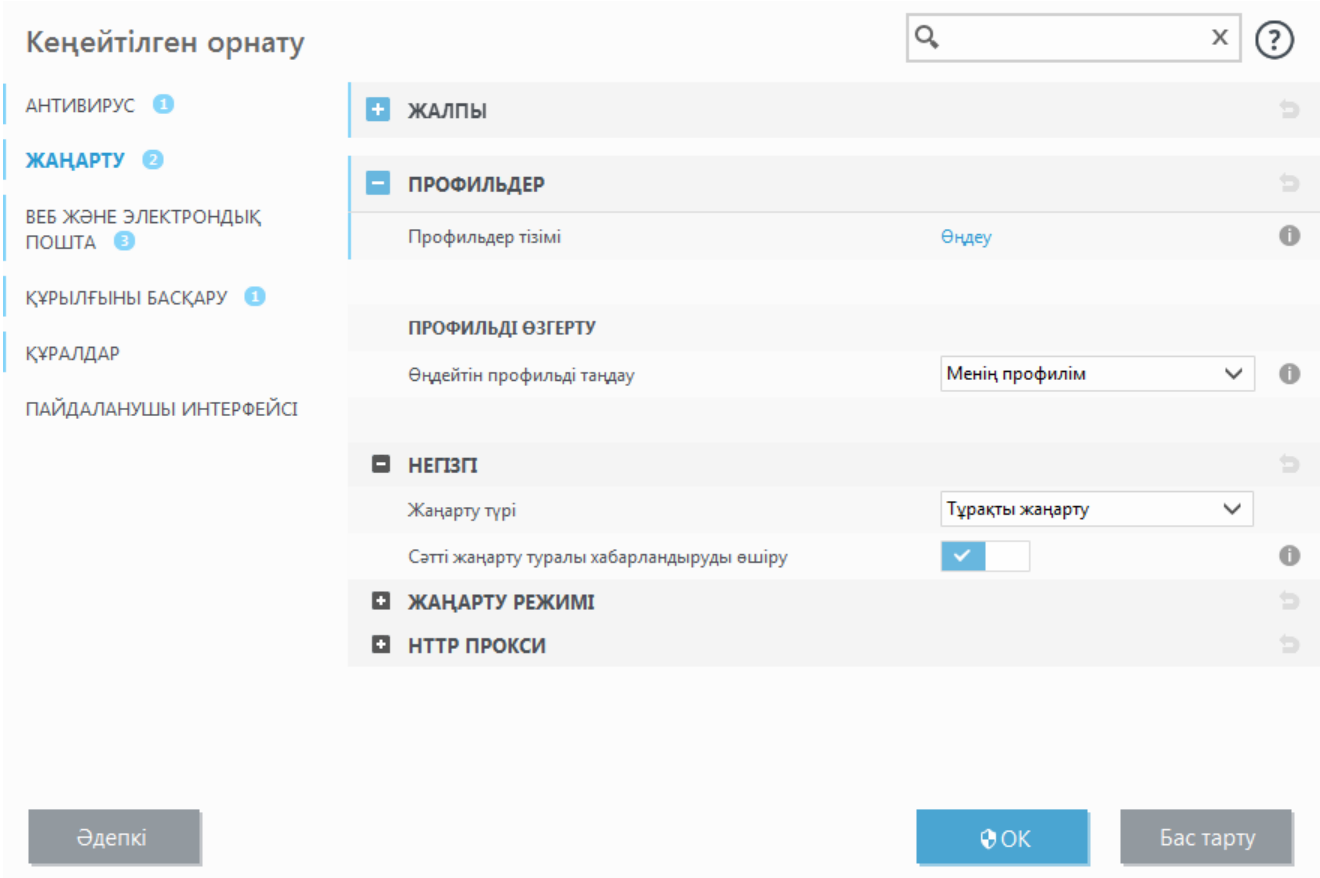
Анықтау механизмінің жаңартуларын жүктеп алуға әрекеттенгенде қиындық болса, уақытша жаңарту файлдарын/кэшті тазалау үшін **Тазалау** пәрменін басыңыз.

Қайтару

Егер вирус дерекқорының жаңа жаңартуы және/немесе бағдарлама модульдері тұрақсыздығына не зақымдалғанына күмәндансаңыз, алдынғы нұсқасына қайта ауысыңыз және орнатылған уақыт мерзімінің жаңартуын өшіре аласыз. Я болмаса, белгісіз уақытқа кейінге қалдырылған, бұрын өшірілген жаңартуларды қоса аласыз.

анықтау механизмінің мен бағдарлама модульдерін *шегіндіру* мүмкіндігімен бірге пайдалану үшін жазады. Вирус дерекқорының лездік суреттерін жасау үшін **Жаңарту файлдарының лездік суреттерін жасау** қосқышын қосулы қалдырыңыз. **Жергілікті сақталған лездік суреттердің саны** өрісі сақталған алдыңғы вирусты дерекқор лездік суреттерінің санын анықтайды.

Шегіндіру (**Кеңейтілген реттеу** (F5) > **Жаңарту** > **Жалпы**) пәрменін бассаңыз, ашылмалы мәзір үшін анықтау механизмі және бағдарлама модулін жаңартулар қанша уақытқа кідіртілетінін білдіретін уақыт аралығын таңдау керек.



Жаңартулар сәйкесінше жүктелуі үшін барлық жаңарту параметрлерін дұрыс толтыру маңызды. Егер брандмауэр пайдаланатын болсаңыз, ESET бағдарламасының интернетпен байланысу (яғни, HTTP байланысы) рұқсаты бар екенін тексеріңіз.

Негізгі

Әдепкі бойынша, **Жаңарту түрі** жаңарту файлдарының ең аз желілік трафик бар ESET серверінен автоматты түрде жүктелуін қамтамасыз ету үшін **Жүйелі түрде жаңарту** параметріне орнатылады. Шығарылуға дейінгі жаңарту (**Шығарылуға дейінгі жаңарту** опциясы) толық ішкі тексеруден өткен жаңартулар болып табылады және жақын арада жалпыға қол жетімді болады. Соңғы табу әдістері мен реттеулерге кіру арқылы шығарылу алдындағы жаңартуларды қосу пайдасын көруге болады. Дегенмен, шығарылу алдындағы жаңартулар барлық кездерде тұрақты болмауы мүмкін және ең жоғары қол жетімділік пен тұрақтылықты қажет ететін шығарылым серверлері мен автоматты жұмыс орындарында пайдаланылмауы КЕРЕК.

Сәтті жаңарту туралы хабарландыру көрсетуді өшіру – Экранның төменгі оң жағындағы жүйелік тақта хабарландыруын өшіреді. Толық экрандық бағдарлама немесе ойын орындалып жатқан жағдайда осы опцияны таңдау қолайлы. Ойыншы режимі барлық хабарландыруларды өшіретінін ескеріңіз.

4.3.1.1 Жаңарту профильдері

Жаңарту профилдерін әр түрлі жаңарту конфигурациялары және тапсырмалар үшін жасауға болады. Жаңарту профильдерін жасау - тұрақты өзгеретін интернет байланысының сипаттарына баламалы профильді қажет ететін мобильді пайдаланушылар үшін пайдалы.

Жаңарту профилі ашылмалы мәзірі қазіргі уақытта таңдалған профильді көрсетеді әдепкі бойынша **Менің профилім** деп орнатылады. Жаңа профиль жасау үшін **Профильдер тізімі** жанында **Өңдеу** түймешігін басыңыз, содан кейін **Қосу** түймешігін басып, жеке **Профиль атауы** енгізілуі керек.

4.3.1.2 Кеңейтілген жаңарту параметрлері

Жаңартуды кеңейтілген реттеу опциялары **Жаңарту режимі**, **HTTP прокси-сервері** опцияларын конфигурациялауды қамтиды.

4.3.1.2.1 Жаңарту режимі

Жаңарту режимі қойындысы жүйелік бағдарламаны жаңартуларға қатысты опцияларды қамтиды. Бұл параметрлер анықтау механизмінің жаңа нұсқасы немесе бағдарлама құрамдасын жаңартулар қолжетімді кезде бағдарлама әрекетін алдын-ала анықтауға мүмкіндік береді.

Бағдарлама құрамдасын жаңартулар жаңа мүмкіндіктерді қамтиды немесе алдыңғы нұсқалардағы мүмкіндіктерге өзгертулер енгізеді әрі жүйелі (анықтау механизмінің) жаңартулар бөлігі ретінде қамтылады. Бағдарлама компонентін жаңарту орнатылғаннан кейін қайта іске қосу қажет болуы мүмкін.

Келесі параметрлер қол жетімді:

Қолданбаны жаңарту – Қосулы болса, әрбір бағдарлама құрамдасын жаңарту автоматты түрде және өнімді толық жаңартусыз тыныш орындалады.

Бағдарлама құрамдасын қолмен жаңартуды қосу – Әдепкі бойынша өшірілген. Қосылған болса және жаңарақ ESET NOD32 Antivirus нұсқасы қолжетімді болса, **Жаңарту** тақтасында жаңартулар бар-жоғын тексеруге және жаңарақ нұсқаны **орнатуға** болады.

Жаңартуды жүктеп алу алдында сұрау — Бұл опциясы белсенді болса, кез келген қолжетімді жаңартулардың орнатылуы алдында хабарландыру көрсетіледі және сізден орнатуды растау сұралады.

Жаңарту файлы көрсетілген мәннен үлкенірек пе деп сұрау (КБ) – Жаңарту файлы осында көрсетілген өлшемнен үлкенірек болса, кез келген қолжетімді жаңартулардың орнатылуы алдында хабарландыру көрсетіледі және сізден орнатуды растау сұралады.

4.3.1.2.2 HTTP прокси

Осы жаңарту профилінің прокси сервер параметрлерін орнату опцияларына кіру үшін **Кеңейтілген орнату** тармағында (F5)**Жаңарту** түймесін басып, содан кейін **HTTP прокси** түймесін басыңыз. **Прокси режимі** ашылмалы мәзірін басып, төмендегі үш опцияның бірін таңдаңыз:

- Прокси серверді пайдаланбау
- Прокси сервер арқылы қосылу
- Ғаламдық прокси сервер параметрлерін пайдалану

Глобалдық прокси сервер параметрлерін пайдалану опциясын «Кеңейтілген орнату» тармағының **Құралдар** > **Прокси сервер** тармағында көрсетіліп қойылған прокси сервер конфигурациясын пайдалану үшін таңдаңыз.

ESET NOD32 Antivirus бағдарламасын жаңарту мақсатында прокси сервер пайдаланылмайтынын көрсету үшін **Прокси серверді пайдаланбау** опциясын таңдаңыз.

Прокси сервер арқылы қосылу опциясын келесі жағдайларда таңдау керек:

- **Құралдар** > **Прокси сервер** тармағында анықталғаннан басқа прокси сервер ESET NOD32 Antivirus бағдарламасын жаңарту үшін пайдаланылса. Бұл конфигурацияда жаңа прокси туралы ақпаратты **Прокси сервер** мекенжайы, байланыс **Порт** (әдепкі бойынша, 3128) ішінде және қажет болса, прокси сервердің **Пайдаланушы аты** және **Құпиясөз** опцияларын көрсету керек.
- Прокси сервер параметрлері ғаламдық деңгейде орнатылмаған, бірақ ESET NOD32 Antivirus бағдарламасы жаңартулар үшін прокси серверге қосылады.
- Компьютеріңіз Интернетке прокси сервер арқылы қосылған. Параметрлер бағдарламаны орнату барысында Internet Explorer браузерінен алынған, бірақ егер олар кейінірек өзгертілетін болса (мысалы, егер интернет қызметін жеткізушісін (ISP) өзгертсеңіз), осы терезеде тізілген HTTP проксиі параметрлерінің дұрыс екенін тексеріңіз. Кері жағдайда бағдарлама жаңарту серверлеріне қосыла алмайды.

Прокси сервердің әдепкі параметрі – **Ғаламдық прокси сервер параметрлерін пайдалану**.

Прокси-сервер қолжетімді емес болса, тікелей байланысты пайдалану – Қол жеткізу мүмкін болмаса, жаңарту кезінде прокси-сервер өткізіп жіберіледі.

ЕСКЕРТПЕ

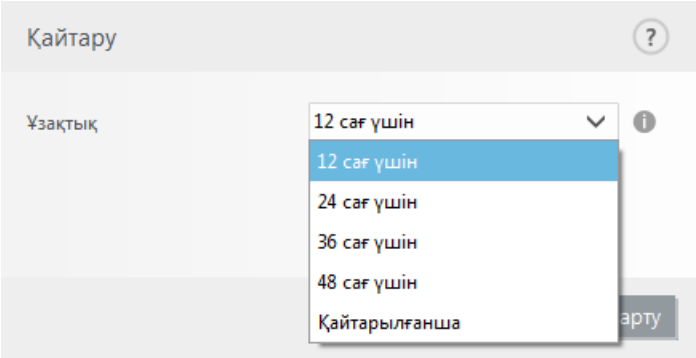
Бұл бөлімдегі **Пайдаланушы аты** және **Құпиясөз** өрістері прокси серверге қатысты. Бұл өрістерді прокси серверге қол жеткізу үшін пайдаланушы аты мен құпия сөз қажет болса ғана толтырыңыз. Бұл өрістер ESET NOD32 Antivirus бағдарламасының пайдаланушы аты және құпия сөзіне арналмаған және оларды прокси сервер арқылы Интернетке қатынасу үшін құпия сөз керек екенін білсеңіз ғана толтыру керек.

4.3.2 Қайтаруды жаңарту

Егер анықтау механизмінің жаңа жаңартуы және/немесе бағдарлама модульдері тұрақсыздығына не зақымдалғанына күмәндансаңыз, алдынғы нұсқасына қайта ауысыңыз және орнатылған уақыт мерзімінің жаңартуын өшіре аласыз. Сондай-ақ, белгісіз уақытқа кейінге қалдырылған, бұрын өшірілген жаңартуларды қоса аласыз.

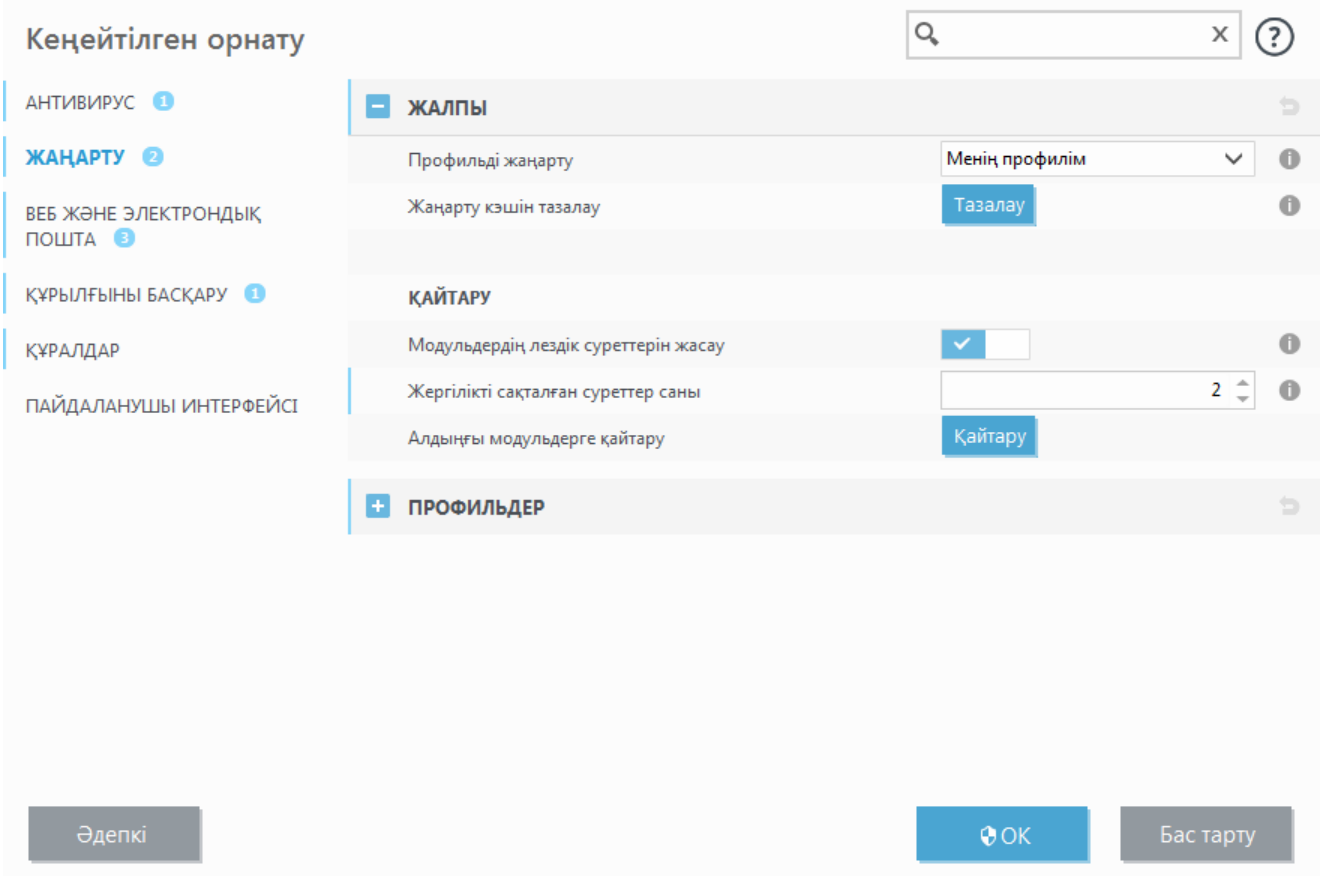
анықтау механизмінің мен бағдарлама модульдерін *шегіндіру* мүмкіндігімен бірге пайдалану үшін жазады. Анықтау механизмінің лездік суреттерін жасау үшін **Жаңарту файлдарының лездік суреттерін жасау** ұяшығында құсбелгіні қалдырыңыз. **Жергілікті сақталған лездік суреттердің саны** өрісі сақталған алдыңғы анықтау механизмі лездік суреттерінің санын анықтайды.

Шегіндіру (**Кеңейтілген реттеу** (F5) > **Жаңарту** > **Жалпы**) пәрменін бассаңыз, **Ұзақтық** ашылмалы мәзірі үшін анықтау механизмі және бағдарлама модулін жаңартулар қанша уақытқа кідіртілетінін білдіретін уақыт аралығын таңдау керек.



Жойылғанға дейін параметрін жаңарту мүмкіндіктерін қолмен қайта сақтағанға дейін тұрақты жаңартуларды кейінге қалдыру үшін басыңыз. Осыған байланысты, ол қауіпсіздікке ықтимал қауіп болып табылғандықтан, бұл опцияны таңдауыңызды ұсынбаймыз.

Егер қайтарылса, **Қайтару** түймесі **Жаңартуларға рұқсат ету** түймесіне өзгереді. **Жаңартуларды тоқтату** ашылмалы мәзірінен таңдалған уақыт аралығына рұқсат етілетін жаңартылулар жоқ. Анықтау механизмінің нұсқасы қолжетімді ең ескі нұсқаға төмендетіледі және жергілікті компьютердің файлдық жүйесінде лездік сурет ретінде сақталады.



ЕСКЕРТПЕ

6871 нөмірі анықтау механизмінің соңғы нұсқасы делік. 6870 және 6868 мәндері анықтау механизмінің лездік суреттері ретінде сақталады. Назар аударыңыз, мысалы, компьютер өшірілгендіктен және 6869-тан бұрын жүктелген соңғы жаңарту қол жетімді болғандықтан 6869 қол жетімді емес. **Жергілікті сақталған лездік суреттердің саны** өрісі 2 мәніне орнатылған болса және **Шегіндіру** пәрменін бассаңыз, анықтау механизмі (соның ішінде бағдарлама модульдері) 6868 нөмірлі нұсқаға қалпына келтіріледі. Бұл процесс біраз уақыт алуы мүмкін. ESET NOD32 Antivirus бағдарламасының негізгі терезесінде Жаңарту бөлімінде анықтау механизмінің нұсқасы төмендетілгенін тексеріңіз.

4.3.3 Жаңарту тапсырмаларын жасау туралы

Негізгі мәзірде **Жаңарту** пәрменін басудан кейін негізгі терезеде **Жаңартулар бар-жоғын тексеру** пәрменін басу арқылы жаңартуларды қолмен іске қосуға болады.

Сондай-ақ, жаңартуларды жоспарланған тапсырмалар ретінде орындауға болады. Жоспарланған тапсырманы конфигурациялау үшін **Құралдар** > **Жоспарлағыш** тармағын таңдаңыз. Әдепкі бойынша, ESET NOD32 Antivirus бағдарламасында келесі тапсырмалар іске қосылады:

- **Тұрақты автоматты жаңарту**
- **Телефон желісі арқылы қосылғаннан кейін автоматты жаңарту**
- **Пайдаланушы жүйеге кіргеннен кейін автоматты жаңарту**

Әр жаңарту тапсырмасын қажеттіліктерге сай болатындай өзгертуге болады. Әдепкі жаңарту тапсырмаларына қоса, пайдаланушы жаңа жаңарту тапсырмаларын пайдаланушылық конфгурациямен жасай алады. Жаңарту тапсырмаларын жасау және конфигурациялау туралы қосымша мәліметтер алу үшін Жоспарлағыш бөлімін қараңыз.

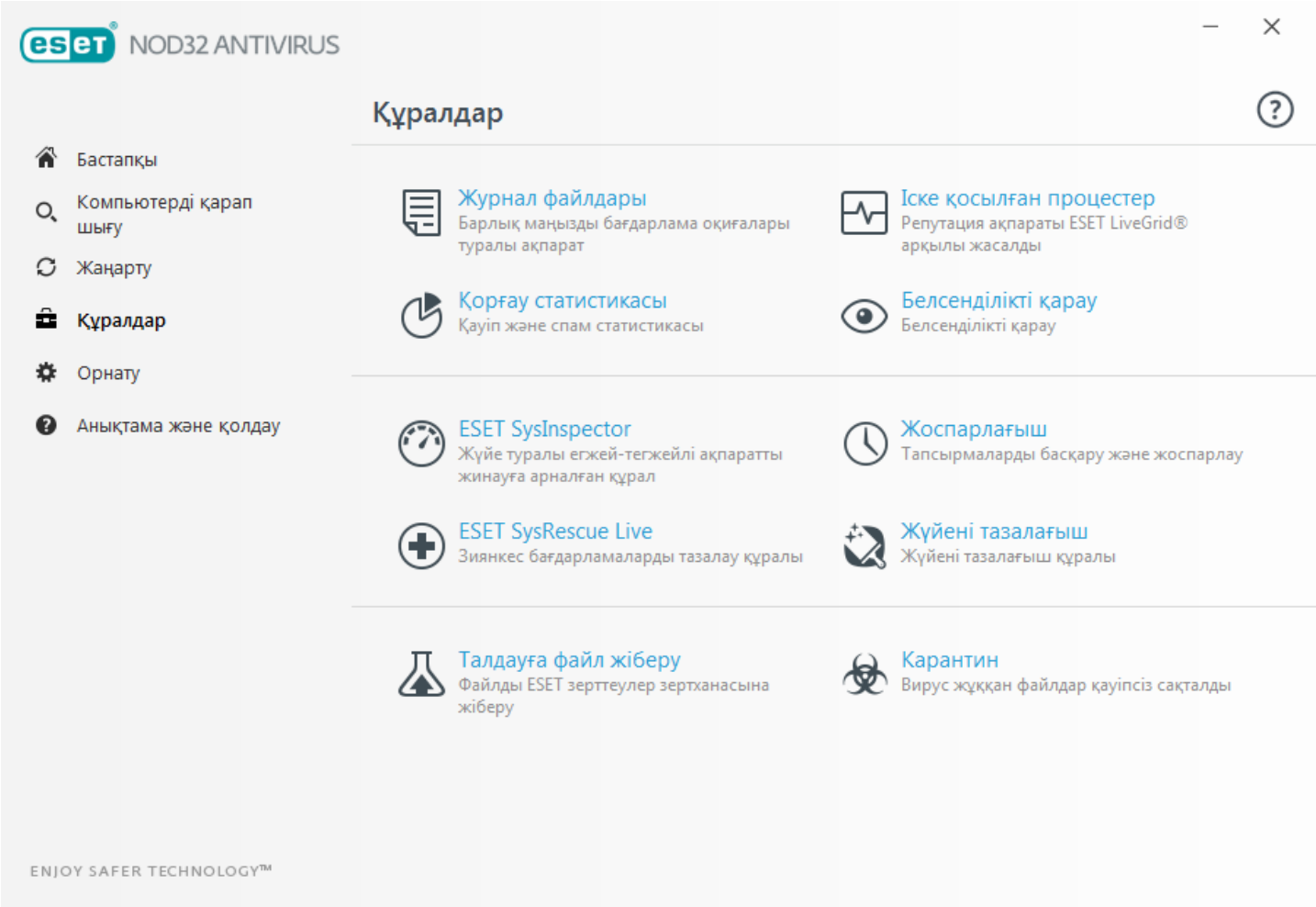
4.4 Құралдар

Құралдар мәзірі бағдарламаны басқаруды жеңілдетуге көмектесетін мәзірді қамтиды және озық пайдаланушылар үшін қосымша опцияларды ұсынады.

Компьютерді қорғайтын басқа құралдарды көрсету үшін Қосымша құралдар тармағын басыңыз.

4.4.1 ESET NOD32 Antivirus бағдарламасындағы құралдар

Бірінші **Құралдар** мәзірі бағдарламаны басқаруды жеңілдетуге көмектесетін мәзірді қамтиды және озық пайдаланушылар үшін қосымша опцияларды ұсынады.



Бұл мәзір келесі құралдарды қамтиды:

 Журнал файлдары

 Қорғау статистикасы

 Белсенділікті қарау

 Іске қосылған процестер (ESET LiveGrid® ESET NOD32 Antivirus бағдарламасында қосулы болса)

 ESET SysInspector

 ESET SysRescue Live – Сізді Microsoft Windows операциялық жүйелеріне арналған ESET SysRescue Live кескінін жүктеп алуға Live CD/USB Creator құралын жүктеп алуға болатын ESET SysRescue Live бетіне қайта бағыттайды.

 Жоспарлағыш

 Жүйені тазалағыш — Қауіпті тазалаудан кейін компьютерді пайдалануға болатын күйге қалпына келтіруге көмектеседі.

 Үлгіні талдауға жіберу – күдікті файлды талдау үшін ESET вирус зертханасына жіберуге мүмкіндік береді. Осы опцияны басудан кейін көрсетілетін диалогтық терезе осы бөлімде сипатталған.

 Карантин

ЕСКЕРТПЕ
ESET SysRescue ESET өнімдерінің алдыңғы нұсқаларында Windows 8 жүйесі үшін қол жетімді болмауы мүмкін. Бұл жағдайда өніміңізді жаңартуға немесе ESET SysRescue дискісін Microsoft Windows жүйесінің басқа нұсқасында жасауға кеңес беріледі.

4.4.1.1 Журнал файлдары

Журнал файлдары орын алған барлық маңызды бағдарлама оқиғалары туралы ақпаратты қамтиды және анықталған қауіптерді шолуды қамтамасыз етеді. Журналға тіркеу - жүйені талдаудың, қауіптерді анықтаудың және ақауларды жоюдың маңызды бөлігі. Журналға жазу пайдаланушының араласуынсыз фонда белсенді орындалады. Ақпарат ағымдағы журнал көбею параметрлері негізінде жазылады. Мәтіндік хабарлар мен журналдарды тікелей ESET NOD32 Antivirus ортасынан көруге, сондай-ақ, журналдарға мұрағаттауға болады.

Журнал файлдарына негізгі мәзір терезесінде **Құралдар** > **Журнал файлдары** тармағын басу арқылы қатынасуға болады. Ашылмалы мәзірінен **Журнал** керекті журналды таңдаңыз. Келесі тіркеулерге қол жетімді:

- **Анықталған қауіптер** – Қауіптер журналы ESET NOD32 Antivirus модульдері анықтаған инфильтрациялар туралы егжей-тегжейлі ақпаратты ұсынады. Журнал ақпараты анықтау уақытын, инфильтрация атауын, орнын, орындалған әрекетті және инфильтрация анықталған уақытта кірген пайдаланушы атын қамтиды. Мазмұнын бөлек терезеде мәліметтерін көрсету үшін жұрнал жазбасын екі рет басыңыз.
- **Оқиғалар** – ESET NOD32 Antivirus орындайтын барлық маңызды әрекеттер оқиғалар журналында жазылады. Оқиғалар журналының құрамында бағдарламада орын алған оқиғалар мен қателер туралы ақпарат бар. Ол жүйелік әкімшілер мен пайдаланушылар ақауларын шешуіне арналған. Осында табылатын ақпарат бағдарламада орын алатын ақаудың шешімін табуыңызға жиі көмектеседі.
- **Компьютерді қарап шығу** — Бұл терезеде барлық қолмен орындалған немесе жоспарланған қарап шығуларының нәтижелері көрсетіледі. Әр жол компьютердің бір басқару элементіне сәйкес келеді. Сәйкес қарап шығудың мәліметтерін көру үшін кез келген жазбаны екі рет басыңыз.
- **HIPS** — Жазу үшін деп белгіленген арнайы HIPS ережелерінің жазбаларын қамтиды. Протокол әрекетті іске қосатын қолданбаны, нәтижені (ережеге рұқсат етілгенін немесе тыйым салынғанын) және ереже атауын көрсетеді.
- **Сүзілген веб-сайттар** – Осы тізім - Веб қатынасты қорғау функциясы блоктаған веб-сайттардың тізімін көруге пайдалы. Әр журнал нақты веб-сайтқа байланыс орнатылған уақытты, URL-мекенжайын, пайдаланушыны және қолданбаны қамтиды.

- **Құрылғы басқару** – Компьютерге қосылған алынбалы медиа немесе құрылғылар жазбасын қамтиды. Тиісті құрылғы басқару ережесіне ие құрылғылар ғана тіркеу файлдарына жазылады. Егер ереже қосылған құрылғыға сәйкес келмесе, қосылған құрылғыға арналған тіркеу жазбасы жасалады. Сондай-ақ, құрылғы түрі, сериялық нөмірі, жеткізушінің аты және тасушының өлшемі (егер болса) сияқты мәліметтерді көруге болады.

Аралық сақтағышқа көшіру үшін кез келген журналдың мазмұнын таңдап, **Ctrl + C** пернелер тіркесімін басыңыз . Бірнеше жазбаны таңдау үшіе **Ctrl** және **Shift** пернелерін ұстап тұрыңыз.

Click Сүзу шарттарын анықтауға болатын **Журналды сүзу** терезесін ашу үшін **Сүзу** түймешігін басыңыз.

Мәтімәндік мәзірді ашу үшін нақты жазбаны тінтуірдің оң жақ түймешігімен басыңыз. Мәтінмәндік мәзірде келесі опциялар қол жетімді:

- **Көрсету** – Жаңа терезеде таңдалған журнал туралы егжей-тегжейлі ақпаратты көрсетеді.
- **Бірдей жазбаларды сүзу** – осы сүзгіні белсендіргеннен кейін тек бір түрге (диагностика, ескертулер...) жататын жазбаларды көресіз.
- **Сүзу.../Табу...** – Осы параметрді басқаннан кейін Журналда іздеу терезесі белгілі бір журнал жазбалары үшін сүзу шарттарын анықтауға мүмкіндік береді.
- **Сүзгіні қосу** – сүзгі параметрлерін белсендіреді.
- **Сүзуді өшіру** – Барлық сүзгі параметрлерін тазалайды (жоғарыда сипатталғандай).
- **Көшіру/барлығын көшіру** – терезедегі барлық жазбалар туралы ақпаратты көшіреді.
- **Жою/барлығын жою** – Таңдалған жазбаны(ларды) немесе көрсетілген жазбалардың барлығын жояды – бұл әрекет әкімшілік артықшылықтарды қажет етеді.
- **Экспорттау...** – Жазба(лар) туралы ақпаратты XML пішімінде экспорттайды.
- **Барлығын экспорттау...** – Барлық жазбалар туралы ақпаратты XML пішімінде экспорттайды.
- **Журналды айналдыру** – **Журнал файлдары** терезесінде ескі журналдарды авто айналдыру және белсенді журналдарды көру үшін бұл опцияны қосулы қалдырыңыз.

4.4.1.1.1 Журнал файлдары

ESET NOD32 Antivirus бағдарламасының журналға жазу конфигурациясына бағдарламаның негізгі терезесінен қатынасуға болады. **Орнату** > **Кеңейтілген орнатуға кіру...** > **Құралдар** > **Тіркеу файлдары**. Журналдар бөлімі журналдар қалай басқарылатынын анықтау үшін пайдаланылады. Бағдарлама қатты дискіде бос орын сақтау үшін ескірек журналдарды автоматты түрде жояды. Журнал файлдары үшін келесі опцияларды көрсетуге болады:

Ең аз тіркеу мәліметтері – жұрналға енгізілетін оқиғалардың ең аз сөзбен толтыру деңгейін көрсетеді.

- **Диагностика** – Бағдарламаны және жоғарыдағы барлық жазбаларды дәл реттеу үшін керек ақпаратты журналға тіркейді.
- **Ақпараттық** – Ақпараттық хабарларды, соның ішінде сәтті жаңарту туралы хабарларды, оған қоса жоғарыдағы жазбалардың барлығын жазып алады.
- **Ескертулер** – Сындарлы қателерді және ескерту хабарларын жазып алады.
- **Қателер** – *«Файлды жүктеп алу кезіндегі қате»* сияқты қателер және сындарлы қателер жазып алынады.
- **Сындарлы** – Тек сындарлы қателерді (антивирустық қорғауды іске қосу кезіндегі қате) журналға тіркейді, т.б қосатын қателерді) ғана журналға жазады.

(күндер) күннен бұрынғы жазбаларды автоматты түрде жою өрісіндегі көрсетілген күндер санынан бұрынғы журнал жазбалары автоматты түрде жойылады.

Журнал файлдарын автоматты түрде оңтайландыру - Құсбелгі қойылған болса, пайыздық шама **Егер пайдаланылмайтын жазбалардың саны мынадан (%) асса** өріс ішінде көрсетілген мәннен жоғары болса, журнал файлдарының үзінділерін жинақтау автоматты түрде орындалады.

Журнал файлдарын дефрагментациялауды бастау үшін **Оңтайландыру** түймесін басыңыз. Барлық бос журнал жазбалары осы процесс кезінде жойылады. Бұл өнімділік пен журналға тіркеу жылдамдығын жақсартады. Бұл жақсартуды әсіресе журналдарда жазбалардың көп саны болса байқауға болады.

Мәтіндік протоколды қосу Журнал файлдарынан бөлек басқа файл пішімінде журналдарды сақтауды қосады:

- **Мақсатты каталог** - журнал файлдары сақталатын каталог (тек мәтін/CSV файлдарына қатысты). Әр журнал бөлімінде алдын ала анықталған файл атауы бар жеке файлы бар (мысалы, журналдарды сақтау үшін кәдімгі мәтін файл пішімін пайдалансаңыз, *virlog.txt* файлы журнал файлдарының **Анықталған қауіптер** бөлімі үшін).

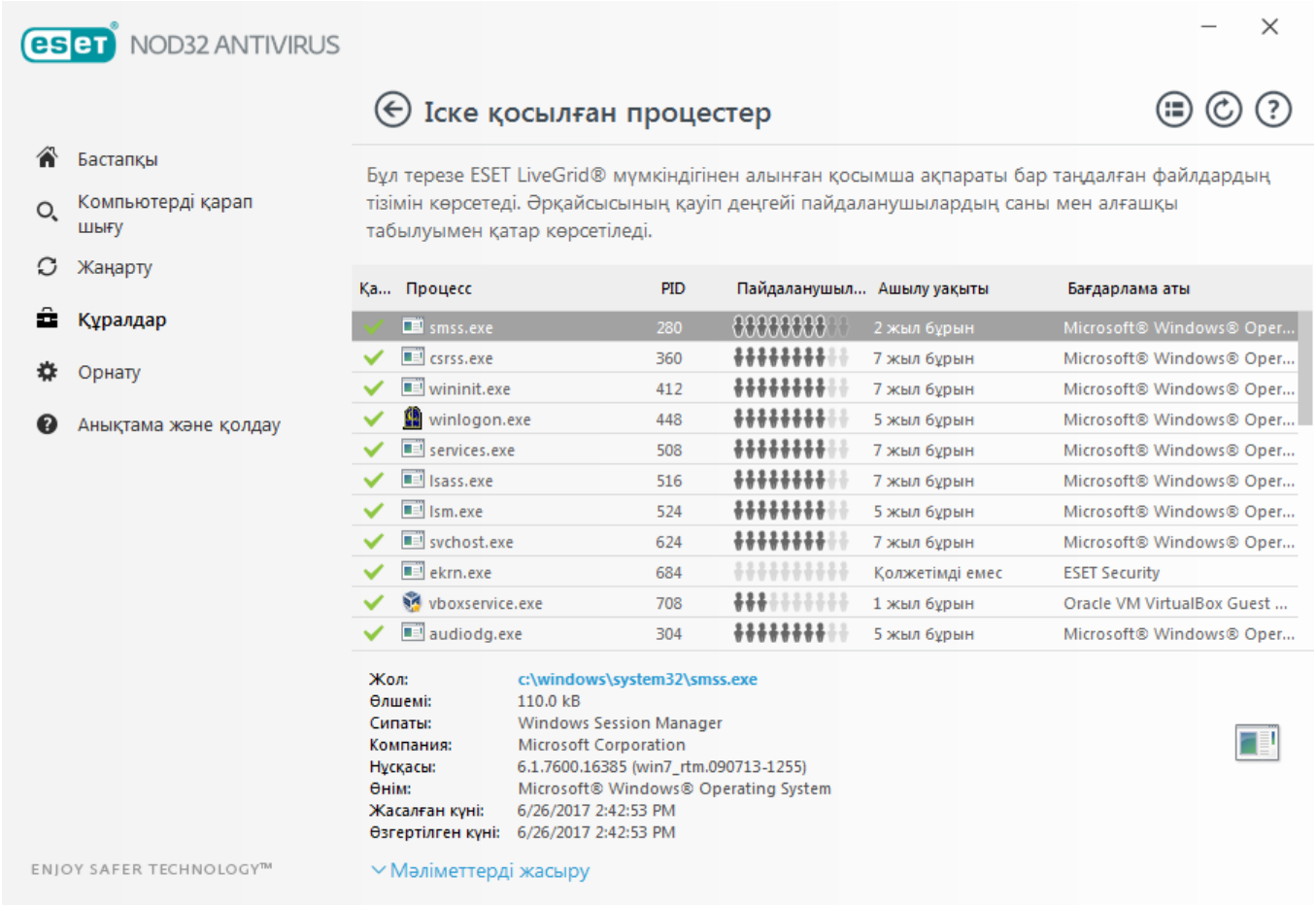
- **Түрі** – егер **Мәтін** файл пішімін таңдасаңыз, журналдар мәтіндік файлда сақталады; деректер қойындылармен бөлінеді. Дәл осы үтірлермен бөлінген **CSV** файл пішіміне қатысты. Егер **Оқиға** опциясын таңдасаңыз, журналдар файлда емес, Windows оқиғалар журналында сақталады («Басқару тақтасы» ішінде «Оқиғаларды көру құралын» пайдаланып көруге болады).

Барлық журнал файлдарын жою – қазіргі уақытта **Түрі** ашылмалы мәзірінде таңдалған барлық сақталған журналдарды өшіреді. Журналдарды сәтті жою туралы хабарландыру көрсетіледі.

ЕСКЕРТПЕ
мәселелерді жылдамырақ шешу үшін ESET компьютерден журналдарды беруді сұрауы мүмкін. ESET Log Collector қажет ақпаратты жинауды оңай етеді. ESET Log Collector туралы қосымша ақпарат алу үшін ESET білім қоры мақаласына кіріңіз.

4.4.1.2 Іске қосылған процестер

Іске қосылған процестер компьютеріңізде іске қосылған бағдарламалар немесе процестерді көрсетеді және ESET компаниясына жаңа инфильтрациялар туралы жылдам және тұрақты түрде хабарлап тұрады. Пайдаланушыларды ThreatSense технологиясының көмегімен қорғау үшін ESET NOD32 Antivirus іске қосылған процестер туралы егжей-тегжейлі ақпаратпен қамтамасыз етеді.



Процесс - Компьютерде қазіргі уақытта іске қосылған бағдарламаның немесе процестің сурет аты. Сондай-ақ, компьютердегі барлық іске қосылған процестерді көру үшін Windows тапсырмалар реттеушісін пайдалануға болады. «Тапсырмалар реттеушісін» ашу үшін тапсырмалар тақтасындағы бос аумақты тінтуірдің оң жағын басыңыз, содан кейін **Тапсырмалар реттеушісі** түймешігін басыңыз немесе пернетақтада **Ctrl**+**Shift**+**Esc** пернелер тіркесімін басыңыз.

Қауіп деңгейі – Көп жағдайларда, ESET NOD32 Antivirus бағдарламасы және ThreatSense технологиясы әр нысанның сипаттамаларын бақылайтын, содан кейін олардың зиянды әрекет ықтималдылығын бағалайтын эвристикалық ережелер қатарын пайдаланып, нысандарға (файлдар, процестер, тіркелім кілттері, т.б.) қауіп деңгейлерін тағайындайды. Осы эвристикаға негізделіп, нысандарға *1 – Жақсы (жасыл)* мен *9 – Қауіпті (қызыл)* аралығындағы қауіп деңгейі тағайындалады.

ЕСКЕРТПЕ
Жақсы (жасыл) ретінде белгіленген белгілі қолданбалар таза (ақ тізімде) және өнімділікті жақсарту үшін қарап шығуға қосылмайды.

PID - Процестің идентификациялық нөмірі процесс басымдығын реттеу сияқты әр түрлі функцияны шақыруларда пайдаланылуы мүмкін.

Пайдаланушылар саны - Осы бағдарламаны пайдаланатын пайдаланушылардың саны. Бұл ақпарат ThreatSense технологиясымен жиналған.

Анықтау уақыты - ThreatSense технологиясы бағдарламаны анықтағаннан бергі уақыт.

ЕСКЕРТПЕ
Белгісіз (сарғылт) ретінде белгіленген қолданба міндетті түрде зиянкес бағдарламалық құрал болып табылмайды. Әдетте бұл жай жаңа бағдарлама. Егер файлға сенімді болмасаңыз, ESET вирус зертханасына файлды талдауға жіберуге болады. Егер файл зиянкес қолданба немесе веб-сайт болып шықса, оны анықтау келесі жаңартуға қосылады.

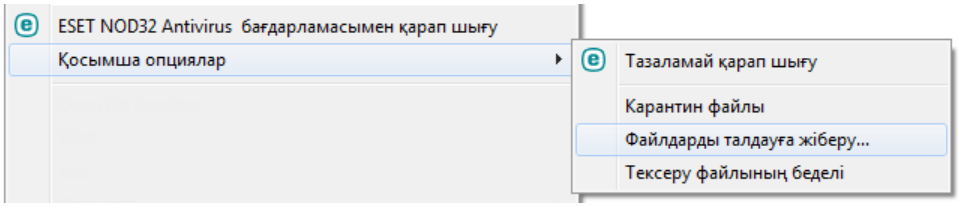
Бағдарлама аты — Бағдарламаға немесе процеске берілген ат.

Жаңа терезеде ашу — Іске қосылған процестер туралы ақпарат жаңа терезеде ашылады.

Қолданбаның келесі мәліметтерін көрсету үшін қолданбаны басыңыз:

- **Жол** — бағдарламаның компьютердегі орны.
- **Өлшемі** — B (байт) түріндегі файл өлшемі.
- **Сипаттама** — операциялық жүйедегі сипаттамаға негізделген файл сипаттамалары.
- **Компания** — жеткізушінің немесе бағдарлама процесінің аты.
- **Нұсқа** — бағдарлама жариялаушысының ақпараты.
- **Өнім** — бағдарлама аты және/немесе компания аты.
- **Жасалған/Өзгертілген** - Жасау (өзгерту) күні мен уақыты.

ЕСКЕРТПЕ
Сондай-ақ, іске қосылған бағдарламалар/процестер ретінде әрекет етпейтін файлдардың репутациясын тексеруге болады. Мұны істеу үшін оларды тінтуірдің оң жақ түймешігімен басып, **Кеңейтілген опциялар** > **Файлдың репутациясын тексеру** тармағын таңдаңыз.



4.4.1.3 Қорғау статистикасы

ESET NOD32 Antivirus қорғау модульдеріне қатысты статистикалық деректердің графигін көру үшін **Құралдар** > **Қорғау статистикасы**тармағына өтіңіз. Тиісті график пен шартты белгілерді көру үшін қажетті қорғау модулін **Статистика** ашылмалы мәзірінен таңдаңыз. Егер сіз шартты белгілердегі элементті тінтуірмен түртсеңіз, сол элементке ғана арналған деректер графиктен көрсетіледі.

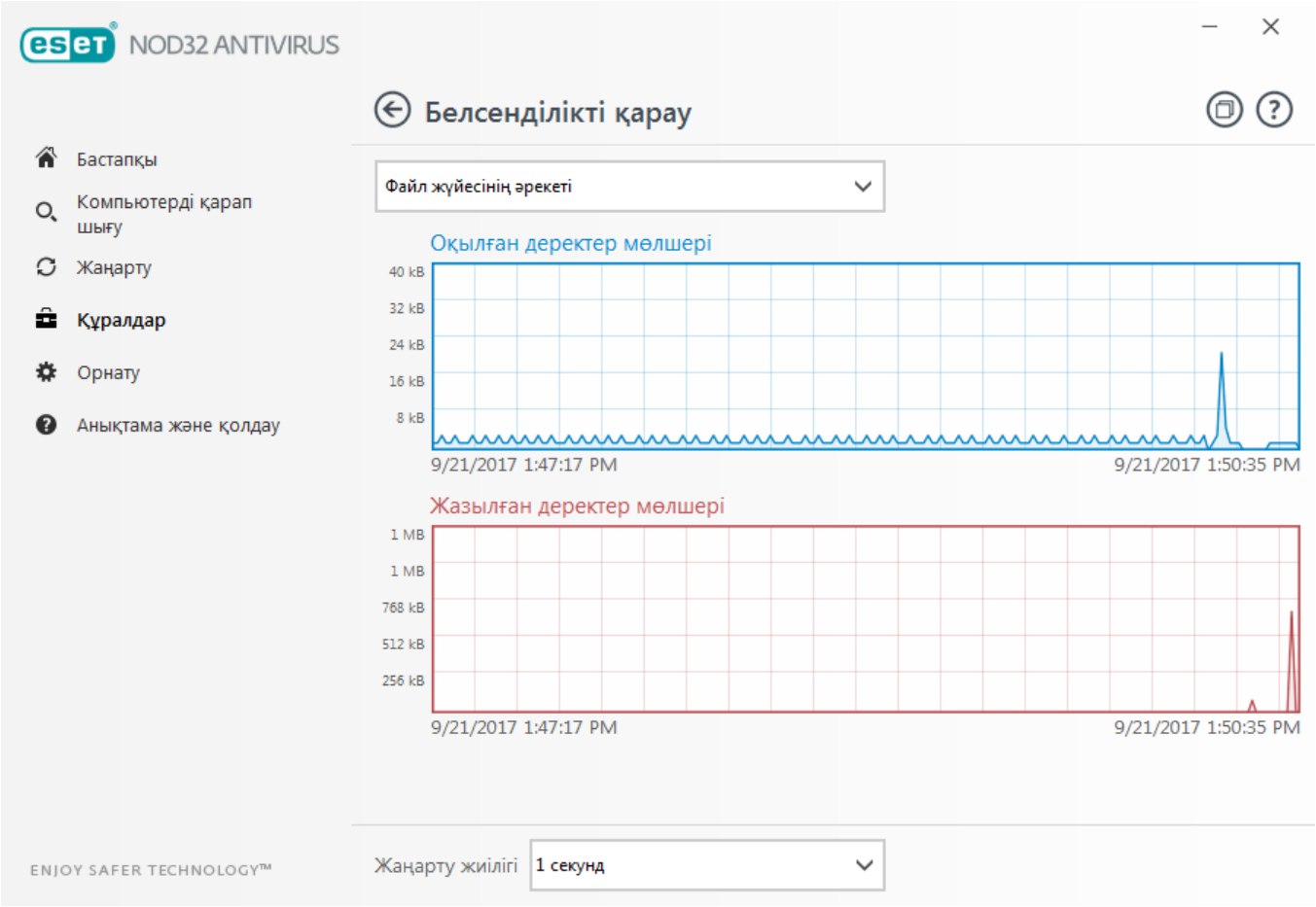
Төмендегі статистикалық графиктер қолжетімді:

- **Антивирустық және антишпиондық қорғау** – Жұққан және тазаланған нысандардың санын көрсетеді.
- **Файл жүйесін қорғау** – тек файлдық жүйеден оқылған немесе жазылған нысандарды көрсетеді.
- **Электрондық пошта клиентін қорғау** – Тек электрондық пошта клиенттері жіберілген немесе алынған нысандарды көрсетеді.
- **Вебке кіру және антифишингтік қорғау** – тек веб-браузерлер жүктеген нысандарды көрсетеді.

Статистика графигінің астында жалпы қарап шыққан нысандардың санын, соңғы қарап шыққан нысанды және статистика уақыт белгісін көруге болады. Бүкіл статистика туралы ақпаратты тазалау үшін **Ысыру** пәрменін таңдаңыз.

4.4.1.4 Белсенділікті қарау

График пішінінде ағымдағы **Файл жүйесінің әрекетін** көру үшін **Құралдар** > **Белсенділікті қарау** тармағын басыңыз. Графиктің төменгі жағында файлдық жүйе белсенділігін нақты уақытта таңдалған уақыт аралығы негізінде жазатын уақыт шкаласы беріледі. Уақыт аралығын өзгерту үшін **Жаңарту жиілігі** ашылмалы мәзірінен таңдаңыз.



Мына опциялар қол жетімді:

- **Қадам: 1 секунд** - График секунд сайын жаңартылады және уақыт шкаласы соңғы 10 минутты қамтиды.
- **Қадам: 1 минут (соңғы 24 сағат)** - график минут сайын жаңартылады және уақыт шкаласы соңғы 24 сағатты қамтиды.
- **Қадам: 1 сағат (соңғы ай)** - график сағат сайын жаңартылады және уақыт шкаласы соңғы айды қамтиды.
- **Қадам: 1 сағат (таңдалған ай)** - график сағат сайын жаңартылады және уақыт шкаласы таңдалған X айды қамтиды.

Файл жүйесі әрекеттерінің кестесі тік осі оқылған деректерді (көк) және жазылған деректерді (қызыл) білдіреді. Екі мән де Кбайт (килобайт)/Мбайт/Гбайт өлшемімен беріледі. Егер сіз графиктің төменгі жағындағы шартты белгілердегі оқылған деректерді не жазылған деректерді тінтуірмен бассаңыз, график сол белсенділік түріне арналған деректерді ғана көрсетеді.

4.4.1.5 ESET SysInspector

ESET SysInspector компьютеріңізді мұқият тексеріп, орнатылған драйверлер мен бағдарламалар, желілік қосылымдар немесе маңызды тізбе жазбалары сияқты жүйелік компоненттер туралы егжей-тегжейлі ақпаратты жинайтын және әр компоненттің қауіп деңгейін бағалайтын бағдарлама. Осы ақпарат бағдарламалық құрал немесе аппараттық құрал үйлесімсіздігінен немесе зиянкес бағдарламаның вирусынан болуы мүмкін күдікті жүйе тәртібінің себебін анықтауға көмектеседі.

SysInspector терезесі жасалған журналдар туралы төмендегі ақпаратты көрсетеді:

- **Уақыт** – Журнал жасалған уақыт.
- **Түсініктеме** – Қысқаша түсініктеме.
- **Пайдаланушы** – Журналды жасаған пайдаланушының аты.
- **Күй** – Журналды жасау күйі.

Келесі әрекеттер қол жетімді:

- **Көрсету** - Жасалған журналды ашады. Сондай-ақ, журнал файлын тінтуірдің оң жақ түймешігімен басуға және контексттік мәзірде **Көрсету** мәзірін таңдауға болады.
- **Салыстыру** – Екі бар журналды салыстырады.
- **Жасау...** – Жаңа журналды жасайды. Журналды ашу әрекетін жасау алдында ESET SysInspector аяқталғанша күтіңіз (журналдың күйі «Жасалған» ретінде көрсетіледі).
- **Жою** – Таңдалған журналдарды тізімнен жояды.

Бір немесе бірнеше журнал файлы таңдалғанда контексттік мәзірде келесі элементтер қол жетімді болады:

- **Көрсету** – Таңдалған журналды ESET SysInspector ішінде ашады (дәл журналды екі рет басу сияқты функция).
- **Салыстыру** – Екі бар журналды салыстырады.
- **Жасау...** – Жаңа журналды жасайды. Журналды ашу әрекетін жасау алдында ESET SysInspector аяқталғанша күтіңіз (журналдың күйі «Жасалған» ретінде көрсетіледі).
- **Жою** – Таңдалған журналдарды тізімнен жояды.
- **Барлығын жою** – Барлық журналдарды жояды.
- **Экспорттау...** – Журналды *.xml* файлына немесе экспортталған *.xml* файлына экспорттайды.

4.4.1.6 Жоспарлағыш

Жоспарлағыш конфигурациясы мен сипаттары алдын ала орнатылған жоспарланған тапсырмаларды басқарады және іске қосады.

Жоспарлағышқа ESET NOD32 Antivirus негізгі бағдарлама терезесінде, **Құралдар** > **Жоспарлағыш** басып қатынасуға болады. **Жоспарлағыш** барлық жоспарланған тапсырмалардың тізімін және алдын ала анықталған күн, уақыт және пайдаланылатын қарап шығу профилі сияқты конфигурация сипаттарын қамтиды.

Жоспарлағыш келесі тапсырмаларды жоспарлау үшін қызмет етеді: модульдерді жаңарту, қарап шығу тапсырмасы, жүйелік жүктеу файлын тексеру және журнал жүргізу. Тапсырмаларды тікелей негізгі жоспарлағыш терезесінен қосуға немесе жоюға болады (астында **Қосу...** немесе **Delete** түймешігін басыңыз). Мына әрекеттерді орындау үшін Жоспарлағыш терезесінің кез келген жерін тінтуірдің оң жақ түймесімен басыңыз: егжей-тегжейлі ақпаратты көрсету, тапсырманы дереу орындау, жаңа тапсырма қосу және бар тапсырманы жою. Тапсырмаларды іске қосу/ажырату үшін әр жазбаның басындағы құсбелгілерді пайдаланыңыз.

Әдепкі бойынша, **Жоспарлағыш** ішінде келесі жоспарланған тапсырмалар көрсетіледі:

- **Журнал жүргізу**
- **Тұрақты автоматты жаңарту**
- **Телефон желісі арқылы қосылғаннан кейін автоматты жаңарту**
- **Пайдаланушы жүйеге кіргеннен кейін автоматты жаңарту**
- **Соңғы өнім нұсқасын тұрақты түрде тексеру** (Жаңарту режимі бөлімін қараңыз)
- **Іске қосылғанда автоматты түрде файлдарды тексеру** (пайдаланушы кіргеннен кейін)
- **Іске қосылғанда автоматты түрде файлдарды тексеру** (анықтау механизмін сәтті жаңартудан кейін)

Бар жоспарланған тапсырманың (әдепкі мен пайдаланушы орнататын) конфигурациясын өзгерту үшін тапсырманы тінтуірдің оң жағымен басып, **Өңдеу...** пәрменін таңдаңыз немесе өзгерту керек тапсырманы таңдап, **Өңдеу...** түймесін басыңыз.

Жаңа тапсырманы қосу

1. Терезенің төменгі жағында **Тапсырма қосу** түймесін басыңыз.
2. Тапсырма атауын енгізіңіз.

3. Ашылмалы мәзірден қалаған тапсырманы таңдаңыз:

- **Сыртқы қолданбаны іске қосу** – Сыртқы қолданбаның орындалуын жоспарлайды.
- **Журналды сақтау** – Журнал файлдары жойылған жазбалардың қалдықтарын да қамтиды. Бұл тапсырма тиімді жұмыс істеу үшін журнал файлдарындағы жазбаларды тұрақты түрде оңтайландырады.
- **Жүйені іске қосу кезіндегі файлдарды тексеру** – Жүйені іске қосқанда немесе жүйеге кіргенде орындалуға рұқсат етілген файлдарды тексереді.
- **Компьютерді қарап шығуды жасау** – ESET SysInspector компьютер лездік суретін жасайды - жүйе компоненттері (мысалы, драйверлер, бағдарламалар) туралы егжей-тегжейлі ақпаратты жинайды және әр компоненттің қауіп деңгейін бағалайды.
- **Талап бойынша компьютерді қарап шығу** – Компьютердегі файлдар мен қалталарды қарап шығуды орындайды.
- **Жаңарту** – Модульдерді жаңарту арқылы «Жаңарту» тапсырмасын жоспарлайды.

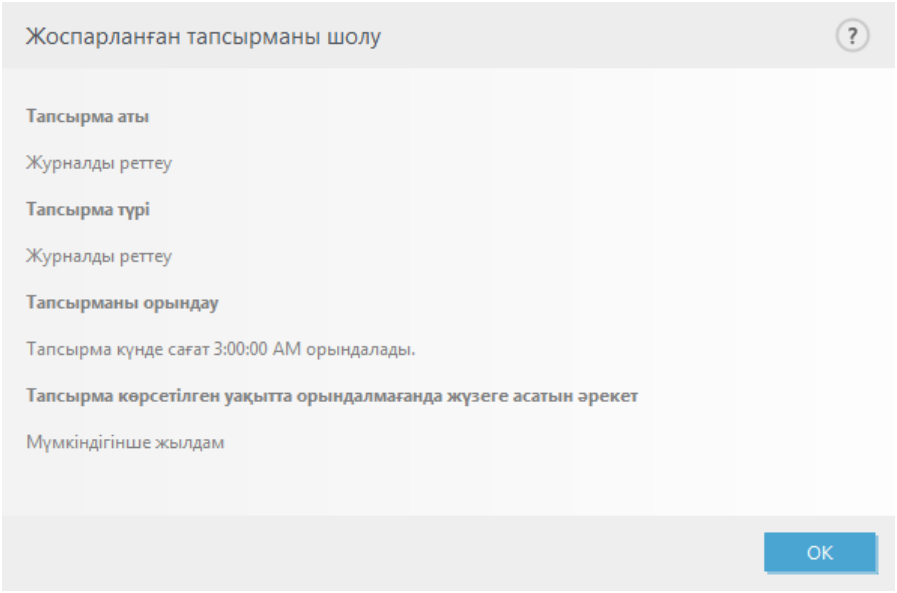
4. Тапсырманы белсендіру керек болса **Қосылған** қосқышын қосыңыз (мұны кейінірек жоспарланған тапсырмалар тізімінде құсбелгіні қою/алу арқылы істеуге болады), **Келесі** түймесін басыңыз және аралық опцияларының біреуін таңдаңыз:

- **Бір рет** – Тапсырма алдын ала белгіленген күн мен уақытта орындалады.
- **Қайталап** – Тапсырма көрсетілген уақыт аралығында орындалады.
- **Күнделікті** – Тапсырма күн сайын көрсетілген уақытта қайталап орындалады.
- **Апта сайын** – Тапсырма таңдалған күн мен уақытта орындалады.
- **Оқиға іске қосады** – Тапсырма көрсетілген оқиғада орындалады.

5. Ноутбук батареядан жұмыс істегенде жүйе ресурстарын барынша аз пайдалану үшін **Батареядан жұмыс істегенде тапсырманы өткізіп жіберу** опциясын таңдаңыз. Тапсырма **Тапсырманы орындау** өрістерінде көрсетілген күн мен уақытта орындалады. Егер тапсырманы алдын ала анықталған уақытта орындау мүмкін емес болса, оның қашан қайта орындалатынын көрсетуге болады:

- **Келесі жоспарланған уақытта**
- **Мүмкіндігінше жылдам**
- **Соңғы орындаудан бергі уақыт көрсетілген мәннен асса, дереу** (аралықты **Соңғы орындаудан бергі уақыт** жүгіртпесін пайдаланып анықтауға болады)

Тінтуірдің оң жақ түймесін басып, **Тапсырма туралы мәліметтерді көрсету** түймесін абсқанда жоспарлы тапсырманы қарап шығуға болады.



4.4.1.7 Жүйені тазалағыш

Жүйені тазалағыш — қауіпті тазалаудан кейін компьютерді пайдалануға болатын күйге қалпына келтіруге көмектесетін құрал. Зиянкес бағдарлама «Тізбе өңдегіші», «Тапсырмалар реттеушісі» немесе Windows Updates сияқты жүйелік қызметтік бағдарламаларды өшіруі мүмкін. Жүйені тазалағыш осы жүйе үшін әдепкі мәндерді қалпына келтіреді.

Жүйені тазалау мына жағдайларда сұралуы мүмкін:

- қауіп табылғанда
- пайдаланушы **«Ысыру» пәрменін басқанда**

Сіз өзгертулерді қарап шығып, тиісті болса, параметрлерді ысыра аласыз.

ЕСКЕРТПЕ
Жүйені тазалағышта әкімші құқықтары бар пайдаланушы ғана әрекеттер орындай алады.

4.4.1.8 ESET SysRescue

ESET Security шешімдерінің (ESET NOD32 Antivirus, <%ESET_INTERNET_SECURITY%>, ESET Smart Security, <% ESET_SMART_SECURITY_PREMIUM%>) біреуін немесе белгілі бір серверлік өнімдерді қамтитын жүктелетін дискіні жасауға мүмкіндік беретін қызметтік бағдарлама. ESET SysRescue бағдарламасының негізгі артықшылығы — ESET Security шешімі хост операциялық жүйесінен тәуелсіз жұмыс істейтін, бірақ дискіге және файлдық жүйеге тікелей қатынасы бар шешімді іске қосады. Бұл әдетте, мысалы, операциялық жүйе жұмыс істеп тұрғанда т.б. жағдайда жою мүмкін емес инфильтрацияларды жоюды мүмкін етеді.

4.4.1.9 ESET LiveGrid®

ESET LiveGrid® (ендірілген ESET ThreatSense.Net озық ерте ескерту жүйесі) ESET пайдаланушылары дүние жүзінде жіберген деректерді пайдаланады және оны ESET вирус зертханасына жібереді. Жабайы жағдайлардан күдікті үлгілер мен метадеректерді ұсыну арқылы ESET LiveGrid® бағдарламасы клиенттеріміздің қажеттіліктеріне дер кезінде көңіл бөлуге және ESET бағдарламасын жаңа қауіптерге дер кезінде сақтануға мүмкіндік береді. ESET LiveGrid® бағдарламасы туралы қосымша ақпаратты глоссарий бөлімінен оқыңыз.

Пайдаланушы іске қосылған процестер мен файлдардың репутациясын тікелей бағдарлама интерфейсінен немесе ESET LiveGrid® арқылы қол жетімді қосымша ақпаратқа ие контекстік мәтіннен тексере алады. Екі опция бар:

1. ESET LiveGrid® бағдарламасын қоспауды таңдай аласыз. Бағдарламалық құралдың ешбір функцияларын жоғалтпайсыз, бірақ ESET Live Grid қосулы кезде кейбір жағдайларда ESET NOD32 Antivirus бағдарламасы жаңа қауіптерге анықтау механизмін жаңартудан тезірек реакция көрсетуі мүмкін.
2. ESET LiveGrid® бағдарламасын жаңа қауіптер мен жаңа қауіпті код қайда орналасқаны туралы анонимді ақпаратты жіберуге конфигурациялауға болады. Бұл файл ESET компаниясына егжей-тегжейлі талдау үшін жіберілуі мүмкін. Осы қауіптерді зерттеу ESET компаниясына қауіптерді табу қасиеттерін жаңартуға көмектеседі.

ESET LiveGrid® бағдарламасы компьютеріңізде жаңадан анықталған қауіптер туралы ақпаратты жинайды. Бұл ақпарат қауіп пайда болған файлдың үлгісін немесе көшірмесін, сол файлдың жолын, файл атауын, күн мен уақытты, қауіп компьютерде қандай процеспен көрінгенін және компьютердің операциялық жүйесі туралы ақпаратты қамтуы мүмкін.

Әдепкі бойынша, ESET NOD32 Antivirus бағдарламасы күдікті файлдарды «ESET вирус зертханасына» егжей-тегжейлі талдауға жіберу конфигурацияланған. *.doc* немесе *.xls* сияқты белгілі бір кеңейтімдері бар файлдар әрқашан қосылмайды. Сіз немесе ұйымыңыз жіберуді қаламайтын нақты файлдар болса, басқа кеңейтімдерді де қосуға болады.

ESET LiveGrid® орнату мәзірі ESET зертханаларына күдікті файлдар мен анонимді статистикалық ақпаратты жіберу үшін қызмет ететін ESET LiveGrid® технологиясын қосудың / өшірудің бірнеше опциясын қамтамасыз етеді. Оған «Кеңейтілген орнату» тармағында, **Құралдар** > **ESET LiveGrid®** басып қатынасуға болады.

ESET LiveGrid® репутация жүйесін қосу (ұсынылады) – ESET LiveGrid® репутация жүйесі қарап шығылған файлдарды бұлттағы ақ тізімге қосылған және қара тізімге қосылған элементтердің дерекқорымен салыстыру арқылы ESET зиянкес бағдарламалармен күресу шешімдерінің тиімділігін жақсартады.

Анонимді статистиканы жіберу – ESET бағдарламасына жаңадан анықталған қауіптер туралы ақпаратты жинауға рұқсат етеді, мысалы, қауіп атауы, анықтау күні мен уақыты, анықтау әдісі және байланысты метадеректер, өнім нұсқасы және конфигурация, соның ішінде жүйе туралы ақпарат.

Файлдарды жіберу – Қауіптерге ұқсайтын күдікті файлдар және/немесе әдеттен тыс сипаттамалар немесе әрекет ESET компаниясына талдауға жіберіледі.

Файлды және статистикалық ақпарат жіберулерін жазатын оқиғалар журналын жасау үшін **Тіркеуді қосу** опциясын таңдаңыз. Бұл файлдар немесе статистикалар жіберілген кезде Оқиғалар журналына тіркелуді қосады.

Байланыс электрондық поштасы (міндетті емес) – Байланыс электрондық поштаңыз кез келген күдікті файлдармен бірге жіберілуі және талдауға қосымша ақпарат керек болса, сізге хабарласу үшін пайдаланылуы мүмкін. Қосымша ақпарат қажет болмаса, ESET компаниясынан жауап алмайтыныңызды ескеріңіз.

Ерекшелік – «Ерекшелік» сүзгісі белгілі бір файлдарды/қалталарды жіберуге қоспауға мүмкіндік береді (мысалы, құжаттар немесе электрондық кестелер сияқты құпия ақпарат болуы мүмкін файлдарды қоспау пайдалы болуы мүмкін). Тізімдегі файлдардың құрамында күдікті код болса да, олар ешқашан ESET зертханаларына талдауға жіберілмейді. Ең жиі файл түрлері әдепкі бойынша қосылмайды (.doc, т.б.). Қаласаңыз, қосылмаған файлдар тізіміне қоса аласыз.

Егер бұрын ESET LiveGrid® технологиясын пайдаланып, оны өшірсеңіз, әлі де жіберетін деректер бумалары болуы мүмкін. Тіпті өшіргеннен кейін де мұндай бумалар ESET зертханаларына жіберіледі. Бүкіл ағымдағы ақпарат жіберілгеннен кейін қосымша бумалар жасалмайды.

4.4.1.9.1 Күдікті файлдар

Егер күдікті файлды тапсаңыз, оны ESET вирус зертханасына талдауға жібере аласыз. Егер бұл зиянды бағдарлама болса, оны анықтау келесі вирус қолтаңбасын жаңартуға қосылады.

Қиыс жағдайлар сүзгісі – Қиыс жағдайлар сүзгісі белгілі бір файлдарды/қалталарды жіберуге қоспауға мүмкіндік береді. Тізімдегі файлдардың құрамында күдікті код болса да, олар ешқашан ESET вирус зертханасына талдауға жіберілмейді. Мысалы, құжаттар немесе электрондық кестелер сияқты құпия ақпарат болуы мүмкін файлдарды қоспау пайдалы. Ең жиі файл түрлері әдепкі бойынша қосылмайды (.doc, т.б.). Қаласаңыз, қосылмаған файлдар тізіміне қоса аласыз.

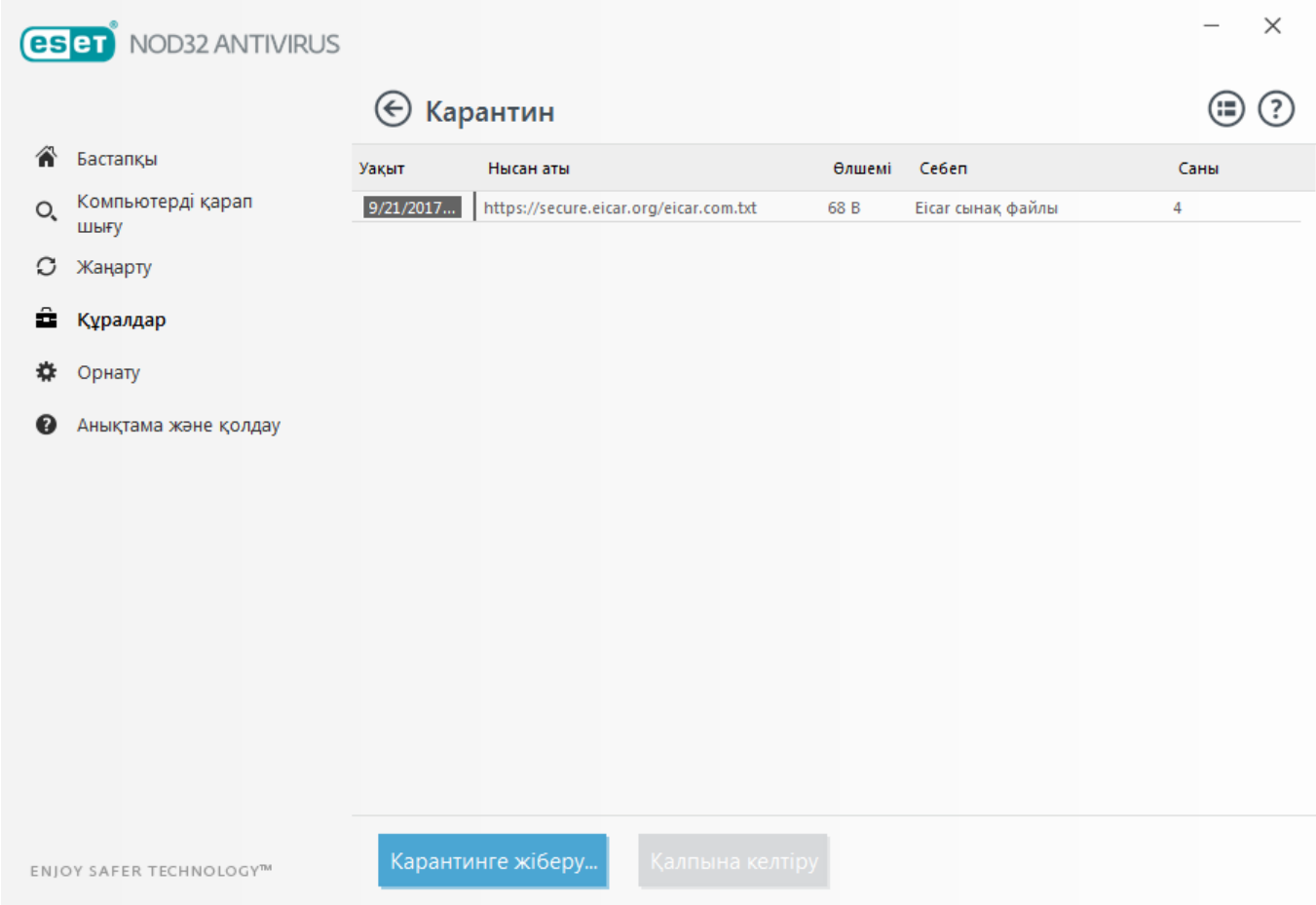
Байланыс электрондық поштасы (міндетті емес) – Байланыс электрондық поштаңыз кез келген күдікті файлдармен бірге жіберілуі және талдауға қосымша ақпарат керек болса, сізге хабарласу үшін пайдаланылуы мүмкін. Қосымша ақпарат қажет болмаса, ESET компаниясынан жауап алмайтыныңызды ескеріңіз.

Файлды және статистикалық ақпарат жіберулерін жазатын оқиғалар журналын жасау үшін **Тіркеуді қосу** опциясын таңдаңыз. Бұл файлдар немесе статистикалар жіберілген кезде Оқиғалар журналына тіркелуді қосады.

4.4.1.10 Карантин

Карантиннің негізгі функциясы – вирус жұққан файлдарды қауіпсіз сақтау. Файлдарды тазалау мүмкін емес болса, жою қауіпсіз емес болса немесе кеңес берілмесе немесе ESET NOD32 Antivirus бағдарламасы оларды жалған анықтап жатса карантинге көшіру керек.

Кез келген файлды карантинге көшіруге болады. Егер файл күдікті болса және антивирус бағдарламасы арқылы табылмайтын болса оны орындау ұсынылады. Карантинге қойылған файлдарды ESET вирус зертханасына талдауға жіберуге болады.



Карантин қалтасында сақталған файлдарды карантинге көшірілген күні, уақыты, вирус жұқтырған файлдың ағымдағы орналасуы, оның байттармен өлшемі, себебі (мысалы, пайдаланушы қосқан нысан) және қауіптердің саны көрсетілген кестеден көруге болады (мысалы, егер бінеше инфильтрация бар мұрағат болса).

Файлдарды карантинге көшіру

ESET NOD32 Antivirus бағдарламасы жойылған файлдарды автоматты түрде карантинге жібереді (егер сіз ескерту терезесінде осы опцияны өшірмеген болсаңыз). Қаласаңыз, **Карантин..** түймесін басу арқылы кез келген күдікті файлды карантинге көшіруге болады. Егер осы жағдай болса, бастапқы файл өзінің бастапқы орналасуынан жойылмайды. Контекстік мәзірді де осы мақсатта пайдаланылуы мүмкін, карантин терезесінде тінтуірдің оң жағын басып, **Карантин** терезесін тінтуірдің оң жақ пернесімен басып, **Карантин...** түймесін басыңыз.

Карантиннен қалпына келтіру

Сондай-ақ, карантинге қойылған файлдарды бастапқы орнына қалпына келтіруге болады. Бұл үшін **Қалпына келтіру** опциясын пайдаланыңыз; оған мазмұн мәзіріндегі Карантин терезесінде берілген файлда тінтуірдің оң жағын басу арқылы қол жеткізуге болады. Егер файл ықтимал қалаусыз бағдарлама болып белгіленсе, **Қалпына келтіру және қарап шығуға қоспау** опциясы қосылады. Глоссарий ішінде бағдарламаның осы түрі жөніндегі толығырақ ақпаратты оқыңыз. Мазмұн мәзірі, сонымен бірге, **Қалпына келтіру...** опциясын ұсынады, файлды бастапқы орналасқан жерінен басқа, яғни жойылған орналасу жерінен басқа орналасқан жерге қалпына келтіруге мүмкіндік береді.

Карантиннен жою – Элементті тінтуірдің оң жақ түймешігімен басып, **Карантиннен жою** пәрменін таңдаңыз немесе жою керек элементті таңдап, пернетақтада **Delete** пернесін басыңыз. Сондай-ақ, бірнеше элементті таңдауға және бірге жоюға болады.

ЕСКЕРТПЕ
Егер бағдарлама қателесіп зиянсыз файлды карантинге қойса, қалпына келтіргеннен кейін файлды қарап шығудан шығарып, «ESET тұтынушыларды қолдау қызметіне» жіберіңіз.

Карантиндегі файлды жіберу

Егер бағдарлама таппаған күдікті файлды карантинге көшірсеңіз немесе файл қателік салдарынан вирус жұқтырған деп табылса (мысалы, кодтың эвристикалық талдауымен) және карантинге көшірілсе, оны «ESET вирус зертханасына» жіберіңіз. Карантинге көшірілген файлды жіберу үшін, файлды тінтуірдің оң жағымен басыңыз да, мазмұн мәзірінен **Талдауға жіберу** тармағын таңдаңыз.

4.4.1.11 Прокси сервер

Үлкен жергілікті желілерде компьютер және интернет арасындағы байланыс аралығына прокси серверді қолдануға болады. Бұл конфигурацияны пайдаланғанда келесі параметрлерді анықтау керек. Әйтпесе, бағдарлама өзін автоматты түрде жаңарта алмайды. ESET NOD32 Antivirus бағдарламасында прокси-серверді орнату «Кеңейтілген орнату» тармағындағы екі түрлі бөлімде қол жетімді.

Алдымен, прокси сервер параметрлерін **Кеңейтілген орнату** ішінде, **Құралдар** > **Прокси сервер** астында конфигурациялауға болады. Прокси серверді осы деңгейде көрсету ESET NOD32 Antivirus бағдарламасының ғаламдық прокси сервер параметрлерін анықтайды. Мұндағы параметрлерді интернетке қосылымды қажет ететін барлық модульдер пайдаланады.

Осы деңгей үшін прокси-сервер параметрлерін көрсету үшін **Прокси серверді пайдалану** құсбелгісін қойып, **Прокси сервер** өрісіне прокси сервердің мекенжайын, сонымен бірге, прокси сервердің **Порт** нөмірін енгізіңіз.

Егер прокси-сервермен байланыс түпнұсқалық растаманы қажет етсе, **Прокси сервер түпнұсқалықты растауды қажет етеді** құсбелгісін қойып, сәйкес өрістерге жарамды **Пайдаланушы аты** мен **Құпиясөз** енгізіңіз. Прокси-сервер параметрлерін автоматты түрде анықтау және толтыру үшін **Анықтау** түймесін басыңыз. Internet Explorer ішінде көрсетілген параметрлер көшіріледі.

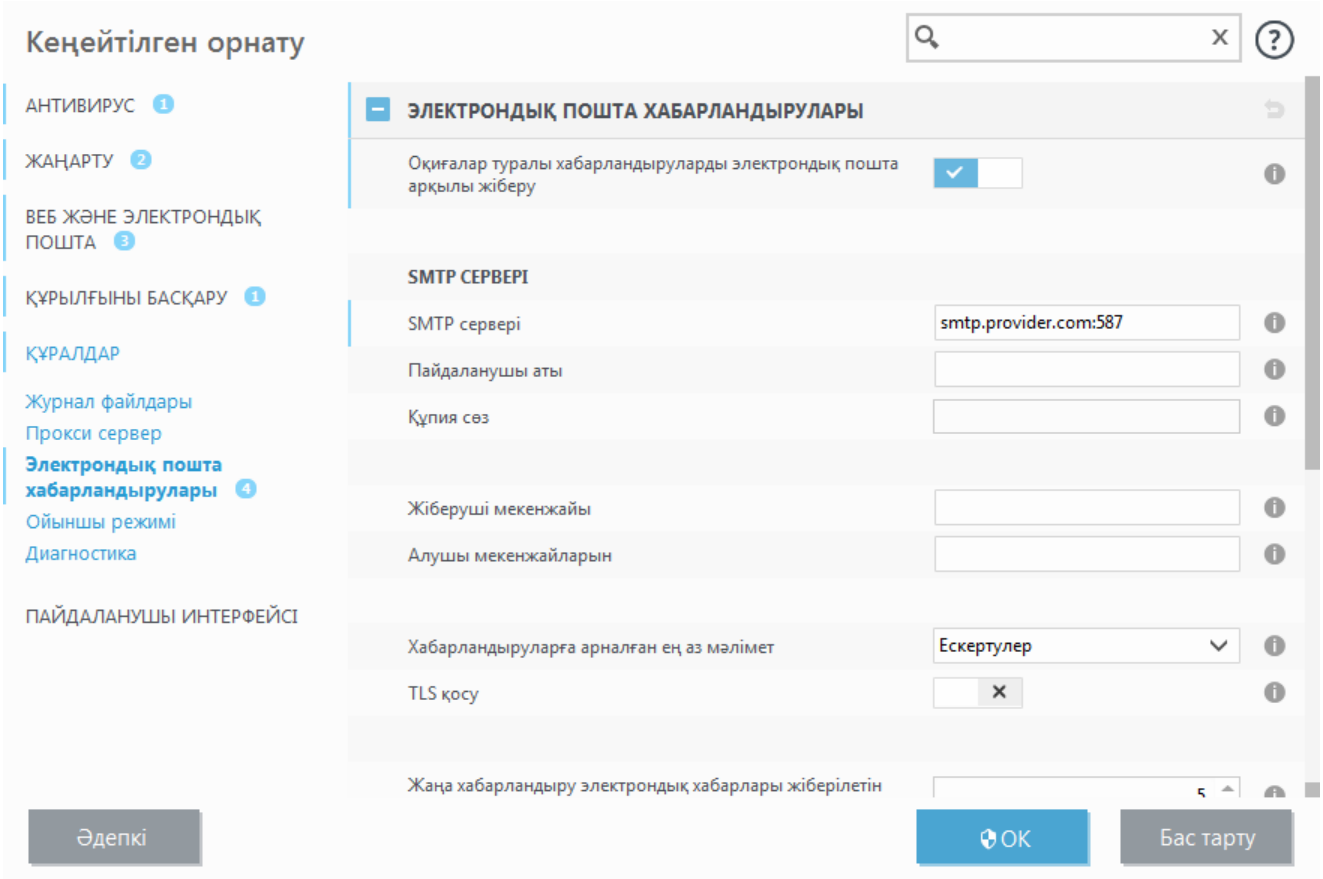
ЕСКЕРТПЕ
Прокси-сервер параметрлерінде пайдаланушы атын және құпия сөзді қолмен енгізу керек.

Прокси қол жетімді болмаса, тікелей байланысты пайдалану – Өнім HTTP проксиін пайдалануға конфигурацияланған болса және проксиге қол жеткізу мүмкін болмаса, өнім проксиді айналып өтеді және ESET серверлерімен тікелей байланысады.

Сондай-ақ, прокси-сервер параметрлерін «Кеңейтілген орнату» ішінде орнатуға болады (**Кеңейтілген орнату** > **Жаңарту** > **HTTP прокси-сервері**, **Прокси режимі** ашылмалы мәзірінен **Прокси сервер арқылы қосылу** опциясын таңдау арқылы). Бұл параметр осы жаңарту профиліне қолданылады және ноутбуктер үшін ұсынылады, ол көбінесе вирус қолтаңбасын жаңартуларды әр түрлі орындардан алады. Бұл параметр туралы қосымша ақпарат алу үшін Кеңейтілген жаңарту параметрлері бөлімін қараңыз.

4.4.1.12 Электрондық пошта хабарландырулары

Таңдалған ең аз мәлімет бар оқиға орын алса, ESET NOD32 Antivirus бағдарламасы хабарландыру электрондық хабарларын автоматты түрде жібере алады. Электрондық пошта хабарландыруларын белсендіру үшін **Электрондық пошта арқылы оқиға туралы хабарландырулар жіберу** опциясын қосыңыз.



SMTP сервері

SMTP сервері – хабарландырулар жіберу үшін пайдаланылатын SMTP сервері (мысалы, *smtp.provider.com:587*, алдын-ала анықталған порт — 25).

ЕСКЕРТПЕ
TLS шифрлауы бар SMTP серверлеріне ESET NOD32 Antivirus қолдау көрсетеді.

Пайдаланушы аты және **Құпия сөз** – егер SMTP сервері аутентификацияны қажет етсе, бұл өрістерге SMTP серверіне қатынасу мүмкіндігін беретін дұрыс пайдаланушы аты мен құпия сөз енгізілуі керек.

Жіберушінің мекенжайы – Бұл өріс хабарландыру электрондық хабарларының тақырыбында көрсетілетін жіберушінің мекенжайын көрсетеді.

Алушының мекенжайы – Бұл өріс хабарландыру электрондық хабарларының тақырыбында көрсетілетін алушының мекенжайын көрсетеді.

Хабарландыруларға арналған ең аз мәлімет ашылмалы мәзірінен жіберілетін хабарландырулардың бастапқы маңыздылық деңгейін таңдауға болады.

- **Диагностика** – Бағдарламаны және жоғарыдағы барлық жазбаларды дәл реттеу үшін керек ақпаратты журналға тіркейді.
- **Ақпараттық** – ақпараттық хабарларды, соның ішінде сәтті жаңарту хабарларын, сондай-ақ, барлық жоғарыдағы жазбаларды жазады.
- **Ескертулер** – маңызды қателерді және ескерту хабарларын жазады (Antistealth дұрыс жұмыс істеп жатқан жоқ немесе жаңарту сәтсіз аяқталды).
- **Қателер** – Қателер (құжатты қорғау басталған жоқ) және маңызды қателер жазылады.
- **Маңызды** – Тек антивирустық қорғауды немесе вирус жұққан жүйені іске қосатын маңызды қателерді журналға тіркейді.

TLS қосу – TLS шифрлау қолдау көрсететін ескерту және хабарландыру хабарларын жіберуді қосу.

Жаңа хабарландыру электрондық хабарлары жіберілетін аралық (мин) – өткеннен кейін жаңа хабарландырулар электрондық поштаға жіберілетін минуттар түріндегі аралық. Бұл мәнді 0 деп орнатсаңыз, хабарландырулар бірден жіберіледі.

Әр хабарландыруды бөлек электрондық хабарда жіберу – қосылған болса, алушы әр жеке хабарландыру үшін жаңа электрондық хабар алады. Бұл қысқа уақыт кезеңінде электрондық хабарлардың көп санын алуға әкелуі мүмкін.

Хабар пішімі

Оқиға туралы хабарлардың пішімі – қашықтағы компьютерлерде көрсетілген оқиға туралы хабарлардың пішімі.

Қауіп туралы ескерту хабарларының пішімі – қауіп туралы ескерту және хабарландыру хабарларында алдын ала анықталған әдепкі пішім бар. Бұл пішімді өзгертпеуге кеңес беріледі. Дегенмен, кейбір жағдайларда (мысалы, сізде автоматты электрондық поштаны өңдеу жүйесі болғанда), хабар пішімін өзгерту қажет болуы мүмкін.

Таңбалар жинағы – Windows жүйесінің аймақтық параметрлерінің негізінде электрондық пошта хабарын ANSI (мысалы, windows-1250), Unicode (UTF-8), ACSII 7 биттік (мысалы, «á» таңбасы «a» таңбасына, ал белгісіз таңба «?» таңбасына өзгертіледі) немесе жапондық (ISO-2022-JP) таңбалармен кодтауға түрлендіреді.

Quoted-printable кодтауын пайдалану – электрондық пошта хабарының көзі ASCII таңбаларын пайдаланатын Quoted-printable (QP) пішіміне кодталып және электрондық поштамен арнайы халықаралық таңбаларды 8 битті пішімде (áéíóú) дұрыс жібере алады.

4.4.1.12.1 Хабар пішімі

Қашықтағы компьютерлерден көрсетілетін оқиға хабарларының пішімін осы жерде реттей аласыз.

Қауіп туралы ескерту мен хабарландырулардың алдын ала әдепкі пішімі болады. Бұл пішімді өзгертпеуге кеңес беріледі. Дегенмен, кейбір жағдайларда (мысалы, сізде автоматты электрондық поштаны өңдеу жүйесі болғанда), хабар пішімін өзгерту қажет болуы мүмкін.

Хабардағы кілтсөздер (жолдар % таңбаларымен бөлінген) көрсетілген нақты ақпаратпен алмастырылады. Келесі кілтсөздер қолжетімді:

- — Оқиға күні мен уақыты.
- — Қатысты модуль
- — Ескерту орын алған компьютердің аты.
- — Ескертуді тудырған бағдарлама.
- — Вирус жұққан файлдың, хабардың, т.с.с. атауы
- — Жұққан зиянды элементтің атауы.
- **%ErrorDescription%** – Вирустық емес оқиғаның сипаттамасы

%InfectedObject% and **%VirusName%** кілт сөздері тек қауіп туралы ескерту хабарларында, ал **%ErrorDescription%** тек оқиға хабарларында пайдаланылады.

Жергілікті әліпби таңбаларын пайдалану — Электрондық поштаның хабарларын Windows жүйесінің жергілікті параметрлері негізінде кодталған (мысалы,Windows-1250) ANSI таңбасына түрлендіреді. Егер осы опцияға белгі қойылмаса, хабар ACSII 7 битте түрлендіріліп, кодталады (мысалы, «б» таңбасы «a» таңбасына және белгісіз таңба «?» таңбасына өзгереді).

Жергілікті таңбаны кодтауды пайдалану – электрондық пошта хабарының көзі ASCII таңбаларын пайдаланатын «Квоталанған басып шығару» (QP) пішіміне кодталып және электрондық поштамен арнайы халықаралық таңбаларды 8 битті пішімде (áéíóú) дұрыс жібере алады.

4.4.1.13 Талдайтын үлгіні таңдау

Файлды жіберу диалогтық терезесі файлды немесе сайтты ESET компаниясына талдауға жіберуге мүмкіндік береді және **Құралдар** > **Үлгіні талдауға жіберу** тармағынан табуға болады. Егер компьютеріңізден күдікті әрекет ететін файлды немесе интернеттен күдікті сайтты тапсаңыз, оны ESET вирус зертханасына талдауға жіберуіңізге болады. Егер файл зиянды бағдарлама немесе веб-сайт болып шықса, оны анықтау келесі жаңартуға қосылатын болады.

Оның орнына файлды электрондық пошта арқылы жіберуіңізге болады. Егер бұл опцияны дұрыс көрсеңіз, файл(дар)ды WinRAR/ZIP арқылы мұрағаттап, мұрағатты «infected» құпиясөзімен қорғаңыз да, оны samples@eset.com мекенжайына жіберіңіз. Сипаттаушы тақырыпты пайдаланыңыз және мүмкіндігінше көп ақпарат қосыңыз (мысалы, одан жүктелген веб-сайт).

ЕСКЕРТПЕ
Файлды «ESET» зертханасына жіберер алдында, оның төмендегі шарттардың біреуіне немесе бірнешеуіне сай екеніне көз жеткізіңіз:

- файл мүлдем анықталмайды
- файл қауіп ретінде қате анықталған

Талдау үшін қосымша ақпарат қажет болмаса, сіз жауап алмайсыз.

Файлды жіберу себебі ашылмалы мәзірінен хабарға ең сәйкес келетін сипаттаманы таңдаңыз:
- **Күдікті файл**
- **Күдікті сайт** (қандай да бір зиянкес бағдарламадан жұққан веб-сайт),
- **Жалған қате файл** (жұққан деп анықталған, бірақ жұқпаған файл),
- **Жалған қате сайт**
- **Басқа**

Файл/Сайт – Сіз жібергіңіз келіп жатқан файлдың немесе веб-сайттың жолы.

Байланыс электрондық поштасы – Бұл байланыс электрондық поштасы күдікті файлдармен бірге ESET компаниясына жіберіледі және талдауға қосымша ақпарат керек болса, сізге хабарласу үшін пайдаланылуы мүмкін. Электрондық байланыс поштасын енгізу міндетті емес. Үлгіні **анонимді түрде жіберуге** болады. Қосымша ақпарат қажет болмаса, барлық жазылымдарға жауап беруге мүмкіндік туғыза отырып, күн сайын біз серверлеріміз он мыңдаған файлдар алғанға дейін ESET компаниясынан жауап алмайсыз.

4.4.1.14 Microsoft Windows® жаңарту

Windows жаңарту мүмкіндігі – пайдаланушыларды зиянды бағдарламалық құралдан қорғаудың маңызды компоненті. Осы себепті Microsoft Windows жаңартулары қол жетімді болған кезде оларды орнату маңызды болып табылады. ESET NOD32 Antivirus бағдарламасы көрсетілген деңгейге сәйкес жоқ жаңартулар туралы хабарлайды. Келесі деңгейлер бар:

- **Жаңартулар жоқ** – Жүктеу үшін жүйелік жаңартулар ұсынылмайды.
- **Қосымша жаңартулар** – Төмен және жоғарырақ басымдылығы бар деп белгіленген жаңартулар жүктеу үшін ұсынылады.
- **Ұсынылған жаңартулар** – Жалпы және жоғарырақ басымдылығы бар деп белгіленген жаңартулар жүктеу үшін ұсынылады.
- **Маңызды жаңартулар** – Маңызды және жоғарырақ басымдылығы бар деп белгіленген жаңартулар жүктеу үшін ұсынылады.
- **Маңызды жаңартулар** – Тек маңызды жаңартулар жүктеу үшін ұсынылады.

Өзгертулерді сақтау үшін **OK** түймешігін басыңыз. Жаңарту серверінде күйді тексергеннен кейін «Жүйелік жаңартулар» терезесі көрсетіледі. Сәйкесінше, өзгертулерді сақтаудан кейін жүйелік жаңарту туралы ақпарат бірден қол жетімді болмауы мүмкін.

4.4.1.15 ESET CMD

Бұл — кеңейтілген ecmd пәрмендерін қосатын мүмкіндік. Ол пәрмен жолын (ecmd.exe) пайдаланып параметрлерді экспорттау және импорттау мүмкіндігін береді. Осы кезге дейін параметрлерді тек графикалық пайдаланушылық интерфейсті пайдаланып экспорттау және импорттау мүмкін болатын. ESET NOD32 Antivirus конфигурацияны *.xml* файлына экспорттауға болады.

ESET CMD пәрмен жолын қосқаннан кейін екі авторизациялау әдісі қолжетімді болады:

- **Жоқ** - авторизациясыз. Бұл әдіс ұсынылмайды, өйткені ол ықтимал қауіп болып табылатын кез келген қол қойылмаған конфигурацияны импорттауға мүмкіндік береді.
- **Кеңейтілген реттеудің құпиясөзі** - құпиясөзбен қорғау пайдаланылады. *.xml* файлынан конфигурацияны импорттағанда бұл файлға қол қойылуы керек (*.xml* конфигурация файлына қол қоюды төменде қараңыз). Бұл авторизациялау әдісі конфигурацияны импорттау кезінде Қатынасты реттеу ішінде көрсетілген құпиясөзге сәйкес келуін тексеру үшін құпиясөзді тексереді. Қатынасты реттеу қосылмаған болса, құпиясөз сәйкес емес болса немесе *.xml* конфигурация файлына қол қойылмаған болса, конфигурация импортталмайды.

ESET CMD пәрмен жолын қосқаннан кейін ESET NOD32 Antivirus конфигурациясын экспорттау/импорттау үшін пәрмен жолын пайдалануды бастауға болады. Мұны қолмен жасауға немесе автоматтандыру мақсатында сценарий жасауға болады.

МАҢЫЗДЫ
Кеңейтілген ecmd пәрмендерін пайдалану үшін әкімші артықшылықтарымен іске қосу керек немесе Windows пәрмен жолын (cmd) **Әкімші ретінде іске қосу** арқылы ашу керек. Олай етпесеңіз, **Error executing command.** хабарын аласыз. Сондай-ақ конфигурацияны экспорттау кезінде межелі қалта бар болуы керек.

ЕСКЕРТПЕ
Кеңейтілген ecmd пәрмендерін тек жергілікті іске қосуға болады. ERA арқылы **Пәрменді іске қосу** клиенттік тапсырмасын орындау жұмыс істемейді.

МЫСАЛ
Параметрлерді экспорттау пәрмені:

```
ecmd /getcfg c:\config\settings.xml
```

Параметрлерді импорттау пәрмені:

```
ecmd /setcfg c:\config\settings.xml
```

.xml конфигурация файлына кіру:

1. **XmlSignTool** құралын ESET құралдары мен қызметтік бағдарламаларын жүктеп алу бетінен жүктеп алып, мұрағаттан шығарыңыз. Бұл құрал арнайы eset *.xml* конфигурация файлдарына қол қою үшін әзірленген.
2. Windows пәрмен жолын (cmd) **Әкімші ретінде іске қосу** арқылы ашыңыз.
3. Орынға `XmlSignTool.exe`.
4. *.xml* конфигурация файлына қол қою пәрменін орындаңыз, пайдалану: `XmlSignTool <xml_file_path>`
5. XmlSignTool сұрағанда Кеңейтілген реттеу құпиясөзін енгізіңіз және қайта енгізіңіз. *.xml* конфигурация файлына енді қол қойылған және оны ESET NOD32 Antivirus бағдарламасының басқа данасында ESET CMD арқылы «Кеңейтілген реттеудің құпиясөзі» авторизациялау әдісін пайдаланып импорттау үшін пайдалануға болады.

ЕСКЕРТУ
ESET CMD пәрмен жолын авторизациялаусыз қосу ұсынылмайды, өйткені бұл кез келген қол қойылмаған конфигурацияны импорттауға мүмкіндік береді. Пайдаланушылардың рұқсат етілмеген өзгертуін болдырмау үшін **Кеңейтілген реттеу** > **Пайдаланушы интерфейсі** > **Қатынасты реттеу** тармағында құпиясөзді орнатыңыз.

4.5 Пайдаланушы интерфейсі

Пайдаланушы интерфейсі бөлімі бағдарламаның (GUI) «Графикалық пайдаланушы интерфейсінің» әрекетін конфигурациялауға мүмкіндік береді.

Графикалар құралын пайдаланып бағдарламаның көрінісін және пайдаланылатын әсерлерді реттеуге болады.

Ескертулер мен хабарландырулар конфигурациялау арқылы анықталған қауіп туралы ескертулер мен жүйелік хабарландырулардың әрекетін өзгертуге болады. Бұларды қажеттіліктеріңізге сай теңшеуге болады.

Қауіпсіздік бағдарламасының ең жоғары қауіпсіздігін қамтамасыз ету үшін Кіру параметрлері құралын пайдаланып параметрлерді құпиясөзбен қорғай отырып, барлық рұқсат етілмеген өзгертулерді болдырмауға болады.

4.5.1 Пайдаланушы интерфейсі элементтері

ESET NOD32 Antivirus бағдарламасындағы пайдаланушы интерфейсінің конфигурация опциялары жұмыс ортасын қажеттіліктеріңізге сай болатындай реттеуге мүмкіндік береді. Бұл конфигурация опцияларына ESET NOD32 Antivirus «Кеңейтілген орнату» тармағының **Пайдаланушы интерфейсі** > **Пайдаланушы интерфейсінің элементтері** тармағында кіруге болады.

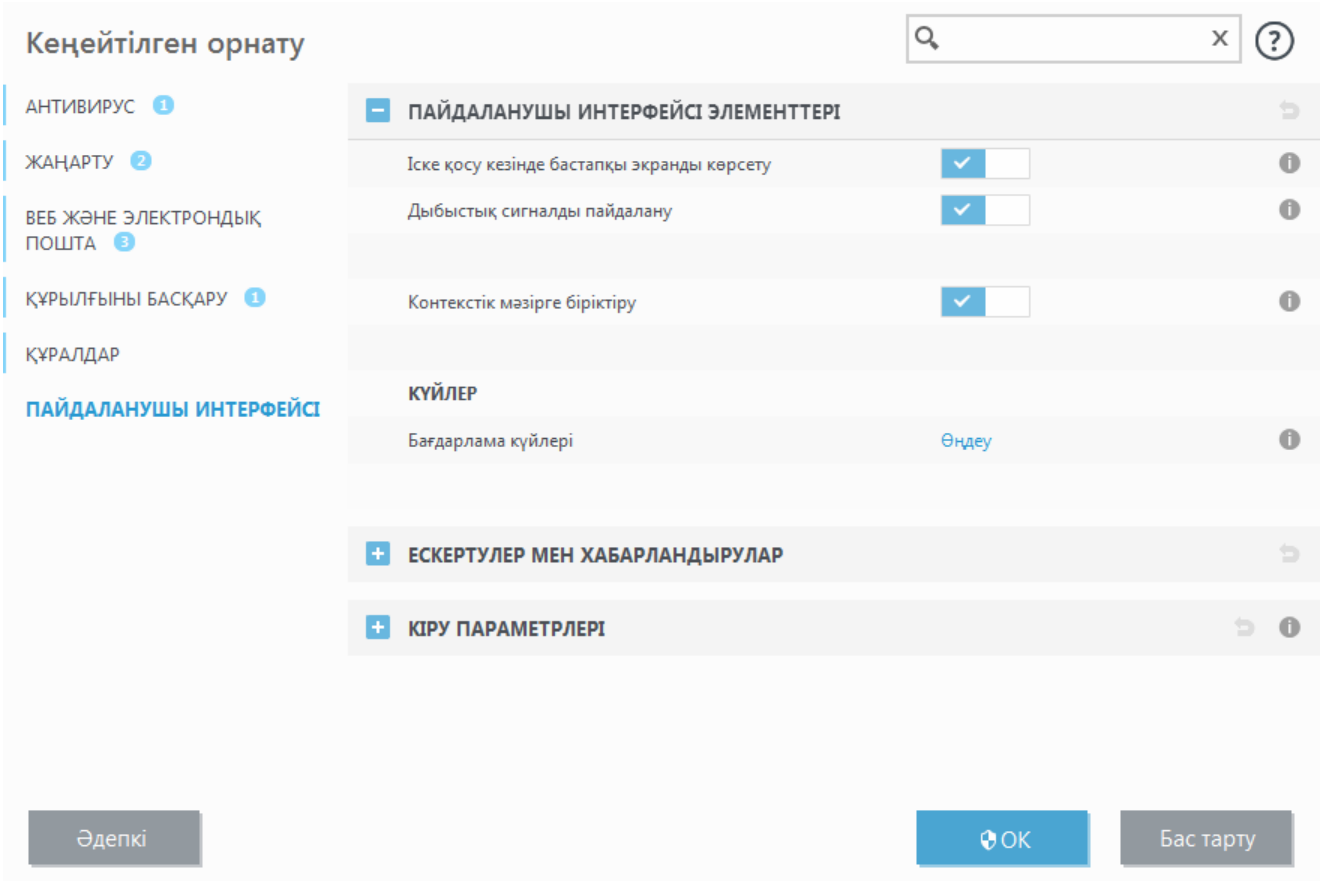
Егер ESET NOD32 Antivirus бастапқы экранын өшіргіңіз келсе, **Бастау кезінде жетілдірілген экранды көрсету** опциясын таңдаудан бас тартыңыз.

Қарап шығу кезінде маңызды оқиғалар болса, мысалы, қауіп анықталса немесе қарап шығу аяқталса, ESET NOD32 Antivirus бағдарламасында дыбыс ойнауы керек болса, **Дыбыс сигналын пайдалану** опциясын таңдаңыз.

Мәтінмәндік мәзірге біріктіру – Мәтінмәндік мәзірге ESET NOD32 Antivirus басқару элементтерін біріктіру.

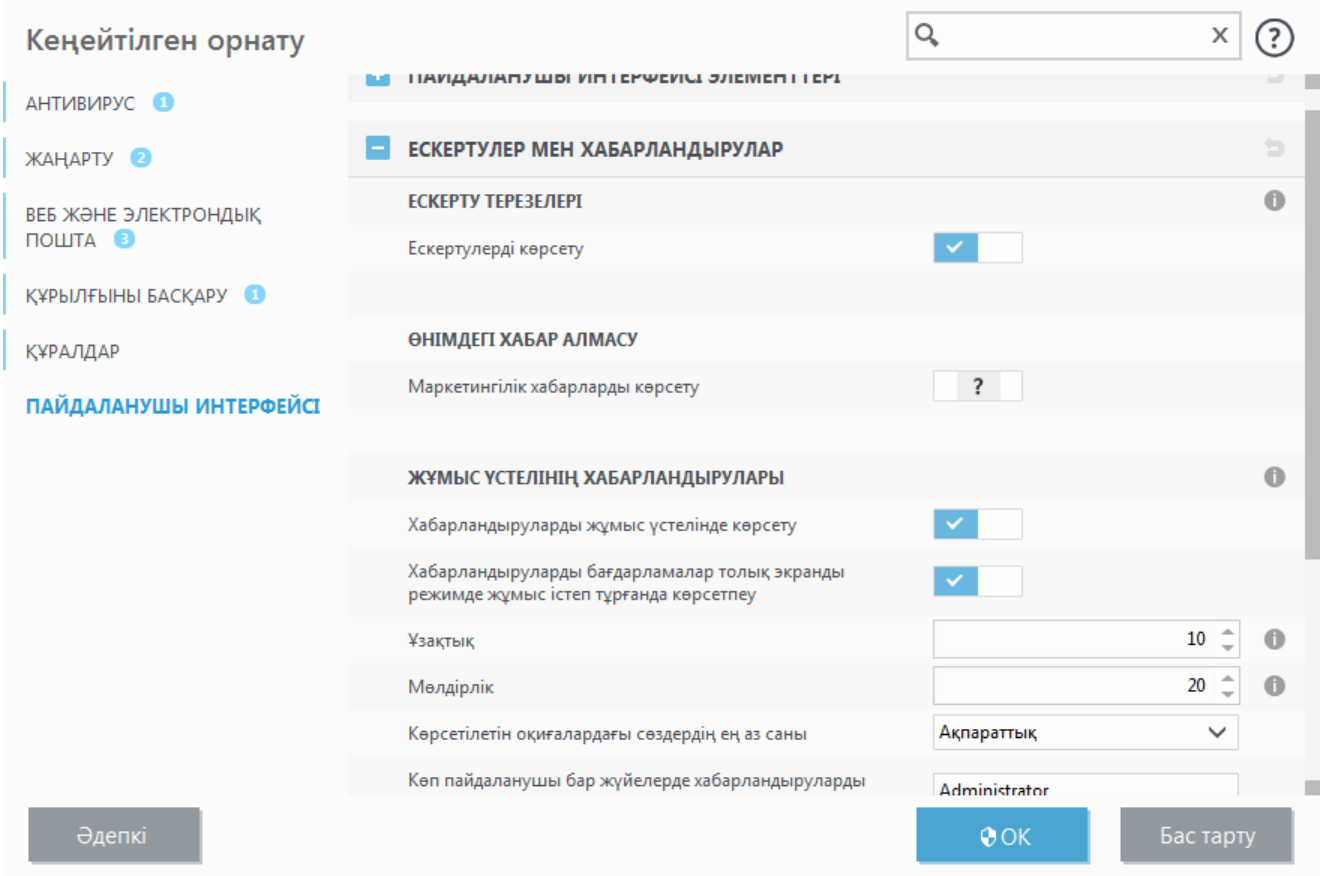
Күйлер

Қолданба күйлері – негізгі мәзірдің **Қорғау күйі** тақтасында көрсетілетін күйлерді басқару (өшіру) үшін **Өңдеу** түймесін басыңыз.



4.5.2 Ескертулер мен хабарландырулар

Пайдаланушы интерфейсі тармағындағы **Ескертулер мен хабарландырулар** бөлімі ESET NOD32 Antivirus бағдарламасы қауіп туралы ескертулер мен жүйе хабарландыруларын (мысалы, сәтті жаңарту туралы хабарлар) қолдану әдісін реттеуге мүмкіндік береді. Сондай-ақ, көрсету уақыты мен жүйелік тақта хабарландыруларының мөлдірлілік деңгейін (бұл тек жүйелік тақта хабарландыруларын қолдайтын жүйелерге қатысты) орнатуыңызға болады.



Ескерту терезелері

Ескертулерді көрсету опциясын өшіру барлық ескерту терезелерін өшіреді және белгілі бір жағдайлардың шектеулі санында ғана қолайлы. Пайдаланушылардың көпшілігі үшін бұл опцияның әдепкі параметрін (қосылған) қалдыру ұсынылады.

Өнімдегі хабар алмасу

Маркетингтік хабарларды көрсету – Өнім ішіндегі хабар алмасу пайдаланушыларға ESET жаңалықтарын және басқа хабарларды хабарлауға арналған. Маркетингілік хабарларды алғыңыз келмесе, бұл опцияны өшіріңіз.

Жұмыс үстелінің хабарландырулары

Жұмыс үстеліндегі хабарландырулар мен шығарылған аңғартпа көмексөздері тек ақпарат беруге арналған және пайдаланушының араласуын қажет етпейді. Олар экранның төменгі оң жақ бұрышындағы хабарландыру аумағында көрсетіледі. Жұмыс үстеліндегі ескертулерді іске қосу үшін **Хабарландыруларды жұмыс үстелінде көрсету** опциясын таңдаңыз.

Барлық интерактивті емес хабарландыруларды басу үшін **Хабарландыруларды бағдарламалар толық экранды режимде жұмыс істеп тұрғанда көрсетпеу** параметрін қосыңыз. Хабарландыруды көрсету уақыты мен терезе мөлдірлігі сияқты басқа егжей-тегжейлі опцияларды төменде өзгертуге болады.

Көрсетілетін оқиғалардағы сөздердің ең аз саны ашылмалы мәзірінен көрсетілетін ескертулер мен хабарландырулардың қауіптілік деңгейін таңдауға болады. Мына опциялар қол жетімді:

- **Диагностика** – Бағдарламаны және жоғарыдағы барлық жазбаларды дәл реттеу үшін керек ақпаратты журналға тіркейді.
- **Ақпараттық** – Ақпараттық хабарларды, соның ішінде сәтті жаңарту туралы хабарларды, оған қоса жоғарыдағы жазбалардың барлығын жазып алады.
- **Ескертулер** – Сындарлы қателерді және ескерту хабарларын жазып алады.
- **Қателер** – «Файлды жүктеп алу кезіндегі қате» сияқты қателер және сындарлы қателер жазып алынады.
- **Сындарлы** – Тек сындарлы қателерді (антивирустық қорғауды іске қосу кезіндегі қате) журналға тіркейді, т.б қосатын қателерді) ғана журналға жазады.

Бұл бөлімдегі соңғы мүмкіндік бірнеше пайдаланушы ортасында хабарландырулардың тағайындалған орнын конфигурациялауға мүмкіндік береді. **Көп пайдаланушы бар жүйелерде хабарландыруларды мына пайдаланушының экранынан көрсетіңіз** өрісінде бір уақытта бірнеше пайдаланушының қосылуына мүмкіндік беретін жүйелерде жүйелік және басқа хабарландыруларды қай пайдаланушы алатынын көрсетеді. Әдетте бұл жүйе немесе әкімші болады. Барлық жүйе ескертулері әкімшіге жіберілетін болса, бұл опция терминалдар серверлері үшін ерекше пайдалы.

Хабар терезелері

Белгілі бір уақыт кезеңінен кейін қалқымалы терезелерді автоматты түрде жабу үшін **Хабар терезелерін автоматты түрде жабу** опциясын таңдаңыз. Егер олар қолмен жабылмаса, ескерту терезелері көрсетілген уақыт аралығы біткеннен кейін автоматты түрде жабылады.

Растау хабарлары – Сіз көрсетуді немесе көрсетпеуді таңдай алатын растау хабарларының тізімін көрсетеді.

4.5.2.1 Кеңейтілген орнату

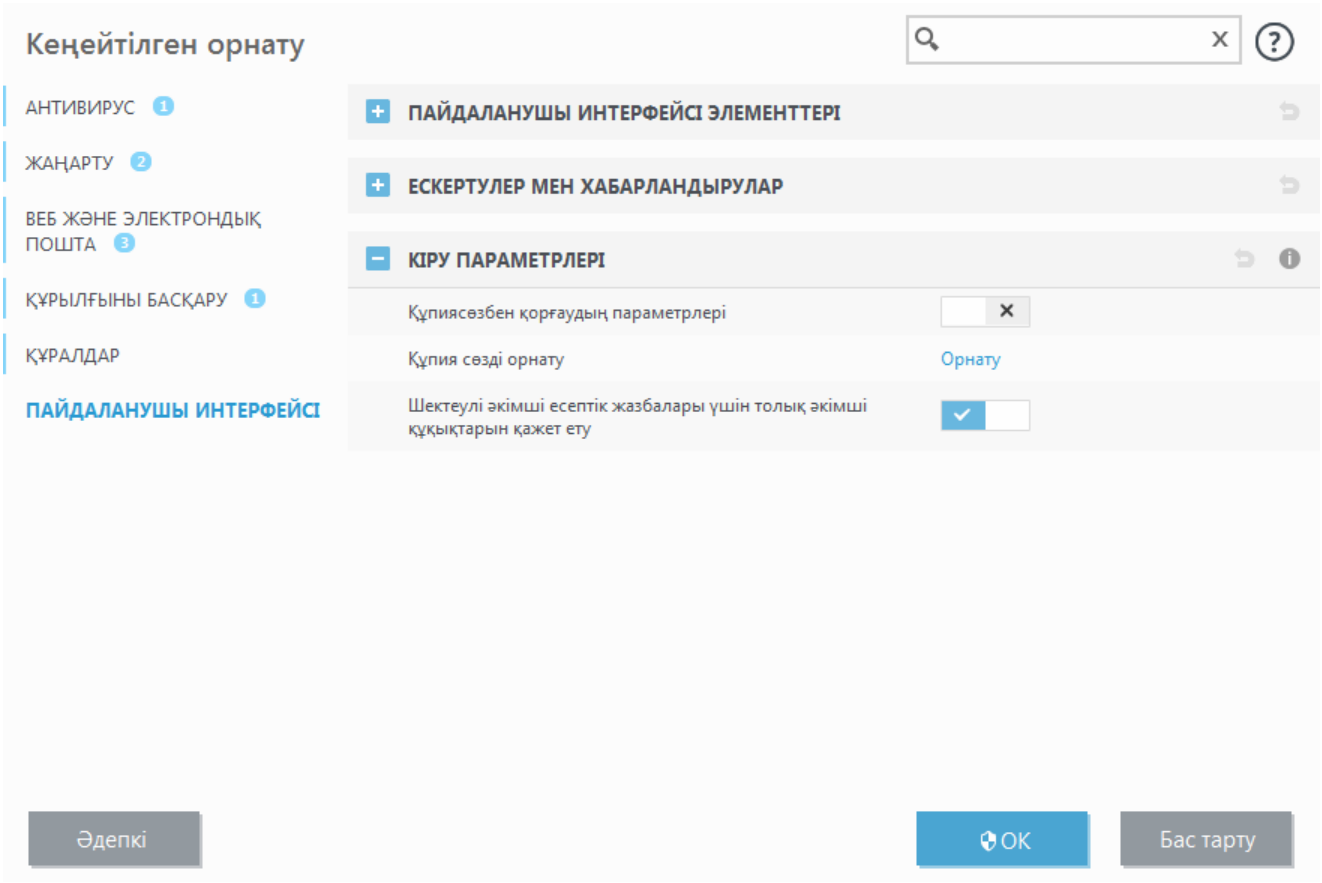
Көрсетілетін оқиғалардағы сөздердің ең аз саны ашылмалы мәзірінде көрсетілетін ескертулер мен хабарландырулардың бастапқы қауіптілік деңгейін таңдауға болады.

- **Диагностика** – Бағдарламаны және жоғарыдағы барлық жазбаларды дәл реттеу үшін керек ақпаратты журналға тіркейді.
- **Ақпараттық** – Ақпараттық хабарларды, соның ішінде сәтті жаңарту туралы хабарларды, оған қоса жоғарыдағы жазбалардың барлығын жазып алады.
- **Ескертулер** – Сындарлы қателерді және ескерту хабарларын жазып алады.
- **Қателер** – *«Файлды жүктеп алу кезіндегі қате»* сияқты қателер және сындарлы қателер жазып алынады.
- **Сындарлы** – Тек сындарлы қателерді (антивирустық қорғауды іске қосу кезіндегі қате) журналға тіркейді, т.б қосатын қателерді) ғана журналға жазады.

Бұл бөлімдегі соңғы мүмкіндік бірнеше пайдаланушы ортасында хабарландырулардың тағайындалған орнын конфигурациялауға мүмкіндік береді. **Көп пайдаланушы бар жүйелерде хабарландыруларды мына пайдаланушының экранынан көрсетіңіз** өрісінде бір уақытта бірнеше пайдаланушының қосылуына мүмкіндік беретін жүйелерде жүйелік және басқа хабарландыруларды алатын пайдаланушы көрсетіледі. Әдетте бұл жүйе немесе әкімші болады. Барлық жүйе ескертулері әкімшіге жіберілетін болса, бұл опция терминалдар серверлері үшін ерекше пайдалы.

4.5.3 Кіру параметрлері

ESET NOD32 Antivirus параметрлері қауіпсіздік саясатының шешуші бөлімі болып табылады. Рұқсат етілмеген өзгертулер жүйенің тұрақтылығы мен қорғанысына ықтимал қауіп төндіруі мүмкін. Рұқсат етілмеген өзгертулерді болдырмау үшін ESET NOD32 Antivirus бағдарламасының орнатылған параметрлерін құпиясөзбен қорғауға болады.



Құпиясөзбен қорғау параметрлері – құпиясөз параметрлерін көрсетіңіз. «Құпия сөзді орнату» терезесін ашу үшін басыңыз.

Орнату параметрлерін қорғайтын құпия сөзді орнату немесе өзгерту үшін **Орнату** түймесін басыңыз.

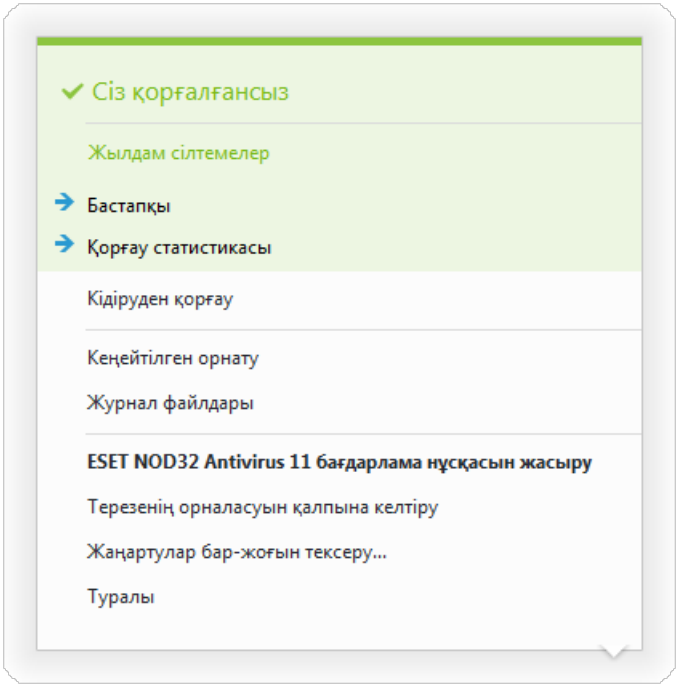
Шектеулі әкімші жазбалары үшін толық әкімші құқықтарын қажет ету — Белгілі бір жүйелік параметрлерді (Windows Vista және Windows 7 жүйелерінде Пайдаланушы есептік жазбасын бақылау (UAC) параметріне ұқсас) өзгерту барысында әкімшінің пайдаланушы аты мен құпия сөзін енгізуге ағымдағы пайдаланушыны шақыру (егер оның әкімші құқығы болмаса) үшін осы параметрді таңдаңыз. Осындай өзгертулер қорғау модульдерін ажыратуды қамтиды. UAC іске қосылмайтын Windows XP жүйесінде пайдаланушылардың **Әкімші құқықтарын талап ету (UAC қолдауы жоқ жүйе)** опциясы қол жетімді.

Тек Windows XP үшін:

Әкімші құқықтарын талап ету (UAC қолдауы жоқ жүйе) – ESET NOD32 Antivirus әкімші тіркелгі деректерін талап етуі үшін осы опцияны қосыңыз.

4.5.4 Бағдарлама мәзірі

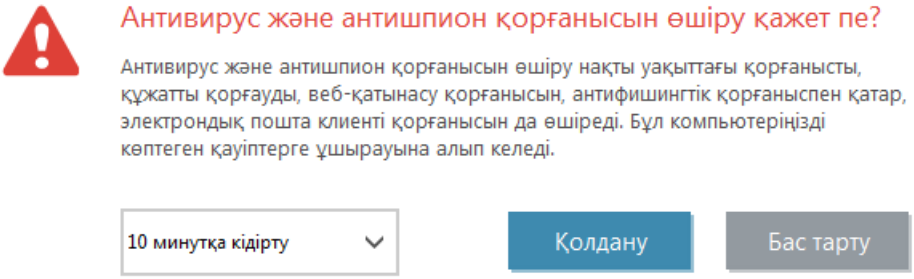
Кейбір ең маңызды реттеу опциялары және мүмкіндіктері жүйелік тақта белгішесін тінтуірдің оң жақ түймесімен басу арқылы қол жетімді.



Жылдам сілтемелер - ESET NOD32 Antivirus бағдарламасының ең жиі пайдаланылатын бөліктерін көрсетеді. Бұларға бағдарлама мәзірінен тез қатынасуға болады.

Қорғауды кідірту - Антивирустық және антишпиондық қорғауды өшіретін растау диалогтық терезесін көрсетеді, ол файл, веб және электрондық пошта байланысын басқару арқылы зиянкес жүйелік шабуылдардан қорғайды.

Уақыт аралығы ашылмалы мәзірі «Антивирустық және антишпиондық» қорғау өшірулі болатын уақыт аралығын білдіреді.



Кеңейтілген орнату — Бұл опцияны **Кеңейтілген реттеу** ағашына кіру үшін таңдаңыз. Сондай-ақ, Кеңейтілген орнатуды ашудың басқа жолдары бар, мысалы, F5 пернесін басу немесе **Орнату** > **Кеңейтілген орнату** тармағына өту.

Журнал файлдары - Журнал файлдары орын алған маңызды бағдарлама оқиғалары туралы ақпаратты қамтиды және анықталған қауіптерді шолуды береді.

ESET NOD32 Antivirus жасыру – ESET NOD32 Antivirus терезесін экраннан жасыру.

Терезенің орналасуын қалпына келтіру – ESET NOD32 Antivirus бағдарламасының терезесін экранда әдепкі өлшеміне және орнына қалпына келтіреді.

Жаңартулар бар-жоғын тексеру — Зиянкес кодқа қарсы қорғау деңгейін қамтамасыз ету үшін анықтау механизмін (бұрын «вирус қолтаңбаларының дерекқоры» ретінде белгілі болған) жаңартуды бастайды.

Туралы - жүйе туралы ақпаратты, орнатылған ESET NOD32 Antivirus нұсқасы және орнатылған бағдарлама модульдері туралы мәліметтерді береді. Осы жерден операциялық жүйе мен жүйе ресурстары туралы ақпаратты және лицензия мерзімінің аяқталу күнін таба аласыз.

5. Озық пайдаланушы

5.1 Профильдер

Профиль реттегіші ESET NOD32 Antivirus ішінде екі жерде пайдаланылады – **Талап бойынша компьютерді қарап шығу** бөлімінде және **Жаңарту** бөлімінде.

Компьютерді қарап шығу

Таңдаулы қарап шығу параметрлерін болашақ қарап шығу үшін сақтауға болады. Әр тұрақты түрде пайдаланылатын қарап шығу үшін басқа профильді (әр түрлі қарап шығу нысандары, қарап шығу әдістері және басқа параметрлер бар) жасау ұсынылады.

Жаңа профиль жасау үшін «Кеңейтілген орнату» терезесін ашып (F5), **Антивирус** > **Талап бойынша компьютерді қарап шығу** > **Негізгі** > **Профильдер тізімі** тармағын басыңыз. **Профиль реттегіші** терезесі бар қарап шығу профильдері және жаңасын жасау опциясы берілген **Таңдалған профиль** ашылмалы мәзірін қамтиды. Қажеттіліктеріңізге сай қарап шығу профилін жасауда көмек алу үшін ThreatSense механизмінің параметрлерін орнату бөлімінде қарап шығуды реттеудің әр параметрінің сипаттамасын қараңыз.

ЕСКЕРТПЕ
Жеке қарап шығу профилін жасау керек және **Компьютерді қарап шығу** конфигурациясы ішінара қолайлы, бірақ орындау уақыты бумалаушыларын немесе ықтимал қауіпті бағдарламаларды қарап шығу керек емес және **Қатаң тазалау** опциясын қолдану керек делік. Жаңа профиль атауын **Профильдер реттегіші** терезесінде енгізіп, **Қосу** түймесін басыңыз. Жаңа профильді **Таңдалған профиль** ашылмалы мәзірінен таңдаңыз және қалған параметрлерді талаптарға сай реттеңіз және жаңа профильді сақтау үшін **OK** түймесін басыңыз.

Жаңарту

«Жаңартуды орнату» бөліміндегі профиль өңдегіші пайдаланушыларға жаңа жаңарту профильдерін жасауға мүмкіндік береді. Компьютеріңіз жаңарту серверлеріне қосылу үшін бірнеше әдісті пайдаланса ғана жеке теңшелетін профильдерді (әдепкі **Менің профилім** профилінен басқа) жасаңыз және пайдаланыңыз.

Мысалы, әдетте жергілікті желідегі жергілікті серверге (айна) қосылатын, бірақ жергілікті желіден ажыратылған кезде (іссапар) жаңартуларды тікелей ESET жаңарту серверлерінен жүктеп алатын екі профильді пайдалануы мүмкін: біріншісін жергілікті серверге қосылу үшін; екіншісін ESET серверлеріне қосылу үшін. Профильдер конфигурацияланғаннан кейін **Құралдар** > **Жоспарлағыш** тармағына өтіп, жаңарту тапсырмасының параметрлерін өңдеңіз. Бір профильді негізгі ретінде және екіншісін қосымша ретінде белгілеңіз.

Жаңарту профилы – Қазіргі уақытта пайдаланылатын жаңарту профилі. Оны өзгерту үшін ашылмалы мәзірде профильді таңдаңыз.

Профильдер тізімі – Жаңасын жасау немесе бар жаңарту профильдерін жою.

5.2 Пернелер тіркесімдері

ESET өнімінде жақсырақ шарлау үшін келесі перне тіркесімдерін пайдалануға болады:

F1	анықтама беттерін ашады
F5	Қосымша орнатуды ашады
Up/Down	өнімдегі элементтерді шарлау
-	"Кеңейтілген орнату" ағаш түбірін қайырады
TAB	терезеде меңзерді жылжытады
Esc	белсенді диалогтық терезені жабады

5.3 Диагностикалар

Диагностикалар ESET процестерінің (мысалы, *ekrn*) бағдарламаның бұзылуының дамптарын қамтамасыз етеді. Бағдарлама бұзылса, дамп жасалады. Бұл әзірлеушілерге ақауларды жоюға және әр түрлі ESET NOD32 Antivirus мәселелерін түзетуге көмектеседі. **Дамп түрі** жанындағы ашылмалы мәзірді басып, үш қол жетімді опцияның біреуін таңдаңыз:

- Осы мүмкіндікті өшіру үшін **Өшіру** (әдепкі) опциясын таңдаңыз.
- **Шағын** – Қолданба неге күтпеген жерде жағылысқанын анықтауға көмектесуі мүмкін пайдалы ақпараттың ең шағын жиынын жазып алады. Бұл дамп файлының түрін бос орын шектеулі болғанда пайдалы болуы мүмкін, бірақ, шектеулі ақпарат болғандықтан, мәселе пайда болған уақытта орындалып жатқан ағын тікелей тудырмаған қателер осы файлды талдау кезінде анықталмауы мүмкін.
- **Толық** – Қолданба күтпеген жерде тоқтағанда жүйелік жадтың бүкіл мазмұнын жазып алады. Толық жад дампында жад дампы жиналып жатқанда орындалып жатқан процестердің деректері болуы мүмкін.

Протокол сүзудің кеңейтілген журнал жүргізуін қосу – әзірлеушілерге протоколды сүзуге қатысты мәселелерді диагностикалауға және шешуге көмектесу үшін протоколды сүзу арқылы өтетін бүкіл желілік деректерді PCAP пішімінде жазады.

«Жаңарту механизмінің кеңейтілген журналын жүргізу» параметрін қосу – Жаңарту процесінің барысында орын алатын барлық оқиғаларды жазып алады. Бұл әзірлеушілерге жаңарту механизміне қатысты мәселелерді диагностикалауға және шешуге көмектеседі.

Журнал файлдарын келесі сілтемеден табуға болады:
Windows Vista және одан кейінгі нұсқаларда *C:\ProgramData\ESET\ESET NOD32 Antivirus\Diagnostics* немесе Windows жүйесінің ескірек нұсқаларында *C:\Documents and Settings\All Users\...*.

Мақсатты каталог – Жағылыс кезіндегі дамп жасалатын каталог.

Диагностика қалтасын ашу – Осы каталогты жаңа *Windows explorer* терезесінде ашу үшін **Ашу** түймесін басыңыз.

Диагностикалық дампты жасау – **Мақсатты каталог** ішінде диагностикалық дампты жасау үшін **Жасау** түймесін басыңыз.

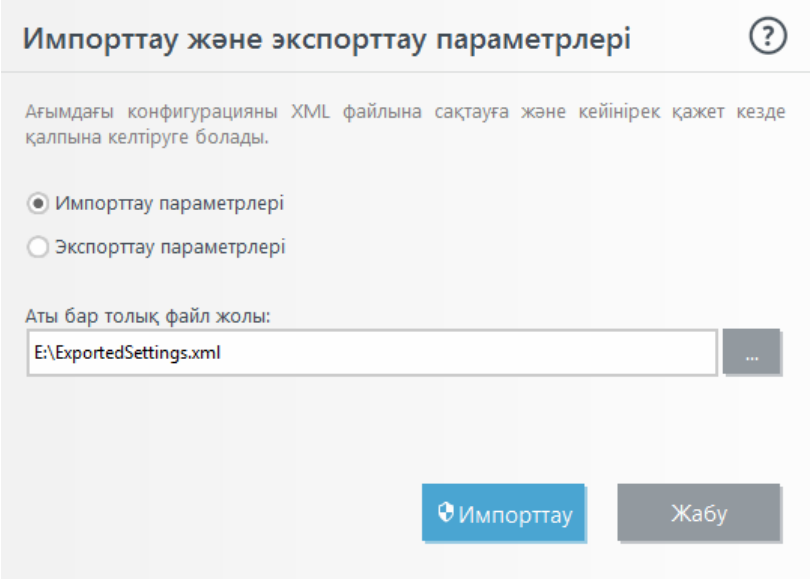
5.4 Импорттау және экспорттау параметрлері

Реттелген ESET NOD32 Antivirus .xml конфигурация файлын **Орнату** мәзірінен импорттауға немесе экспорттауға болады.

Кейінгі уақытты қолдану үшін ESET NOD32 Antivirus бағдарламасының ағымдағы конфигурациясының сақтық көшірмесін жасау қажет болса, конфигурация файлдарын импорттау және экспорттау пайдалы. Сондай-ақ, экспорттау параметрлері опциясы бірнеше жүйеде таңдаулы конфигурацияны пайдаланғысы келетін пайдаланушылар үшін қолайлы, олар параметрлерді тасымалдау үшін *.xml* файлын оңай импорттай алады.

Конфигурацияны импорттау өте оңай. Негізгі бағдарлама терезесінде **Орнату** > **Импорттау және экспорттау параметрлері** тармағына өтіңіз де, **Импорттау параметрлері** опциясын таңдаңыз. Конфигурацияның файл атауын енгізіңіз немесе импорттау керек конфигурацияға өту үшін **...** түймешігін басыңыз.

Конфигурацияны экспорттау қадамдары осыған ұқсас. Негізгі бағдарлама терезесінде **Орнату** > **Импорттау және экспорттау параметрлері** тармағын басыңыз. **Экспорттау параметрлері** опциясын таңдап, конфигурацияның файл атауын (мысалы *export.xml*) енгізіңіз. Браузерді пайдаланып компьютерде конфигурация файлын сақтау орнын таңдаңыз.



ЕСКЕРТПЕ
Экспортталған файлды арнайы каталогқа жазуға жеткілікті құқықтарыңыз болмаса, параметрлерді экспорттау кезінде қате пайда болуы мүмкін.

5.5 ESET SysInspector

5.5.1 ESET SysInspector бағдарламасына кіріспе

ESET SysInspector – компьютеріңізді мұқият тексеріп шығып, жиналған деректерді жан-жақты көрсететін бағдарлама. Орнатылған драйверлер мен бағдарламалар, желілерге қосылу немесе маңызды тіркелім жазбалары туралы ақпарат сияқты мәліметтер жүйедегі не бағдарламаға, не аппараттық құрал үйлесімді болмауына, не зиянды бағдарламаның жұғуына байланысты жүйедегі күдікті әрекеттерді зерттеуге көмектеседі.

ESET SysInspector бағдарламасына екі жолмен кіруге болады: ESET Security шешіміндегі біріктірілген нұсқадан немесе «ESET» веб-сайтынан оқшау нұсқаны (SysInspector.exe) тегін жүктеу арқылы. Екі нұсқаның да қызмет етуі бірдей және бағдарламаны басқару элементтері бірдей. Жалғыз айырмашылық – шығыстарды басқару әдісі. Оқшауланған және біріктірілген нұсқалардың әрқайсысы жүйе суреттерін *.xml* файлға экспорттауға және оларды дискіге сақтауға мүмкіндік береді. Бірақ, біріктірілген нұсқа, сонымен бірге, жүйе суреттерін тікелей **Құралдар** > **ESET SysInspector** бағдарламасына сақтауға мүмкіндік береді (ESET Remote Administrator басқа). Қосымша ақпарат алу үшін мына бөлімді қараңыз ESET NOD32 Antivirus бағдарламасының бөлімі ретінде ESET SysInspector.

ESET SysInspector бағдарламасы компьютерді қарап шығуын күте тұрыңыз. Жабдық конфигурациясына, операциялық жүйеге және компьютерде орнатылған бағдарламалар санына байланысты 10 секундтан бірнеше минутқа дейін созылуы мүмкін.

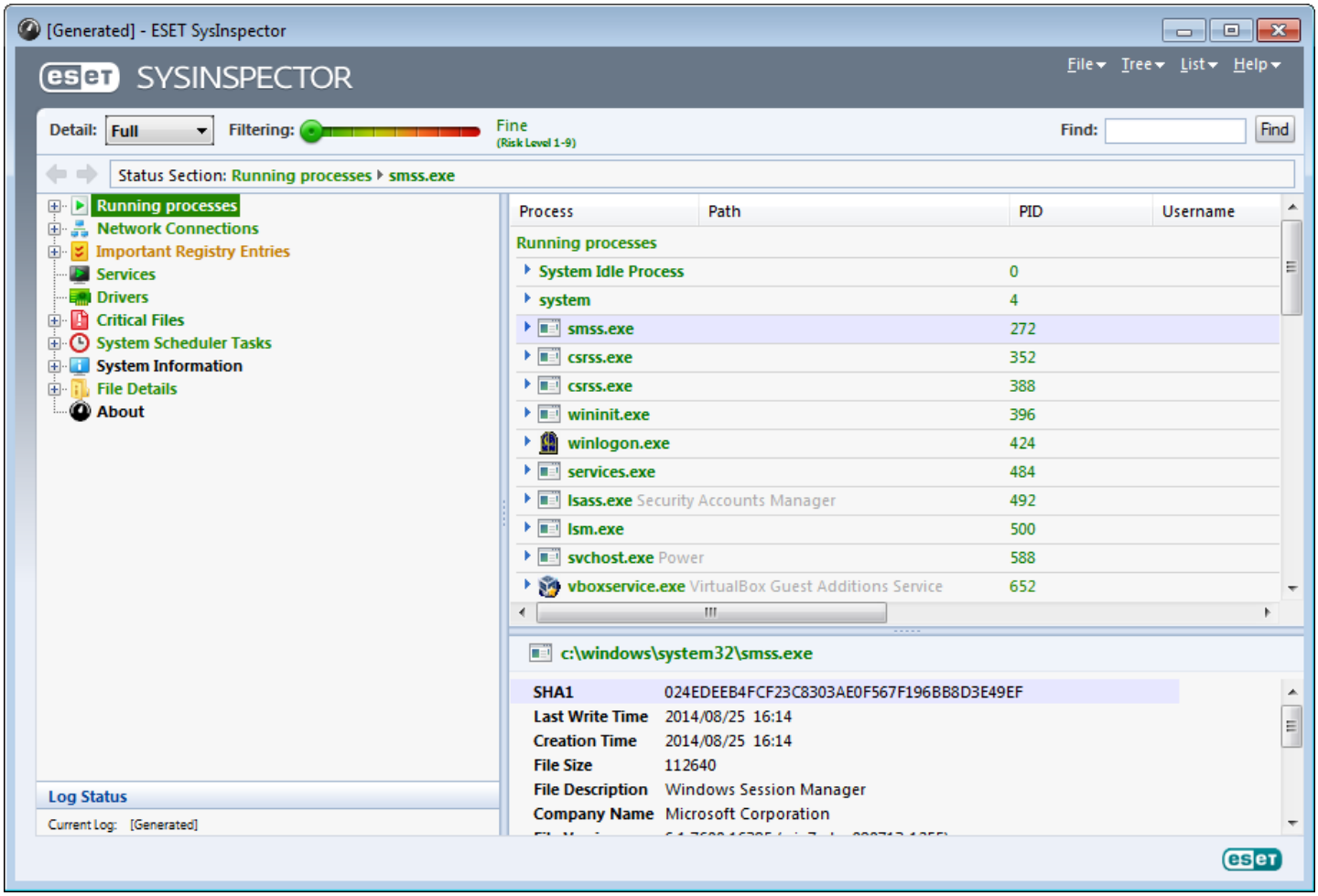
5.5.1.1 ESET SysInspector бағдарламасын іске қосу

ESET SysInspector бағдарламасын іске қосу үшін ESET веб-торабынан жүктеген *SysInspector.exe* орындалатын файлын жай ғана орындаңыз. Егер орнатылған ESET Security шешімдерінің бірі әлдеқашан бар болса, ESET SysInspector бағдарламасын тікелей «Бастау мәзірінен» (**Бағдарламалар** > **ESET** > **ESET NOD32 Antivirus** түймешігін басыңыз) іске қосуыңызға болады.

Бірнеше минутқа созылуы мүмкін бағдарламаның жүйені тексеруін күте тұрыңыз.

5.5.2 Пайдаланушы интерфейсі мен бағдарламаның пайдаланылуы

Түсінікті болуы үшін бағдарламаның негізгі терезесі төрт бөлімге бөлінген – бағдарламаның басқару элементтері бағдарламаның негізгі терезесінің жоғарғы жағында, шарлау терезесі сол жағында, сипаттама терезесі оң жағында, ал мәліметтер терезесі төменде орналасқан. Журнал күйі бөлімінде журналдың негізгі параметрлерінің тізімі (пайдаланылған сүзгі, сүзгі түрі, журналдың салыстырудың нәтижесі екені, т.б.) беріледі.



5.5.2.1 Бағдарламаның басқару элементтері

Бұл бөлімде ESET SysInspector бағдарламасында бар басқару элементтерінің барлығының сипаттамасы бар.

Файл

File тармағын басу арқылы ағымдағы есеп күйін кейінірек зерттеу үшін сақтауға немесе бұрын сақталған есепті ашуға болады. Жариялау мақсаттарында **Жіберуге ыңғайлы** журналын жасау ұсынылады. Бұл формада журнал маңызды ақпаратты қалдырып кетеді (ағымдағы пайдаланушы аты, компьютер атауы, домен атауы, ағымдағы пайдаланушы артықшылықтары, орта айнымалылары, т.б.).

Ескертпе: Бұрын сақталған ESET SysInspector есептерін бағдарламаның негізгі терезесіне апарып тастау арқылы ғана ашуға болады.

Тармақ

Барлық түйіндерді шығарып алуға немесе жабуға және таңдалған бөлімдерді қызметтік сценарийге экспорттауға мүмкіндік береді.

Тізім

Оның құрамында бағдарламада шарлауды жеңілдететін функциялар мен желіде ақпарат табу сияқты басқа функциялар бар.

Анықтама

Мұның құрамында бағдарлама мен оның функциялары туралы ақпарат бар.

Мәлімет

Бұл параметр ақпаратты жұмыс істеуге жеңілдету үшін бағдарламаның негізгі терезесінде көрсетілетін ақпаратқа әсер етеді. «Негізгі» режимде жүйедегі әдеттегі мәселелердің шешімдерін табу үшін пайдаланылатын ақпаратқа рұқсатыңыз болады. "Орташа" режимде бағдарлама азырақ пайдаланылатын мәліметтерді көрсетеді. "Толық" режимде ESET SysInspector өте спецификалық мәселелерді шешуге арналған барлық ақпаратты көрсетеді.

Сүзу

Элементтерді сүзуді жүйедегі күдікті файлдарды немесе тіркелім жазбаларын табу үшін пайдаланған дұрыс. Жүгірткіні реттеу арқылы элементтерді қауіп деңгейлері бойынша сүзуге болады. Егер жүгірткі шеткі сол жаққа орнатылған болса (1 қауіп деңгейі), онда барлық элементтер көрсетіледі. Жүгірткіні оңға қарай жылжытқанда, бағдарлама ағымдағы қауіп деңгейінен қаупі төменірек барлық элементтерді сүзеді және көрсетілген деңгейден күдіктірек элементтерді ғана көрсетеді. Жүгірткі шеткі оң жақта болса, бағдарлама тек белгілі қауіпті элементтерді көрсетеді.

6-дан 9-ға дейінгі қауіп деңгейіне қойылған барлық элементтер қауіпсіздік қатерін тудыруы мүмкін. Егер қауіпсіздік шешімін ESET арқылы пайдаланбайтын болсаңыз, жүйені ESET Online Scanner арқылы ESET SysInspector қандай да бір элементті тапқан жағдайда қарап шығу ұсынылады. ESET Online Scanner тегін қызмет болып табылады.

Ескертпе: Элементтің қауіп деңгейін элементтің түсін «Қауіп деңгейі» жүгірткісінің түсімен салыстыру арқылы тез анықтауға болады.

Салыстыру

Екі журналды салыстыру үшін барлық элементтерді көрсетуді, тек қосылған элементтерді көрсетуді, тек жойылған элементтерді немесе тек орны ауыстырылған элементтерді көрсетуді таңдауға болады.

Табу

Іздеуді белгілі бір элементті аты немесе атының бір бөлігі арқылы табу үшін пайдалануға болады. Іздеу сұрауының нәтижелері сипаттама терезесінде көрсетіледі.

Қайтару

Кері немесе алға көрсеткілерін түрту арқылы сипаттама терезесінде бұрын көрсетілген ақпаратқа оралуға болады. Кері немесе алға басу орнына Backspace және Space пернелерін пайдалануға болады.

Күй бөлімі

Шарлау терезесінде ағымдағы түйінді көрсетеді.

Маңызды: Қызылмен ерекшеленген элементтер белгісіз, осы себепті бағдарлама оларды ықтимал қауіпті деп белгілейді. Егер элемент қызыл болса, бұл автоматты түрде файлды жоюға болатынын білдірмейді. Жоюдан бұрын, файлдардың шынымен қауіпті немесе қажет емес екеніне көз жеткізіңіз.

5.5.2.2 ESET SysInspector бағдарламасында шарлау

ESET SysInspector әртүрлі ақпарат түрлерін түйіндер деп аталатын бірнеше негізгі бөлімдерге бөледі. Бар болған жағдайда әр түйіннің ішіндегі түйіндерді шығарып алу арқылы қосымша мәліметтерді табуға болады. Түйінді ашу немесе қайыру үшін түйіннің атын екі рет басыңыз немесе түйін атының жанындағы ⊞ немесе ⊟ түймешігін басыңыз. Шарлау терезесіндегі түйіндер мен ішкі түйіндердің тармақты құрылымын шолу барысында сипаттама терезесінде көрсетілген әрбір түйін туралы әртүрлі мәліметтерді табуға болады. Сипаттама терезесіндегі элементтерді шолу барысында мәліметтер терезесінде әрбір элемент үшін қосымша мәліметтер көрсетілуі мүмкін.

Төменде шарлау терезесіндегі негізгі түйіндеріне арналған сипаттамалар мен сипаттама және мәліметтер терезелеріндегі қатысты ақпарат берілген.

Іске қосылған процестер

Бұл түйіннің құрамында есепті жасау барысында жұмыс істеп жатқан бағдарламалар мен процестер туралы ақпарат бар. Сипаттама терезесінде әр үрдіс туралы қосымша мәліметтерді, мысалы, үрдіс пайдаланып жатқан динамикалық кітапханалар мен олардың жүйедегі орналасуы, бағдарлама жеткізушісі мен файлдың қауіп деңгейі, т.б. туралы мәліметтерді, табуға болады.

Мәліметтер терезесінде сипаттама терезесінде таңдалған элементтер туралы ақпарат, мысалы, файлдың өлшемі немесе оның тор белгісі туралы ақпарат бар.

Ескертпе: Операциялық жүйе басқа пайдаланушылық бағдарламалар үшін негізгі және аса маңызды функцияларды қамтамасыз ететін үздіксіз жұмыс істейтін және бірнеше маңызды ядро компоненттерінен тұрады. Белгілі бір жағдайларда, мұндай процестер ESET SysInspector құралында \??\ деп басталатын файл жолымен бірге көрсетіледі. Бұл таңбалар мұндай үрдістер үшін орнату алдындағы оңтайландырумен қамтамасыз етеді, олар жүйе үшін қауіпсіз болып табылады.

Желілік қосылымдар

Сипаттама терезесінде желіде шарлау терезесінде таңдалған хаттаманы (TCP немесе UDP) пайдаланып, желі арқылы байланысатын үрдістер мен бағдарламалардың тізімін бағдарлама қосылатын қашықтағы мекенжаймен бірге қамтиды. Сондай-ақ, DNS серверлердің IP мекенжайларын тексеруге болады.

Мәліметтер терезесінде сипаттама терезесінде таңдалған элементтер туралы ақпарат, мысалы, файлдың өлшемі немесе оның тор белгісі туралы ақпарат бар.

Маңызды тіркеу енгізілімдері

Жүйеге қатысты түрлі мәселелерге, мысалы іске қосылған кездегі бағдарламаларды көрсету, браузердің көмекші нысандары (BHO), т.б. сияқты қатысты таңдалған тіркелім жазбаларының тізімі бар.

Сипаттама терезесінде белгілі бір тіркеу жазбаларына қай файлдар қатысты екенін табуға болады. Қосымша мәліметтерді мәліметтер терезесінен көруге болады.

Қызметтер

Сипаттама терезесінде Windows қызметтері ретінде тіркелген файлдардың тізімі бар. Қызметтің мәліметтер терезесіндегі файлдың белгілі бір мәліметтерімен бірге іске қосылуы үшін орнатылатын жолын тексеруге болады.

Драйверлер

Жүйеде орнатылған драйверлердің тізімі.

Маңызды файлдар

Сипаттама терезесі Microsoft Windows операциялық жүйесіне қатысты маңызды файлдардың мазмұнын көрсетеді.

Жүйе жоспарлағышы тапсырмалары

Көрсетілген уақытта/аралықта «Windows тапсырма жоспарлағышымен» басталған тапсырмалар тізімін құрайды.

Жүйелік ақпарат

Аппараттық құрал мен бағдарламалық құрал туралы егжей-тегжейлі ақпаратты, сондай-ақ, орнатылған орта айнымалылары, пайдаланушы құқықтары және жүйелік оқиғалар журналы туралы ақпаратты қамтиды.

Файл туралы мәліметтер

Маңызды жүйелік файлдар мен «Program Files» қалтасындағы файлдардың тізімі. Сипаттама және мәліметтер терезелерінен файлдарға қатысты қосымша ақпаратты табуға болады.

Туралы

Бағдарлама модульдері тізімі және ESET SysInspector нұсқасы туралы ақпарат.

5.5.2.2.1 Пернелер тіркесімдері

ESET SysInspector бағдарламасымен бірге жұмыс істегенде пайдалануға болатын пернетақта тіркесімдері мыналарды қамтиды:

Файл

Ctrl+O	бар журналды ашады
Ctrl+S	жасалған журналдарды сақтайды

Жасау

Ctrl+G	компьютер күйінің стандартты суретін жасайды
Ctrl+H	Сондай-ақ, құпия ақпаратқа кіре алатын компьютер күйінің суретін жасайды

Элементтерді сүзу

1, O	жақсы, қауіп деңгейі 1 мен 9 аралығындағы элементтер көрсетіледі
2	жақсы, қауіп деңгейі 2 мен 9 аралығындағы элементтер көрсетіледі
3	жақсы, қауіп деңгейі 3 мен 9 аралығындағы элементтер көрсетіледі
4, U	белгісіз, қауіп деңгейі 4 пен 9 аралығындағы элементтер көрсетіледі
5	белгісіз, қауіп деңгейі 5 пен 9 аралығындағы элементтер көрсетіледі
6	белгісіз, қауіп деңгейі 6 пен 9 аралығындағы элементтер көрсетіледі
7, B	қауіпті, қауіп деңгейі 7 мен 9 аралығындағы элементтер көрсетіледі
8	қауіпті, қауіп деңгейі 8 мен 9 аралығындағы элементтер көрсетіледі
9	қауіпті, қауіп деңгейі 9 деген элементтер көрсетіледі
-	қауіп деңгейін азайтады
+	қауіп деңгейін көбейтеді
Ctrl+9	сүзу режимі, тең немесе жоғарырақ деңгей
Ctrl+0	сүзу режимі, тек тең деңгей

Көрініс

Ctrl+5	жеткізуші бойынша қарау, барлық жеткізушілер
Ctrl+6	жеткізуші бойынша қарау, тек Microsoft
Ctrl+7	жеткізуші бойынша қарау, барлық басқа жеткізушілер
Ctrl+3	толық мәліметтерді көрсетеді
Ctrl+2	орташа мәліметтерді көрсетеді
Ctrl+1	негізгі бейнебет
BackSpace	бір қадам кері жылжытады
Бос орын	бір қадам алға жылжытады
Ctrl+W	ағашты шығарып алады
Ctrl+Q	ағашты тасалайды

Басқа басқару элементтері

Ctrl+T	іздеу нәтижелерінде таңдағаннан кейін элементтің бастапқы орнына өтеді
Ctrl+P	элемент туралы негізгі ақпаратты көрсетеді
Ctrl+A	элемент туралы толық ақпаратты көрсетеді
Ctrl+C	ағымдағы элементтің ағашын көшіреді
Ctrl+X	элементтерді көшіреді
Ctrl+B	таңдалған файлдар туралы интернеттен ақпарат табады
Ctrl+L	таңдалған файл орналасқан қалтаны ашады
Ctrl+R	тіркелім өңдегішінде сәйкес жазбаны ашады
Ctrl+Z	файлдың жолын көшіреді (егер элемент файлға байланысты болса)
Ctrl+F	іздеу өрісіне ауысады
Ctrl+D	іздеу нәтижелерін жабады
Ctrl+E	қызметтік сценарийді орындау

Салыстыру

Ctrl+Alt+O	бастапқы / салыстырмалы журналды ашады
Ctrl+Alt+R	салыстырудан бас тартады

Ctrl+Alt+1	барлық элементтерді көрсетеді
Ctrl+Alt+2	тек қосылған элементтерді көрсетеді, журнал ағымдағы журналда бар элементтерді ғана көрсетеді
Ctrl+Alt+3	тек жойылған элементтерді көрсетеді, журнал бұрынғы журналда бар элементтерді ғана көрсетеді
Ctrl+Alt+4	тек ауыстырылған элементтерді (файлдармен қоса) көрсетеді
Ctrl+Alt+5	тек журналдардың арасындағы айырмашылықтарды көрсетеді
Ctrl+Alt+C	салыстыруды көрсетеді
Ctrl+Alt+N	ағымдағы журналды көрсетеді
Ctrl+Alt+P	бұрынғы журналды ашады

Аралас

F1	анықтаманы қарап шығу
Alt+F4	бағдарламаны жабу
Alt+Shift+F4	бағдарламаны сұрамай жабу
Ctrl+I	журнал статистикасы

5.5.2.3 Салыстыру

Салыстыру мүмкіндігі пайдаланушыға екі қолданыстағы журналды салыстыруға мүмкіндік береді. Бұл мүмкіндіктің нәтижесі – екі журналға ортақ емес элементтер жиыны. Бұл жүйедегі өзгерістерді бақылау үшін ыңғайлы, зиянды кодты табуға көмектесетін құрал болып табылады.

Ол іске қосылғаннан кейін, бағдарлама жаңа терезеде көрсетілетін жаңа журналды жасайды. Журналды файлға сақтау үшін **Файл** > **Журналды сақтау** түймешігін басыңыз. Тіркеу файлдарын кейінірек ашуға және көруге болады. Қолданыстағы журналды ашу үшін **Файл** > **Журналды ашу** түймешігін басыңыз. Бағдарламаның негізгі терезесінде ESET SysInspector бағдарламасы әрқашан бір уақытта бір журналды көрсетеді.

Екі журналды салыстырудың пайдасы: ағымдағы белсенді журналды және файлда сақталған журналды көруге болады. Журналдарды салыстыру үшін **Файл** > **Журналдарды салыстыру** түймешігін басып, **Файлды таңдау** параметрін таңдаңыз. Таңдалған журнал бағдарламаның негізгі терезесіндегі белсенді журналмен салыстырылады. Салыстырмалы журнал тек осы екі журналдың арасындағы айырмашылықты көрсетеді.

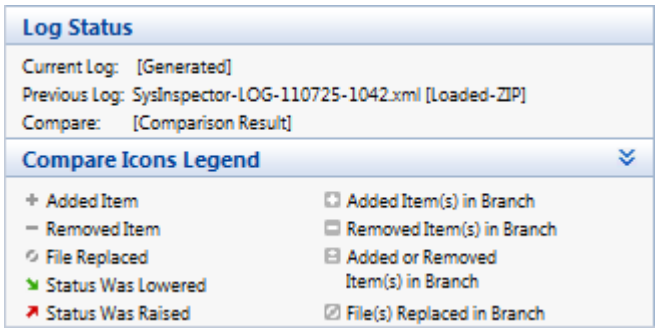
Ескертпе: Екі тіркеу файлын салыстырған жағдайда **Файл** > **Журналды сақтау** түймешігін оны ZIP файл ретінде сақтау үшін басыңыз; екі файл да сақталады. Егер кейінірек осы файлда ашсаңыз, журналдар автоматты түрде салыстырылады.

Көрсетілген элементтердің жанында ESET SysInspector салыстырылған журналдардың арасындағы айырмашылықтарды білдіретін таңбаларды көрсетеді.

Элементтердің жанында көрсетуге болатын барлық таңбалардың сипаттамасы:

- + жаңа мән, алдыңғы журналда жоқ
- ▫ ағаш құрылымы бөлімінде жаңа мәндер бар
- − жойылған мән, тек алдыңғы журналда бар
- ▫ ағаш құрылымы бөлімінде жойылған мәндер бар
- ✎ мән / файл өзгертілді
- ▫ ағаш құрылымы бөлімінде өзгертілген мәндер / файлдар бар
- ↘ қауіп деңгейі артты / ол алдыңғы журналда жоғарырақ еді
- ↗ қауіп деңгейі артты / ол алдыңғы журналда төменірек еді

Сол жақтағы төменгі бұрышта көрсетілетін түсіндіру бөлімі барлық таңбаларды сипаттайды, сондай-ақ салыстырылып жатқан журналдардың аттарын көрсетеді.



Кез келген салыстырмалы журналды файлға сақтап, кейінірек ашуға болады.

Мысал

Жүйе туралы бастапқы ақпаратты жазатын журналды жасап, оны previous.xml деп аталатын файлға сақтаңыз. Жүйеге өзгертулер жасалғаннан кейін, ESET SysInspector бағдарламасын ашыңыз, ол жаңа журнал жасайды. Оны *current.xml* атты файлға сақтаңыз.

Осы екі журнал арасындағы өзгерістерді бақылау үшін **Файл** > **Журналдарды салыстыру** түймешігін басыңыз. Бағдарлама журналдардың арасындағы айырмашылықтарды көрсететін салыстырмалы журналды жасайды.

Егер сіз төмендегі команда жолы опциясын пайдалансаңыз, дәл осы нәтижеге қол жеткізуге болады:

SysIsnpector.exe current.xml previous.xml

5.5.3 Команда жолының параметрлері

ESET SysInspector бағдарламасы осы параметрлердің көмегімен есептер жасауды қолдайды:

/gen	GUI орнатусыз журналды тікелей пәрмен жолынан жасау
/privacy	маңызды ақпараты жоқ журнал жасау
/zip	шығыс журналын zip мұрағатында қысылған күйде сақтау
/silent	пәрмен жолынан журнал жасау кезінде өңдеу терезесін қысу
/бос	ESET SysInspector қызметін журнал жасамай/жүктемей іске қосу

Мысалдар

Пайдалану:
`Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]`

Белгілі бір журналды тікелей браузерге жүктеу үшін мынаны пайдаланыңыз: *SysInspector.exe .\clientlog.xml*
Журналды пәрмен жолынан жасау үшін мынаны пайдаланыңыз: *SysInspector.exe /gen=.\mynewlog.xml*
Құпия ақпарат қосылмаған журналды тікелей қысылған файлда жасау үшін мынаны пайдаланыңыз: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Екі журнал файлын салыстырып, ерекшеліктерді шолу үшін мынаны пайдаланыңыз: *SysInspector.exe new.xml old.xml*

Ескертпе: Файл/қалта атауында бос орын бар болса, онда атты тырнақшаға алу керек.

5.5.4 Қызметтік сценарий

Қызметтік сценарийі жүйеден қалаусыз нысандарды оңай алып тастау арқылы ESET SysInspector пайдаланатын тұтынушыларға көмек көрсетеді.

Қызметтік сценарий пайдаланушыға бүкіл ESET SysInspector журналын немесе оның таңдалған бөліктерін экспорттауға мүмкіндік береді. Экспорттаудан кейін қалаусыз нысандарды жойылсын деп белгілеуге болады. Содан кейін белгіленген нысандарды жою үшін өзгертілген журналды іске қосуға болады.

Қызметтік сценарий жүйелік мәселелерді диагностикалауда тәжірибесі бар озық пайдаланушылар үшін жасалған. Сәйкес емес өзгертулер операциялық жүйенің бүлінуіне әкелуі мүмкін.

Мысал

Егер компьютерге антивирус бағдарламасы таппаған вирус жұққан деп күмәндансаңыз, төмендегі қадамдық нұсқауларды орындаңыз:

1. Жаңа жүйе суретін жасау үшін ESET SysInspector құралын іске қосыңыз.
2. Сол жақ бөлімдегі (ағаш құрылымда) бірінші элементті таңдап, Shift пернесін басып, барлық элементтерді белгілеу үшін соңғы элементті таңдаңыз.
3. Таңдалған нысандарды тінтуірдің оң жақ түймешігімен басып, **Қызметтік сценарийге таңдалған бөлімдерді экспорттау** опциясын таңдаңыз.
4. Таңдалған нысандар жаңа журналға экспортталады.
5. Бұл бүкіл процедурадағы ең шешуші қадам: жаңа журналды ашып, жойғыңыз келетін барлық нысандар үшін - төлсипатын + төлсипатына өзгертіңіз. Ешқандай маңызды операциялық жүйе файлдарын/нысандарын таңбаламағаныңызға көз жеткізіңіз.
6. ESET SysInspector ашып, **Файл** > **Қызметтік сценарийді орындау** тармағына өтіп, сценарий жолын енгізіңіз.
7. Сценарийді орындау үшін **OK** түймешігін басыңыз.

5.5.4.1 Қызметтік сценарийді жасау

Сценарий құру үшін ESET SysInspector негізгі терезесіндегі мәзір тармағынан (сол жақ аумақта) кез келген элементті тінтуірдің оң жақ пернесімен басыңыз. Контекстік мәзірде **Қызметтік сценарийге барлық бөлімдерді экспорттау** немесе **Қызметтік сценарийге таңдалған бөлімдерді экспорттау** опциясын таңдаңыз.

Ескертпе: Екі журналды салыстырып жатқанда қызметтік сценарийді экспорттау мүмкін емес.

5.5.4.2 Қызметтік сценарийдің құрылымы

Сценарийдің тақырыбындағы бірінші жолда Механизмдік нұсқа (ev), GUI нұсқасы (gv) және Журнал нұсқасы (lv) туралы ақпаратты табуыңызға болады. Бұл деректерді сценарийді жасайтын .xml файлындағы ықтимал өзгертулерді бақылау және орындау кезіндегі кез келген үйлесімсіздіктерді болдырмау үшін пайдалануға болады. Сценарийдің бұл бөлігін өзгертпеу керек.

Файлдың қалған бөлігі элементтерді өңдеуге (сценарий өңдейтіндерін көрсетуге) болатын бөлімдерге бөлінеді. Өңдеу керек элементтерді элемент алдындағы «-» таңбасын «+» таңбасына ауыстыру арқылы белгілейсіз. Сценарийдегі бөлімдер бір бірінен бос жолмен бөлінеді. Әр бөлімнің нөмірі мен тақырыбы бар.

01) Іске қосылған процестер

Бұл бөлімде жүйеде іске қосылған барлық процестердің тізімі болады. Әр процесс UNC жолымен, содан кейін, жұлдызшалар ішіндегі (*) CRC16 хэш кодымен анықталады.

Мысал:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Бұл мысалда module32.exe процесі таңдалды («+» таңбасымен белгіленген); процесс сценарий орындалғанда аяқталады.

02) Жүктелген модульдер

Бұл бөлімде қазіргі уақытта пайдаланылып жатқан жүйелік модульдер тізілген.

Мысал:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Бұл мысалда khbekhb.dll модулі «+» таңбасымен белгіленді. Сценарий іске қосылғанда, ол сол нақты модульді пайдаланып процестерді танып, оларды аяқтайды.

03) TCP қосылымдары

Бұл бөлімде бар TCP қосылымдары туралы ақпарат бар.

Мысал:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Сценарий іске қосылғанда, ол белгіленген TCP қосылымдарындағы сокет иесін тауып, сокетті тоқтатып, жүйе ресурстарын босатады.

04) UDP соңғы нүктелері

Бұл бөлімде бар UDP соңғы нүктелері туралы ақпарат бар.

Мысал:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Сценарий іске қосылғанда, ол белгіленген UDP соңғы нүктелерінде сокет иесін оқшаулап, сокетті тоқтатады.

05) DNS серверінің жазбалары

Бұл бөлімде ағымдағы DNS серверінің конфигурациясы туралы ақпарат бар.

Мысал:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Белгіленген DNS серверінің жазбалары сценарийді іске қосқанда жойылады.

06) Маңызды тіркелім жазбалары

Бұл бөлімде маңызды тіркелім жазбалары туралы ақпарат бар.

Мысал:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Белгіленген жазбалар сценарийді іске қосқанда жойылады, 0 байт мәндеріне азайтылады немесе әдепкі мәндеріне ысырылады. Нақты жазбаға қолданылатын әрекет жазба санатына және нақты тіркелімдегі кілт мәніне байланысты.

07) Қызметтер

Бұл бөлімде жүйеде тіркелген қызметтер тізілген.

Мысал:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Сценарий орындалғанда, қызметтер белгіленеді және тәуелді қызметтер тоқтатылып, жойылады.

08) Драйверлер

Бұл бөлімде орнатылған драйверлер тізілген.

Мысал:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:
\windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Сценарийді орындағанда, таңдалған драйверлер тоқтатылады. Кейбір драйверлер тоқтауға рұқсат бермейтінін ескеріңіз.

09) Маңызды файлдар

Бұл бөлімде амалдық жүйенің тиісті түрде қызмет етуі үшін маңызды файлдар туралы ақпарат бар.

Мысал:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Таңдалған элементтер жойылады немесе бастапқы мәндеріне қойылады.

10) Жоспарланған тапсырмалар

Бұл бөлім жоспарланған тапсырмалар туралы ақпаратты қамтиды.

Мысал:

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.5.4.3 Қызметтік сценарийлерді орындау

Барлық қалаған элементтерді белгілеп, сақтап, сценарийді жабыңыз. Өңделген сценарийді ESET SysInspector негізгі терезесінен **Қызметтік сценарийді іске қосу** параметрін Файл мәзірінен таңдау арқылы іске қосыңыз. Сценарийді ашқанда, бағдарлама келесі хабарды шығарады: **Шынымен «%Scriptname%» қызметтік сценарийін іске қосқыңыз келе ме?** Таңдауды растағаннан кейін іске қосуға тырысып жатқан қызметтік сценарийге әлі қол қойылмағаны туралы хабарлайтын басқа ескерту пайда болуы мүмкін. Сценарийді іске қосу үшін **Іске қосу** түймешігін басыңыз.

Диалогтық терезе сценарийдің сәтті орындалғанын растайды.

Егер сценарийді тек ішінара өңдеу мүмкін болса, келесі хабар бар диалогтық терезе пайда болады: **Қызметтік сценарий жартылай іске қосылды. Қателер туралы есепті қарап шыққыңыз келе ме?** Орындалмаған әрекеттер тізілген күрделі қате туралы есепті көру үшін **Иә** параметрін таңдаңыз.

Егер сценарий танылмаса, диалогтық терезе келесі хабармен шығады: **Таңдалған қызметтік сценарийге қол қойылмаған. Қол қойылмаған және белгісіз сценарийлерді іске қосу компьютер деректеріне айтарлықтай зиян келтіруі мүмкін. Шынымен сценарийді іске қосып, әрекеттерді орындағыңыз келе ме?** Мұны сценарий ішіндегі үйлесімсіздіктер (бүлінген тақырып, бүлінген бөлім тақырыбы, бөлімдер арасындағы жоқ бос жол, т.б.) тудыруы мүмкін. Сценарий файлын қайта ашып, қателерді түзетуге немесе жаңа қызметтік сценарийді жасауға болады.

5.5.5 ЖҚС

ESET SysInspector бағдарламасын іске қосу үшін әкімшілік артықшылықтар қажет пе?

ESET SysInspector іске қосылу үшін әкімшілік артықшылықтарды қажет етпегенімен, жинақтардағы кейбір деректерге тек әкімші есептк жазбасынан кіруге болады. Оны стандартты пайдаланушы немесе шектеулі пайдаланушы ретінде іске қосу операциялық орта туралы аз ақпарат жинауға алып келеді.

ESET SysInspector бағдарламасы журнал файлын жасай ма?

ESET SysInspector бағдарламасы компьютер конфигурациясының журнал файлын жасай алады. Мұндай жұрналды сақтау үшін бағдарламаның негізгі мәзірдегі **Файл** > **Журналды сақтау** түймешігін басыңыз. Журналдар XML пішімінде сақталады. Әдепкі мәні бойынша, файлдар *%USERPROFILE%\Менің құжаттарым*\ каталогында "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML" файл атауымен сақталады. Қаласаңыз, тіркеу файлының орны мен атын сақтаудан бұрын басқаша етіп өзгерте аласыз.

ESET SysInspector журнал файлын қалай көруге болады?

ESET SysInspector жасаған тіркеу файлын қарап шығу үшін бағдарламаны іске қосып, бағдарламаның негізгі мәзірдегі **Файл** > **Журнал ашу** түймешігін басыңыз. Сондай-ақ, файлдарды ESET SysInspector бағдарламасына апарып тастауға болады. Егер ESET SysInspector журнал файлдарын жиі көру керек болса, жұмыс үстелінде SYSINSPECTOR.EXE файлына тіркесімді жасау ұсынылады; журнал файлдарын көру үшін соған апарып тастауға болады. Қауіпсіздік себептері бойынша Windows Vista/7 жүйесі әр түрлі қауіпсіздік рұқсаттары бар терезелердің арасында апарып тастауға тыйым салуы мүмкін.

Тіркеу файлы пішімінің сипаттамасы бар ма? SDK бумасы үшін ше?

Қазіргі уақытта тіркеу файлы үшін де, SDK бумасы үшін де сипаттама жоқ, өйткені бағдарлама әлі әзірленуде. Бағдарлама шығарылғаннан кейін, біз оларды тұтынушылардың кері байланысына және талаптарына қарай қамтамасыз ете аламыз.

ESET SysInspector белгілі бір нысан тудыратын қауіпті қалай бағалайды?

Көп жағдайларда, ESET SysInspector әр нысанның сипаттамасын тексеріп, зиянды әрекет ықтималдылығын бағалайтын бірқатар эвристикалық ережелерді пайдаланып, нысандарға (файлдар, үрдістер, тіркелім пернесі және т.с.с.) қауіп деңгейлерін тағайындайды. Осы эвристикаға негізделіп, нысандарға *1 - Жақсы (жасыл)* – *9 - Қауіпті (қызыл)* аралығындағы қауіп деңгейі тағайындалады. Сол жақтағы шарлау аумағында, бөлімдер ішіндегі нысанның ең жоғары қауіп деңгейіне қарай боялады.

«6 – Белгісіз (қызыл)» қауіп деңгейі қауіпті дегенді білдіре ме?

ESET SysInspector бағалары нысанның зиянды екеніне кепілдік бермейді, бұл шешімді қауіпсіздік сарапшысы қабылдауы керек. ESET SysInspector қауіпсіздік сарапшыларын жылдам бағалаумен қамтамасыз ету үшін жасалған. Осылайша сарапшылар жүйедегі қандай нысандарда әдеттен тыс әрекеттерді бақылау керек екенін біледі.

ESET SysInspector іске қосылғанда неліктен интернетке қосылады?

Көптеген бағдарламалар секілді, ESET SysInspector бағдарламасына «ESET» компаниясы шығарғанына және өзгертілмегеніне көз жеткізу үшін сандық қолтаңба – «куәлік» қолы қойылған. Куәлікті тексеру үшін операциялық жүйе бағдарламаны шығарушының мәліметтерін тексеруге куәлік орталығына хабарласады. Бұл Microsoft Windows жүйесіндегі барлық сандық қолтаңба қойылған бағдарламалардың қалыпты әрекеттері.

Ұрлыққа қарсы технология дегеніміз не?

Ұрлыққа қарсы технология руткитті тиімді табумен қамтамасыз етеді.

Егер жүйеге руткит секілді әрекет ететін зиянды код шабуыл жасаса, пайдаланушыға деректерді жоғалуы немесе ұрлануы қаупі туады. Руткитке қарсы арнайы құралсыз руткиттерді табу мүмкін емес дерлік.

Неліктен кейде бір уақытта әр түрлі «Компания атауы» жазбасы бар, «MS қол қойған» ретінде белгіленген файлдар болады?

Орындалатын файлдың сандық қолтаңбасын анықтауға әрекет жасағанда, ESET SysInspector алдымен файлға енгізілген сандық қолтаңба бар-жоқтығын тексереді. Егер сандық қолтаңба табылса, онда файл осы ақпараттың көмегімен тексеріледі. Файлда сандық қолтаңба табылмаса, «ESI» өңделген орындалатын файл туралы ақпаратты қамтитын сәйкес «CAT» файлды («Қауіпсіздік каталогы» - *%systemroot%\system32\catroot*) іздей бастайды. Тиісті CAT файлы табылған жағдайда, орындалатын файлды тексеру үрдісінде аталған CAT файлдың сандық қолтаңбасы қолданылады.

«MS қол қойған» деп белгіленген, бірақ басқа «КомпанияАтауы» жазбасы бар файлдардың болу себебі осы.

Мысал:

Windows 2000 жүйесіне *C:\Program Files\Windows NT* жолында орналасқан HyperTerminal бағдарламасы кіреді. Негізгі бағдарламаның орындалатын файлына сандық қолтаңба қойылмайды, бірақ ESET SysInspector оны Microsoft қол қойған файл ретінде белгілейді. Мұның себебі – *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* ішіндегі to *C:\Program Files\Windows NT\hypertrm.exe* файлына (HyperTerminal бағдарламасының негізгі орындалатын файлы) нұсқайтын сілтеме және *sp4.cat* файлына Microsoft компаниясының сандық қолтаңба қоюы.

5.5.6 ESET NOD32 Antivirus ESET SysInspector бөлімі ретінде

ESET SysInspector бөлімін ESET NOD32 Antivirus ашу үшін **Құралдар** > **ESET SysInspector** тармағын басыңыз. ESET SysInspector терезесіндегі басқару жүйесі компьютерді қарап шығу журналдарының немесе жоспарланған тапсырмалардағы басқару жүйелерімен бірдей. Жүйелік суреттермен орындалатын барлық әрекеттерге – жасау, қарап шығу, салыстыру, жою және экспорттау – бір немесе екі рет басумен жетуге болады.

ESET SysInspector терезесінде жасалған суреттер туралы негізгі ақпарат, мысалы, жасалған уақыты, қысқа түсініктеме, суретті жасаған пайдаланушының аты және суреттің күйі сияқты ақпарат болады.

Суреттерді салыстыру, жасау немесе жою үшін ESET SysInspector терезесіндегі суреттер тізімінің астында орналасқан сәйкес түймелерді пайдаланыңыз. Бұл опциялар да контекстік мәзірде бар. Таңдалған суретті көру үшін контекстік мәзірден **Көрсету** опциясын таңдаңыз. Таңдалған суретті файлға экспорттау үшін оны тінтуірдің оң жақ түймесімен басып, **Экспорттау...** командасын таңдаңыз.

Төменде қол жетімді опциялардың егжей-тегжейлі сипаттамасы берілген:

- **Салыстыру** - Бар екі журналды салыстыруға мүмкіндік береді. Бұл ағымдағы жұрнал мен ескірек жұрналдың арасындағы өзгерістерді бақылау үшін ыңғайлы. Опция күшіне енуі үшін салыстырылатын екі суретті таңдау керек.
- **Жасау...** - Жаңа жазба жасайды. Бұдан бұрын жазба туралы қысқа түсініктеме енгізу керек. Сурет (ағымдағы жасалатын сурет) жасау прогресін анықтау үшін **Күй** бағанын қараңыз. Барлық аяқталған суреттерге **Жасалған** күйінің белгісі қойылады.
- **Жою/Барлығын жою** - Жазбаларды тізімнен алып тастайды.
- **Экспорттау...** - Таңдалған жазбаны XML файлында сақтайды (сондай-ақ, қысылған ZIP нұсқасында).

5.6 Команда жолы

антивирустық модулін пәрмен жолы арқылы іске қосуға болады – қолмен («ecls» пәрмені арқылы) немесе бума («bat») файлы арқылы. ESET команда жолы сканерін пайдалану:

```
ecls [ОПЦИЯЛАР..] ФАЙЛДАР..
```

Команда жолынан талап бойынша қарап шығу құралын іске қосқанда келесі параметрлер мен қосқыштарды пайдалануға болады:

Опциялар

/base-dir=FOLDER	ҚАЛТА ішінен модульдерді жүктеу
/quar-dir=FOLDER	ҚАЛТАНЫ карантинге көшіру
/exclude=MASK	БҮРКЕНІШКЕ сәйкес келген файлдарды қарап шықпау
/subdir	ішкі қалталарды қарап шығу (әдепкі)
/no-subdir	ішкі қалталарды қарап шықпау

/max-subdir-level=LEVEL	қаралатын қалталардың жоғарғы ішкі деңгейі
/symlink	таңбалық сілтемелермен жүру (әдепкі)
/no-symlink	таңбалық сілтемелерді өткізу
/ads	ADS қарап шығу (әдепкі)
/no-ads	ADS қарап шықпау
/log-file=FILE	ФАЙЛ шығысын тіркеу
/log-rewrite	шығыс файлды қайта жазу (әдепкі – үстеу)
/log-console	пульт шығысын тіркеу (әдепкі)
/no-log-console	пульт шығысын тіркемеу
/log-all	таза файлдарды да тіркеу
/no-log-all	таза файлдарды тіркемеу (әдепкі)
/aind	әрекеттер көрсеткішін көрсету
/auto	барлық жергілікті дискілерді қарап шығу және автоматты түрде тазалау

Қарап шығу опциялары

/files	файлдарды қарап шығу (әдепкі)
/no-files	файлдарды қарап шықпау
/memory	жадты қарап шығу
/boots	жүктеу бөліктерін қарап шығу
/no-boots	жүктеу бөліктерін қарап шықпау (әдепкі)
/arch	мұрағаттарды қарап шығу (әдепкі)
/no-arch	мұрағаттарды қарап шықпау
/max-obj-size=SIZE	ӨЛШЕМ мегабайттан кем файлдарды ғана қарап шығу (әдепкі 0 = шексіз)
/max-arch-level=LEVEL	қаралатын мұрағаттар (енгізілген мұрағаттар) ішіндегі мұрағаттардың жоғарғы ішкі деңгейі
/scan-timeout=LIMIT	мұрағаттарды көп дегенде ШЕК секунд қарап шығу
/max-arch-size=SIZE	ӨЛШЕМ мегабайттан кем болған жағдайда ғана мұрағаттағы файлдарды қарап шығу (әдепкі 0 = шексіз)
/max-sfx-size=SIZE	ӨЛШЕМ мегабайттан кем болған жағдайда ғана өздігінен ашылатын мұрағаттағы файлдарды қарап шығу (әдепкі 0 = шексіз)
/mail	электрондық пошта файлдарын қарап шығу (әдепкі)
/no-mail	электрондық пошта файлдарын қарап шықпау
/mailbox	пошта жәшіктерін қарап шығу (әдепкі)
/no-mailbox	пошта жәшіктерін қарап шықпау
/sfx	өздігінен ашылатын файлдарды қарап шығу (әдепкі)
/no-sfx	өздігінен ашылатын файлдарды қарап шықпау
/rtp	орындалатын бумалаушыларды қарап шығу (әдепкі)
/no-rtp	орындалатын бумалаушыларды қарап шықпау
/unsafe	ықтимал қауіпті бағдарламарды қарап шығу
/no-unsafe	ықтимал қауіпті бағдарламарды қарап шықпау
/unwanted	ықтимал қауіпті бағдарламаларды қарап шығу
/no-unwanted	ықтимал қауіпті бағдарламаларды қарап шықпау (әдепкі)
/suspicious	күдікті бағдарламаларды қарап шығу (әдепкі)
/no-suspicious	күдікті бағдарламалар үшін қарап шықпау
/pattern	қолтаңбаларды пайдалану (әдепкі)
/no-pattern	қолтаңбаларды пайдаланбау
/heur	эвристиканы қосу (әдепкі)
/no-heur	эвристиканы өшіру
/adv-heur	Кеңейтілген эвристиканы қосу (әдепкі)
/no-adv-heur	Кеңейтілген эвристиканы өшіру
/ext=EXTENSIONS	тек бағанмен бөлінген КЕҢЕЙТІМДЕРДІ қарап шығу
/ext-exclude=EXTENSIONS	бағанмен бөлінген КЕҢЕЙТІМДЕРДІ қарап шығуға қоспау

/clean-mode=MODE	вирус жұққан нысандар үшін тазалау РЕЖИМІН пайдалану Мына опциялар қол жетімді: • **none** – Автоматты түрде тазалау орын алмайды. • **standard** (әдепкі) – ecls.exe вирус жұққан файлдарды автоматты түрде тазалауға немесе жоюға әрекет жасайды. • **strict** – ecls.exe пайдаланушының араласуынсыз вирус жұққан файлдарды автоматты түрде тазалауға немесе жоюға әрекеттенеді (файлдарды жою алдында сізден сұралмайды). • **rigorous** – ecls.exe қандай файл екеніне қарамастан тазалауға әрекеттенусіз файлдарды жояды. • **delete** – ecls.exe тазалауға әрекеттенусіз файлдарды жояды, бірақ Windows жүйелік файлдары сияқты құпия файлдарды жоймайды.
/quarantine	жұққан файлдарды «Карантинге» көшіру (егер тазаланса) (тазалау кезіндегі орындалатын қосымша әрекеттер)
/no-quarantine	вирус жұққан файлдарды Карантинге көшірмеу

Жалпы опциялары

/help	анықтаманы көрсету және шығу
/version	нұсқа ақпаратын көрсету және шығу
/preserve-time	соңғы кіру уақыт белгісін сақтау

Шығу кодтары

0	ешқандай қауіп табылған жоқ
1	қауіп табылып тазаланды
10	кейбір файлдарды қарап шығу мүмкін емес (қауіптер болуы мүмкін)
50	қауіп табылды
100	қате

ЕСКЕРТПЕ
Шығу коды 100-ден көп болса, файл қарап шығылмағанын білдіреді және ол вирус жұқтырған болуы мүмкін.

6. Глоссарий

6.1 Инфильтрация түрлері

Инфильтрация – пайдаланушы компьютеріне кіруге және/немесе зақымдауға тырысатын зиянды бағдарламаның бір бөлігі.

6.1.1 Вирустар

Компьютер вирусы - компьютеріңіздегі бар файлдарға қосылады немесе алдын ала аяқталмаған зиянды кодты тасымалдаудың бөлігі. Вирустар бір компьютерден екіншісіне таралу үшін ұқсас әдісті пайдаланатын биологиялық вирустар сияқты сол атпен аталған. Ал «вирус» терминіге келетін болсақ, кез келген қауіп түріне дұрыс емес мәнін жиі пайдаланады. Оның орнына нақтырақ «зиянды бағдарлама» (зиянды бағдарлама) термині бірте-бірте пайдаланылуда.

Компьютер вирустары негізінен орындалатын файлдар мен құжаттарға шабуыл жасайды. Қысқаша айтқанда, компьютер вирусы жұмысы: жұққан файлды іске қосқаннан кейін, зиянды код шақырылып және бастапқы бағдарламасына дейін орындалады. Жазу рұқсаты бар пайдаланушының барлық файлдарын вирус жұқтыра алады.

Компьютер вирустарының мақсаты мен қауіптілігі әр түрлі болады. Кейбірі файлдардың қатты дискіден арнайы жою мүмкіндігіне байланысты аса қауіпті. Екінші жағынан, кейбір вирустар ешбір зиян келтірмейді: олар тек пайдаланушының мазасын алып, авторларының техникалық біліктілігін көрсету үшін ғана қызмет етеді.

Егер компьютеріңізге вирус жұққан болса және тазалау мүмкін болмаған жағдайда танысу үшін «ESET» зерханасына жіберіңіз. Кейбір кездерде жұқан файлдар тазалау мүмкін болмайтын деңгейге дейін өзгеруі мүмкін және ол файлдар таза көшірмесіне ауыстырылады.

6.1.2 Құрттар

Компьютер құрты — басты компьютерлерді шабуылдап, желі арқылы тарайтын зиянды коды бар бағдарлама. Вирус пен құрт арасындағы басты айырмашылық, құрттың өздігінен көбею қабілетінде; олар басты файлдарға (немесе жүктеу бөліктеріне) тәуелсіз болады. Құрттар контактілер тізіміндегі электрондық пошта мекенжайларына таралады немесе желілік бағдарламалардағы қауіпсіздіктің осал тұстарын пайдаланады.

Сондықтан, құрттар компьютер вирустарына қарағанда әлдеқайда көп өмір сүреді. Интернеттің қол жетімді болуының арқасында олар ғаламға шығарылғаннан кейін бірнеше сағат ішінде немесе тіпті бірнеше минут ішінде тарап кете алады. Тәуелсіз әрі жылдам көбею қабілеті зиянды бағдарламаның басқа түрлеріне қарағанда оларды әлдеқайда қауіпті етеді.

Жүйеде іске қосылған құрт бірқатар қолайсыздықтар тудыруы мүмкін: Ол файлдарды жойып жіберуі, жүйе жұмысын нашарлатуы немесе бағдарламаларды тіпті аштыртпай қоюы мүмкін. Компьютер құртының табиғаты оны инфильтрацияның басқа түрлері үшін «тасымал құралы» ретінде анықтайды.

Егер компьютеріңіз құрт жұқтырса, вирус жұққан файлдарыңызды жою ұсынылады, себебі оларда зиянды код болуы мүмкін.

6.1.3 Троялық

Тарихы жағынан, компьютерлік «Троялық» (троялық аттар) пайдаланушылардың оларды алдап іске қостыра отырып, өздерін пайдалы бағдарламалар ретінде көрсететін инфильтрациялар класы ретінде сипатталған.

Троялық өте кең санат болғандықтан, ол бірнеше ішкі санаттарға жиі бөлінеді:

- **Жүктеуші**– Интернеттен басқа инфильтрацияларды жүктей алатын зиянкес бағдарламалар.
- **Тастаушы** – Жұққан компьютерде басқа да зиянды бағдарламалардың түрінен бас тарту мүмкіндіктері бар зиянкес бағдарламалар.
- **Жүйеге жасырын кіруші**– Қашықтағы шабуылдаушылармен байланысып, компьютермен қатынасып және оны басқаруға мүмкіндік беретін зиянкес бағдарламалар.
- **Пернетақталық шпион** – (пернетақта тіркеуші) – пайдаланушы терген әр пернедегі әріпті жазып, ақпаратты қашықтағы шабуылдаушыларға жіберетін бағдарлама.
- **Нөмір теруші** – Пайдаланушының Интернет жеткізушінің дәрежелі нөмірі арқылы қосылуына арналған зиянкес бағдарламалар. Пайдаланушы үшін жаңа қосылым жасалғанын аңғару мүмкін емес дерлік. Нөмір терушілер бұдан кейін тұрақты пайдаланылмайтын телефон желісіндегі модемдері бар пайдаланушыларға ғана зиян келтіре алады.

Егер компьютеріңіздегі файл троялық ретінде анықталса, онда зиянды кодтан басқа еш мәлімет жоқ екеніне ұқсайтындықтан, оны жоюға кеңес беріледі.

6.1.4 Руткиттер

Руткиттер – интернет шабуылдаушыларына бар екенін жасырып, жүйеге шектеусіз қатынас беретін зиянды бағдарламалар. Жүйемен қатынас орнатқаннан кейін (әдетте жүйедегі осалдықты пайдаланып) руткиттер антивирус бағдарламасының табуын алдын алу үшін операциялық жүйедегі функцияларды пайдаланады: олар үрдістерді, файлдарды және Windows тіркелім деректерін жасырады. Осы себепті оларды әдеттегі тексеру әдістерін пайдаланып табу мүмкін емес дерлік.

Руткиттерді болдырмау үшін анықтаудың екі деңгейі бар:

1. Олар жүйеге қатынасуға тырысады: Олар әлі жоқ, сондықтан енжар. Бұл деңгейде антивирус жүйелерінің көпшілігі руткиттерді жоя алады (олар мұндай файлдарға шын мәнінде вирус жұққанын табады деп жорамалдағанда).
2. Әдеттегі тексеруден жасырынған кезде: ESET NOD32 Antivirus пайдаланушыларының белсенді руткиттерді анықтап, жоя алатын ұрлыққа қарсы технологиясының артықшылығы бар.

6.1.5 Жарнама бағдарламасы

Жарнама бағдарламасы дегеніміз – жарнаманы қолдайтын бағдарлама. Жарнамалық материалдарды көрсететін бағдарламалар осы санатқа жатады. Жарнамалық қолданбалар көбінесе интернет браузерінде жарнамаларды қамтитын жаңа қалқымалы терезені автоматты түрде ашады немесе браузердің басты бетін өзгертеді. Жарнамалық бағдарлама жиі тегін бағдарламалардың ішіне салынып, жасаушыларға олардың бағдарламаларын (әдетте пайдалы) әзірлеу шығындарын жабуға мүмкіндік береді.

Жарнамалық бағдарламаның өзі қауіпті емес, пайдаланушыларды тек жарнамалар мазалайды. Оның қауіптілігі жарнама бағдарламасының да қадағалау функцияларын орындау мүмкіндігінде жатыр (шпион бағдарлама сияқты).

Егер тегін бағдарламаны пайдалануды ұйғарсаңыз, орнату бағдарламасына ерекше назар аударыңыз. Орнатушы қосымша жарнама бағдарламасының орнатылатыны туралы хабарландырады. Көбінесе, сізге одан бас тартып, бағдарламаны жарнама бағдарламасынсыз орнату мүмкіндігі беріледі.

Кейбір бағдарламалар жарнама бағдарламасынсыз орнатылмайды немесе оның функциялары шектеулі болады. Яғни, бұл жарнамалық бағдарлама көбінесе жүйеге «заңды» жолмен, пайдаланушылар бұған келіскендіктен қатынасуы мүмкін. Бұл жағдайда, сақ болған жөн. Егер компьютерде жарнама бағдарламасы ретінде анықталған файл болса, оны жойған абзал, себебі оның құрамында зиянды код болу мүмкіндігі зор.

6.1.6 Шпиондық бағдарлама

Бұл санат жеке ақпаратты пайдаланушының келісімінсіз/білуінсіз жеке ақпаратты жіберетін бағдарламаларды қамтиды. Шпиондық бағдарлама кірген веб-тораптардың тізімі, пайдаланушының істес кісілер тізіміндегі электрондық пошта мекенжайлары немесе жазылған пернелердің тізімі сияқты әртүрлі статистикалық деректерді жіберу үшін бақылау функцияларын пайдаланады.

Шпиондық бағдарламалардың авторлары бұл әдістер пайдаланушылардың қажеттіліктері мен қызығушылықтары туралы көбірек білуге көмектеседі және нысананы жақсырақ көздейтін жарнама жасауға мүмкіндік береді деп мәлімдейді. Мұндағы мәселе пайдалы және зиянды бағдарламалардың арасында анық айырмашылықтың жоқтығында және шығарып алынған ақпарат дұрыс пайдаланылмайтынына ешкім сенімді бола алмайды. Шпиондық бағдарламалар алатын деректерде қауіпсіздік кодтары, PIN кодтары, банк шотының нөмірлері, т.б. болуы мүмкін. Шпиондық бағдарлама жиі оның ақша тапқысы келетін немесе бағдарламалық құралды сатып алуға ынталандырғысы келетін авторы жасаған тегін нұсқаларымен бірге келеді. Бағдарламаны орнату кезінде онсыз төленген нұсқасына олардың жаңартуға ынталандыру үшін пайдаланушыларға шпиондық бағдарламаның бар екені туралы жиі хабарлап отырады.

Ішінде шпиондық бағдарлама бар болып келетін белгілі тегін бағдарламалар – P2P (бір дәрежелі) желілерінің клиенттік бағдарламалары. Spyfalcon немесе Spy Sheriff (және басқалары) белгілі бір шпиондық бағдарлама санатына жатады – антишпиондық бағдарламалар болып көрінеді, бірақ шындығында олар өздері шпиондық бағдарламалар болып табылады.

Егер компьютеріңіздегі файл шпиондық бағдарлама ретінде анықталса, онда зиянды код болатынға ұқсайтындықтан, оны жоюға кеңес беріледі.

6.1.7 Бумалаушылар

Бумалаушы дегеніміз бірнеше түрлі вирусты бір бумаға жинақтайтын өздігінен ашылатын, атқарушы файл.

Жиі қолданылатын бумалаушылар: UPX, PE_Compact, PKLite және ASPack. Ұқсас вирустарды түрлі бумалаушы қысқан кезде олар әр түрлі анықталады. Бумалаушылардың уақыт бойы "сигнатураларды" өзгертіп, оларды анытауға және жоюға қиындық туғызатын мүмкіндігі бар.

6.1.8 Ықтимал қауіпті бағдарламалар

Желіге қосылған компьютерлерді басқару барысын жеңілдету үшін қызмет ететін көптеген заңды бағдарламалар бар. Дегенмен, кейбір адамдар оларды зиянды мақсаттарда пайдалануы мүмкін. ESET NOD32 Antivirus бағдарламасы осындай қауіптерді анықтау опциясын қамтамасыз етеді.

Қаупі ықтимал бағдарламалар – коммерциялық, заңды бағдарламалар үшін пайдаланылатын жіктеу. Бұл жіктеу қашықтағы қатынас құралдары, құпиясөзбен қорғауды бұзатын бағдарламалар және пернетақталық шпиондар (пайдаланушы терген әр пернедегі әріпті жазатын бағдарлама) сияқты бағдарламаларды қамтиды.

Егер сіз компьютеріңізде қауіпі ықтимал бағдарлама барын және іске қосулы екенін (және оны сіз орнатпаған болсаңыз) анықтасаңыз, желі әкімшісімен кеңесіңіз немесе ол бағдарламаны жойып тастаңыз.

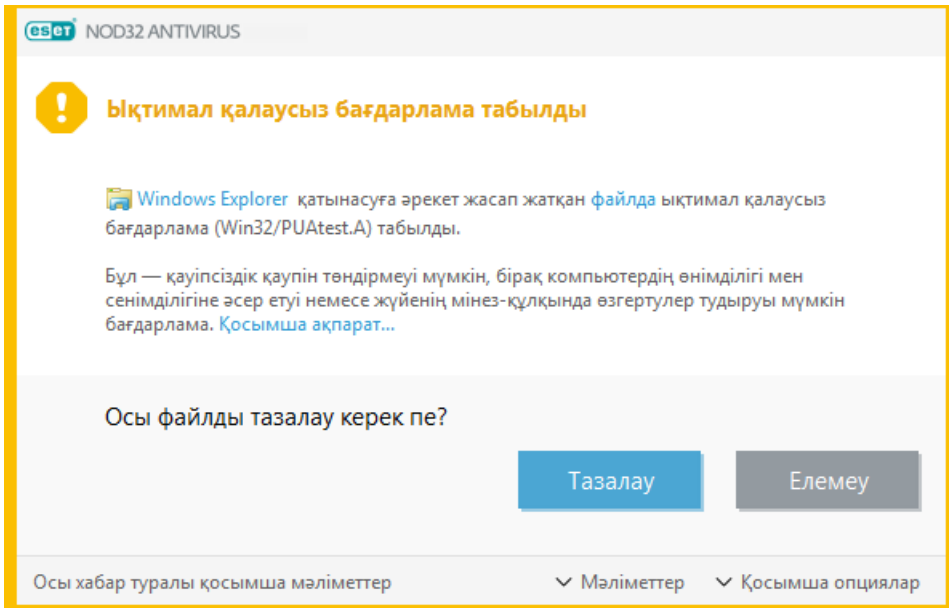
6.1.9 Ықтимал қалаусыз бағдарламалар

Ықтимал қалаусыз қолданба — жарнамалық бағдарламаны қамтитын, құралдар тақталарын орнататын немесе басқа анық емес мақсатары бар бағдарлама. Пайдаланушы ықтимал қалаусыз қолданбаның артықшылықтары қауіптерден асып түсетінін сезуі мүмкін кейбір жағдайлар бар. Осы себепті ESET мұндай қолданбаларға трояндық аттар немесе құрттар сияқты зиянкес бағдарламалардың басқа түрлерімен салыстырғанда төменірек қауіп санатын тағайындайды.

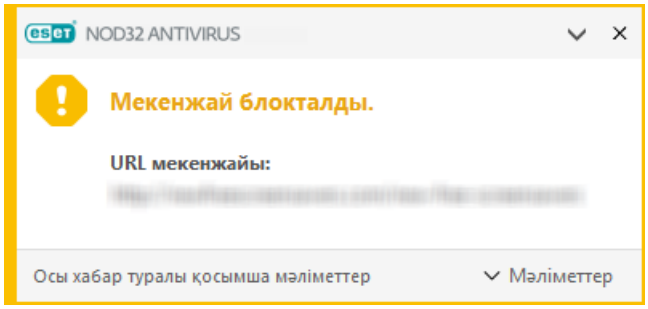
Ескерту - Ықтимал қауіп табылды

Ықтимал қалаусыз қолданба анықталғанда сіз қай әрекетті орындау керектігі туралы шешім қабылдай аласыз:

1. **Тазалау**/**Ажырату**: бұл опция әрекетті аяқтайды және ықтимал қауіптің жүйеге кіруін болдырмайды.
2. **Елемеу**: бұл опция ықтимал қауіпке жүйеге кіруге рұқсат етеді.
3. Қолданбаға болашақта үзіліссіз компьютерде жұмыс істеуге рұқсат ету үшін **Кеңейтілген опциялар** тармағын басыңыз, содан кейін **Анықтауға қоспау** жанында құсбелгі қойыңыз.

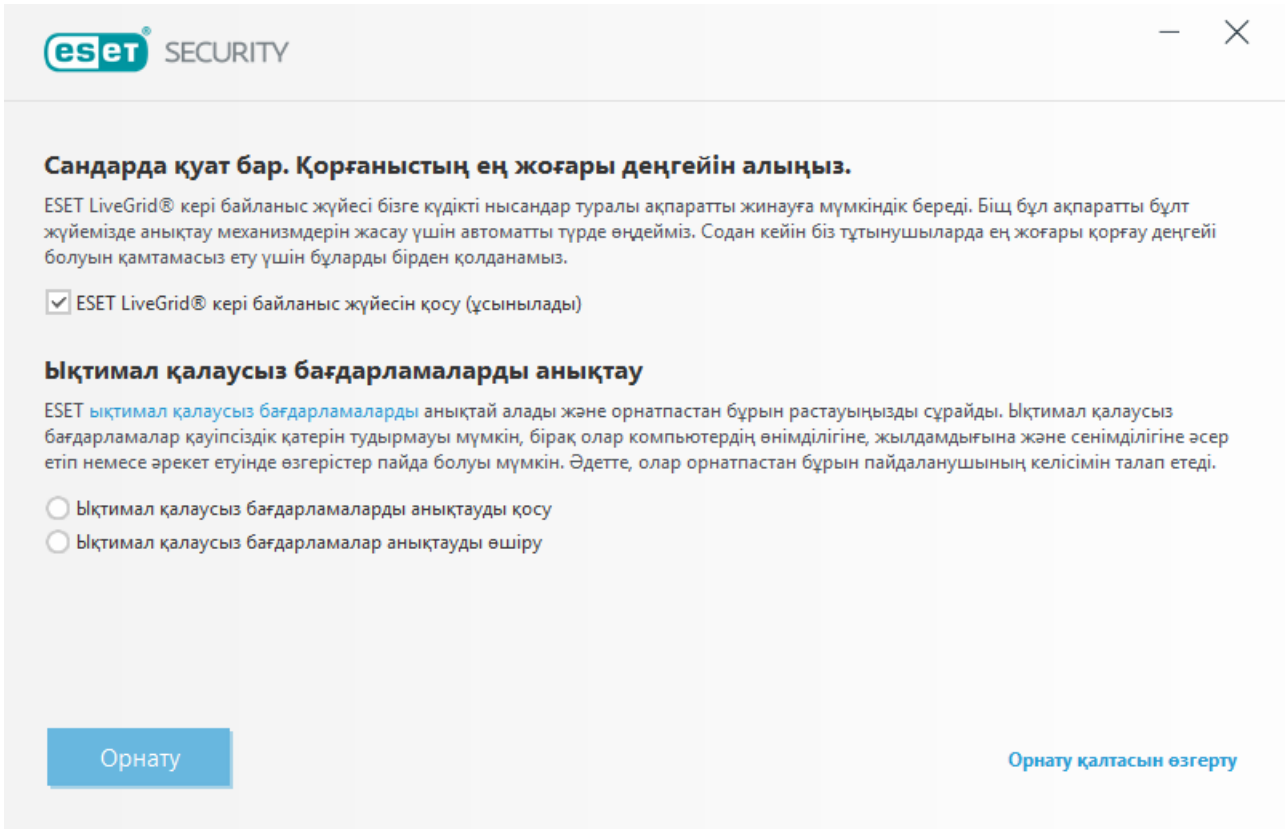


Ықтимал қалаусыз қолданба анықталса және оны тазалау мүмкін болмаса, **Мекенжай блокталды** хабарландыруы көрсетіледі. Бұл оқиға туралы қосымша ақпарат алу үшін негізгі мәзірде **Құралдар** > **Журналд файлдары** > **Сүзілген веб-сайттар** тармағына өтіңіз.



Ықтимал қалаусыз қолданбалар - Параметрлер

ESET өнімін орнатып жатқанда төменде көрсетілгендей ықтимал қалаусыз қолданбаларды анықтауды қосу-қоспау туралы шешім қабылдай аласыз:

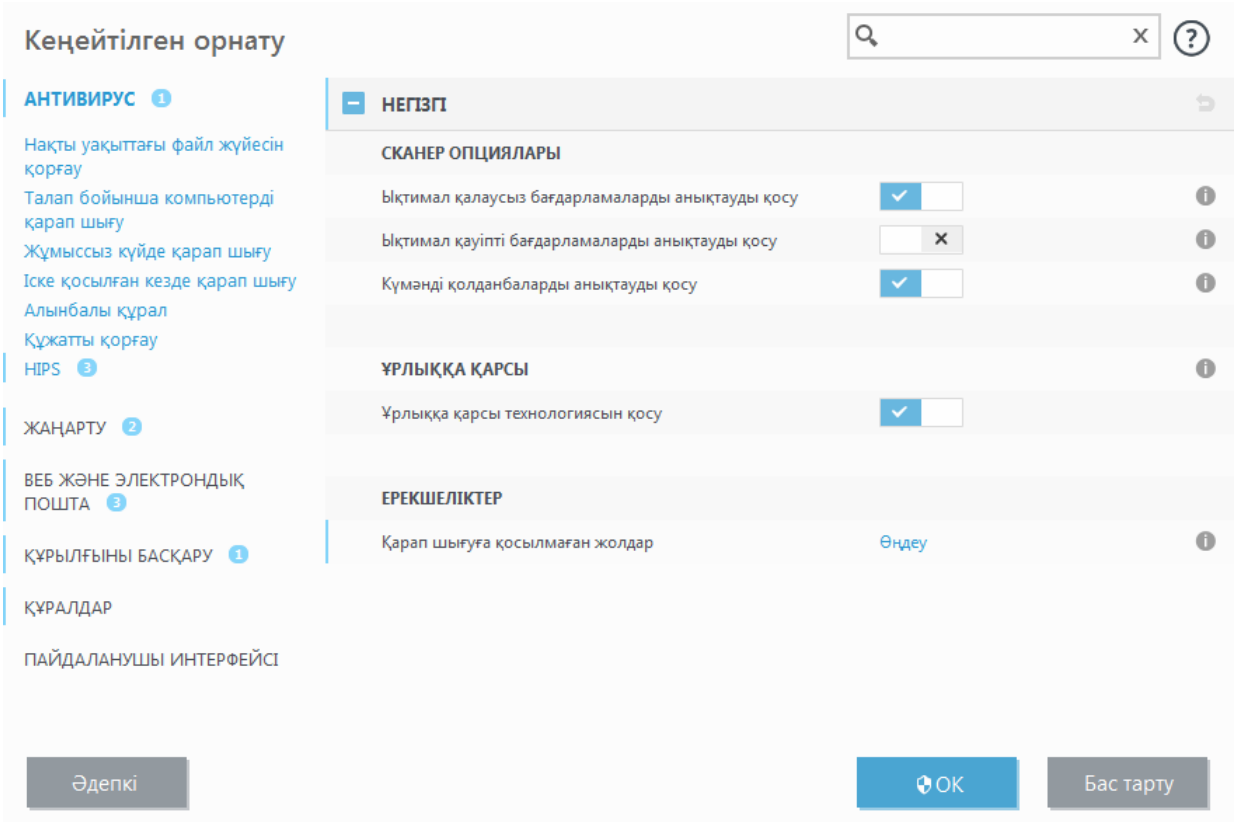


ЕСКЕРТУ

Ықтимал қалаусыз қолданбалар жарнамалық бағдарламаларды, құралдар тақталарын орнатуы немесе басқа қалаусыз және қауіпті бағдарлама мүмкіндіктерін қамтуы мүмкін.

Бұл параметрлерді бағдарлама параметрлерінде кез келген уақытта өзгертуге болады. Ықтимал қалаусыз, қауіпті немесе күдікті қолданбаларды анықтауды қосу немесе өшіру үшін мына нұсқауларды орындаңыз:

1. ESET өнімін ашыңыз. ESET өнімін қалай ашуға болады?
2. **F5** пернесін басып, **Кеңейтілген орнату** тармағын ашыңыз.
3. **Антивитус** тармағын басыңыз және таңдауыңызға сай **Ықтимал қалаусыз қолданбаларды анықтауды қосу**, **Ықтимал қалаусыз қолданбаларды анықтауды қосу** және **Күдікті қолданбаларды анықтауды қосу** опцияларын қосыңыз немесе өшіріңіз. **OK** түймесін басу арқылы растаңыз.



Ықтимал қалаусыз қолданбалар - Бағдарлама орау құралдары

Бағдарламаны орау құралы — кейбір файл-хостинг веб-сайттары пайдаланатын қолданбаны өзгертудің арнайы түрі. Бұл — сіз жүктегіңіз келген бағдарламаны орнататын, бірақ құралдар тақталары немесе жарнамалық бағдарлама сияқты қосымша бағдарламаны қосатын бағдарлама. Сондай-ақ қосымша бағдарламалық құрал веб-браузердің басты бетіне және іздеу параметрлеріне өзгертулер енгізуі мүмкін. Сондай-ақ, файл-хостинг веб-сайттары көбінесе бағдарламалық құрал жеткізушісіне немесе жүктеуді алушыға өзгертулер жасалғаны туралы хабарламайды және көбінесе өзгертуден бас тарту опцияларын жасырады. Осы себептермен ESET бағдарлама орау құралдарын пайдаланушыларға жүктеуді қабылдамау немесе қабылдамауға рұқсат ету үшін ықтимал қалаусыз қолданбаның түрі ретінде жіктейді.

Осы анықтама бетінің жаңартылған нұсқасын алу үшін осы ESET білім қоры мақаласы бөлімін қараңыз.

6.2 ESET технологиясы

6.2.1 Бүлдіруді блоктаушы

Бүлдіруді блоктаушы веб-браузерлер, PDF оқу құралдары, электрондық пошта клиенттері мен MS Office компоненттері сияқты әдетте пайдаланатын бағдарлама түрлерін жақсарту үшін жасалған. Ол бүлдіруді көрсетуі мүмкін күдікті әрекет процестерін орындауды бақылаудың есебінен жұмыс істейді.

Бүлдіруді блоктаушы күдікті процесті анықтаған кезде ол процесті дереу тоқтатып, қауіп туралы деректерді жаза алады, ал олар кейін ThreatSense бұлт жүйесіне жіберіледі. Бұл деректертерді ESET лабораториясы өңдеп, белгісіз қауіптерден және нөлдік күн шабуылдардан (алдын ала конфигурацияланбаған шешімі жоқ жаңадан шығарылған зиянкес бағдарламалар) барлық пайдаланушыларды жақсырақ қорғау үшін пайдаланады.

6.2.2 Êåңåéò³ëãåí æàä ñêàíåð³

Кеңейтілген жад сканері шатастыру және/немесе шифрлау әрекетін пайдалану арқылы антивирустық өнімдердің анықтауын болдырмау үшін жасалған зиянкес бағдарламалардан қорғануды күшейту үшін «Бүлдіруді блоктаушы» құралымен үйлесімді жұмыс істейді. Әдепкі эмуляция немесе эвристика қауіпті анықтамайтын жағдайда кеңейтілген жад сканері күдікті әрекетті анықтап және олар жүйе жадында өздерін көрсеткен кезде қауіптерді ұрап шығу мүмкіндігі бар. Бұл шешімді тіпті күрделі шатастырылған зиянкес бағдарламасына қолдануға болады.

«Бүлдіруді блоктаушы» құралына қарағанда, «Кеңейтілген жад сканері» пост-орындау әдісін болып табылады, демек, кейбір зиянды әрекеттер оның анықталуына дейін орындалуы мүмкін, бірақ мұндай жағдайда басқа анықтау әдістері орындалмайтын кезде ол қосымша қауіпсіздік деңгейін ұсынады.

6.2.3 ESET LiveGrid®

ThreatSense.Net® озық ерте ескерту жүйесі негізінде жасалған ESET LiveGrid® ESET пайдаланушылары дүние жүзінде жіберген деректерді пайдаланады және оларды ESET вирустар зертханасына жібереді. Жабайы жағдайлардан күдікті үлгілер мен метадеректерді ұсыну арқылы ESET LiveGrid® бағдарламасы клиенттеріміздің қажеттіліктеріне дер кезінде көңіл бөлуге және ESET бағдарламасын жаңа қауіптерге дер кезінде сақтануға мүмкіндік береді. ESET зиянкес бағдарламаларының зерттеушілері дұрыс нысанға көзделуге мүмкіндік беретін глобалдық қауіптердің дәл лездік суреті мен масштабын құрастыру ақпаратын пайдаланады. ESET LiveGrid® деректері автоматтандырылған өңдеудегі басымдылықты анықтауда маңызды рөлді атқарады.

Сондай-ақ, анти зиянкес бағдарламалар шешімдерінің жалпы тиімділігін көтеруге көмектесетін жүйелік репутациясын пайдаланады. Пайдаланылатын файл немесе мұрағат пайдаланушының жүйесінде тексерілген кезде оның хэш тегі ақ және қара тізімдегі элементтердің дерекқорларымен салыстырылады. Егер ақ тізімінде табылса, тексерілетін файл таза ретінде есептеледі және белгіленген келесі қарап шығулардан алынуы тиіс. Егер ол қара тізімде болса, қауіптің түріне байланысты тиісті әрекеттер қолданылады. Егер сәйкестік табылмаса, файл мұқият қарап шығылды. Осы қарап шығудың нәтижелері негізінде файлдар қауіптілер немесе қауіпті еместер болып санатталады. Бұл әрекет қарап шығуға едеуір оң әсерін береді.

Бұл репутация жүйесі зиянкес бағдарламалардың үлгілерін олардың қолтаңбалары пайдаланушының компьютеріне жаңартылған вирус дерекқоры (күніне бірнеше рет болады) арқылы жеткізілулеріне дейін тиімді анықтауға көмектеседі.

6.2.4 Java бүлдірулерін блоктаушы

Java бүлдірулерін блоктаушы — бар бүлдірулерді блоктаушы қорғауының кеңейтімі. Ол Java бағдарламасын бақылайды және бүлдіруге ұқсайтын мінез-құлықты іздейді. Блокталған үлгілер туралы зиянкес бағдарламаларды талдаушыларға есеп беруге болады, осылайша олар оларды әр түрлі қабаттарда (URL мекенжайын блоктау, файл жүктеу, т.б.) блоктау үшін сигнатуралар жасай алады.

6.2.5 Сценарийлерге негізделген шабуылдардан қорғау

Сценарийлерге негізделген шабуылдардан қорғау веб-браузерлердегі Javascript сценарийлерінен қорғаудан және Antimalware Scan Interface (AMSI) Powershell сценарийлерінен қорғаудан тұрады.

ЕСКЕРТУ
Бұл мүмкіндік жұмыс істеуі үшін HIPS жүйесін қосу керек.

Сценарийлерге негізделген шабуылдардан қорғау келесі веб-браузерлерді қолдайды:

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

ЕСКЕРТПЕ
Браузерлердің ең төмен қолдау көрсетілетін нұсқалары өзгеріп отыруы мүмкін, өйткені браузерлердің файл қолтаңбасы жиі өзгереді. Веб-браузердің соңғы нұсқасына әрқашан қолдау көрсетіледі.

6.2.6 Зиянкес хакерлік бағдарламалардан қорғау

Зиянкес хакерлік бағдарлама — жүйенің экранын құлыптау немесе файлдарды шифрлау арқылы пайдаланушылардың жүйелеріне қатынасуын блоктайтын зиянкес бағдарлама түрі. Зиянкес хакерлік бағдарламалардан қорғау жеке деректеріңізді өзгертуге әрекеттенетін қолданбалар мен процестердің мінез-құлқын бақылайды. Қолданбаның мінез-құлқы зиянкес деп есептелсе немесе репутацияға негізделген қарап шығу қолданбаның күдікті екенін көрсетсе, қолданба блокталады немесе пайдаланушыдан оны блоктау немесе оған рұқсат ету сұралады.

МАҢЫЗДЫ
Зиянкес хакерлік бағдарламалардан қорғау тиісті түрде жұмыс істеуі үшін ESET Live Grid мүмкіндігін қосу керек.

6.3 Электрондық пошта

Электрондық пошта – артықшылықтары көп заманауи байланыс үлгісі. Ол икемді, жылдам және бағытталған әрі 1990 жылдардың басында интернеттің таралуында маңызды рөл ойнады.

Өкінішке орай, жоғары анонимдік деңгейі бар электрондық пошта мен интернетте спаминг сияқты заңсыз әрекеттерге арналған орын қалған. Спам қалаусыз жарнамаларды, әзіл әрекеттерді және зиянкес бағдарламалық құралдардың таралуын қамтиды. Қолайсыздық және сізге төнген қауіп-қатер хабар жіберу шығындарының өте аз және спам авторларында жаңа электрондық пошта мекенжайларға қол жеткізуге мүмкіндік беретін түрлі құралдардың болуынан артып отыр. Сонымен бірге, спамның көптігі мен сан әлуандығы оларды реттеуге қиындық тұғызады. Электрондық пошта мекенжайын қаншалықты көп пайдалансаңыз, соншалықты спам дерекқорына оның қосылып қалуы ықтималдығы жоғары болады. Оны алдын алуға арналған бірнеше кеңес:

- Мүмкін болса, электрондық пошта мекенжайыңызды интернетте жарияламаңыз
- Электрондық поштаңыздың мекенжайын тек сенімді адамдарға беріңіз
- Мүмкін болса, жиі кездесетін бүркеншік аттарды пайдаланбаңыз — бүркеншік аттар күрделірек болса, сізді бақылаудың ықтималдығы төменірек болады
- Кіріс қалтаңызға келіп қойған спамға жауап бермеңіз
- Интернет пішіндерін толтырғанда сақ болыңыз, әсіресе «Иә, ақпарат алғым келеді» сияқты опциялардан сақтаныңыз.
- «Арнайы» электрондық пошта мекенжайларын пайдаланыңыз – мысалы, біреуін бизнес үшін, біреуін достармен байланысу үшін, т.с.с.
- Электрондық поштаңыздың мекенжайын уақыт өте ауыстырып тұрыңыз
- Спамға қарсы шешімді пайдаланыңыз

6.3.1 Жарнамалар

Интернеттегі жарнама – жарнаманың ең қарқынды дамып келе жатқан салаларының бірі. Оның негізгі маркетингтік артықшылықтары: ең аз шығындар және бағытталудың жоғары деңгейі; бұған қоса, хабарлар бірден дерлік жеткізіледі. Бірнеше компаниялар ағымдағы және алдағы тұтынушылармен оңай байланысу үшін электрондық сату құралдарын пайдаланады.

Бұл жарнамалау түрі заңды болып табылады, себебі сіз кейбір өнімдер туралы коммерциялық ақпарат алуға мүдделі болуыңыз мүмкін. Бірақ, көптеген компаниялар коммерциялық хабарларды сұрамастан топтап жібереді. Мұндай жағдайларда, электрондық пошта жарнамасы шектен шығып, спамға айналады.

Сұрамай жіберілетін электрондық поштаның мөлшері мәселеге айналды және оның азаятын нышаны байқалмайды. Сұрамай жіберілетін электрондық поштаның авторлары жиі спамды заңды хабар түрінде бүркемелеуге тырысады.

6.3.2 Алаяқтықтар

Жалған хабар – интернетте таратылатын дұрыс емес ақпарат. Жалған хабарлар әдетте электрондық пошта немесе ICQ және Skype сияқты байланыс құралдары арқылы жіберіледі. Хабардың өзі көбінесе әзіл немесе ойлап шығарылған әңгіме болады.

Компьютерлік вирус әзілдері алушыларда қорқыныш, сенімсіздік және күмән тудыруға әрекеттенеді, оларды файлдарды жоятын және құпиясөздерді шығарып алатын немесе жүйесінде кейбір басқа зиянды әрекетті орындайтын «анықтау мүмкін емес вирус» бар деп ойлатқызады.

Кейбір жалған хабарлар алушылардан хабарларды контактілеріне қайта жіберуді сұрап, жалған хабарды мәңгі сақтау арқылы жұмыс істейді. Адамдар шетелден ақша жіберуіңізге ұсыныс жасайды, т.б. сияқты көмек сұрайтын ұялы телефонның жалған хабарлары бар. Көбінісе жасағандардың мақсатын түсіну мүмкін емес.

Егер сіз білетін адамдарыңыздың барлығына жіберуіңізді сұранған хабарды көрсеңіз, ол іс жүзінде жалған хабар болуы мүмкін. Интернетте электрондық пошта хабары заңды ма, соны тексеруге болатын көп веб-тораптар бар. Кез келген хабарды қайта жібермес бұрын, жалған хабар деп күдіктенген хабарыңызды интернеттен іздеп көріңіз.

6.3.3 Фишинг

Фишинг термині әлеуметтік жобалаудың тәсілдерін (құпия ақпарат алу үшін пайдаланушыларды қолдан жасау) пайдаланатын қылмыстық әрекетті анықтайды. Оның мақсаты банктегі есепшот нөмірлері, PIN кодтары, т.б. сияқты құпия ақпаратқа қол жеткізу болып табылады.

Әдетте, сенімді адам немесе ұйым (қаржы институты, сақтандыру компаниясы) ретінде таныстыратын электрондық пошта жіберу арқылы қол жеткізеді. Электрондық пошта шынайы болып көрінуі мүмкін және ол басқа біреу орнына таныстыратын жерден келуі мүмкін суреттер мен мазмұнды қамтиды. Сізден әр түрлі алдау жолдарымен (деректерді тексеру, қаржы жұмыстары) кейбір жеке деректеріңізді – банктегі есепшот нөмірлерін немесе пайдаланушы аттары мен құпиясөздерді енгізуді сұрайды. Мұндай деректердің барлығы жіберілген жағдайда оңай ұрланып, басқа мақсатқа пайдаланылуы мүмкін.

Банктер, сақтандыру компаниялары және басқа да заңды компаниялар ешқашанда пайдаланушы аттары мен құпиясөздерді ерікті электрондық поштамен сұрамайды.

7. Жалпы сұрақтар

Бұл тарауда ең жиі қойылатын сұрақтар мен кездесетін мәселелердің кейбірі қамтылған. Мәселеңізді шешу жолын табу үшін тақырып атауын басыңыз:

ESET NOD32 Antivirus қалай жаңарту керек
Компьютерден вирусты жою жолы
Жоспарлағышта жаңа тапсырманы жасау әдісі
Қарап шығу тапсырмасын жоспарлау (24 сағат сайын)

Егер мәселе жоғарыдағы анықтама беттерінің тізіміне кірмесе, ESET NOD32 Antivirus анықтама беттерін іздеп көріңіз.

Мәселеге/сұраққа шешімді анықтама беттерінде таба алмасаңыз, үнемі жаңартылып отыратын желілік ESET білім қорына кіре аласыз. Қарапайым ақауларды жоюға көмектесу үшін белгілі Білім қоры мақалаларына сілтемелер төменде берілген:

ESET өнімін орнату кезінде іске қосу қатесі пайда болды. Бұл нені білдіреді?
ESET Windows home өнімімді пайдаланушы атымды, құпиясөзімді немесе лицензиялық кілтімді пайдаланып белсендіру
ESET home өнімімді жою немесе қайта орнату
ESET бағдарламасын орнату уақытынан бұрын аяқталды деген хабар алдым
Лицензиямды жаңартқан соң не істеуім қажет? (Үй пайдаланушылары)
Электрондық пошта мекенжайын өзгерткенде не болады?
Windows жүйесін қауіпсіз режимде немесе желісі бар қауіпсіз режимде іске қосу әдісі

Қажет болса, сұрақтармен немесе мәселелермен тұтынушыларды қолдау қызметіне хабарласуға болады. Байланыс пішінін ESET NOD32 Antivirus өнімінің **Анықтама және қолдау** қойындысынан табуға болады.

7.1 ESET NOD32 Antivirus бағдарламасын жаңарту туралы

ESET NOD32 Antivirus бағдарламасын қолмен немесе автоматты түрде жаңартуға болады. Жаңартуды іске қосу үшін **Жаңарту** бөліміндегі **Қазір жаңарту** түймесін басыңыз.

Әдепкі орнату сағат сайын орындалатын автоматты жаңарту тапсырмасын жасайды. Аралығын өзгерту қажет болса, **Құралдар** > **Жоспарлаушы** тармағына өтіңіз (Жоспарлаушы туралы қосымша мәлімет үшін осы жерді басыңыз).

7.2 Компьютерден вирусты жою жолы

Егер компьютеріңіз зиянды жұқтыру белгілері көрсетсе, мысалы ол баяулап қалса, жиі қатып қалса, мына әрекеттерді орындау ұсынылады:

1. Бағдарламаның негізгі терезесінде **Шығу** түймешігін басыңыз.
2. Жүйені қарап шығуды бастау үшін **Компьютерді қарап шығу** түймесін басыңыз.
3. Қарап шығу аяқталғаннан кейін жұрналдан тексерілген, вирус жұққан және тазаланған файлдардың санын қарап шығыңыз.
4. Дисктің белгілі бір бөлігін қарап шығуды қаласаңыз, **Арнайы қарап шығу** түймешігін басып, вирусқа тексерілетін нысандарды таңдаңыз.

Қосымша ақпарат алу үшін жаңартылып тұратын ESET білім қоры мақаласын қараңыз.

7.3 Жоспарлағышта жаңа тапсырманы жасау әдісі

Құралдар > **Жосарлағыш** ішінен жаңа тапсырма жасау үшін **Қосу** түймесін басыңыз немесе тінтуірдің оң жағын басып, контекстік мәзірден **Қосу...** түймесін таңдаңыз. Жоспарланған тапсырмалардың бес түрі бар:

- **Сыртқы қолданбаны іске қосу** – Сыртқы қолданбаның орындалуын жоспарлайды.
- **Журналды сақтау** – Журнал файлдары жойылған жазбалардың қалдықтарын да қамтиды. Бұл тапсырма тиімді жұмыс істеу үшін журнал файлдарындағы жазбаларды тұрақты түрде оңтайландырады.
- **Жүйені іске қосу кезіндегі файлдарды тексеру** – Жүйені іске қосқанда немесе жүйеге кіргенде орындалуға рұқсат етілген файлдарды тексереді.
- **Компьютер күйінің лездік суретін жасау** – ESET SysInspector компьютер лездік суретін жасайды – жүйе құрамдастары (мысалы, драйверлер, қолданбалар) туралы егжей-тегжейлі ақпаратты жинайды және әрбір құрамдастың қауіп деңгейін бағалайды.
- **Талап бойынша компьютерді қарап шығу** – Компьютердегі файлдар мен қалталарды қарап шығуды орындайды.
- **Жаңарту** – Модульдерді жаңарту арқылы «Жаңарту» тапсырмасын жоспарлайды.

Жаңарту – ең жиі пайдаланылатын жоспарланған тапсырмалардың бірі болғандықтан, төменде жаңа жаңарту тапсырмасын қосу әдісі түсіндірілген:

Жоспарланған тапсырма ашылмалы мәзірінде **Жаңарту** пәрменін таңдаңыз. **Тапсырма атауы** өрісіне тапсырма атауын енгізіп, **Келесі** түймесін басыңыз. Тапсырманың жиілігін таңдаңыз. Мына опциялар қол жетімді: **Бір рет**, **Қайта-қайта**, **Күнде**, **Апта сайын** және **Оқиға басталған.** Ноутбук батареядан жұмыс істегенде жүйе ресурстарын барынша аз пайдалану үшін **Батареядан жұмыс істегенде тапсырманы өткізіп жіберу** опциясын таңдаңыз. Тапсырма **Тапсырманы орындау** өрістерінде көрсетілген күн мен уақытта орындалады. Содан кейін, тапсырманы жоспарланған уақытта орындау немесе аяқтау мүмкін болмаса орындау керек әрекетті анықтаңыз. Мына опциялар қол жетімді:

- **Келесі жоспарланған уақытта**
- **Мүмкіндігінше жылдам**
- **Соңғы орындаудан бергі уақыт көрсетілген мәннен асса, дереу** (аралықты **Соңғы орындаудан бергі уақыт (сағаттар)** жүгіртпесін пайдаланып анықтауға болады)

Келесі қадамда ағымдағы жоспарланған тапсырма туралы ақпарат бар жиынтық мәлімет терезесі көрсетіледі. Өзгертулер жасауды аяқтағаннан кейін **Аяқтау** түймесін басыңыз.

Жоспарланған тапсырма үшін пайдаланылатын профильдерді таңдауға мүмкіндік беретін диалогтық терезе көрсетіледі. Мұнда негізгі және баламалы профильді орнатуға болады. Баламалы профиль тапсырманы негізгі профильді пайдаланып аяқтау мүмкін болмаса пайдаланылады. **Аяқтау** түймесін басу арқылы растаңыз, сонда жаңа жоспарланған тапсырма қазіргі уақытта жоспарланған тапсырмалар тізіміне қосылады.

7.4 Апта сайын компьютерді қарап шығуды жоспарлау әдісі

Тұрақты тапсырманы жоспарлау үшін бағдарламаның негізгі терезесін ашып, **Құралдар** > **Жоспарлаушы** түймешігін басыңыз. Төменде жергілікті дискілерді 24 сағат сайын қарап шығатын тапсырманы жоспарлау жолы туралы қысқаша нұсқаулық көруге болады. Егжей-тегжейлі нұсқауларды Білім қоры мақаласында қараңыз.

Қарап шығу тапсырмасын жоспарлау үшін:

1. Жоспарлағыштың негізгі терезесіндегі **Қосу** түймешігін басыңыз.
2. Ашылмалы мәзірде **Талап бойынша компьютерді қарап шығу** тармағын таңдаңыз.
3. Тапсырма атауын енгізіп, **Тапсырманың** апта сайынғы жиілігі параметрін таңдаңыз.
4. Тапсырма орындалатын күн мен уақытты орнатыңыз.
5. Жоспарланған тапсырма кез келген себеппен іске қосылмаса (мысалы, компьютер өшірілген болса), тапсырманы кейінірек орындау үшін **Тапсырманы мүмкіндігінше тез орындау** параметрін таңдаңыз.
6. Жоспарланған тапсырманың қорытындысын қарап шығып, **Дайын** түймешігін басыңыз.
7. **Мақсаттар** ашылмалы мәзірінен **Жергілікті дискілер** опциясын таңдаңыз.

8. Тапсырманы қолдану үшін **Дайын** түймешігін басыңыз.