

# ESET ENDPOINT ANTIVIRUS 6

## Пайдаланушы нұсқаулығы

Microsoft® Windows® 10/8.1/8/7/Vista/XP x86 SP3/XP x64 SP2

[Бұл құжаттың ең соңғы нұсқасын жүктеу үшін мына жерді басыңыз](#)

## ESET ENDPOINT ANTIVIRUS 6

**Авторлық құқықтар ©2016 ESET, spol. s r. o.**

ESET Endpoint Antivirus бағдарламасын ESET, spol. s r. o. жасаған

Қосымша ақпарат алу үшін [www.eset.com](http://www.eset.com) сайтына кіріңіз.

Барлық құқықтары қорғалған. Автордың жазбаша рұқсатынсыз бұл құжаттаманың ешбір бөлігін қайта жасауға, ақпараттық-іздеу жүйесінде сақтауға немесе кез келген түрде немесе кез келген әдістермен, электрондық, механикалық, фотокөшіру, жазу, сканерулеу немесе басқа, тасымалдауға болмайды.

ESET, spol. s r. o. сипатталған қолданбалы бағдарламалардың кез келгенін алдын ала ескертусіз өзгерту құқығын сақтайды.

Дүниежүзілік тұтынушыларды қолдау қызметі: [www.eset.com/support](http://www.eset.com/support)

ТҮЗЕТУ 1/18/2016

# Мазмұны

<b>1. ESET Endpoint Antivirus</b> .....	<b>5</b>
1.1 Жаңалықтар.....	5
1.2 Жүйе талаптары.....	6
1.3 Алдын алу.....	6
<b>2. ESET Remote Administrator арқылы қосылған пайдаланушыларға арналған құжаттама</b> .....	<b>7</b>
2.1 ESET Remote Administrator Server.....	8
2.2 Веб-консоль.....	8
2.3 Прокси-сервер.....	9
2.4 Агент.....	9
2.5 RD Sensor.....	9
<b>3. ESET Endpoint Antivirus өзін пайдалану</b> .....	<b>10</b>
3.1 ESET AV Remover арқылы орнату.....	10
3.1.1 ESET AV Remover.....	11
3.1.2 ESET AV Remover арқылы жою қатемен аяқталды.....	14
3.2 Орнату.....	14
3.2.1 Кеңейтілген орнату.....	16
3.3 Өнімді іске қосу.....	19
3.4 Компьютерді қарап шығу.....	19
3.5 Ең соңғы нұсқасына дейін жаңарту.....	19
3.6 Жаңадан пайдаланушыларға арналған нұсқаулық.....	20
3.6.1 Пайдаланушы интерфейсі.....	20
3.6.2 Жаңарту параметрлері.....	22
3.7 Жалпы сұрақтар.....	23
3.7.1 ESET Endpoint Antivirus жаңарту әдісі.....	24
3.7.2 ESET Endpoint Antivirus бағдарламасын белсендіру әдісі.....	24
3.7.3 Жаңа өнімді іске қосу үшін ағымдағы тіркелгі деректерін пайдалану әдісі.....	25
3.7.4 Компьютерден вирусты жою жолы.....	25
3.7.5 Жоспарлағышта жаңа тапсырманы жасау әдісі.....	25
3.7.6 Қарап шығу тапсырмасын жоспарлау (24 сағат сайын).....	26
3.7.7 ESET Endpoint Antivirus бағдарламасын ESET Remote Administrator бағдарламасына қосу әдісі.....	26
3.7.8 Айнаны конфигурациялау әдісі.....	26
3.8 ESET Endpoint Antivirus бағдарламасымен жұмыс істеу.....	27
3.8.1 Компьютер.....	28
3.8.1.1 Антивирус.....	28
3.8.1.1.1 Инфилтрация анықталды.....	29
3.8.1.2 Ортақ жергілікті кэш.....	31
3.8.1.3 Нақты уақыттағы файл жүйесін қорғау.....	31
3.8.1.3.1 Қосымша ThreatSense параметрлері.....	32
3.8.1.3.2 Тазалау деңгейлері.....	33
3.8.1.3.3 Нақты уақыттағы қорғауды тексеру.....	33
3.8.1.3.4 Нақты уақыттағы қорғау конфигурациясын қашан өзгерту керек.....	33
3.8.1.3.5 Нақты уақыттағы қорғау жұмыс істемей жатса не істеу керек.....	33
3.8.1.4 Талап бойынша компьютерді қарап шығу.....	34
3.8.1.4.1 Таңдаулы ретпен қарап шығуды іске қосушы.....	35
3.8.1.4.2 Қарап шығудың орындалуы.....	36
3.8.1.5 Құрылғыны басқару.....	37
3.8.1.5.1 Құрылғы басқару ережелерін өңдеуші.....	38
3.8.1.5.2 Құрылғы басқару ережелерін қосу.....	39
3.8.1.6 Алынбалы құрал.....	40
3.8.1.7 Жұмыссыз күйде қарап шығу.....	41
3.8.1.8 Басты компьютерге басып кіруді болдырмау жүйесі (HIPS).....	41
3.8.1.8.1 Кеңейтілген орнату.....	43
3.8.1.8.2 HIPS интерактивті терезесі.....	44
3.8.1.9 Көрсету режимі.....	44
3.8.1.10 Іске қосылған кезде қарап шығу.....	45
3.8.1.10.1 Файлдарды тексеруді автоматты түрде іске қосу.....	45
3.8.1.11 Құжатты қорғау.....	45
3.8.1.12 Ерекшеліктер.....	46
3.8.1.13 ThreatSense механизмінің параметрлерін орнату.....	47
3.8.1.13.1 Ерекшеліктер.....	52
3.8.2 Веб және электрондық пошта.....	52
3.8.2.1 Протоколды сүзу.....	53
3.8.2.1.1 Веб және электрондық пошта клиенттері.....	53
3.8.2.1.2 Қамтылмаған бағдарламалар.....	53
3.8.2.1.3 Қамтылмаған IP мекенжайлар.....	54
3.8.2.1.4 SSL/TLS протоколын тексеру.....	55
3.8.2.1.4.1 Шифрланған SSL байланысы.....	56
3.8.2.1.4.2 Белгілі куәліктердің тізімі.....	56
3.8.2.2 Электрондық пошта клиентін қорғау.....	57
3.8.2.2.1 Электрондық пошта клиенттері.....	57
3.8.2.2.2 Электрондық пошта протоколдары.....	58
3.8.2.2.3 Ескертулер мен хабарландырулар.....	59
3.8.2.3 Вебке кіруді қорғау.....	60
3.8.2.3.1 Веб-протоколдар.....	61
3.8.2.3.2 URL мекенжайларын басқару.....	61
3.8.2.4 Антифишингтік қорғау.....	62
3.8.3 Бағдарламаны жаңарту.....	63
3.8.3.1 Жаңарту параметрлері.....	67
3.8.3.1.1 Жаңарту профилдері.....	69
3.8.3.1.2 Қайтаруды жаңарту.....	69
3.8.3.1.3 Жаңарту режимі.....	70
3.8.3.1.4 HTTP прокси.....	70
3.8.3.1.5 Жергілікті желіге былайша қосылу.....	71
3.8.3.1.6 Айна.....	71
3.8.3.1.6.1 Айнадан жаңарту.....	74
3.8.3.1.6.2 Айна жаңарту ақаулықтарын жою.....	76
3.8.3.2 Жаңарту тапсырмаларын жасау туралы.....	76
3.8.4 Құралдар.....	77
3.8.4.1 Журнал файлдары.....	78
3.8.4.1.1 Журналда іздеу.....	79
3.8.4.2 Прокси серверді орнату.....	79
3.8.4.3 Жоспарлағыш.....	80
3.8.4.4 Қорғау статистикасы.....	81

3.8.4.5	Белсенділікті қарау.....	82	3.10.2.4	Спам алаяқтығын анықтау.....	115
3.8.4.6	ESET SysInspector.....	82	3.10.3	ESET технологиясы.....	116
3.8.4.7	ESET Live Grid.....	83	3.10.3.1	Бүлдіруді блоктаушы.....	116
3.8.4.8	Іске қосылған процестер.....	84	3.10.3.2	Кеңейтілген жад сканері.....	116
3.8.4.9	Үлгілерді талдауға жіберу.....	85	3.10.3.3	ESET Live Grid.....	116
3.8.4.10	Электрондық пошта хабарландырулары.....	86	3.10.3.4	Java бүлдірулерін блоктаушы.....	116
3.8.4.11	Карантин.....	88			
3.8.4.12	Microsoft Windows update.....	89			
3.8.5	Пайдаланушы интерфейсі.....	89			
3.8.5.1	Пайдаланушы интерфейсі элементтері.....	90			
3.8.5.2	Кіру параметрлері.....	91			
3.8.5.3	Ескертулер мен хабарландырулар.....	92			
3.8.5.4	Жүйелік тақта белгішесі.....	93			
3.8.5.5	Контекстік мәзір.....	94			
<b>3.9</b>	<b>Озық пайдаланушы.....</b>	<b>95</b>			
3.9.1	Профайл реттеуші.....	95			
3.9.2	Диагностикалар.....	95			
3.9.3	Импорттау және экспорттау параметрлері.....	96			
3.9.4	Команда жолы.....	96			
3.9.5	Жұмыссыз күйді анықтау.....	98			
3.9.6	ESET SysInspector.....	98			
3.9.6.1	ESET SysInspector бағдарламасына кіріспе.....	98			
3.9.6.1.1	ESET SysInspector бағдарламасын іске қосу.....	98			
3.9.6.2	Пайдаланушы интерфейсі мен бағдарламаның пайдаланылуы.....	99			
3.9.6.2.1	Бағдарламаның басқару элементтері.....	99			
3.9.6.2.2	ESET SysInspector бағдарламасында шарлау.....	100			
3.9.6.2.2.1	Пернелер тіркесімдері.....	102			
3.9.6.2.3	Салыстыру.....	103			
3.9.6.3	Команда жолының параметрлері.....	104			
3.9.6.4	Қызметтік сценарий.....	104			
3.9.6.4.1	Қызметтік сценарийді жасау.....	105			
3.9.6.4.2	Қызметтік сценарийдің құрылымы.....	105			
3.9.6.4.3	Қызметтік сценарийлерді орындау.....	107			
3.9.6.5	ЖҚС.....	108			
3.9.6.6	ESET Endpoint Antivirus ESET SysInspector бөлімі ретінде.....	109			
<b>3.10</b>	<b>Глоссарий.....</b>	<b>109</b>			
3.10.1	Қауіптердің түрлері.....	109			
3.10.1.1	Вирустар.....	109			
3.10.1.2	Құрттар.....	110			
3.10.1.3	Троялық.....	110			
3.10.1.4	Руткиттер.....	110			
3.10.1.5	Жарнама бағдарламасы.....	111			
3.10.1.6	Шпиондық бағдарлама.....	111			
3.10.1.7	Бумалаушылар.....	111			
3.10.1.8	Ықтимал қауіпті бағдарламалар.....	112			
3.10.1.9	Ықтимал қалаусыз бағдарламалар.....	112			
3.10.2	Электрондық пошта.....	114			
3.10.2.1	Жарнамалар.....	115			
3.10.2.2	Алаяқтықтар.....	115			
3.10.2.3	Фишинг.....	115			

# 1. ESET Endpoint Antivirus

ESET Endpoint Antivirus 6 шынымен біріктірілген компьютер қауіпсіздігіне жаңа көзқарасты білдіреді. ThreatSense® 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 интеллектуалды жүйе.

ESET Endpoint Antivirus 6 – ең жоғары қорғау мен ең аз жүйе іздерін біріктіруге деген біздің ұзақ уақыттық күш салуымыздан туындаған толық қауіпсіздік шешімі. Жасанды интеллектке негізделген озық технологиялар жүйе өнімділігіне кедергі келтірмей немесе компьютерді бұзбай вирустардың, шпиондық бағдарламалардың, троялық аттардың, құрттардың, жарнама бағдарламаларының, руткиттердің және басқа интернет шабуылдарының инфильтрациясын проактивті түрде жоя алады.

ESET Endpoint Antivirus 6 негізінен шағын бизнес/кәсіпорын ортасындағы жұмыс станцияларында пайдалануға арналған. ESET Remote Administrator қосылымдары кез келген желі компьютерінен қашықтан конфигурациялау және анықтауды бақылау, ережелер мен саясаттарды қолдана отырып, кез келген клиенттік жұмыс станцияларын оңай басқаруға мүмкіндік береді.

## 1.1 Жаңалықтар

ESET Endpoint Antivirus графикалық пайдаланушы интерфейсінің дизайны жақсырақ көрінуді және көбірек интуитивті пайдаланушы тәжірибесін қамтамасыз ету үшін толығымен қайта жасалған. ESET Endpoint Antivirus бағдарламасының 6-нұсқасына қосылған көп жақсартулар мыналарды қамтиды:

### Функционалдық және пайдалану ыңғайлылығының жақсартулары

- Құрылғыны басқару - енді құрылғы түрін және сериялық нөмірді анықтау, әрі бірнеше құрылғы үшін бір ережені анықтау мүмкіндігін қамтиды.
- HIPS үшін жаңа зерделі режим - автоматты және интерактивтік режим арасында орналастырылады. Жүйедегі күмәнді әрекеттерді және зиянкес процестерді анықтау мүмкіндігі.
- Жаңартушы/айна жақсартулары - енді вирус қолтаңбасы дерекқорының және/немесе өнім модульдерінің сәтсіз жүктеулерін жалғастыруға болады.
- ESET Remote Administrator бағдарламасындағы компьютерлер үшін қашықтан басқаруға жаңа көзқарас - ERA бағдарламасын қайта орнату жағдайында немесе сынау үшін журналдарды қайта жіберу, ESET қауіпсіздік шешімдерін қашықтан орнату, желілік ортаның қауіпсіздік күйіне шолуды алу және әр түрлі деректерді кейінірек пайдалану үшін сұрыптау.
- Пайдаланушы интерфейсінің жақсартулары - Windows жүйелік тақтасынан вирус қолтаңбасы дерекқорын және модульдерін қолмен жаңартуды орындау үшін бір рет басу опциясын қосады. Сенсорлы экрандарды және ажыратымдылығы жоғары дисплейлерді қолдау.
- Үшінші тарап қауіпсіздік шешімдерін жақсартылған анықтау және жою.

### Жаңа функциялар

- Антифишинг - заңды болып көрінетін зиянкес веб-сайттарға қатынасты шектеу арқылы құпия сөздерді және басқа құпия ақпаратты алу әрекеттерінен қорғайды.
- Қарап шығу жылдамдығының жақсарулары - виртуалды орталарда ортақ жергілікті кәшті пайдалану.

### Анықтау және қорғау технологиялары

- Жақсартылған орнату жылдамдығы және сенімділігі.
- Жақсартылған жад сканері - процесс мінез-құлқын бақылайды және жадта ашылғанда зиянкес процестерді қарап шығады.
- Жақсартылған бүлдіруді блоктаушы - Веб-браузерлер, PDF оқу құралдары, электрондық пошта клиенттері мен MS Office компоненттері сияқты әдетте пайдаланатын бағдарлама түрлерін жақсарту үшін жасалған. Бүлдіруді блоктаушы енді Java бағдарламасын қолдайды және осы осалдық түрлерін анықтауды және олардан қорғауды жақсартуға көмектеседі.
- Руткиттерді анықтаудың және жоюдың жақсаруы.
- Жұмыссыз күйдегі қарап шығу құралы - компьютер жұмыссыз күйде болғанда барлық жергілікті дискілерде тыныш қарап шығуды орындайды.

## 1.2 Жүйе талаптары

ESET Endpoint Antivirus бағдарламасы біркелкі әрекет етуі үшін жүйе келесі жабдық және бағдарламалық құрал талаптарына сай болуы керек:

Қолдау көрсетілетін процессорлар: Intel® немесе AMD x86-x64

Операциялық жүйелер: Microsoft® Windows® 10/8.1/8/7/Vista/XP SP3 32 биттік/XP SP2 64 биттік

## 1.3 Алдын алу

Компьютермен жұмыс істеген кезде, әсіресе интернетті шолғанда дүниеде ешқандай антивирус жүйесінің [инфльтрациялардың](#) 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

ESET Live Grid статистикасына сәйкес, мыңдаған жаңа, бірегей инфльтрациялар қолданыстағы қауіпсіздік шараларын айналып өтіп, авторларға пайда әкелу үшін барлығы пайдаланушылардың есебінен жасалады. ESET компаниясындағы 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 зиянкес 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 жеңілдірек 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 кемінде айына бір рет компьютерді толық қарап шығуды орындауды ұсынамыз, себебі вирустар өзгеруі мүмкін және вирус сигнатурасының дерекқоры өздігінен күн сайын жаңарады.

### Негізгі қауіпсіздік ережелерін орындау

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

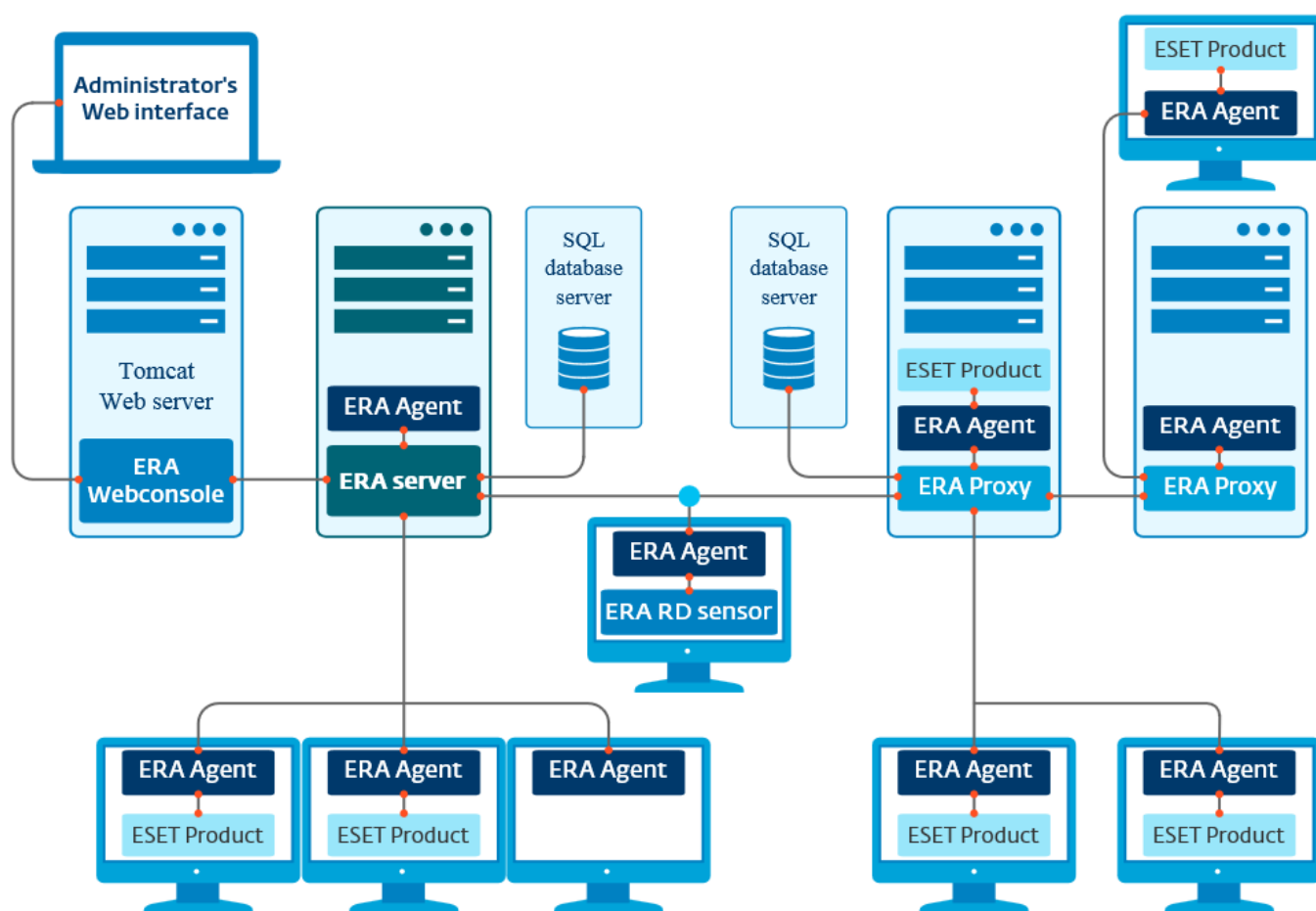
- Қалқымалы терезелері мен жыпылықтаған жарнамалары көп күдікті веб-тораптарға кірмеңіз.
- Тегін бағдарламаларды, кодек пакеттерін, т.б. орнатқан кезде сақ болыңыз. Тек қауіпсіз бағдарламаларды пайдаланып, интернеттегі қауіпсіз веб-тораптарға кіріңіз.
- Электрондық пошта тіркемелерін, әсіресе көп пайдаланушыға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

## 2. ESET Remote Administrator арқылы қосылған пайдаланушыларға арналған құжаттама

ESET Remote Administrator (ERA) — желілік ортада ESET өнімдерін бір орталық орыннан басқаруға мүмкіндік беретін бағдарлама. ESET Remote Administrator тапсырмаларды басқару жүйесі ESET қауіпсіздік шешімдерін қашықтағы компьютерлерде орнатуға және жаңа мәселелерге және қауіптерге жылдам жауап беруге мүмкіндік береді. ESET Remote Administrator зиянкес кодтан қорғауды қамтамасыз етпейді, ол әр клиентте ESET қауіпсіздік шешімінің болуына сенеді.

ESET қауіпсіздік шешімдері бірнеше платформа түрін қамтитын желілерді қолдайды. Желі ағымдағы Microsoft, Linux, Mac OS жүйелерінің және мобильді құрылғыларда (мобильді телефондар және планшеттер) жұмыс істейтін операциялық жүйелерді қамтуы мүмкін.

Төмендегі суретте ERA басқаратын ESET қауіпсіздік шешімдері арқылы қорғалған желі архитектурасының үлгісі көрсетілген:



**ЕСКЕРТПЕ:** қосымша ақпаратты [ESET Remote Administrator пайдаланушы нұсқаулығынан](#) қараңыз.

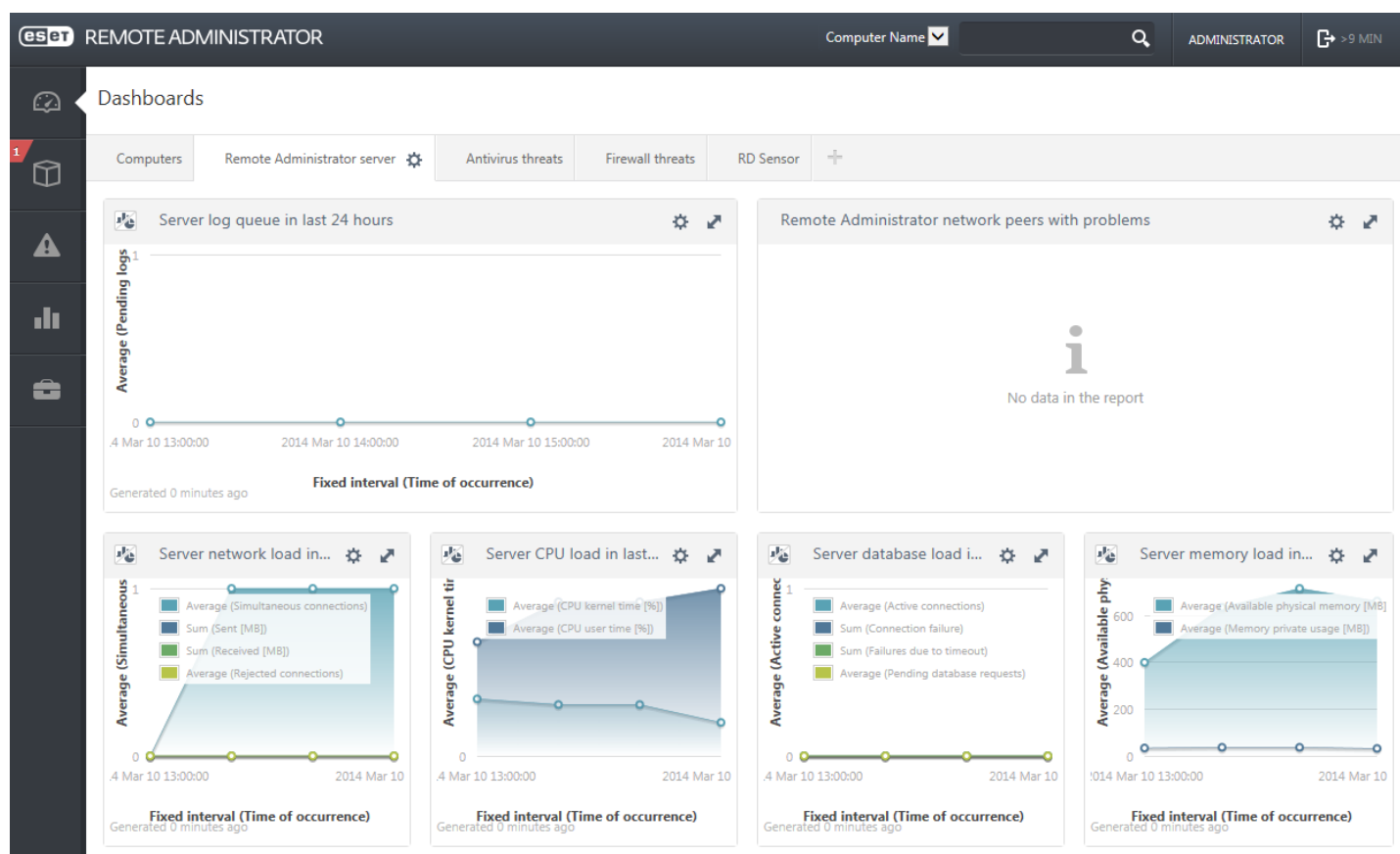
## 2.1 ESET Remote Administrator Server

**ESET Remote Administrator Server** — ESET Remote Administrator бағдарламасының негізгі компоненті. Бұл — Server бағдарламасына ([ERA Agent](#) арқылы) қосылатын клиенттерден алынған барлық деректерді өңдейтін басқарушы бағдарлама. ERA Agent клиент пен сервер арасындағы байланысты жеңілдетеді. Деректер (клиент журналдары, конфигурация, агентті репликалау, т.б.) дерекқорда сақталады. Деректерді дұрыс өңдеу үшін ERA Server дерекқор серверіне тұрақты қосылымды қажет етеді. Өнімділікті оңтайландыру үшін ERA Server және дерекқорды бөлек серверлерде орнату ұсынылады. ERA Server орнатылған компьютерді сертификаттарды пайдаланып верификацияланатын Agent/Proxy/RD Sensor қосылымдарының барлығын қабылдауға конфигурациялау қажет. Орнатқаннан кейін ERA Server бағдарламасына қосылатын [ERA веб-консолін](#) ашуға болады (диаграммада көруге болады). Веб-консольден желідегі ESET қауіпсіздік шешімдерін басқарғанда барлық ERA Server әрекеттері орындалады.

## 2.2 Веб-консоль

**ERA веб-консолі** — [ERA Server](#) ішіндегі деректерді көрсететін және сізге желідегі ESET қауіпсіздік шешімдерін басқаруға мүмкіндік беретін пайдаланушылық веб-интерфейс. Веб-консольге браузерді пайдаланып қатынасуға болады. Ол желідегі клиенттердің күйін шолуды көрсетеді және оны басқарылмайтын компьютерлерде ESET шешімдерін қашықтан жаю үшін пайдалануға болады. ESET Remote Administrator бағдарламасын кез келген дерлік жерден немесе құрылғыдан пайдалануға мүмкіндік беру үшін веб-серверге интернеттен қатынасуды мүмкін ете аласыз.

Бұл — веб-консольдің бақылау тақтасы:



**Жылдам іздеу** құралы веб-консольдің жоғарғы жағында орналасқан. Ашылмалы мәзірде **Компьютер атауы**, **IPv4/IPv6 мекенжайы** немесе **Қауіп атауы** тармағын таңдаңыз, іздеу жолын мәтіндік өріске теріңіз, содан кейін іздеу үшін ұлғайтқыш таңбасын басыңыз немесе **Enter** пернесін басыңыз. Сіз іздеу нәтижесі көрсетілетін **Топтар** бөліміне қайта бағытталасыз.

**ЕСКЕРТПЕ:** қосымша ақпаратты [ESET Remote Administrator пайдаланушы нұсқаулығынан](#) қараңыз.



## 2.3 Прокси-сервер

**ERA Proxy** — ESET Remote Administrator бағдарламасының тағы бір компоненті, оның екі мақсаты бар. Орташа өлшемді немесе көп клиенттер бар қауымдық желіде (мысалы, 10 000 клиент немесе көбірек), ERA Proxy компонентін жүктемені бірнеше ERA прокси-сервері арасында үлестіріп, негізгі [ERA Server](#) жүктемесін жеңілдету үшін пайдалануға болады. ERA Proxy компонентінің тағы бір артықшылығы — оны әлсіз байланысы бар қашықтағы филиалға қосылғанда пайдалануға болады. Яғни, әр клиенттегі ERA Agent басты ERA Server серверіне филиалдың жергілікті желісіндегі ERA Proxy прокси-сервері арқылы тікелей қосылып жатқан жоқ. Бұл конфигурация филиалмен байланысты босатады. ERA Proxy прокси-сервері барлық жергілікті ERA Agent агенттерінен қосылымдарды қабылдайды, олардан алынған деректерді компиляциялайды және басты ERA Server серверіне (немесе басқа ERA Proxy прокси-серверіне) кері жүктейді. Бұл желіге желі және дерекқор сұрауларының сапасын төмендетпестен қосымша клиенттерді қабылдауға мүмкіндік береді.

Желі конфигурациясына байланысты Proxy бағдарламасы басқа Proxy бағдарламасына қосылып, содан кейін басты ERA Server бағдарламасына қосыла алады.

ERA Proxy дұрыс қызмет етуі үшін ESET Proxy бағдарламасы орнатылған хост компьютерде ESET Agent орнатылған болуы және бұл компьютер желінің жоғарғы деңгейіне (ERA Server немесе жоғарғы ERA Proxy, бар болса) қосылған болуы керек.

## 2.4 Агент

**ERA Agent** — ESET Remote Administrator өнімінің негізгі бөлігі. Клиенттік компьютерлердегі ESET қауіпсіздік шешімдері (мысалы, ESET Endpoint security) ERA Server бағдарламасымен Agent арқылы байланысады. Бұл байланыс барлық қашықтағы клиенттердегі ESET қауіпсіздік шешімдерін бір орталық орыннан басқаруға мүмкіндік береді. Agent клиенттен ақпаратты жинайды және оны Server бағдарламасына жібереді. Server клиентке тапсырманы жіберсе, тапсырма Agent бағдарламасына жіберіледі, содан кейін Agent клиентпен байланысады. Бүкіл желілік байланыс агент пен ERA желісінің жоғарғы бөлігі болып табылатын сервер мен прокси-сервер арасында орын алады.

ESET Agent серверге қосылу үшін келесі үш әдістердің біреуін пайдаланады:

1. Клиенттің агенті серверге тікелей қосылады.
2. Клиенттің агенті серверге қосылған прокси-сервер арқылы қосылады.
3. Клиенттің агенті серверге бірнеше прокси-сервер арқылы қосылады.

ESET Agent клиентте орнатылған ESET шешімдерімен байланысады, сол клиенттегі бағдарламалардан ақпарат жинайды және серверден алынған конфигурация туралы ақпаратты клиентке береді.

**ЕСКЕРТПЕ:** ESET прокси-серверінің клиенттер, басқа прокси-серверлер және сервер арасындағы бүкіл байланыс тапсырмаларын өңдейтін жеке агенті бар.

## 2.5 RD Sensor

**RD (Rogue Detection) Sensor** — ESET Remote Administrator бағдарламасының желідегі компьютерлерді табуға арналған бөлігі. Ол қолмен іздеу және қосу қажеттілігінсіз жаңа компьютерлерді ESET Remote Administrator бағдарламасына қосудың ыңғайлы жолын қамтамасыз етеді. Желіде табылған әр компьютер Веб-консольде көрсетіледі және әдепкі **Барлығы** тобына қосылады. Осы жерден жекелеген клиенттік компьютерлерде қосымша әрекеттерді орындауға болады.

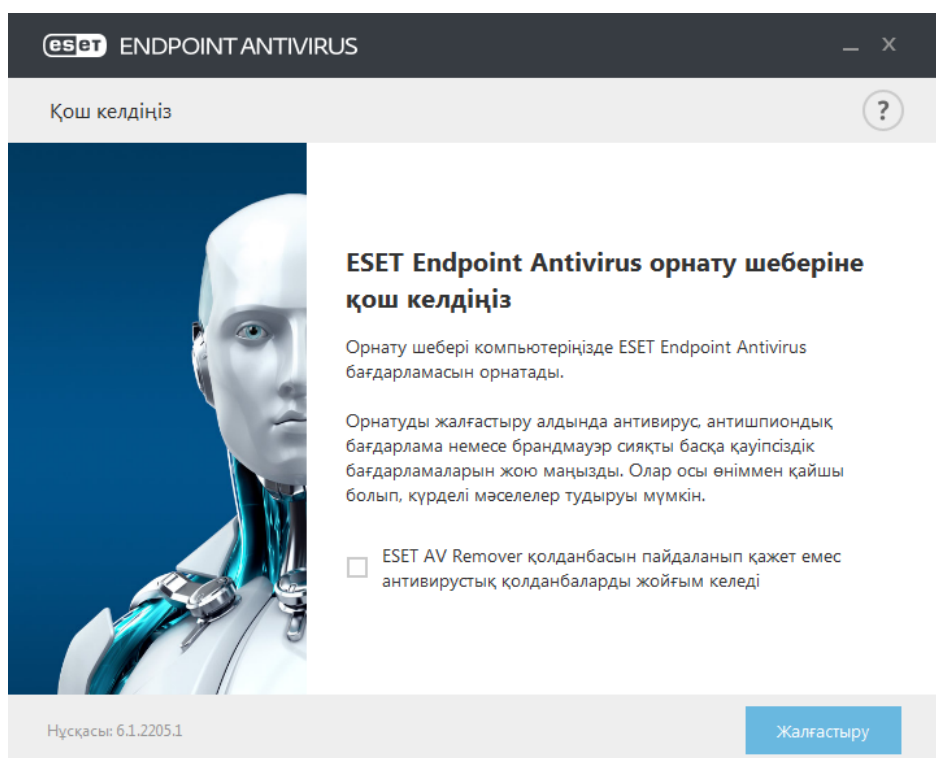
RD Sensor — желіде бар компьютерлерді анықтайтын және олар туралы ақпаратты ERA Server бағдарламасына жіберетін пассивті тыңдаушы. ERA Server желіде табылған дербес компьютерлер белгісіз екенін немесе әлдеқашан басқарылатынын бағалайды.

### 3. ESET Endpoint Antivirus өзін пайдалану

Пайдаланушы нұсқаулығының бұл бөлімі ESET Endpoint Antivirus бағдарламасын ESET Remote Administrator бағдарламасынсыз пайдаланып жатқан пайдаланушыларға арналған. Пайдаланушы есептік жазбасының құқықтарына байланысты ESET Endpoint Antivirus бағдарламасының барлық мүмкіндіктеріне және функцияларына толығымен қатынасуға болады.

#### 3.1 ESET AV Remover арқылы орнату

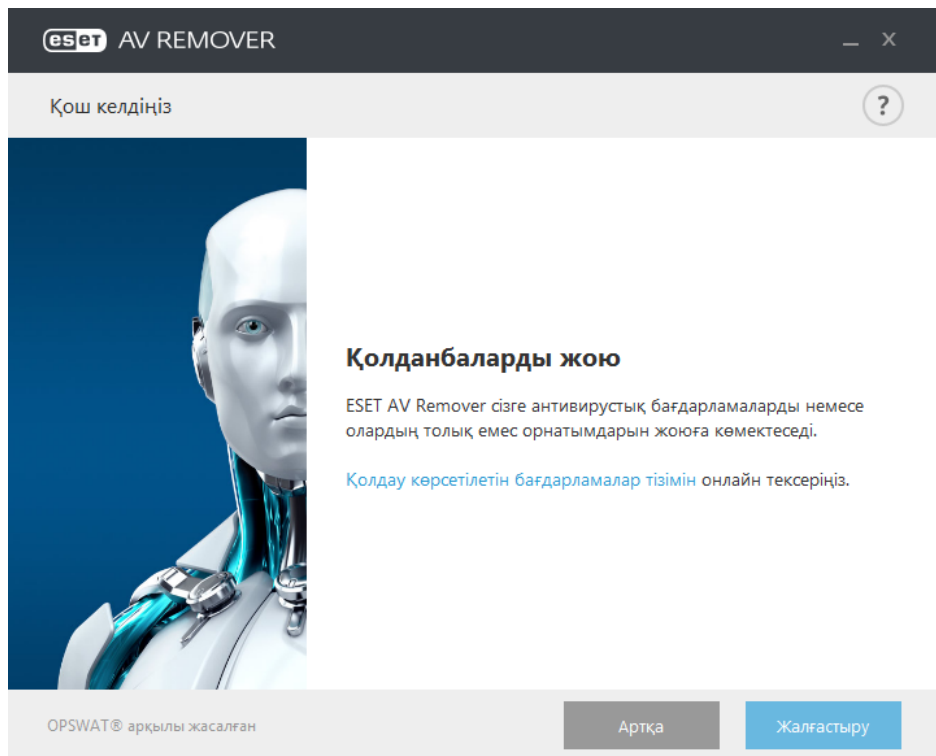
Орнату процесін жалғастырмай тұрып компьютердегі кез келген бар қауіпсіздік қолданбасын жою маңызды. ESET AV Remover жүйені қарап шығу және кез келген [қолдау көрсетілетін қауіпсіздік қолданбаларын](#) жою үшін **Қажет емес антивирустық қолданбаларды ESET AV Remover арқылы жойғым келеді** жанындағы құсбелгіні қойыңыз. ESET Endpoint Antivirus бағдарламасын ESET AV Remover бағдарламасын іске қоспай орнату үшін құсбелгіні қоймаңыз және **Жалғастыру** түймесін басыңыз.



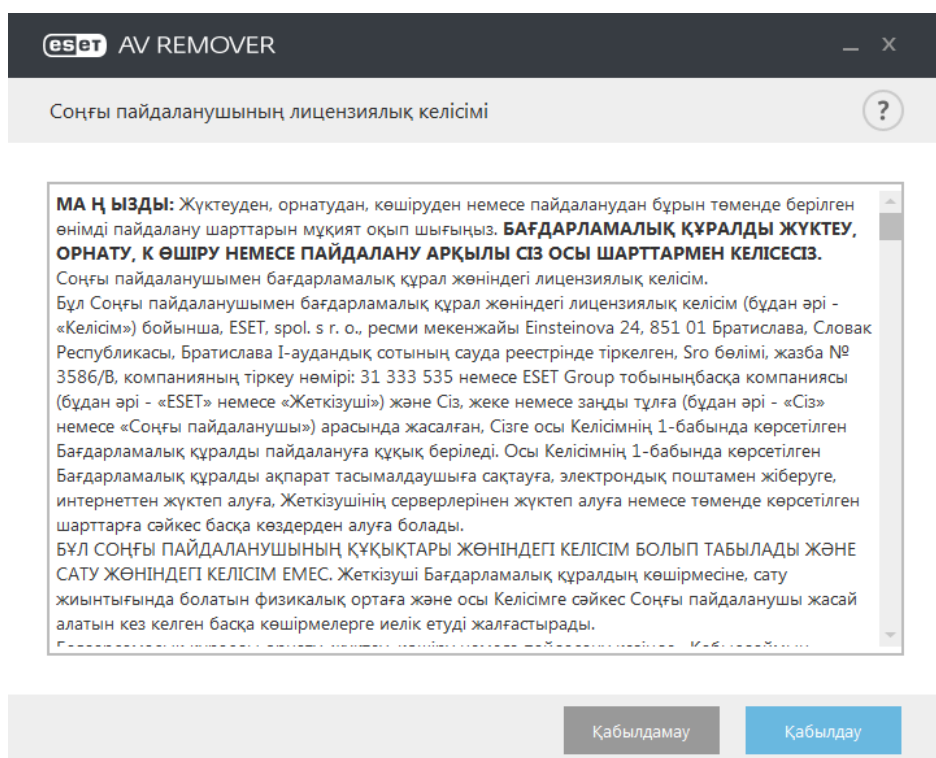
### 3.1.1 ESET AV Remover

ESET AV Remover құралы сізге жүйеде бұрын орнатылған кез келген дерлік антивирустық бағдарламаны жоюға көмектеседі. ESET AV Remover арқылы бар антивирустық бағдарламаны жою үшін төмендегі нұсқауларды орындаңыз:

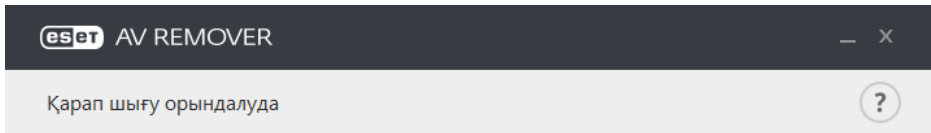
1. ESET AV Remover жоя алатын антивирустық бағдарламалар тізімін көру үшін ESET [білім қорының мақаласына](#) кіріңіз.



2. Оқып шығып, соңғы пайдаланушы лицензиялық келісiмiн қабылдауыңызды растау үшін **Қабылдау** түймесiн басыңыз. **Қабылдамау** түймесiн бассаңыз, компьютердегi бар қауiпсiздiк қолданбасы жойылмастан ESET Endpoint Antivirus бағдарламасын орнату жалғасады.



3. ESET AV Remover жүйеде антивирустық бағдарламаны іздеуді бастайды.



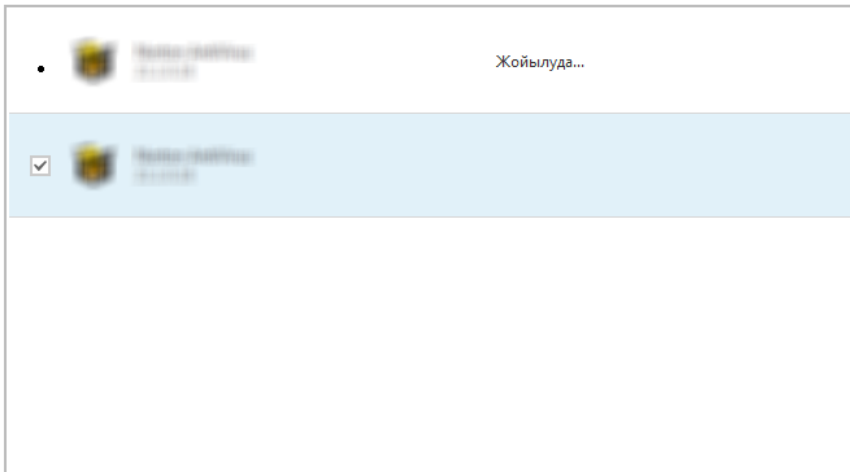
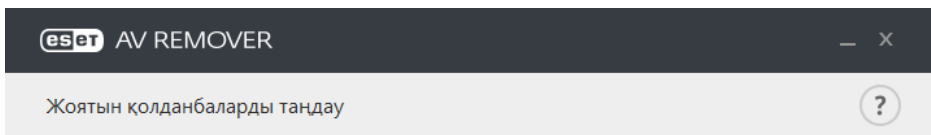
### Орнатылған қолданбалар қарап шығылуда

Бұған бірнеше минут қажет болуы мүмкін

• • •

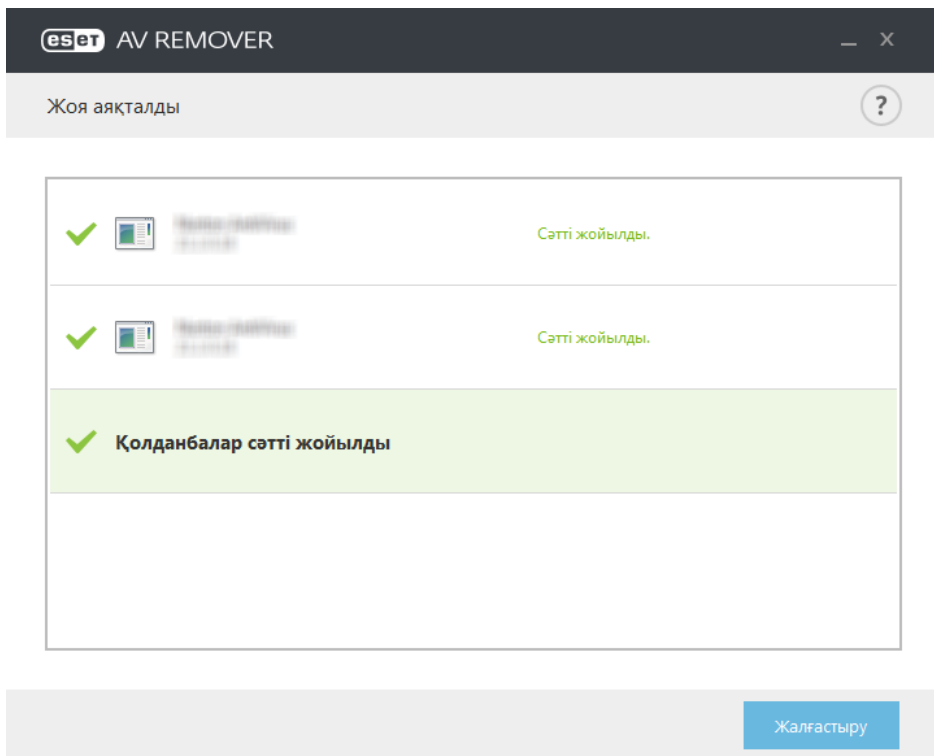
Бас тарту

4. Тізімдегі кез келген антивирустық қолданбаны таңдап, «Жою» түймесін басыңыз. Жоюға бірнеше минут қажет болуы мүмкін.

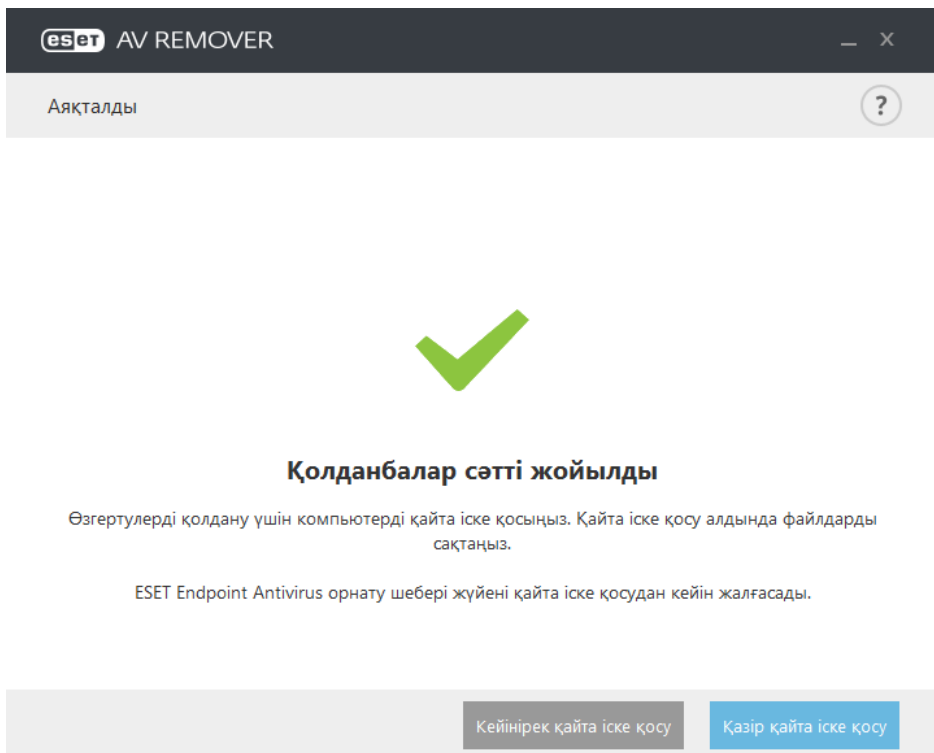


Бас тарту

5. Жою сәтті аяқталғанда **Жалғастыру** түймесін басыңыз.



6. Өзгертулерді қолдану және ESET Endpoint Antivirus бағдарламасын орнатуды жалғастыру үшін компьютерді қайта іске қосыңыз. Жою сәтсіз болса, осы нұсқаулықтың [ESET AV Remover арқылы жою қатемен аяқталды](#) бөлімін қараңыз.



### 3.1.2 ESET AV Remover арқылы жою қатемен аяқталды

Антивирустық бағдарламаны ESET AV Remover арқылы жою алмасаңыз, жоюға тырысып жатқан қолданбаға ESET AV Remover қолдау көрсетпеуі мүмкін екені туралы хабарландыру аласыз. Нақты осы бағдарламаны жою мүмкін бе, соны көру үшін ESET білім қорында [қолдау көрсетілетін өнімдер тізіміне](#) немесе [жиі кездесетін Windows антивирустық бағдарламаларына арналған жоюшыларға](#) кіріңіз.

Қауіпсіздік өнімін жою сәтсіз болса немесе оның құрамдасының бір бөлігі ішінара жойылса, сізге **Қайта іске қосу және қайта қарап шығу** ұсынылады. Іске қосудан кейін UAC растаңыз және қарап шығу мен жою процесін жалғастырыңыз.

Қажет болса, қолдауды сұрауды ашу үшін ESET тұтынушыларды қолдау қызметіне хабарласыңыз және ESET техникалық мамандарына көмектесу үшін **AppRemover.log** файлын дайындаңыз. **AppRemover.log** файлы **eset** қалтасында орналасқан. Бұл қалтаға қатынасу үшін Windows Explorer ішінде `%TEMP%` қалтасына өтіңіз. ESET тұтынушыларды қолдау қызметі мәселеңізді шешу үшін мүмкіндігінше тез жауап береді.

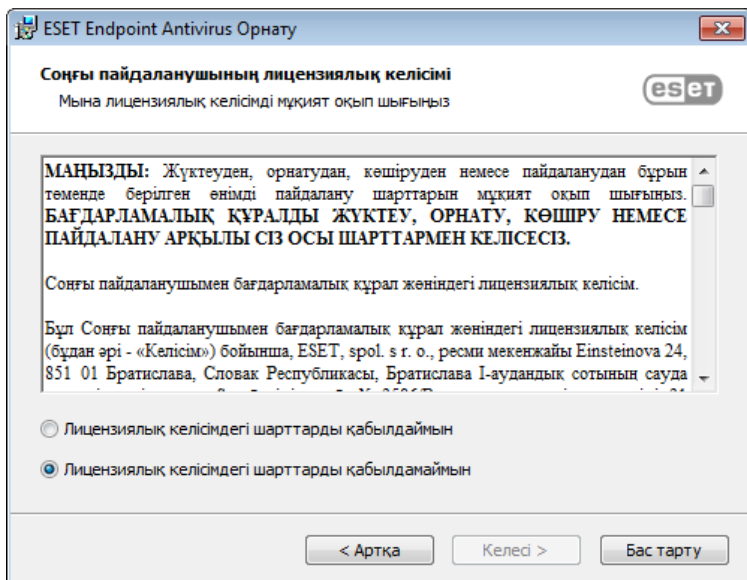
## 3.2 Орнату

Орнатқышты іске қосқаннан кейін орнату шебері орнату процесі арқылы өткізеді.

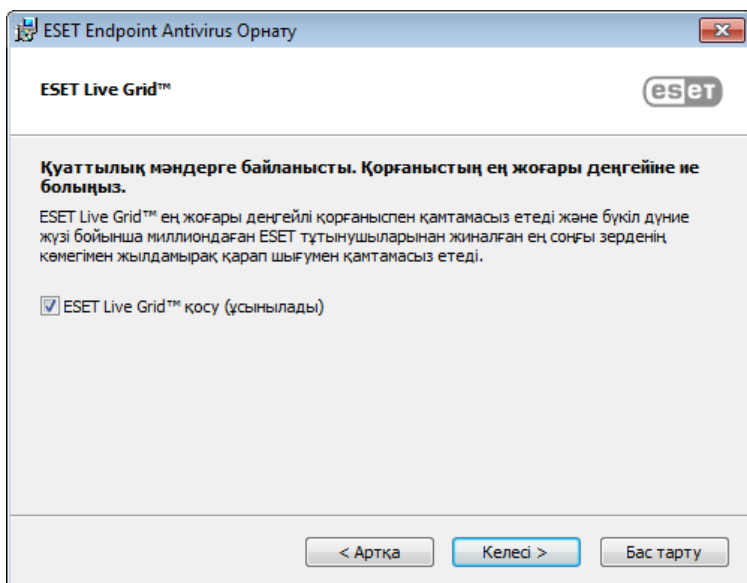
**Маңызды:** Компьютерде басқа антивирустық бағдарламалардың орнатылмағанына көз жеткізіңіз. Егер бір компьютерде екі немесе одан көп антивирустық шешімдер орнатылған болса, олардың арасында қайшылықтар болуы мүмкін. Жүйеден басқа антивирустық бағдарламаларды жою ұсынылады. Жалпы антивирустық бағдарламаны құралдар тізімінен жою үшін [білім қоры мақаласын](#) (ағылшын және бірнеше басқа тілдерде қол жетімді) қараңыз.



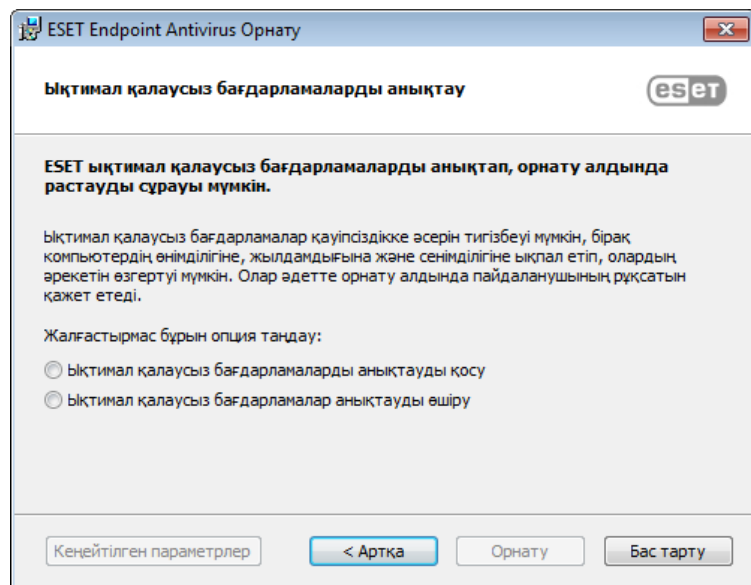
Келесі қадамда соңғы пайдаланушы лицензиялық келісімі көрсетіледі. Оқып шығып, соңғы пайдаланушы лицензиялық келісімін қабылдауыңызды растау үшін **Қабылдау** түймесін басыңыз. Орнатуды жалғастыру үшін шарттарды қабылдаудан кейін **Келесі** түймесін басыңыз.



«Қабылдаймын...» пәрменін таңдап, **Келесі** түймесін басқаннан кейін сізге ESET Live Grid бағдарламасын конфигурациялау ұсынылады. ESET Live Grid бағдарламасы ESET компаниясы жаңа инфильтрациялар туралы бірден және үздіксіз хабардар етілуін қамтамасыз етуге көмектеседі, бұл бізге тұтынушыларымызды жақсырақ қорғауға көмектеседі. Жүйе сізге жаңа қауіптерді ESET вирус зертханасына жіберуге мүмкіндік береді. Онда олар талданады, өңделеді және вирус қолтаңбасының дерекқорына қосылады.



Орнату процесіндегі келесі қадам — міндетті түрде зиянкес болып табылмайтын, бірақ жиі операциялық жүйенің мінез-құлқына тері әсер ете алатын ықтимал қалаусыз бағдарламаларды анықтауды конфигурациялау. Қосымша мәліметтерді алу үшін [Қажетсіздігі ықтимал бағдарламалар](#) тарауын қараңыз. Қосымша параметрлерді **Кеңейтілген параметрлер** түймесін басу арқылы ашуға болады (мысалы, ESET өнімін белгілі бір қалтада орнату немесе орнатудан кейін автоматты түрде қарап шығуды қосу үшін).



Соңғы қадам — **Орнату** түймесін басу арқылы орнатуды растау.

### 3.2.1 Кеңейтілген орнату

Кеңейтілген орнату әдеттегі орнатуды орындау кезінде қол жетімді емес бірқатар орнату параметрлерін теңшеуге мүмкіндік береді.

Ықтимал қалаусыз бағдарламаларды анықтау параметрін таңдау және **Қосымша параметрлер** тармағын басқаннан кейін сізге өнімді орнату қалтасының орнын таңдау ұсынылады. Әдепкі бойынша бағдарлама келесі каталогқа орнатылады:

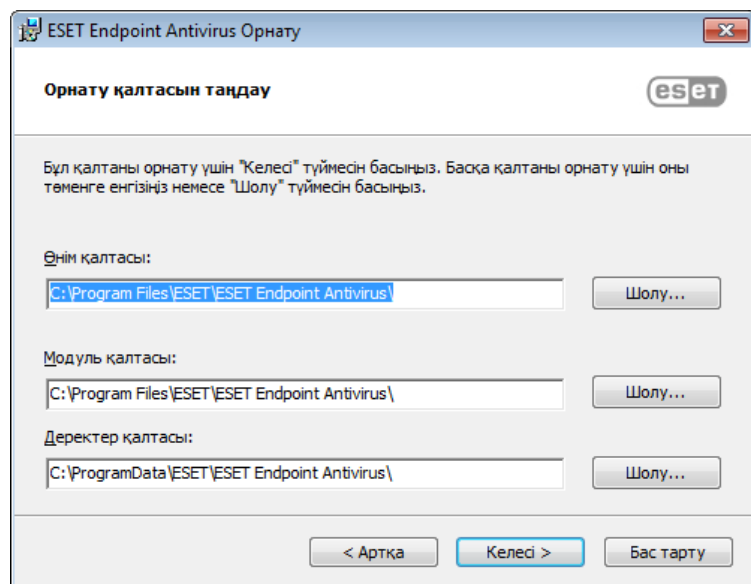
```
C:\Program Files\ESET\ESET Endpoint Antivirus\
```

Бағдарлама модульдері және деректер үшін орынды көрсетуге болады. Әдепкі бойынша, олар келесі каталогтарға орнатылады:

```
C:\Program Files\ESET\ESET Endpoint Antivirus\
```

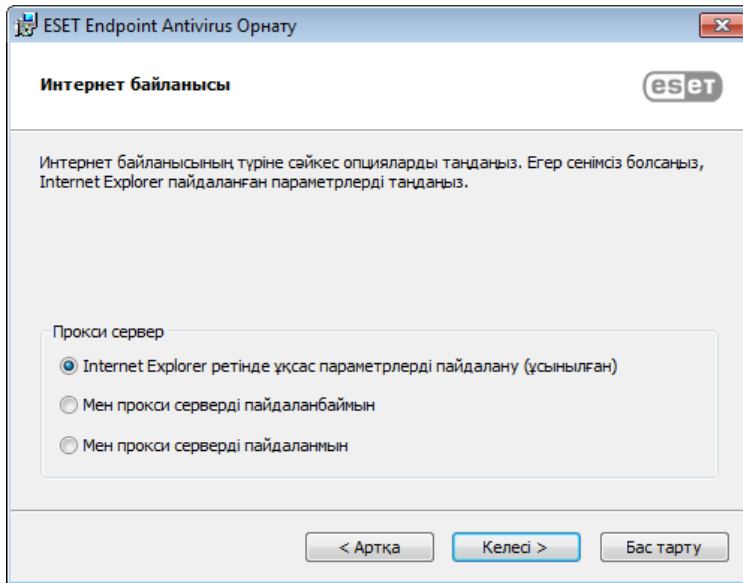
```
C:\ProgramData\ESET\ESET Endpoint Antivirus\
```

Бұл орындарды өзгерту үшін **Шолу** түймесін басыңыз (ұсынылмайды).

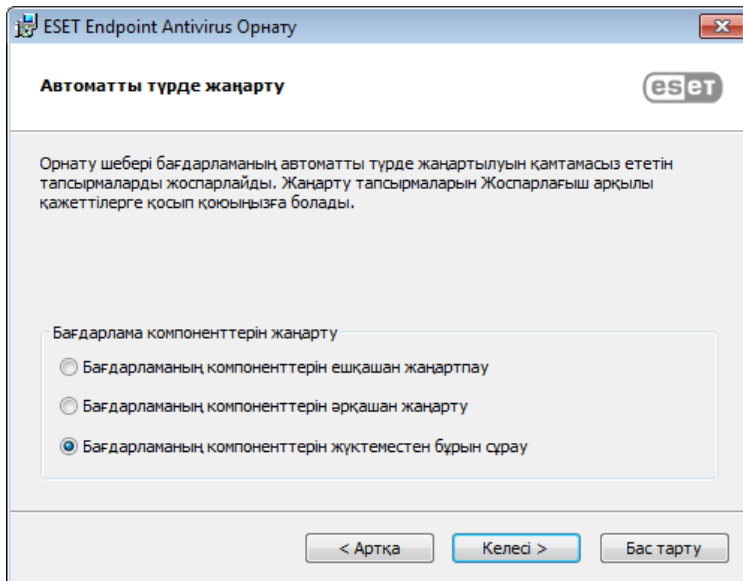




Прокси сервер параметрлерін конфигурациялау үшін **Мен прокси серверді пайдаланамын** опциясын таңдап, **Келесі** түймешігін басыңыз. Прокси сервердің IP мекенжайын немесе URL мекенжайын **Мекенжай** өрісіне енгізіңіз. Егер интернетке қосылу үшін прокси сервері пайдаланылатынына сенімді болмасаңыз, **Internet Explorer сияқты бірдей параметрлер пайдалану (Ұсынылады)** тармағын басыңыз, **Келесі** тармағын басыңыз. Егер прокси серверді пайдаланбасаңыз, **Мен прокси серверді пайдаланбаймын** опциясын таңдаңыз. Қосымша ақпарат алу үшін [Прокси-сервер](#) бөлімін қараңыз.

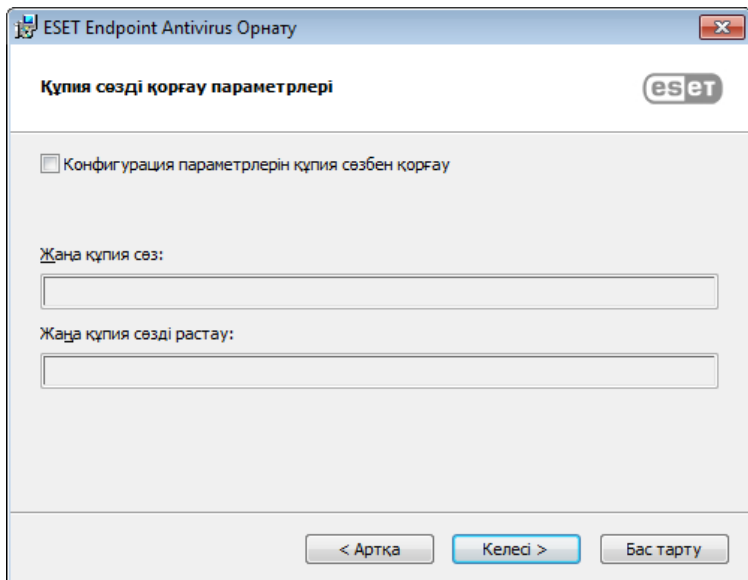


Таңдамалы орнату автоматты түрде бағдарлама жаңартуларымен жүйеде қалай жұмыс істелетінін анықтауға мүмкіндік береді. Кеңейтілген параметрлерге кір үшін **Өзгерту...** түймесін басыңыз.

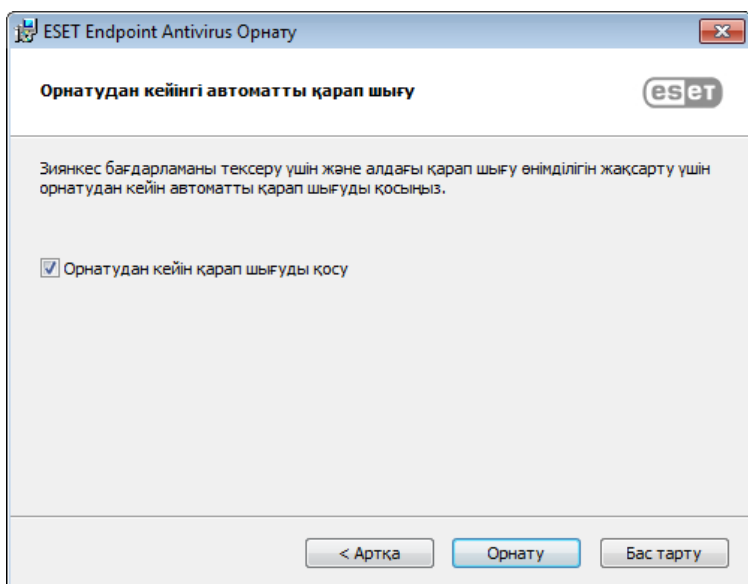


Бағдарлама компоненттерінің жаңартылуын қаламасаңыз, **Бағдарлама компоненттерін өш қаш ан жаңартпау** опциясын таңдаңыз. Жүйе бағдарлама құрамдастарын әр жүктеу кезінде растау терезесін көрсету үшін **Бағдарлама компоненттерін жүктеу алдында сұрау** опциясын таңдаңыз. Бағдарлама компоненті жаңартуларын автоматты түрде жүктеу үшін **Бағдарлама компоненттерін әрдайым жаңарту** опциясын таңдаңыз.

Келесі орнату терезесі бағдарлама параметрлерін қорғау үшін құпиясөз орнату опциясын ұсынады. **Құпия сөз арқылы конфигурация параметрлерін қорғау** опциясын таңдап, құпия сөзіңізді **Жаңа құпия сөз** және **Жаңа құпия сөзді растау** өрістеріне енгізіңіз. Бұл құпия сөз ESET Endpoint Antivirus параметрлерін өзгертуге немесе оларға кіруге қажет болады. Құпиясөз өрістерінің екеуі сәйкес келгенде, жалғастыру үшін **Келесі** түймесін басыңыз.



Әдетте орнату аяқталғанда орындалатын [орнатудан кейінгі бірінші қарап шығуды](#) өшіру үшін **Орнатудан кейін қарап шығуды қосу** жанындағы құсбелгіні алыңыз.



Орнатуды бастау үшін **Орнату** түймесін басыңыз.

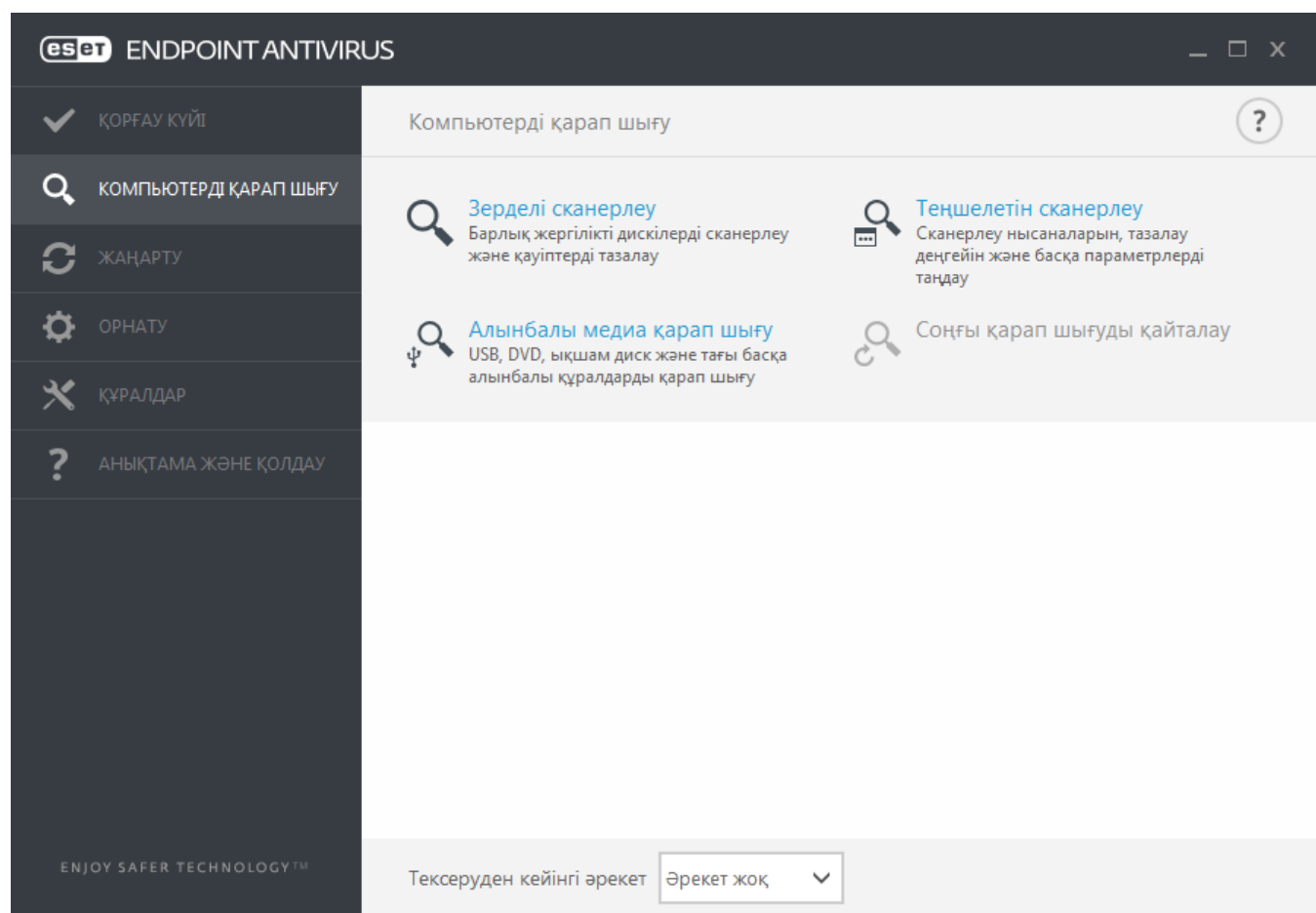
### 3.3 Өнімді іске қосу

Орнату аяқталғаннан кейін өнімді белсендіру сұралады.

ESET Endpoint Antivirus бағдарламасын белсендіру үшін қол жетімді әдістердің біреуін таңдаңыз. Қосымша ақпарат алу үшін [ESET Endpoint Antivirus бағдарламасын белсендіру әдісі](#) бөлімін қараңыз.

### 3.4 Компьютерді қарап шығу

Орнату аяқталғаннан кейін 15 минуттан кешікпей (компьютерді қайта іске қосу қажет болуы мүмкін) ESET Endpoint Antivirus компьютерді қарап шығуды автоматты түрде орындайды. Бастапқы қарап шығуға қоса, қауіптер бар-жоғын тексеру үшін жүйелі компьютерді қарап шығуларды орындау немесе [жүйелі қарап шығуды жоспарлау](#), ұсынылады. Бағдарламаның негізгі терезесінде **Компьютерді қарап шығу** командасын, содан кейін **Зерделі қарап шығу** командасын таңдаңыз. Компьютерді қарап шығулар туралы қосымша ақпарат алу үшін [Компьютерді қарап шығу](#) бөлімін қараңыз.



### 3.5 Ең соңғы нұсқасына дейін жаңарту

Жақсартуларды қамтамасыз ету немесе бағдарлама модульдерін автоматты түрде жаңартулар арқылы түзету мүмкін емес мәселелерді шешу үшін ESET Endpoint 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 алуын ұзақ тексеруден кейін шығарылады. Егер жаңарақ нұсқаға шығарылғаннан кейін дереу өту керек болса, төменде крсетілген әдістердің біреуін пайдаланыңыз.
2. Қолмен, ең соңғы нұсқаны жүктеу және алдыңғысының үстінен орнату арқылы.
3. Қолмен, желі ортасында ESET Remote Administrator арқылы автоматты түрде қолдана отырып.

## 3.6 Жаңадан пайдаланушыларға арналған нұсқаулық

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

### 3.6.1 Пайдаланушы интерфейсі

ESET Endpoint 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:

**Қорғау күйі** - ESET Endpoint Antivirus бағдарламасының қорғау күйі туралы ақпаратты қамтамасыз етеді.

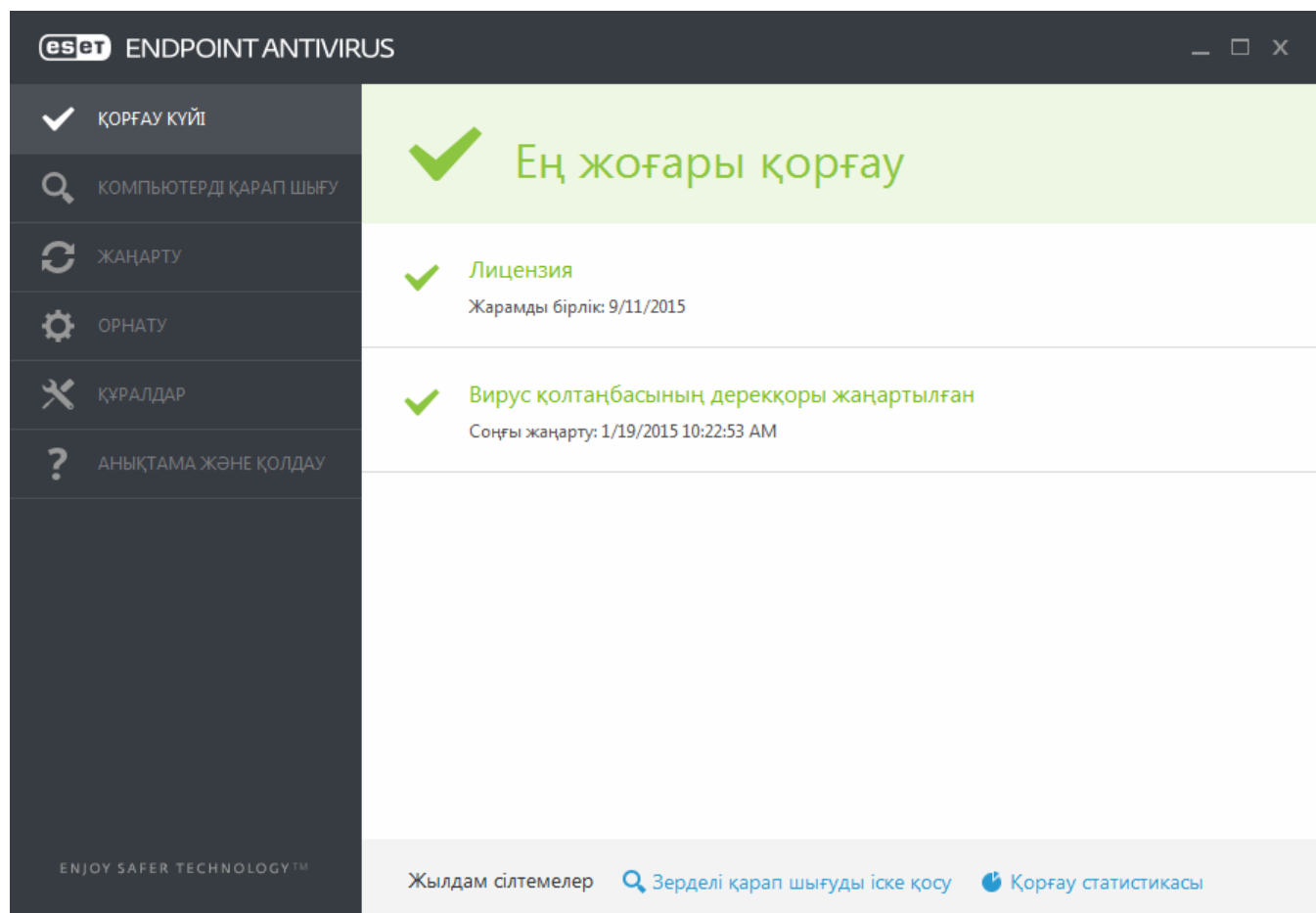
**Компьютерді қарап шығу** - бұл опция зерделі қарап шығуды, таңдамалы қарап шығуды немесе алынбалы құралдарды қарап шығуды конфигурациялауға және іске қосуға мүмкіндік береді. Сондай-ақ, орындалған соңғы қарап шығуды қайталауға болады.

**Жаңарту** - вирус қолтаңбасы дерекқоры туралы ақпаратты көрсетеді.

**Орнату** - бұл опцияны Компьютер немесе Веб және электрондық пошта қауіпсіздік параметрлерін реттеу үшін таңдаңыз.

**Құралдар** - «Журнал файлдары», «Қорғау статистикасы», «Көру белсенділігі», «Іске қосылған процестер», «Жоспарлағыш», «Карантин», ESET SysInspector және ESET SysRescue тармақтарына қалпына келтіру дискін жасау үшін қатынасуды қамтамасыз етеді. Сондай-ақ, үлгіні талдауға жіберуге болады.

**Анықтама және қолдау** - анықтама файлдарына, [ESET білім қорына](#) және ESET компаниясының веб-сайтына қатынасты қамтамасыз етеді. Сондай-ақ, тұтынушыларды қолдау қызметінің қолдауын сұрауды, қолдау құралдарын және өнімді белсендіру туралы ақпаратты ашу сілтемелері қол жетімді.

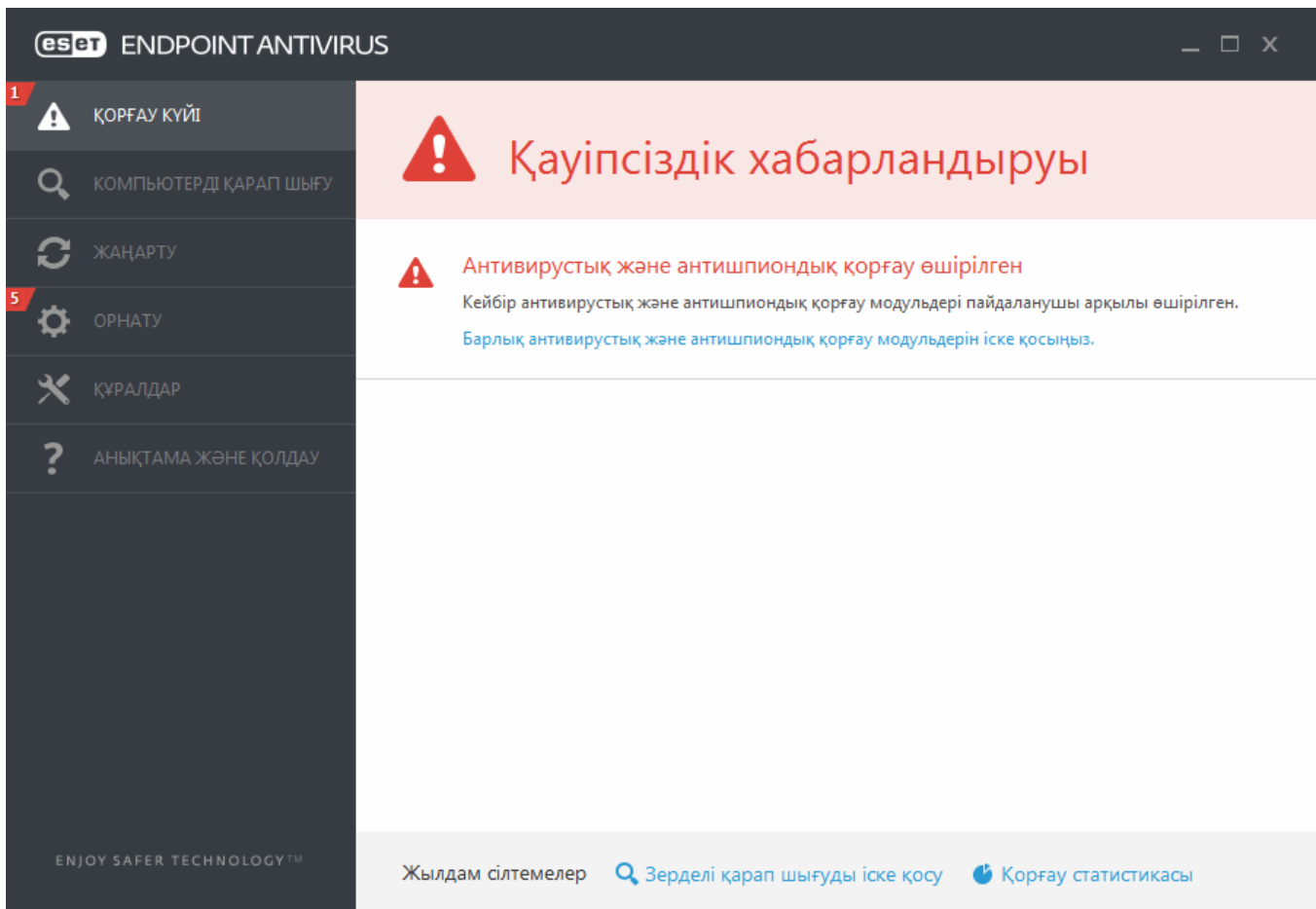



**Қорғау күйі** экраны компьютердің қауіпсіздігі және ағымдағы қорғау деңгейі туралы хабарлайды. Жасыл **Ең жоғары қорғау** күйі ең жоғары қорғау қамтамасыз етілгенін көрсетеді.

Сондай-ақ, күй терезесі ESET Endpoint Antivirus бағдарламасындағы жиі пайдаланылатын мүмкіндіктерге және соңғы жаңарту туралы ақпаратқа жылдам сілтемелерді көрсетеді.


## Бағдарлама тиісті түрде жұмыс істемесе не істеу керек?

Егер қосылған модульдер тиісті түрде жұмыс істеп тұрса, оларға жасыл құсбелгі қойылады. Қойылмаса, қызыл леп белгісі немесе қызғылт сары хабарландыру белгішесі көрсетіледі. Терезенің жоғарғы бөлігінде модуль туралы қосымша ақпарат көрсетіледі. Сондай-ақ, модульді түзету бойынша ұсынылатын шешім көрсетіледі. Жекелеген модульдердің күйін өзгерту үшін негізгі мәзірде **Орнату** түймешігін басып, қалаған модульді басыңыз.



 «!» таңбасы бар қызыл белгіше күрделі мәселелер туралы белгі береді – компьютерді ең жоғары қорғау қамтамасыз етілмеген. Ықтимал себептері:

- **Антивирустық және антишпиондық қорғау өшірілген** - Антивирустық және антишпиондық қорғауды **Қорғау күйі** тақтасында **Нақты уақыттағы қорғауды қосу** немесе басты бағдарлама терезесіндегі **Орнату** тақтасында **Антивирустық және антишпиондық қорғауды қосу** тармағын басып арқылы қайта қосуға болады.
- **Вирус қолтаңбасының деректоры ескірген** - Сіз ескірген вирус қолтаңбасының деректорын пайдаланып жатырсыз.
- **Өнім белсендірілмеген** немесе **Лицензияның мерзімі бітті** - Мұны «Қорғау» күйі белгішесінің қызылға айналуы көрсетеді. Лицензияның мерзімі біткеннен кейін бағдарламаны жаңарту мүмкін емес. Лицензияны жаңарту үшін ескерту терезесіндегі нұсқауларды орындау ұсынылады.

 «!» таңбасы бар сарғылт белгіше ESET өнімі маңызды емес мәселеге назар аударуды қажет ететінін көрсетеді. Ықтимал себептер мыналарды қамтиды:

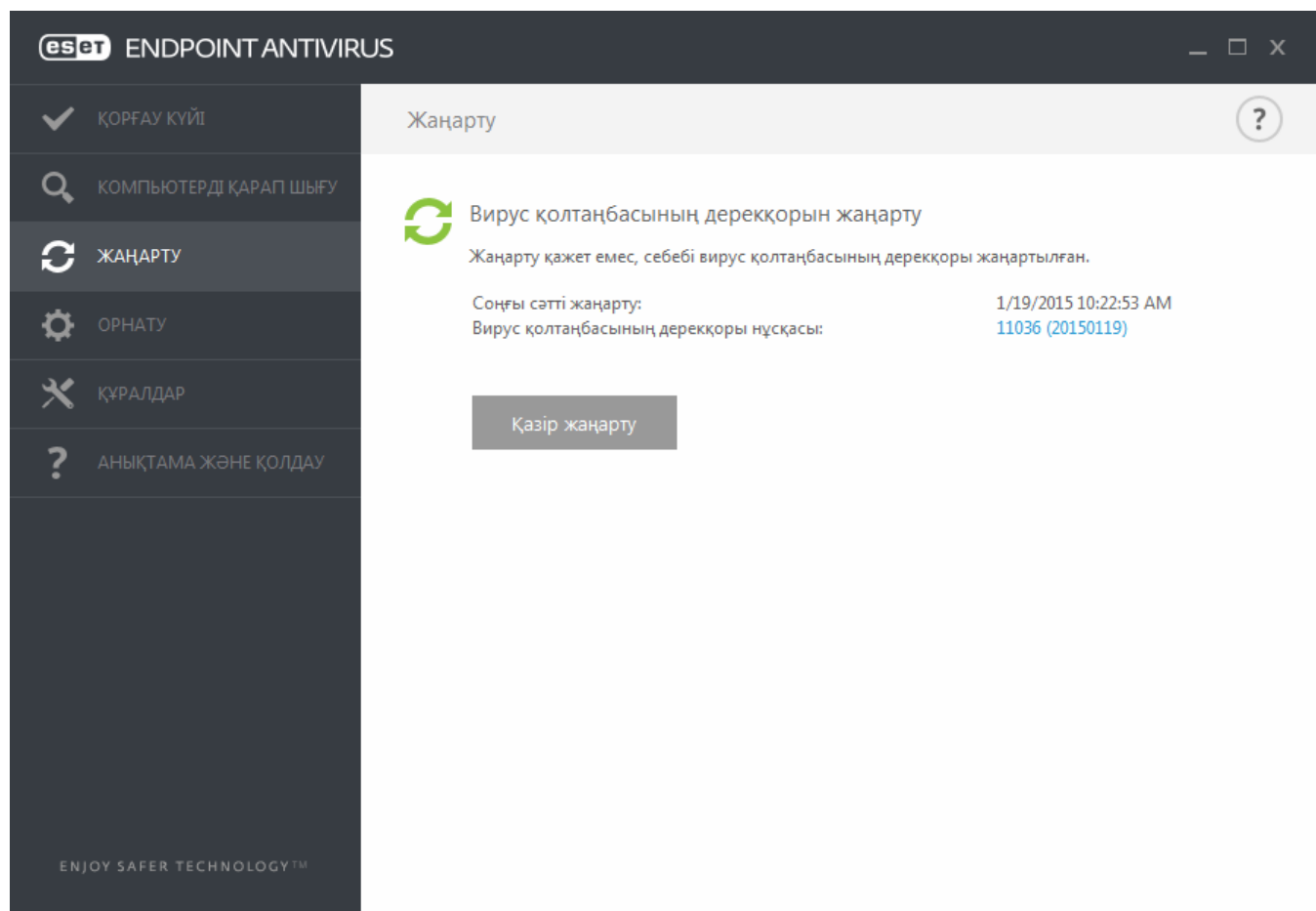
- **Веб-қатынасты қорғау өшірілген** - веб-қатынасты қорғауды қауіпсіздік туралы хабарландыруды басып, содан кейін **Веб-қатынасты қорғауды қосу** тармағын басып арқылы қайта қосуға болады.
- **Лицензияңыздың мерзімі жақында бітеді** - мұны леп белгісі көрсетілген қорғау күйі белгішесі көрсетеді. Лицензияның 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, ESET Тұтынушыларды қолдауды сұрауын жібере аласыз. «ESET» компаниясының тұтынушыларды қолдау бөлімі сұрақтарыңызға тез жауап береді және шешімді табуға көмектеседі.

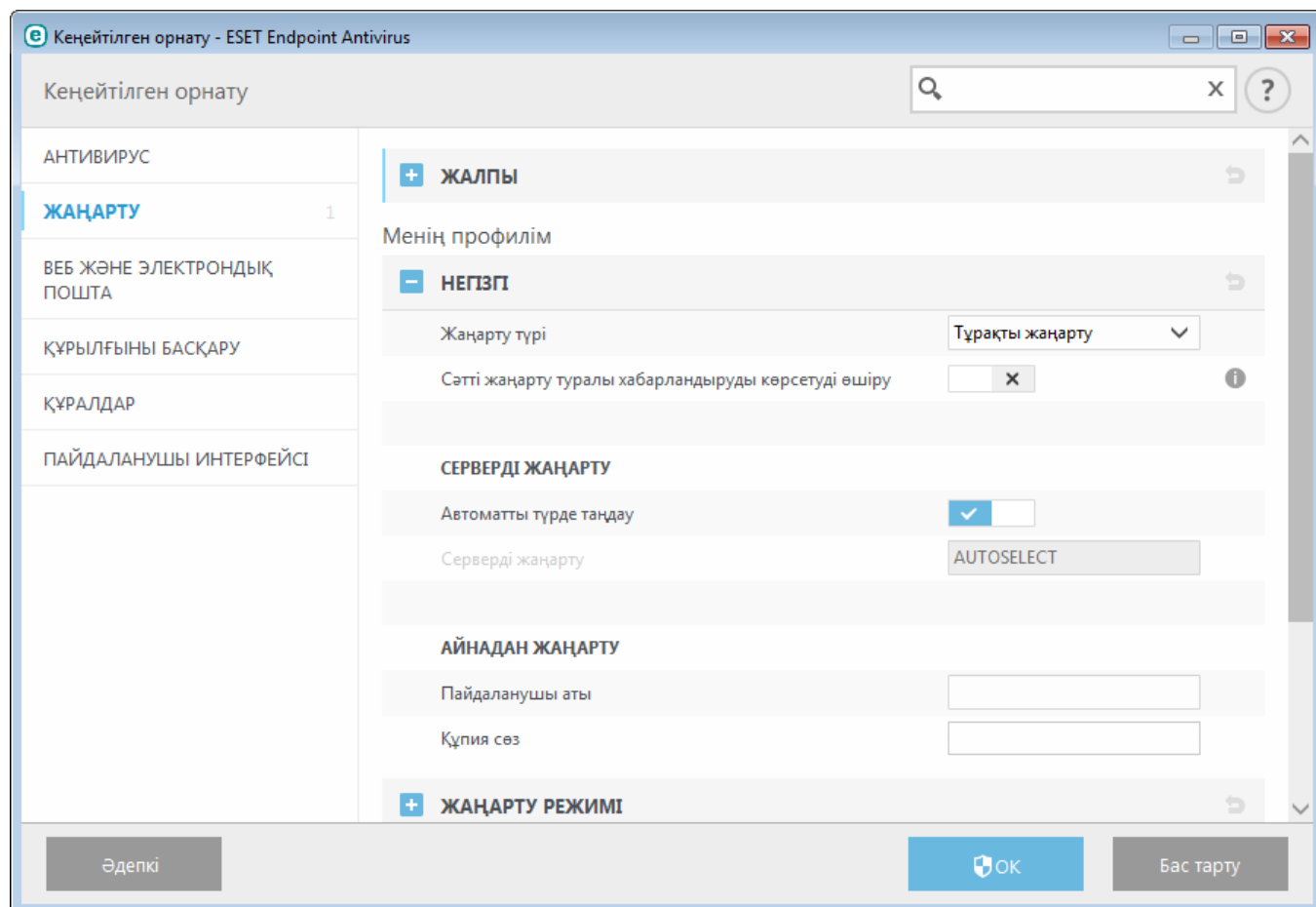
### 3.6.2 Жаңарту параметрлері

Вирус қолтаңбасының дерекқорын және бағдарлама компоненттерін жаңарту зиянкес кодтан толық қорғауды қамтамасыз етудің маңызды бөлігі болып табылады. Оның конфигурациясына және әрекетіне ерекше назар аударыңыз. Жаңарақ дерекқор жаңартуы бар-жоғын тексеру үшін негізгі мәзірде **Жаңарту** > **Қазір жаңарту** тармағын таңдаңыз.

Егер **Лицензия кілті** әлі енгізілмеген болса, жаңа жаңартуларды ала алмайсыз және сізден өнімді белсендіру сұралады.



«Кеңейтілген орнату» терезесі (негізгі мәзірде **Орнату** > **Кеңейтілген орнату** пәрменін басыңыз немесе пернетақтада **F5** пернесін басыңыз) қосымша жаңарту опцияларын қамтиды. Жаңарту режимі, прокси-серверге қатынасу, LAN қосылымдары және вирус қолтаңбасының көшірмелерін жасау сияқты кеңейтілген жаңарту опцияларын конфигурациялау үшін «Кеңейтілген орнату» ағашында **Жаңарту** түймесін басыңыз. Жаңарту кезінде мәселелер кездессе, уақытша жаңарту кәшін тазалау үшін **Тазалау** түймесігін басыңыз. Әдепкі бойынша, **Жаңарту сервері** мәзірі **АВТОТАҢДАУ** опциясына орнатылады. ESET серверін пайдаланғанда **Автоматты түрде таңдау** опциясын таңдалған күйде қалдыру ұсынылады. Экранның төменгі оң жақ бұрышындағы жүйелік тақта хабарландыруының көрсетілуін қаламасаңыз, **Сәтті жаңарту туралы хабарландыруды көрсетуді өшіру** опциясын таңдаңыз.



Оңтайлы жұмыс істеуі үшін бағдарлама автоматты түрде жаңартылып тұруы керек. Бұл **Анықтама және қолдау > Өнімді іске қосу** тармағында дұрыс **Лицензиялық кілт** енгізілген болса ғана мүмкін.

Егер орнатудан кейін **лицензиялық кілтті** енгізбеген болсаңыз, мұны кез келген уақытта істей аласыз. Іске қосу туралы егжей-тегжейлі ақпарат алу үшін [ESET Endpoint Antivirus бағдарламасын іске қосу әдісі](#) бөлімін қараңыз және ESET қауіпсіздік өнімімен бірге алынған лицензия деректерін «Лицензия туралы мәліметтер» терезесіне енгізіңіз.

### 3.7 Жалпы сұрақтар

Бұл тарауда ең жиі қойылатын сұрақтар мен кездесетін мәселелердің кейбірі қамтылған. Мәселенізді шешу жолын табу үшін тақырып атауын басыңыз:

- [ESET Endpoint Antivirus бағдарламасын жаңарту туралы](#)
- [ESET Endpoint Antivirus бағдарламасын белсендіру әдісі](#)
- [Жаңа өнімді іске қосу үшін ағымдағы тіркелгі деректерін пайдалану әдісі](#)
- [Компьютерден вирусты жою жолы](#)
- [Жоспарлағышта жаңа тапсырманы жасау әдісі](#)
- [Қарап шығу тапсырмасын жоспарлау \(24 сағат сайын\)](#)
- [Өнімді ESET Remote Administrator бағдарламасына қосу әдісі](#)
- [Айнаны конфигурациялау әдісі](#)

Егер мәселе жоғарыдағы анықтама беттерінің тізіміне кірмесе, мәселені сипаттайтын кілтсөз немесе сөз тіркесі

бойынша іздеп көріңіз және ESET Endpoint Antivirus анықтама беттерінде іздеп көріңіз.

Егер анықтама беттерінде мәселе/сұрақ шешімі таба алмасаңыз, жалпы сұрақтардың және мәселелердің жауаптары бар [ESET білім қорына](#) кіріңіз.

[Sirefef \(ZeroAccess\) троянын қалай жоюға болады?](#)

[Жаңарту айнасының ақаулықтарын жою бақылау тізімі](#)

[ESET өнімінің толық функцияларына рұқсат ету үшін үшінші тарап брендмауэрының қай мекенжайларын және порттарын ашу керек?](#)

Қажет болса, сұрақтарыңыз немесе мәселелеріңіз жөнінде біздің желідегі техникалық қолдау орталығымызға хабарласуыңызға болады. Онлайн байланысу пішінінің сілтемесін негізгі бағдарлама терезесіндегі **Анықтама және қолдау** тақтасында табуға болады.

### 3.7.1 ESET Endpoint Antivirus жаңарту әдісі


ESET Endpoint Antivirus бағдарламасын қолмен немесе автоматты түрде жаңартуға болады. Жаңартуды іске қосу үшін негізгі мәзірдегі **Жаңарту** бөлімінде **Қазір жаңарту** түймесін басыңыз.

Әдепкі орнату сағат сайын орындалатын автоматты жаңарту тапсырмасын жасайды. Аралығын өзгерту қажет болса, **Құралдар > Жоспарлаушы** тармағына өтіңіз (Жоспарлаушы туралы ақпарат мәлімет үшін [осы жерді](#) басыңыз).

### 3.7.2 ESET Endpoint Antivirus бағдарламасын белсендіру әдісі

Орнату аяқталғаннан кейін өнімді белсендіру сұралады.


Өнімді іске қосудың бірнеше жолы бар. Елге байланысты іске қосу терезесінде іске қосу нақты сценарийі және сол сияқты тарату жолдары (CD/DVD, ESET веб-беті, т.б.) әртүрлі болуы мүмкін.

ESET Endpoint Antivirus көшірмесін тікелей бағдарламадан белсендіру үшін жүйелік тақта белгішесін  басып, мәзірде **Өнім лицензиясын белсендіру** перменін таңдаңыз. Сондай-ақ, өнімді негізгі мәзірде **Анықтама және қолдау > Өнімді белсендіру** немесе **Қорғау күйі > Өнімді белсендіру** тармағында белсендіруге болады.

ESET Endpoint Antivirus бағдарламасын белсендіру үшін келесі әдістердің кез келгенін пайдалануға болады:

- **Лицензия кілті** - лицензия иесін идентификациялау және лицензияны белсендіру үшін пайдаланылатын XXXX-XXXX-XXXX-XXXX пішіміндегі бірегей жол.
- **Қауіпсіздік өкімшісі** - [ESET License Administrator порталында](#) тіркелгі деректерімен (электрондық пошта мекенжайы + құпия сөз) жасалған есептік жазба. Бұл әдіс бір орыннан бірнеше лицензияны басқаруға мүмкіндік береді.
- **Офлайн лицензия** - лицензия туралы ақпаратты беру үшін ESET өніміне тасымалданатын автоматты түрде жасалатын файл. Егер лицензия сізге оффлайн лицензия файлы (.lf) жүктеуге мүмкіндік берсе, сол файлды оффлайн белсендіруді орындау үшін пайдалануға болады. Оффлайн лицензиялардың саны қол жетімді лицензиялардың жалпы санынан шегеріледі. Оффлайн файлды жасау туралы қосымша мәліметтерді алу үшін [ESET License Administrator пайдаланушы нұсқаулығын](#) қараңыз.

Компьютеріңіз басқарылатын желінің мүшесі болса, **Көйінірек белсендіру** түймесін басыңыз, сонда өкімші ESET Remote Administrator арқылы қашықтан белсендіруді орындайды. Сондай-ақ, бұл опцияны осы клиентті кейінірек белсендіру керек болған жағдайда пайдалануға болады.

Өнім лицензиясын негізгі бағдарлама терезесінде **Анықтама және қолдау > Лицензияны басқару** тармағын басып, кез келген уақытта өзгертуге болады. ESET қолдау қызметіне хабарлау керек және лицензияны идентификациялау үшін пайдаланылатын жалпы лицензия идентификаторын көресіз. Компьютер лицензиялау жүйесінде тіркелген пайдаланушы аты **Туралы** бөлімінде сақталады, оны жүйелік тақта белгішесін  тінтуірдің оң жақ түймесімен басу арқылы көруге болады.

**ЕСКЕРТПЕ:** ESET Remote Administrator өкімші қол жетімді еткен лицензияларды пайдаланып клиенттік компьютерлерді тыныш белсендіре алады.



### 3.7.3 Жаңа өнімді іске қосу үшін ағымдағы тіркелгі деректерін пайдалану әдісі

Егер сізде пайдаланушы аты және құпиясөз әлдеқашан бар болса және лицензиялық кілтті алғыңыз келсе, [ESET лицензия өкімшісі порталына](#) кіріңіз, сонда тіркелгі деректерін жаңа лицензиялық кілтке түрлендіре аласыз.

### 3.7.4 Компьютерден вирусты жою жолы

Егер компьютеріңіз зиянды жұқтыру белгілерін 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 **Зерделі қарап шығу** пәрменін басыңыз.
3. Қарап шығу аяқталғаннан кейін журналдан тексерілген, вирус жұққан және тазаланған файлдардың санын қарап шығыңыз.
4. Дисктің белгілі бір бөлігін қарап шығуды қаласаңыз, **Таңдамалы қарап шығу** түймешігін басып, вирустар бар-жоғы тексерілетін нысандарды таңдаңыз.

Қосымша ақпарат алу үшін жаңартылып тұратын [ESET білім қоры мақаласын](#) қараңыз.

### 3.7.5 Жоспарлағышта жаңа тапсырманы жасау әдісі

**Құралдар > Жоспарлағыш** тармағында жаңа тапсырма жасау үшін **Тапсырма қосу** түймесін басыңыз немесе тінтуірдің оң жақ түймесін басып, контексттік мәзірден **Қосу...** пәрменін таңдаңыз. Жоспарланған тапсырмалардың бес түрі бар:

- **Сыртқы бағдарламаларды іске қосу** - Сыртқы бағдарламаның орындалуын жоспарлайды.
- **Журналды реттеу** -Тіркеу файлдарында жойылған жазбалардың қалдықтары да бар. Бұл тапсырма тиімді жұмыс істеу үшін журнал файлдарындағы жазбаларды тұрақты түрде оңтайландырады.
- **Жүйені іске қосу файлы тексеру** - Жүйе іске қосылғанда немесе кіргенде іске қосылуына рұқсат етілген файлдарды тексереді.
- **Компьютер күйінің суретін жасау** - [ESET SysInspector](#) компьютер 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.
- **Бірінші қарап шығу** - әдепкі бойынша, орнатудан кейінгі 20 минут немесе "Шығуды" қайта жүктеу төмен басымдылық тапсырмасы ретінде орындалады.
- **Жаңарту** - вирус қолтаңбасының дерекқорын және бағдарлама модульдерін 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. Тапсырманың атын **Тапсырма аты** өрісіне 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** 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.

### 3.7.6 Қарап шығу тапсырмасын жоспарлау (24 сағат сайын)

Тұрақты тапсырманы жоспарлау үшін бағдарламаның негізгі терезесін ашып, **Құралдар > Жоспарлаушы** түймешігін басыңыз. Төменнен тапсырманы жоспарлау жолдары туралы қысқаша нұсқаулық көруге болады. Ол жергілікті дискілерді 24 сағат сайын қарап шығады.

Қарап шығу тапсырмасын жоспарлау үшін:

1. Жоспарлағыштың негізгі терезесіндегі **Қосу** түймешігін басыңыз.
2. Ашылмалы мәзірде **Шығу** тармағын таңдаңыз.
3. Тапсырма атауын енгізіп, **Қайталау** опциясын таңдаңыз.
4. Тапсырманы 24 сағат сайын іске қосуды таңдаңыз.
5. Жоспарланған тапсырма қандай да бір себеппен орындалмаған жағдайда орындалатын әрекетті 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.

### 3.7.7 ESET Endpoint Antivirus бағдарламасын ESET Remote Administrator бағдарламасына қосу әдісі

ESET Endpoint Antivirus бағдарламасын компьютерде орнатсаңыз және ESET Remote Administrator арқылы қосылғыңыз келсе, клиенттік жұмыс станциясында ERA Agent бағдарламасы да орнатылғанын тексеріңіз. ERA Agent — ERA Server бағдарламасымен байланысатын әр клиенттік шешімнің маңызды бөлігі. ESET Remote Administrator бағдарламасы желіде компьютерлерді іздеу үшін RD Sensor құралын пайдаланады. RD Sensor анықтаған желідегі әр компьютер веб-консоль ішінде көрсетіледі.

Agent жайылғаннан кейін клиенттік компьютерде ESET қауіпсіздік өнімдерін қашықтан орнатуды орындауға болады. Қашықтан орнатудың дәл қадағдары [ESET Remote Administrator пайдаланушы нұсқаулығында](#) сипатталған.

### 3.7.8 Айнаны конфигурациялау әдісі

ESET Endpoint Antivirus бағдарламасын вирус қолтаңбаларының жаңарту файлдарының көшірмелерін сақтауға және жаңартуларды ESET Endpoint Security немесе ESET Endpoint Antivirus орнатылған басқа жұмыс станцияларына таратуға конфигурациялауға болады.

#### Ішкі HTTP сервері арқылы жаңартуларды қамтамасыз ету үшін ESET Endpoint Antivirus айна сервер ретінде конфигурациялау

**F5** пернесін басып, «Кеңейтілген орнату» тармағына кіріп, **Жаңарту > Негізгі** тармағын кеңейтіңіз. **Серверді жаңарту** опциясы **АВТОТАҢДАУ** мәніне орнатылғанын тексеріңіз. **Кеңейтілген орнату > Негізгі > Айна** тармағында **Жаңарту айнасын жасау** және **Ішкі HTTP сервері арқылы жаңарту файлдарын қамтамасыз ету** пәрмендерін таңдаңыз.

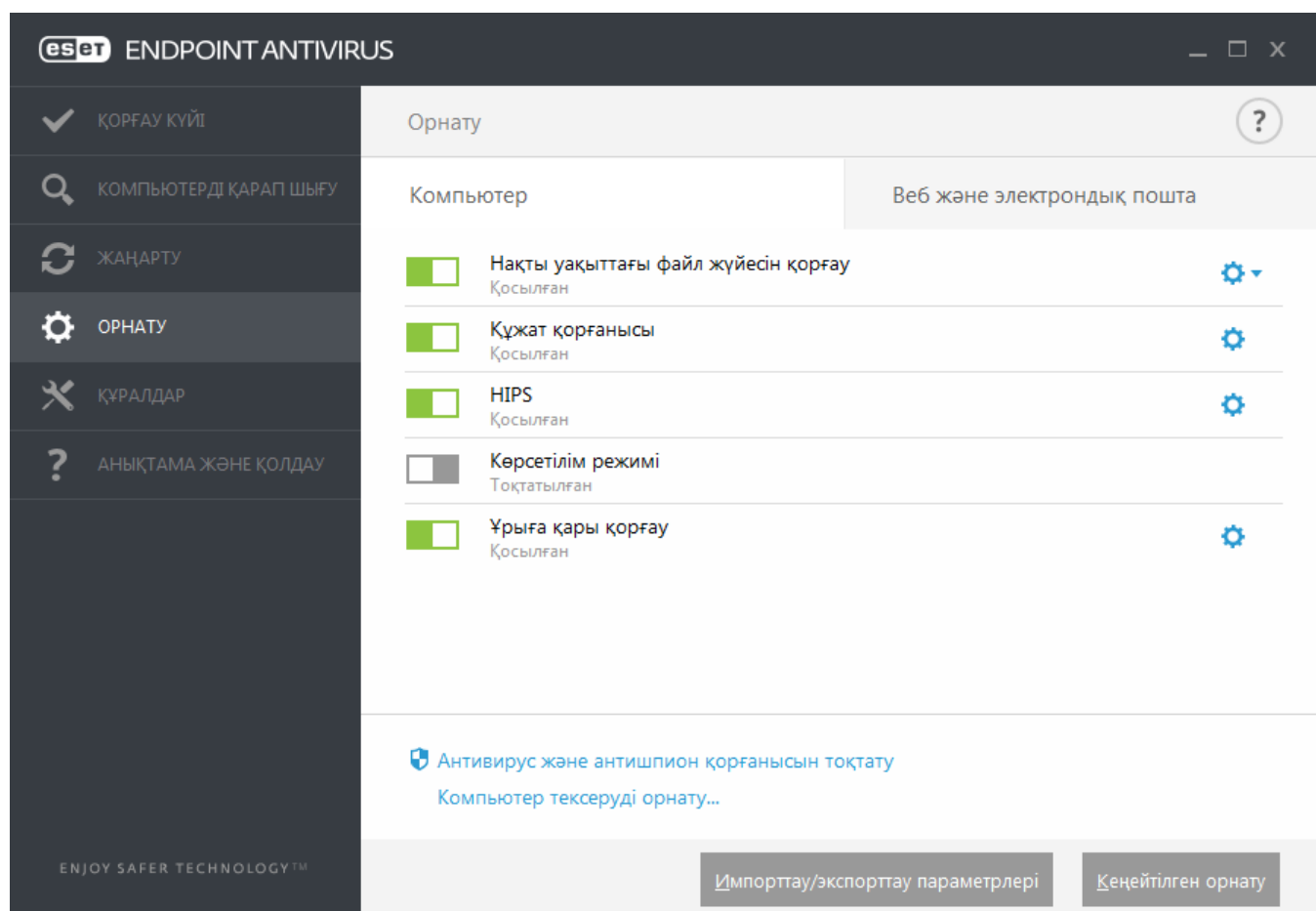
#### Айна серверді ортақ желілік қалта арқылы жаңартуларды қамтамасыз етуге конфигурациялау

Жергілікті немесе желілік құрылғыда ортақ қалта жасаңыз. Бұл қалтаны ESET қауіпсіздік шешімдері орнатылған пайдаланушылар оқи алуы керек және оған жергілікті SYSTEM тіркелгісінен жазу мүмкін болуы керек. **Кеңейтілген орнату > Негізгі > Айна** тармағында **Жаңарту айнасын жасау** параметрін белсендіріңіз. Жасалған ортақ қалтаны шолыңыз және таңдаңыз.

**ЕСКЕРТПЕ:** Ішкі HTTP сервері арқылы жаңартқыңыз келмесе, **Ішкі HTTP сервері арқылы жаңарту файлдарын қамтамасыз ету** параметрінен таңдауды алыңыз.

### 3.8 ESET Endpoint Antivirus бағдарламасымен жұмыс істеу

ESET Endpoint Antivirus бағдарламасының параметрлерінің опциялары компьютер, веб және электрондық пошта қорғау деңгейін реттеуге мүмкіндік береді.



Орнату мәзірінде келесі бөлімдер бар:


- Компьютер
- Веб және электрондық пошта


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

- **Нақты уақыттағы файл жүйесін қорғау** - Барлық файлдарда ашылғанда, жасалғанда немесе компьютерде іске қосылғанда зиянды код бар-жоғы қарап шығылады.
- **Құжат қорғанысы** - Құжатты қорғау мүмкіндігі ашу алдында Microsoft Office құжаттарын, сонымен бірге, Microsoft ActiveX элементтері сияқты Internet Explorer бағдарламасы автоматты түрде жүктеген файлдарды қарап шығады.
- **HIPS** - [HIPS](#) жүйесі операциялық жүйе ішінде орын алатын оқиғаларды бақылайды және теңшелетін ережелер жиынына сай оларға реакция көрсетеді.
- **Көрсетілім режимі** - бағдарламалық жасақтаманы кедергісіз пайдалануды қажет ететін, қалқымалы терезелердің мазалауын қаламайтын және CPU пайдалануды барынша азайтқысы келетін пайдаланушыларға арналған мүмкіндік. [Көрсету режимін](#) қосқаннан кейін сіз ескерту хабарын (ықтимал қауіпсіздік қаупі) аласыз және негізгі терезе қызғылт сары түске боялады.
- **Ұрыға қарсы қорғау** - өздерін операциялық жүйеден жасыра алатын [руткиттер](#) сияқты қауіпті бағдарламаларды анықтауды қамтамасыз етеді. Бұл оларды қарапайым сынақ әдістерін пайдалана отырып, оларды анықтау мүмкін еместігін білдіреді.


**Веб және электрондық пошта қорғау** параметрлері келесі компоненттерді қосуға немесе өшіруге мүмкіндік береді:

- **Вебке кіруді қорғау** - Қосылған болса, HTTP немесе HTTPS арқылы өтетін бүкіл трафикте зиянды бағдарлама бар-жоғын қарап шығады.
- **Электрондық пошта клиентін қорғау** POP3 және IMAP протоколдары бойынша алынатын байланысын бақылайды.
- **Антифишингтік қорғау** - заңды түрде бүркенген заңсыз веб-сайттар арқылы құпия сөздерді, банк деректерін және басқа құпия ақпаратты алу әрекеттерінен қорғайды.

Жекелеген модульдерді уақытша өшіру үшін қажет модуль жанында жасыл қосқышты  басыңыз. Оның компьютер қорғанысын деңгейін төмендететінін ескеріңіз.

Өшірілген қауіпсіздік компонентінің қорғанысын қайта қосу үшін қызыл қосқышты  басып компонентті қосылған күйге қайтарыңыз.

**ЕСКЕРТПЕ:** осылайша өшірілген барлық қорғау шаралары компьютерді қайта іске қосудан кейін қайта қосылады.


Нақты қауіпсіздік компонентінің егжей-тегжейлі параметрлеріне қатынасу үшін кез келген компоненттің жанындағы  тісті дөңгелекті басыңыз.

Орнату терезесінің төменгі жағында қосымша опциялар бар. Орнату параметрлерін *.xml* конфигурация файлы пайдаланып жүктеу немесе ағымдағы орнату параметрлерін конфигурация файлына сақтау үшін **Импорттау/экспорттау параметрлері** опциясын пайдаланыңыз. Егжей-тегжейлі ақпаратты [Импорттау/экспорттау параметрлері](#) бөлімінен қараңыз.

Егжей-тегжейлі опцияларды алу үшін **Кеңейтілген орнату** түймесін немесе **F5** пернесін басыңыз.

### 3.8.1 Компьютер

**Компьютер** модулін **Орнату > Компьютер** тармағында табуға болады. Ол [алдыңғы тарауда](#) сипатталған қорғау модульдеріне шолуды көрсетеді. Бұл бөлімде келесі параметрлер қол жетімді:

**Нақты уақытта файлдық жүйені қорғау** жанындағы тісті дөңгелекті басып , файлдарды және қалталарды қарап шығудан шығаруға мүмкіндік беретін [Ерекшелік](#) орнату терезесін ашу үшін **Ерекш өліктерді өңдеу** түймесін басыңыз.

**ЕСКЕРТПЕ:** құжатты қорғау күйі **Кеңейтілген орнату (F5) > Антивирус > Құжатты қорғау** тармағында қосқанша қол жетімді болмауы мүмкін. Оны қосқаннан кейін «Орнату» тақтасы > «Компьютер» тармағында «Құрылғыларды басқару» астында **Қайта іске қосу** түймесін басу арқылы компьютерді қайта іске қосу керек немесе мұны «Қорғау күйі» тақтасында **Компьютерді қайта іске қосу** түймесін басу арқылы істеуге болады.

**Антивирустық және антишпиондық қорғауды кідірту** - Антивирустық және антишпиондық қорғауды уақытша өшірген кез келген уақытта ашылмалы мәзірді пайдаланып таңдалған компонент өшірулі болуы керек уақыт аралығын таңдап, содан кейін қауіпсіздік компонентін өшіру үшін **Қолдану** түймесін басуға болады. Қорғауды қайта қосу үшін **Антивирустық және антишпиондық қорғауды қосу** түймесін басыңыз.

**Шығу параметрлері...** - компьютерді қарап шығу (қолмен орындалатын қарап шығу) параметрлерін реттеу үшін басыңыз.

#### 3.8.1.1 Антивирус

Антивирус және антишпион қорғанысы файлдарды, электрондық поштаны және интернет байланысын бақылау арқылы зиянды жүйелік шабуылдардан қорғайды. Егер қауіп анықталса, Антивирус модулі оны алдымен блоктау арқылы, ал содан кейін тазалау, жою немесе карантинге жылжыту арқылы жоя алады.

Антивирус модулінің параметрлерін егжей-тегжейлі конфигурациялау үшін **Кеңейтілген орнату** пәрменін немесе **F5** пернесін басыңыз.

Барлық қорғаныс модульдеріне арналған қарап шығу құралының параметрлері (мысалы, Нақты уақыттағы файлдық жүйені қорғау, Веб-қатынасты қорғау,...) мыналардың анықталуын қосуға не өшіруге 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

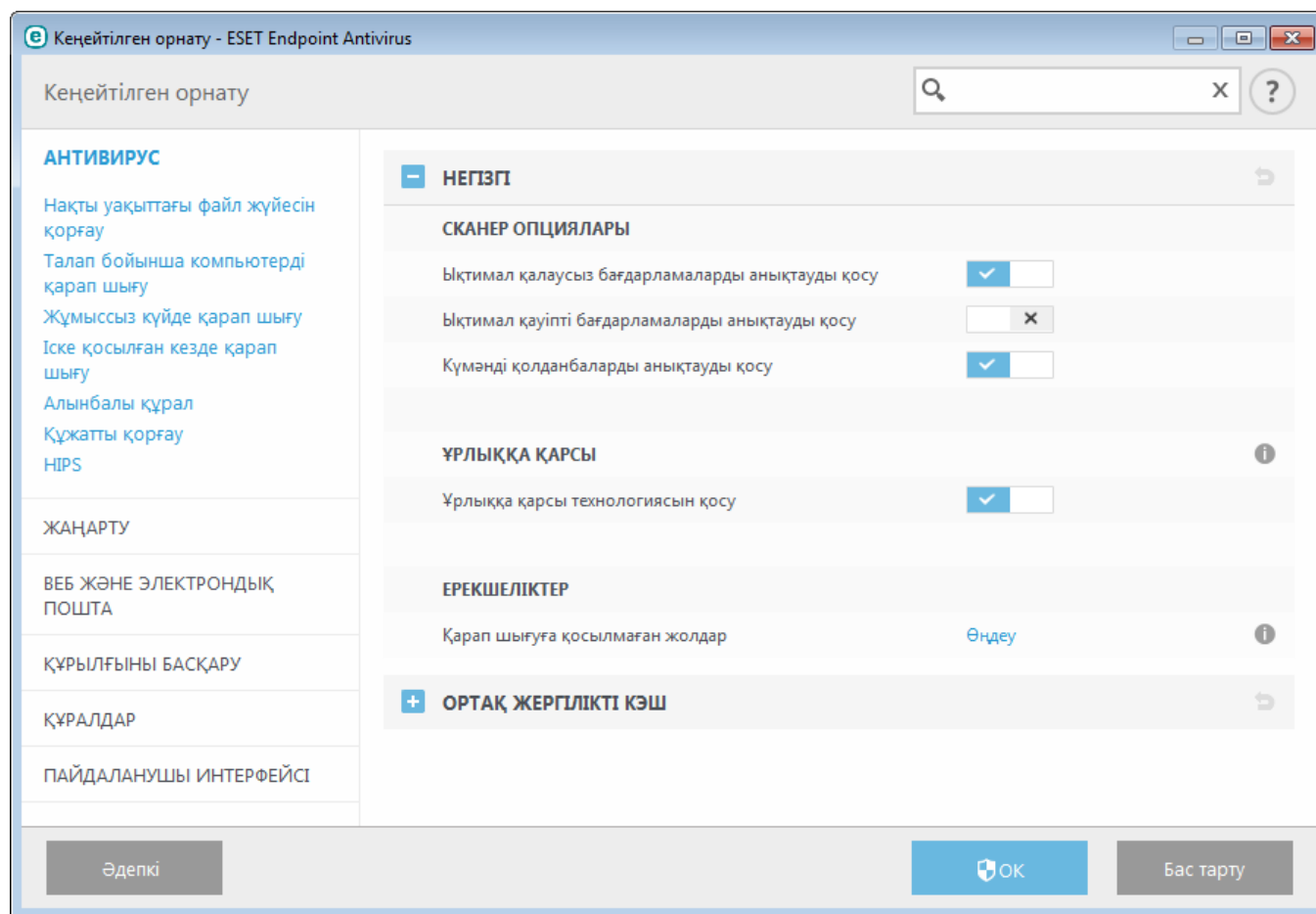
бағдарламалар және пернетақталық шпиондарды (пайдаланушы басқан әрбір пернені жазып отыратын бағдарламалар) сияқты бағдарламалар кіреді. Бұл опция әдепкі мәні бойынша өшірілген.

[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.

**Ерекш өліктер** 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.



### 3.8.1.1.1 Инфильтрация анықталды

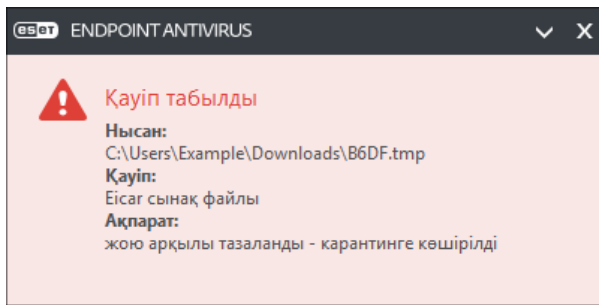
Инфильтрацияларға жүйеге әр түрлі ену нүктелерінен, мысалы, веб-беттерден, ортақ қалталардан, электрондық пошта арқылы немесе алынбалы құрылғыларынан (USB, сыртқы дискілер, ықшам дискілер, DVD дискілері, дискеталар, т.б.) қол жеткізуге болады.

#### Стандартты тәртіп

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

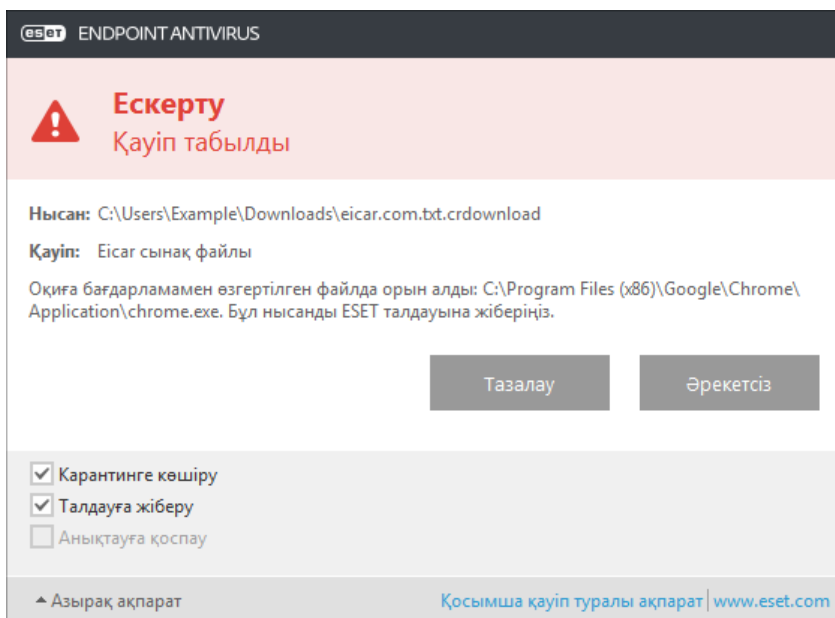
- Нақты уақыттағы файл жүйесін қорғау
- Вебке кіруді қорғау
- Электрондық пошта клиентін қорғау
- Талап бойынша компьютерді қарап шығу

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.

## 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 Endpoint Antivirus бағдарламасын ашып, «Шығу» басыңыз
- **Зөрдәлі қарап шығу** тармағын басыңыз (қосымша ақпарат алу үшін [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.

### 3.8.1.2 Ортақ жергілікті кэш

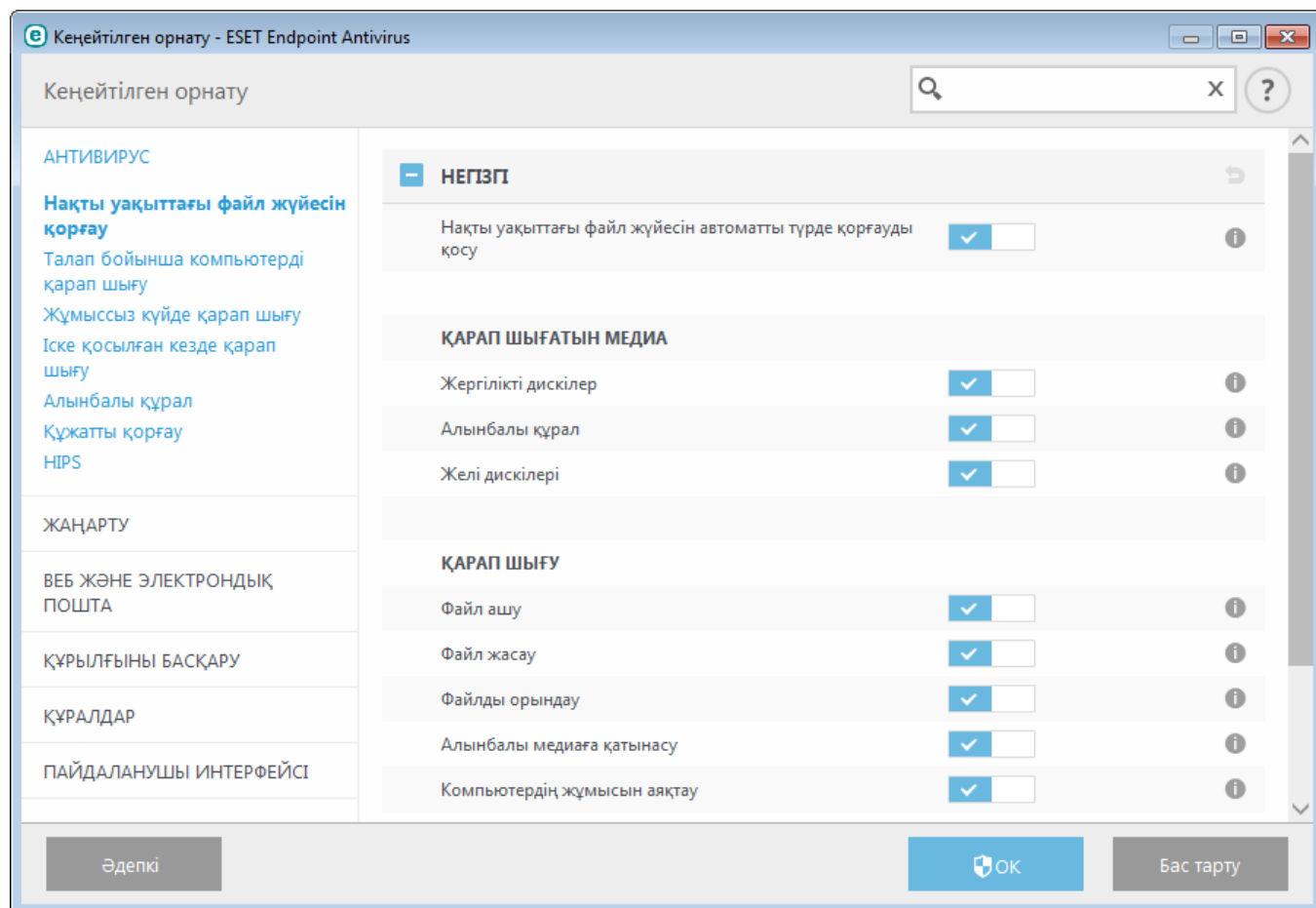
Ортақ жергілікті кэш желіде қайталап қарап шығуды жою арқылы виртуалды орталарда өнімділікті күшейтеді. Бұл әр файлдың тек бір рет қарап шығылуын және ортақ кэште сақталуын қамтамасыз етеді. Желідегі файлдарды және қалталарды қарап шығулар туралы ақпаратты жергілікті кэшке сақтау үшін **Кэш төу опциясы** қосқышын қосыңыз. Егер жаңа қарап шығуды орындасаңыз, ESET Endpoint Antivirus кэште қарап шығылған файлдарды іздейді. Егер әйкес болса, файлдар қарап шығудан шығарылады.

**Кэш сервөрі** параметрлерді мыналарды қамтиды:

- **Хост атауы** - кэш орналасқан компьютердің атауы немесе IP мекенжайы.
- **Порт** - байланыс үшін пайдаланылатын порттың нөмірі («Ортақ жергілікті кэш» ішінде орнатылғанмен бірдей).
- **Құпия сөз** - қажет болса, ESET ортақ жергілікті кэшінің құпия сөзін көрсетіңіз.

### 3.8.1.3 Нақты уақыттағы файл жүйесін 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 **Keңейтілген орнатуда, Нақты уақытта файлдық жүйені қорғау**

> **Нөгізгі 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 бақылайды.

**Алынбалы құрал** - ықшам дискілер/DVD дискілер, USB сақтау құрылғысы, Bluetooth құрылғылары, т.б.

**Жөлі дискілері** - Барлық көрсетілген 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 ашу** - Ашылған файлдарды қарап шығуды қосады не өшіреді.
- **Файл жасау** - файлдар жасалғанда қарап шығуды қосады не өшіреді.
- **Файлды орындау** - файлдар орындалғанда қарап шығуды қосады не өшіреді.
- **Алынбалы медиаға қатынасу** - Сақтау орны бар белгілі бір алынбалы құралға кіру арқылы іске қосылатын қарап шығуды қосады немесе өшіреді.
- **Компьютердің жұмысын аяқтау** - Компьютерді өшіру арқылы басталған 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). Файлдар әр вирус қолтаңбасының дерекқорын жаңартудан кейін бірден 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.

#### 3.8.1.3.1 Қосымша ThreatSense параметрлері

**Жаңадан жасалған, өзг-ген файл-ға арн. қосымша ThreatSense параметрлері** - Жаңадан жасалған немесе өзгертілген файлдардың вирус жұқтыру ықтималдылығы бар файлдарға қарағанда жоғарырақ болады. Осы себепті бағдарлама бұл файлдарды қосымша қарап шығу параметрлерімен тексереді. Жалпы сигнатураға негізделген қарап шығу әдістерімен бірге вирус сигнатурасының дерекқор жаңартуы шықпас бұрын жаңа қауіптерді анықтай алатын кеңейтілген эвристика қолданылады. Жаңадан жасалған файлдарға қоса, қарап шығу, сонымен бірге, өздігінен ашылатын файлдарда (.sfx) және бумалаушының жұмыс уақыты файлдарында (іштей сығылған орындалатын файлдар) орындалады. Әдепкі мәні бойынша, мұрағаттарды 10-шы енгізу деңгейіне дейін қарап шығып, олар іс жүзіндегі өлшеміне қарамастан тексеріледі. Мұрағатты қарап шығу параметрлерін өзгерту үшін **Әдепкі мұрағатты қарап шығу параметрлері** опциясын өшіріңіз.

**Орындалу уақытының бумалаушылары, Өздігінен ашылатын мұрағаттар және Кеңейтілген эвристика** туралы қосымша мәліметтер алу үшін [ThreatSense механизмінің параметрлерін орнату](#) бөлімін қараңыз.

**Орындалатын файлдардың қосымша ThreatSense параметрлері** - Әдепкі бойынша, [Кеңейтілген эвристика](#) файлдар орындалғанда пайдаланылады. Қосылған болса, жүйе өнімділігіне әсерді азайту үшін [Зерделі оңтайландыру](#) опциясын және ESET Live Grid қосылған күйде сақтау ұсынылады.



### 3.8.1.3.2 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 (Стандартты 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.

### 3.8.1.3.3 Нақты уақыттағы қорғауды тексеру

Нақты уақыттағы қорғаудың жұмыс істеп жатқанын және вирустарды анықтағанын тексеру үшін eicar.com торабынан алынған тексеру файлы 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

### 3.8.1.3.4 Нақты уақыттағы қорғау конфигурациясын қашан өзгерту керек

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

ESET Endpoint 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**).

### 3.8.1.3.5 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 **Орнату** тармағына барып, негізгі бағдарлама терезесінің **Нақты уақыттағы файл жүйесін қорғау** бөлімін басыңыз.

Егер нақты уақыттағы қорғаныс жүйені іске қосуда басталмаса, бұл әдетте **Нақты уақыттағы файл жүйесін қорғауды автоматты түрде іске қосу** опциясын өшірмегендіктен болады. Бұл опцияны қосу үшін **Кеңейтілген орнату (F5)** тармағына өтіп, **Антивирус > Нақты уақыттағы файл жүйесін қорғау > Негізгі** тармағын басыңыз. **Нақты уақытта файлдық жүйені қорғауды автоматты түрде іске қосу** қосқышы қосұлы екенін тексеріңіз.

#### Егер нақты уақыттағы қорғау инфильтрацияларды таппаса және тазаламаса

Компьютерде басқа антивирустық бағдарламалардың орнатылмағанына көз жеткізіңіз. Егер бір уақытта екі нақты уақыттағы қорғау құралдары қосылса, олардың 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.

### 3.8.1.4 Талап бойынша компьютерді қарап шығу

Талап бойынша қарап шығу құралы ESET Endpoint Antivirus бағдарламасының маңызды бөлігі болып табылады. Ол компьютеріңіздегі файлдар мен қалталарды қарап шығу үшін пайдаланылады. Қауіпсіздік тұрғысынан, компьютерді қарап шығу вирус жұқты деген күдік болғанда ғана емес, сонымен қатар әдеттегі қауіпсіздік шараларының бөлігі ретінде тұрақты орындалғаны өте маңызды. [Нақты уақытта файлдық жүйені қорғау](#) анықтамаған вирустарды анықтау үшін жүйелі түрде (мысалы, айына бір рет) жүйені терең қарап шығуларды орындау 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. **Зерделі қарап шығу** қарап шығу параметрлерін одан әрі қарап шығу қажеттілігіңіз жүйені тез қарап шығады. **Таңдамалы қарап шығу** кез келген алдын ала анықталған қарап шығу профилдерін таңдауға және нақты қарап шығу нысандарын таңдауға мүмкіндік береді.

Қарап шығу процесі туралы қосымша ақпарат алу үшін [Қарап шығудың орындалуы](#) тармағын қараңыз.

#### Зерделі қарап шығу

Зерделі қарап шығу компьютерді қарап шығуды тез қосуға және пайдаланушы араласуынсыз вирус жұққан файлдарды тазалауға мүмкіндік береді. Зерделі қарап шығу артықшылығы – онымен жұмыс істеудің жеңілдігі және оның егжей-тегжейлі қарап шығу конфигурациясын қажет етпейтіні. Зерделі 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.

#### Таңдамалы қарап шығу

Қарап шығу нысандары және қарап шығу әдістері сияқты қарап шығу параметрлерін көрсеткіңіз келгенде, таңдамалы қарап шығу оңтайлы шешім болып табылады. Таңдамалы қарап шығудың артықшылығы – параметрлерді егжей-тегжейлі конфигурациялау мүмкіндігі. Конфигурацияларды пайдаланушылық қарап шығу профилдеріне сақтауға болады және олар қарап шығу бірдей параметрлермен қайта-қайта орындалса пайдалы.

Нысандарды таңдау үшін **Компьютерді қарап шығу > Таңдамалы қарап шығу** тармағына өтіп, **Қарап шығу нысандары** ашылмалы мәзірінен опцияны таңдаңыз немесе ағаш құрылымынан нақты нысандарды таңдаңыз. Қарап шығу нысанын, сондай-ақ, қалтаға немесе құрамына қосқыңыз келетін файл(дар)ға жол енгізу арқылы да көрсетуге болады. Егер қосымша тазалау әрекеттеріңіз тек жүйені қарап шығу керек болса, **Тазаламай қарап шығу** опциясын таңдаңыз. Қарап шығуды орындау кезінде **Орнату... > ThreatSense parameters > Cleaning >** тармағын басу арқылы үш тазалау деңгейінен таңдауға болады.

Таңдамалы қарап шығу арқылы компьютерді қарап шығуды орындау антивирустық бағдарламаларды пайдалануда тәжірибесі бар озық пайдаланушылар үшін ыңғайлы.

#### Алынбалы құралды қарап шығу

Зерделі 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.

Сондай-ақ, қарап шығудың осы түрін **Таңдамалы қарап шығу**, содан кейін **Қарап шығу нысандары** ашылмалы мәзірінен **Алынбалы құрал** параметрін таңдап, **Қарап шығу** түймесін басу арқылы іске қосуға болады.

**Қарап шығудан кейінгі әрекет** ашылмалы мәзірін қарап шығудан кейін орындалатын әрекетті («Әрекет жоқ», «Өшіру», «Қайта жүктеу» және «Гибернация») әрекетті таңдау үшін пайдалануға болады.

**Қарап шығудан кейін өшіруді қосу** - Талап бойынша компьютерді қарап шығу аяқталғанда жоспарланған өшіруді қосады. Өшіруді растау диалогтық терезесінде 60 секундтық кері санақ көрсетіледі. Сұралған өшіруді тоқтату үшін **Бас тарту** түймесін басыңыз.

**ЕСКЕРТПЕ:** Шығуды кемінде айына бір рет орындау ұсынылады. Қарап шығуды **Құралдар > Жоспарлағыш**

тармағында [жоспарланған тапсырма](#) ретінде конфигурациялауға болады.

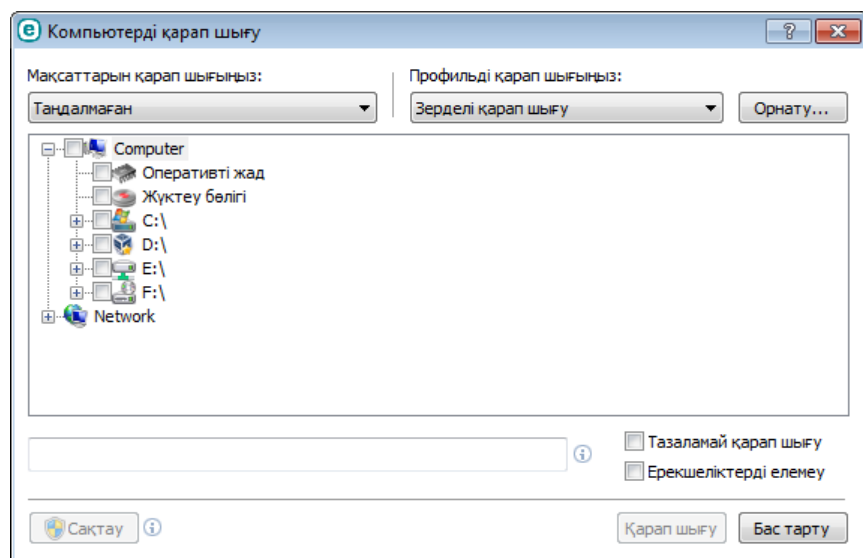
### 3.8.1.4.1 Таңдаулы ретпен қарап шығуды іске қосушы

Егер тек белгілі бір нысанды ғана қарап шыққыңыз келсе, **Компьютерді қарап шығу > Таңдаулы ретпен қарап шығу** тармағын басып, **Қарап шығу нысандары** ашылмалы мәзірінен опцияны таңдау немесе ағаш құрылымынан белгілі бір нысандарды таңдау арқылы Таңдаулы ретпен қарап шығу құралын пайдалануыңызға болады.

Қарап шығу нысандары терезесі қай нысандарда (жад, дискілер, секторлар, файлдар және қалталар) инфильтрациялар бар-жоғы қарап шығылатынын анықтауға мүмкіндік береді. Компьютерде қол жетімді барлық құрылғылар тізілген тармақ құрылымында нысандарды таңдаңыз. **Қарап шығу нысандары** ашылмалы мәзірі алдын ала анықталған қарап шығу нысандарын таңдауға мүмкіндік береді.

- **Профиль параметрлері бойынша** - Таңдалған қарап шығу профилінде орнатылған 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 нысанын жылдам шарлау немесе қажетті нысанды (қалта немесе файл(дар)) тікелей қосу үшін оны қалталар тізімінің төменгі жағындағы бос өріске енгізіңіз. Бұл тармақ құрылымы ешбір нысандар таңдалмаған және **Қарап шығу нысандары** мәзірі **Таңдау жоқ** деп орнатылған болса ғана мүмкін.



Вирус жұққан элементтер автоматты түрде тазаланбайды. Тазаламай қарап шығуды ағымдағы қорғау күйі туралы шолуды алу үшін пайдалануға болады. Егер қосымша тазалау әрекеттерінсіз тек жүйені қарап шығу керек болса, **Тазаламай қарап шығу** опциясын таңдаңыз. Бұған қоса, үш тазалау деңгейлері ішінен **Орнату... > ThreatSense параметрлері > Тазалау** тармағын басу арқылы таңдауға болады. Қарап шығу туралы ақпарат қарап шығу журналына сақталады.

Қарап шығуға таңдалған нысандар үшін пайдаланылатын **Қарап шығу профилі** ашылмалы мәзірінен профиль 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 профилдері бар. Бұл қарап шығу профилдері әр түрлі [ThreatSense механизм параметрлерін](#) пайдаланады. Қарап шығу профилі мәзірінен таңдалған қарап шығу профилін егжейлі-тегжейлі түрде орнату үшін **Орнату...** түймесін басыңыз. Қол жетімді опциялар [ThreatSense механизмінің параметрлерін реттеу](#) бөлімінде **Басқа** тармағында сипатталған.

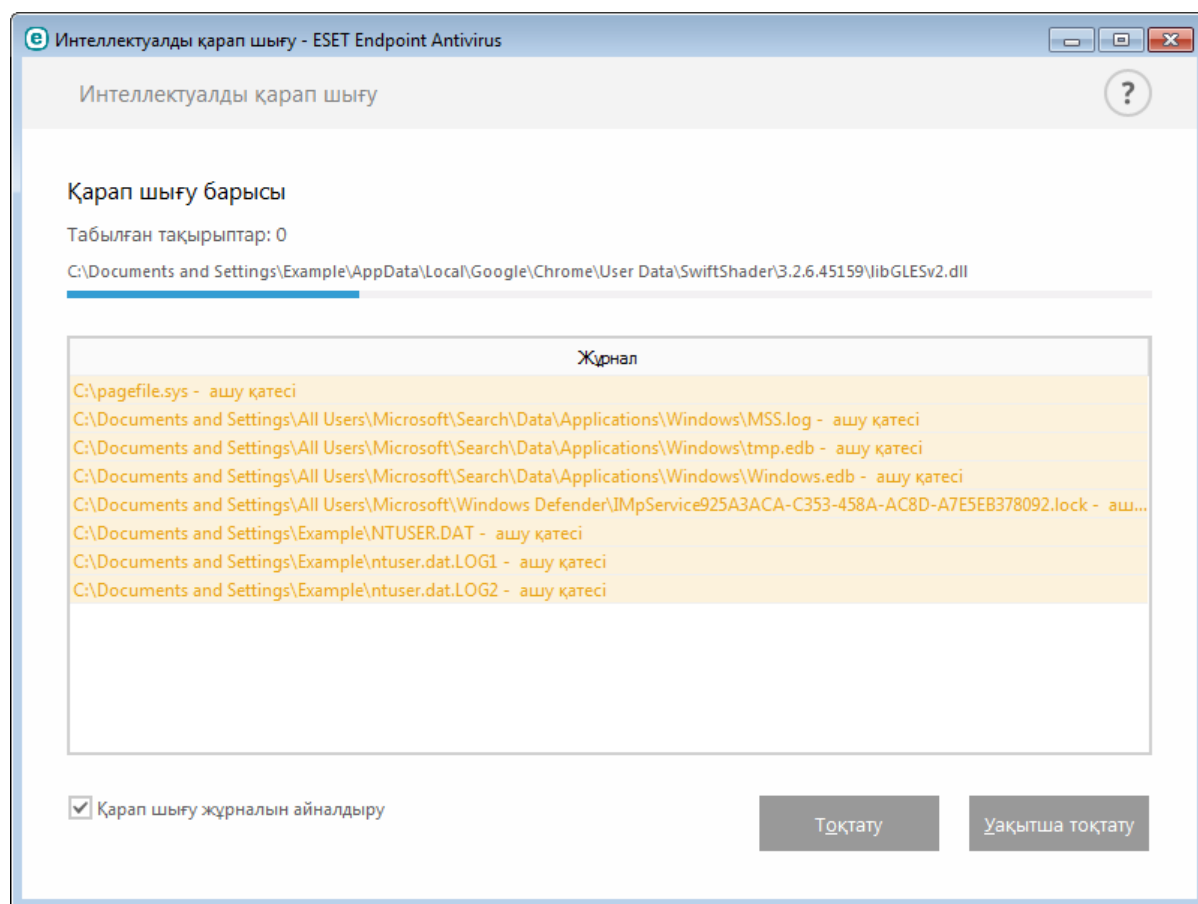
Таңдалған нысандарға, соның ішінде қалталардың ағаш құрылымындағы таңдалған нысандарға енгізілген өзгертулерді сақтау үшін **Сақтау** түймесін басыңыз.

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 тиісті файлдарға кіруі үшін артықшылықтары болмаса, осыны таңдаңыз. Бұл түйме ағымдағы пайдаланушы UAC әрекеттеріне Әкімші ретінде қоңырау шала алмайтын кезде қол жетімді болмайтынын ескеріңіз.

### 3.8.1.4.2 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 журнал 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.

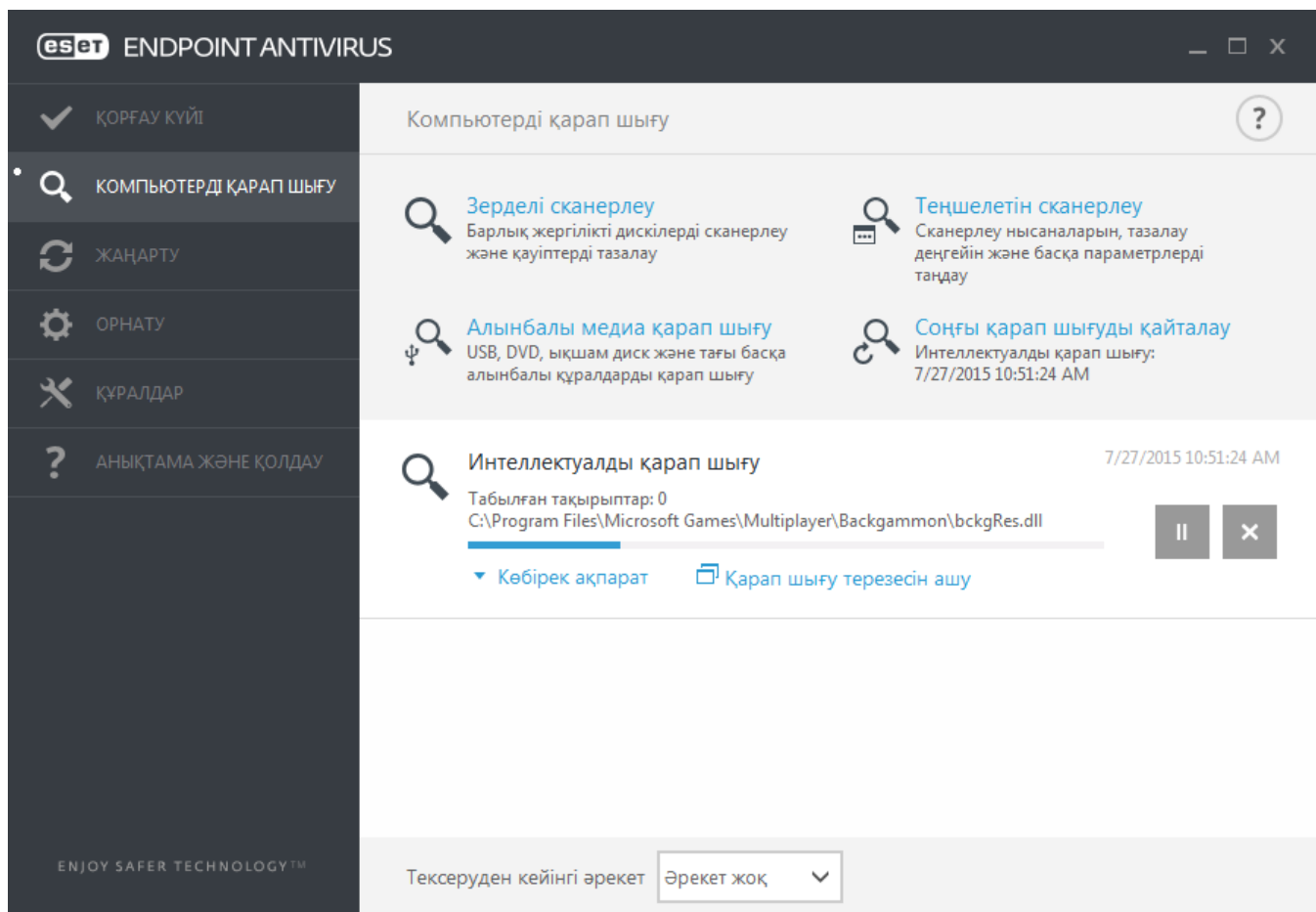
**Қауіптердің саны** - қарап шығу кезінде табылған қауіптердің жалпы санын көрсетеді.

**Кідірту** - қарап шығуды кідіртеді.

**Жалғастыру** - бұл опция қарап шығудың орындалуы кідірілгенде көрсетіледі. Қарап шығуды жалғастыру үшін «Жалғастыру» түймесін басыңыз.

**Тоқтату** - қарап шығуды тоқтатады.

**Қарап шығу журналын айналдыру** - қосылған болса, жаңа жазбалар қосылғанда қарап шығу журналы автоматты түрде төмен айналады, осылайша ең соңғы жазбалар көрсетіледі.



### 3.8.1.5 Құрылғыны басқару

ESET Endpoint Antivirus автоматты құрылғы (CD/DVD/USB/...) басқару элементімен қамтамасыз етеді. Бұл модуль кеңейтілген сүзгілерді/рұқсаттарды қарап шығуға, блоктауға немесе реттеуге және пайдаланушының осы құрылғыға кіру және 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
- Барлық құрылғы түрлері

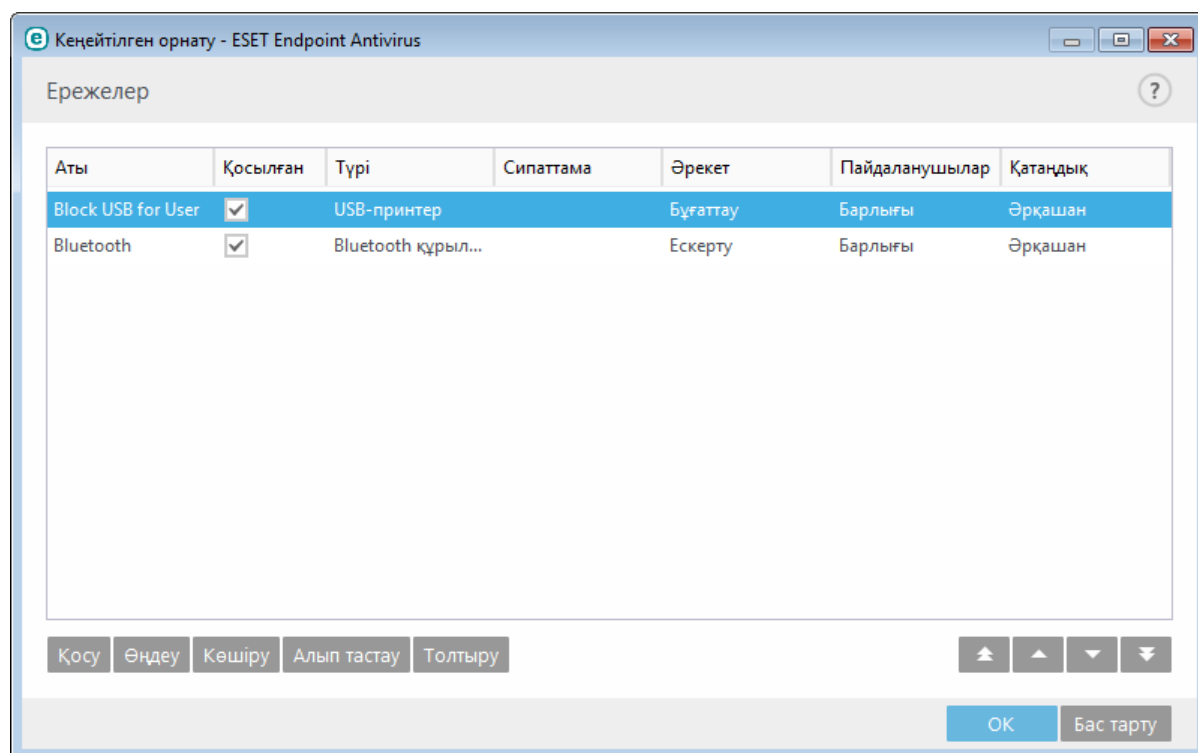
«Құрылғы басқаруды орнату» опцияларын **Кеңейтілген орнату (F5) > Құрылғыны басқару** тармағында өзгертуге болады.

**Жүйеге біріктіру** жанындағы қосқышты қосу ESET Endpoint 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.

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

### 3.8.1.5.1 Құрылғы басқару ережелерін өңдеуші

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



Белгілі бір құрылғыларға пайдаланушы, пайдаланушылар тобы тарапынан немесе ереже конфигурациясында көрсетілуі мүмкін бірнеше қосымша параметрдің кез келгені 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. Болашақта пайдаланғыңыз келгенше өшіру үшін ереже жанындағы **Қосылған** құсбелгісін алыңыз. Бір немесе бірнеше ережені таңдаңыз және ережелерді біржола жою үшін **Жою** түймесін басыңыз.

**Көшіру** - басқа таңдалған ереже үшін пайдаланылатын алдын ала анықталған опциялары бар жаңа ережені жасайды.

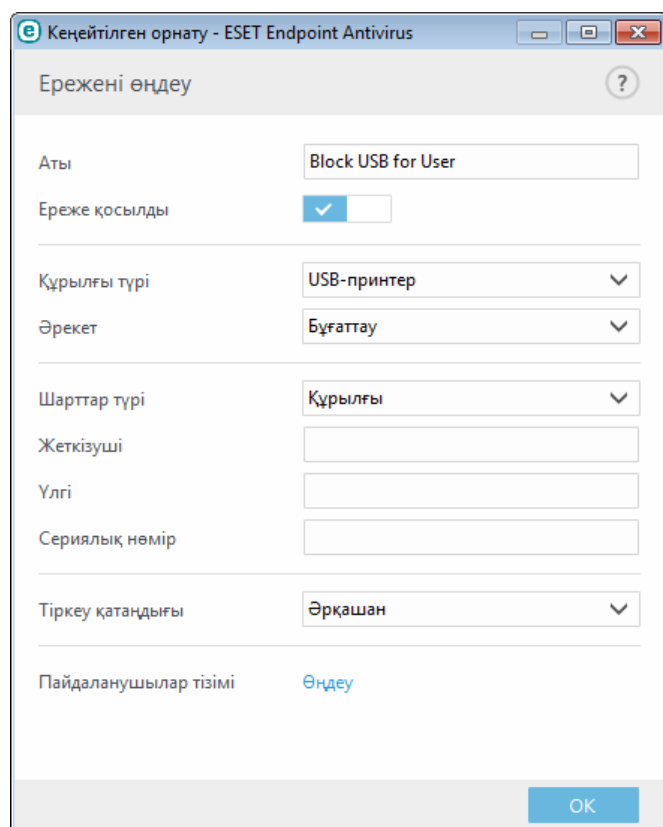
Компьютерге қосылған құрылғылар үшін алынбалы медиа құрылғы параметрлерін автоматты толтыру үшін **Толтыру** түймесін басыңыз.

Ережелер басымдық ретімен тізіледі, басымдығы жоғарырақ ережелер жоғарғы жаққа жақынырақ болады. Ережелерді **Жоғарғы/Жоғары/Төмен/Төменгі** пернелерін басу арқылы жылжытуға болады және жеке-жеке немесе топтар түрінде жылжытуға болады.

Құрылғыны басқару журналы құрылғыны басқару іске қосылған барлық жағдайларды жазады. Журнал жазбаларын ESET Endpoint Antivirus негізгі бағдарлама терезесінде **Құралдар > Журнал файлдары** тармағында көруге болады.

### 3.8.1.5.2 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 керісінше, сақтау құрылғыларының ережелері төмендегі құқықтар параметрлерінің біреуін таңдауға мүмкіндік береді:

- **Оқу/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).

**Ш арттар 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** - Құрылғыға берілген атау.
- **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.

**ЕҢЕС:** құрылғы туралы ақпаратты көру үшін сол құрылғы түрі үшін ережені жасаңыз, құрылғыны компьютерге қосыңыз, содан кейін [Құрылғыны басқару журналы](#) бөлімінде құрылғы мәліметтерін тексеріңіз.

### Қатаңдық

- **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 **Пайдалануш ылар тізімі** ішіне белгілі бір пайдаланушыларды немесе пайдаланушылар тобын қосылу арқылы шектеледі:

- **Қосу** - Келесіні ашады: **Нысан түрлері: Пайдалануш ылар немесе топтар** қалаған пайдаланушыларды таңдауға мүмкіндік беретін диалогтық терезені ашады.
- **Алып тастау** - Таңдалған пайдаланушыны сүзгіден алып тастайды.

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

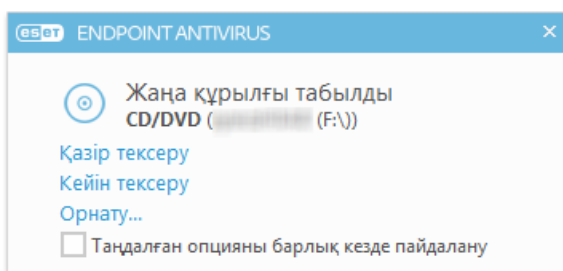
### 3.8.1.6 Алынбалы құрал

ESET Endpoint 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 құралды 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 Endpoint 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.

### 3.8.1.7 Жұмыссыз күйде қарап шығу

Жұмыссыз күйде қарап шығу құралын **Кеңейтілген орнату > Антивирус > Жұмыссыз күйде қарап шығу > Негізгі**. Бұл мүмкіндікті қосу үшін **Жұмыссыз күйде қарап шығуды қосу** жанындағы қосқышты **Қосулы** күйіне орнатыңыз. Компьютер жұмыссыз күйде болған кезде үнсіз компьютерді қарап шығу барлық жергілікті дискілерде орындалады. Өнімділік күйіндегі сканерді шақыру мақсатында орындалу қажет шарттардың толық тізімін алу үшін [Өнімділік күйінде анықтау триггерлері](#) бөлімін қараңыз.

Әдепкі бойынша, компьютер (ноутбук) батарея қуатымен жұмыс істеген кезде өнімділік күйіндегі сканер іске қосылмайды. «Кеңейтілген орнату» ішіндегі **Компьютер батареямен жұмыс істеген кезде де іске қосу** құсбелгісін қою арқылы осы параметрді қайта анықтауға болады.

«Кеңейтілген орнату» ішіндегі **Журналға тіркеуді қосу** қосқышын компьютерді қарап шығу шығысын [Журнал файлдары](#) бөлімінде жазу үшін қосыңыз (бағдарламаның негізгі терезесінде **Құралдар > Журнал файлдары** тармағын басып, **Журнал** ашылмалы мәзірінде **Компьютерді қарап шығу** пәрменін таңдаңыз).

Жұмыссыз күйді анықтау компьютер келесі күйлерде болғанда іске қосылады:

- Экрандық сақтағыш
- Компьютерді құлыптау
- Пайдаланушының жүйеден шығуы

Жұмыссыз күйде қарап шығу құралы үшін қарап шығу параметрлерін (мысалы, анықтау әдістері) өзгерту үшін [ThreatSense механизмінің параметрлерін реттеу](#) түймесін басыңыз.

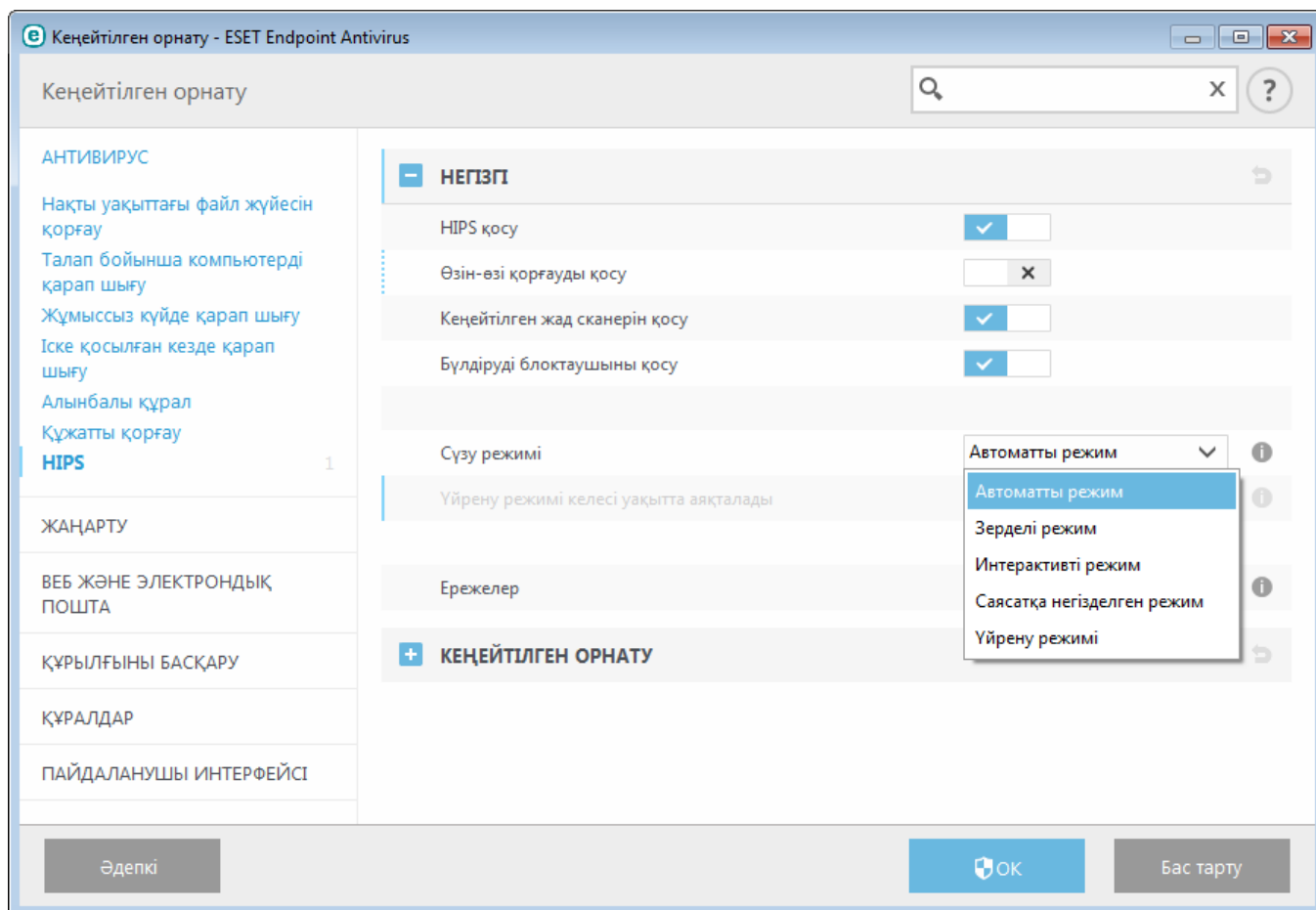
### 3.8.1.8 Басты компьютерге басып кіруді болдырмау жүйесі (HIPS)



HIPS параметрлеріне 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 Endpoint Antivirus негізгі бағдарлама терезесінде, **Орнату > Компьютер** тармағында көрсетіледі.



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

**Keңейтілген 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. Keңейтілген жад сканері әдепкі бойынша қосылған. [Глоссарий](#) бөлімінде қорғаудың осы түрі жөніндегі толығырақ ақпаратты 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.

Сүзуді төрт режимнің бірінде орындауға болады:

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

**Интерактивті режим** - Пайдаланушыға әрекеттерді растау ұсынылады.

**Саясатқа негізделген режим** - Әрекеттер бұғатталады.

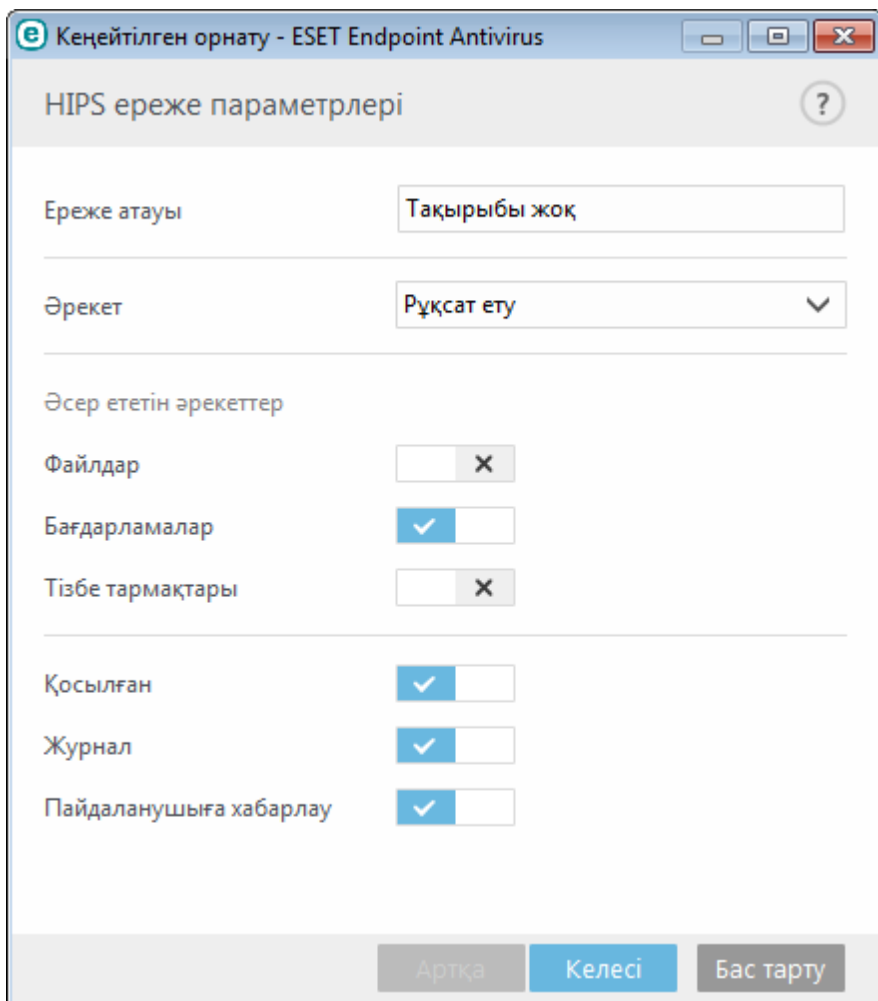
**Үйрену режимі** - Әрекеттер қосылады және әр әрекеттен кейін ереже жасалады. Бұл режимде жасалған ережелерді Ереже өңдеуші ішінде көруге болады, бірақ олардың басымдылығы қолмен немесе автоматты режимде жасалған ережелердің басымдылығынан төменірек. HIPS «Сүзу режимі» ашылмалы мәзірінде «Үйрену режимін» 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.

**Зерделі режим** - пайдаланушыға тек өте күдікті оқиғалар туралы хабарланады.

HIPS жүйесі операциялық жүйе ішіндегі оқиғаларды бақылайды және оларға жеке брандмауэр ережелеріне ұқсас сай әрекет етеді. HIPS ережелерін басқару терезесін ашу үшін **Өңдеу** түймесін басыңыз. Осы жерден ережелерді таңдай, жасай, өңдей не өшіре аласыз.

Келесі мысалда бағдарламалардың қалаусыз әрекетін шектеу әдісі көрсетілген:

1. Ережеге ат беріп және **Блоктау** алынбалы мәзіріндегі **Әрекет** командасын 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 бағдарламаның күйін өзгерту** (барлық әрекеттер F1 пернесін басу арқылы кіруге болатын өнім туралы анықтамада сипатталады).
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.



### 3.8.1.8.1 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.

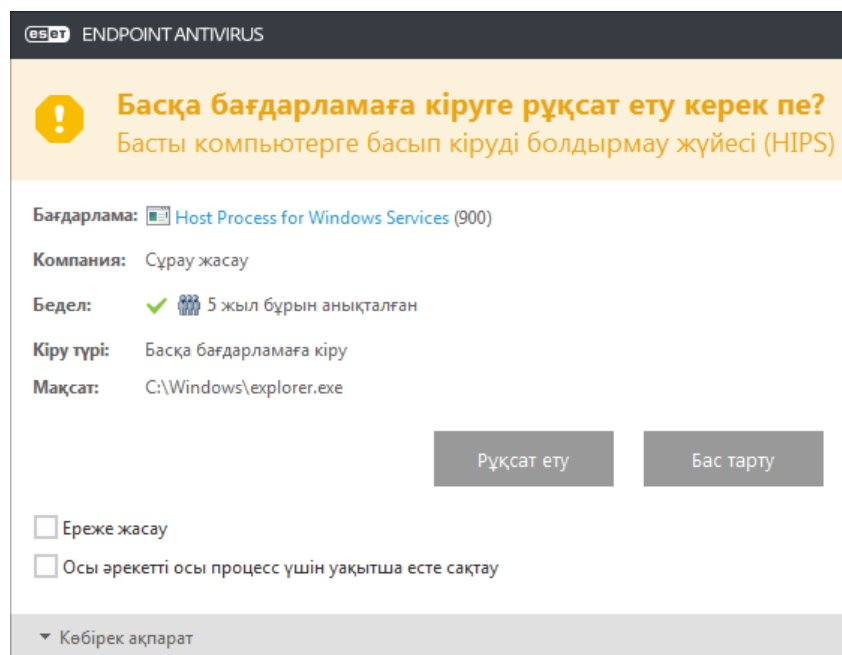
**Барлық блокталған әрекеттерді тіркеу** - Барлық блокталған әрекеттер HIPS журналына жазылады.

**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.

### 3.8.1.8.2 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 **Қосымша ақпарат** түймесін басу арқылы кіруге 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.

**Мына әрекетті осы процесс үшін уақытша есте сақтау** ережелердің немесе сұзу 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.

### 3.8.1.9 Көрсету режимі

Көрсету режимі - бағдарламалық жасақтаманы кедергісіз пайдалануды қажет ететін, қалқымалы терезелердің мазалауын қаламайтын және CPU пайдалануды барынша азайтқысы келетін пайдаланушыларға арналған мүмкіндік. Сондай-ақ, көрсету режимін антивирустың әрекеті үзе алмайтын көрсетілімдер кезінде пайдалануға болады. Қосылған болса, барлық қалқымалы терезелер өшіріледі және жоспарлы тапсырмалар орындалмайды. Жүйені қорғау әлі де фонда орындалады, бірақ ешбір пайдаланушының араласуын қажет етпейді.

Көрсету режимін қолмен қосу үшін **Орнату > Компьютер** тармағын басыңыз, содан кейін **Көрсету режимі** жанындағы қосқышты басыңыз. ESET Endpoint Antivirus толық экранды қолданбалар іске қосылғанда көрсету режимін автоматты түрде қосу үшін **Кеңейтілген орнату (F5) ішінде Құралдар > Көрсету режимі** тармағын басыңыз, содан кейін **Қолданбаларды толық экрандық режимде іске қосқанда көрсету режимін автоматты түрде қосу** жанындағы қосқышты басыңыз. Көрсету режимін қосу қауіпсіздікке ықтимал қауіп болып табылады, сондықтан тапсырмалар тақтасындағы қорғау күйінің белгішесі қызғылт сарыға айналады және ескертуді көрсетеді. Сондай-ақ, бұл ескертуді негізгі бағдарлама терезесінде көресіз, онда **Көрсету режимі қосылған** опциясын қызғылт сары түсте көресіз.

**Бағдарламалар толық экран режимінде іске қосылғанда Көрсету режимін қосу** опциясы қосылған болса, көрсету режимі толық экрандық бағдарламаны іске қосқаннан кейін іске қосылады және бағдарламадан шыққаннан кейін автоматты түрде тоқтайды. Бұл ойынды бастаудан, толық экрандық бағдарламаны ашудан немесе көрмені бастаудан кейін бірден көрсету режимін іске қосу үшін әсіресе пайдалы.

Сондай-ақ, көрсету режимі автоматты түрде қанша минуттан кейін өшірілетінін анықтау үшін **Көрсету режимін автоматты түрде өшіру** опциясын таңдауға болады.

### 3.8.1.10 Іске қосылған кезде қарап шығу

Әдепкі бойынша, жүйе іске қосылғанда немесе вирус қолтаңбасының дерекқоры жаңартылған кезде автоматты түрде файлдарды тексеру орындалады. Бұл қарап шығу [Жоспарлағыш конфигурациясы және тапсырмалар](#) параметріне байланысты болады.

Іске қосу кезінде қарап шығу опциялары **Жүйені іске қосу кезінде файлдарды тексеру** жоспарлағыш тапсырмасының бөлігі болып табылады. Іске қосу кезінде қарап шығу параметрлерін өзгерту үшін **Құралдар > Жоспарлағыш** тармағына өтіп, **Іске қосылғанда автоматты түрде файлдарды тексеру**, содан кейін **Өңдеу** түймесін 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.

#### 3.8.1.10.1 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:

- **Пайдаланушы кірмей тұрып іске қосылатын файлдар** - пайдаланушы жүйеге кірмей тұрып, оларға кіре алатын файлдарды қамтиды (қызметтер, браузер көмек нысандары, winlogon хабарландыру, Windows жоспарлағыш жазбалары, белгілі dll т.б. сияқты барлық 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 басымдылығы** - қарап шығу басталатын уақытын анықтау үшін пайдаланылатын басымдылық деңгейі:

- **Жұмыссыз болғанда** - жүйе жұмыссыз болған кезде ғана тапсырма орындалады.
- **Ең төмен** - жүйе жүктелген кезде ең төмен мүмкін,
- **Төмен** - жүйенің төмен жүктелген кезінде,
- **Қалыпты** - жүйе орташа жүктелген кезде.

#### 3.8.1.11 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 қоса қорғаныстың деңгейін қамтамасыз етеді және Microsoft Office құжаттарының жоғары деңгейіне қаіп төндірмейтін жүйедегі өнімділікті арттыру өшіріледі.

**Жүйеге біріктіру** опциясы қорғау жүйесін іске қосады. Бұл опцияны өзгерту үшін F5 пернесін басып «Кеңейтілген орнату» терезесін ашыңыз да, «Кеңейтілген орнату» тармағында **Антивирус > Құжатты қорғау** тармағына өтіңіз.

Бұл мүмкіндік Microsoft Antivirus API (мысалы, Microsoft Office 2000 және одан кейінгі нұсқалар немесе Microsoft Internet Explorer 5.0 және одан кейінгі нұсқалар) пайдаланатын бағдарламалар арқылы іске қосылады.

### 3.8.1.12 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. Нысанды шығаруды қажет етуі мүмкін жағдайлар қарап шығу кезінде компьютер жұмысын баяулататын үлкен дерекқор жазбаларын немесе қарап шығумен қайшылықтары болатын бағдарламалық құралды (мысалы, сақтық көшірме жасау бағдарламалық құралын) қамтуы мүмкін.

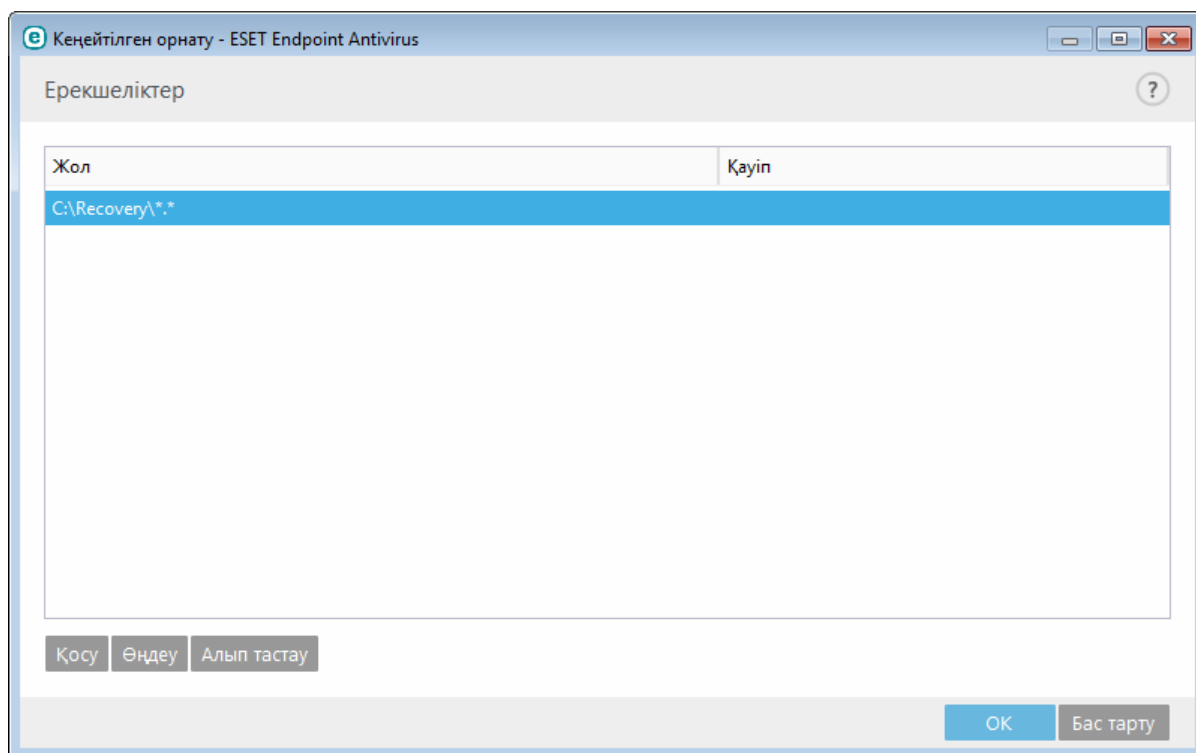
Нысанды қарап шығудан шығару үшін:

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 енгізіңіз және «\*.» бүркенішін пайдаланыңыз.
- Барлық файлдар және ішкі қалталармен бірге дискіні толығымен алып тастау үшін "D:\\*" бүркенішін пайдаланыңыз.
- Тек doc файлдарын алып тастағыңыз келсе, «\*.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 қарап шығуға қоспау шарттарына сәйкес келсе, файлдағы қауіп Нақты уақыттағы файлдық жүйені қорғау модулі немесе компьютерді қарап шығу модулі арқылы анықталмайды.

#### Бағандар

**Жол** - Шығарылған файлдар мен қалталарға жол.

**Қауіп** - егер шығарылған файлдың жанында қауіп атауы көрсетілсе, бұл файлдың тек берілген қауіп бойынша шығарылғанын білдіреді. Егер файлға басқа зиянды бағдарламадан кейінірек вирус жұққан жағдайда, оны антивирус модулі анықтайды. Бұл ерекшелік түрін тек белгілі бір инфильтрациялар түрлеріне пайдалануға болады және оны инфильтрациялар туралы есеп беретін қауіп туралы ескерту терезесінде (**Кеңейтілген опцияларды көрсету**, содан кейін **Анықтауға қоспау** пәрменін таңдаңыз) немесе **Орнату** > **Карантин** тармағын басып, карантинге қойылған файлда тінтуірдің оң жақ түймешігін басыңыз және контекстік мәзірден **Қалпына келтіру**

**және анықтаудан шығару** опциясын таңдаңыз.

### **Басқару элементтері**

**Қосу** - нысандарды анықтаудан шығарады.

**Өңдеу** - таңдалған жазбаларды өңдеу мүмкіндігін береді.

**Алып тастау** - таңдалған енгізбелер алып тастайды.

### **3.8.1.13 ThreatSense механизмінің параметрлерін орнату**

ThreatSense – көптеген кешенді қауіп анықтау әдістері қамтылған технология. 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.

Реттеу терезесіне кіру үшін ThreatSense технологиясын пайдаланатын кез келген модульге арналған «Кеңейтілген орнату» терезесіндегі **ThreatSense механизмінің параметрлерін реттеу** түймесін 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:

- Нақты уақыттағы файл жүйесін қорғау,
- Жұмыссыз күйде қарап шығу,
- Іске қосылған кезде қарап шығу,
- Құжатты қорғау,
- Электрондық пошта клиентін қорғау,
- Веб қатынасын қорғау,
- Компьютерді қарап шығыңыз.

ThreatSense параметрлері әрбір модуль үшін жоғары деңгейде оңтайландырылған және оларды өзгерту жүйенің жұмысына айтарлықтай әсер етуі мүмкін. Мысалы, орындалатын бумалаушылардағы параметрлерді әрдайым өзгерту және «Нақты уақыттағы файл» жүйесін қорғау модулінде кеңейтілген эвристиканы қосу жүйенің баяулауына әкелуі мүмкін (әдетте, жаңадан жасалған файлдар ғана осы әдістер арқылы тексеріледі). 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 ашу үшін арнайы бағдарламалар-мұрағаттарды қажет етпейтін мұрағаттар болып табылады.

**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 белгісіз болған зиянкес бағдарламаларды анықтау қабілеті. Кемшілігі – жалған ескертулердің болу ықтималдығы (өте аз).

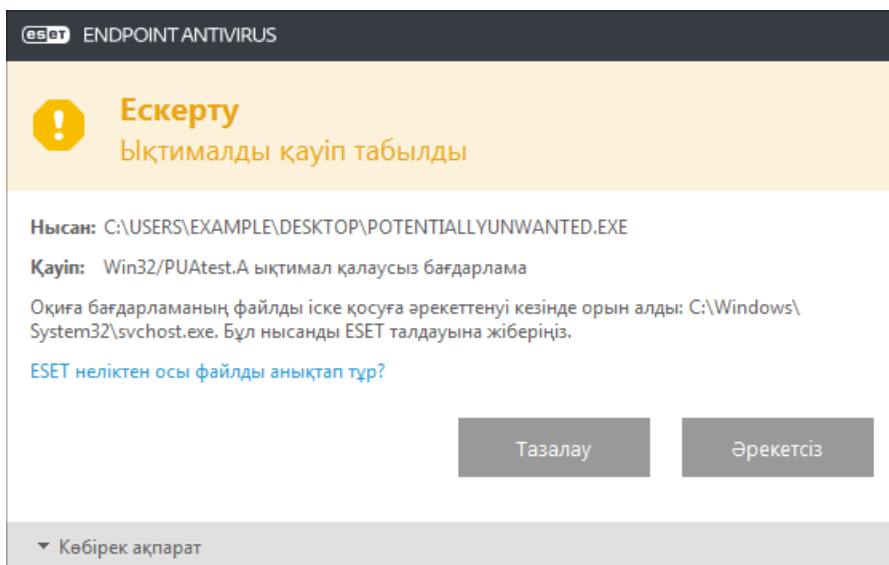
**Кеңейтілген эвристика/DNA/Смарт қолтаңбалар** - кеңейтілген эвристика ESET компаниясы жасаған, компьютер құрттары мен троялық аттарды табу үшін оңтайландырылған және жоғары деңгейлі бағдарламалау тілдерінде жазылған бірегей эвристикалық алгоритм. Кеңейтілген эвристиканы пайдалану ESET өнімдерінің қауіптерді 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.

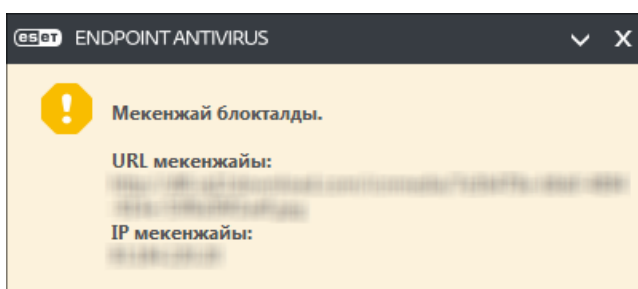
## Ескерту - Ықтимал қауіп табылды

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. **Әрекетсіз**: бұл опция ықтимал қауіпке жүйеге кіруге рұқсат етеді.
3. Қолданбаға болашақта үзіліссіз компьютерде жұмыс істеуге рұқсат ету үшін **Қосымша ақпарат/Кеңейтілген опцияларды көрсету** тармағын басыңыз, содан кейін **Анықтауға қоспау** жанында құсбелгі қойыңыз.



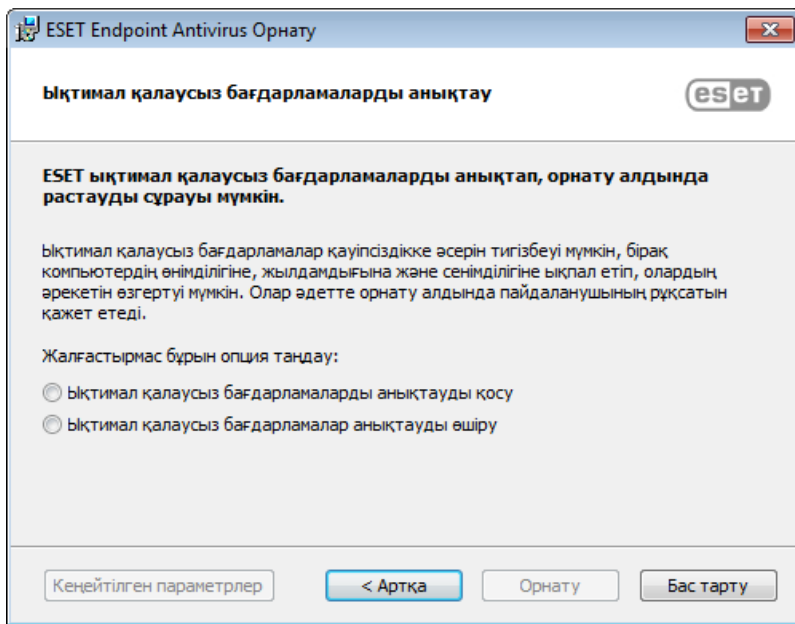
Ықтимал қалаусыз қолданба анықталса және оны тазалау мүмкін болмаса, экранның төменгі оң жақ бұрышында **Мекенжай блокталды** хабарландыру терезесі көрсетіледі. Бұл оқиға туралы қосымша ақпарат алу үшін негізгі мәзірден **Құралдар > Журнал файлдары > Сүзілген веб-сайттар** тармағына өтіңіз.






## Ықтимал қалаусыз қолданбалар - Параметрлер

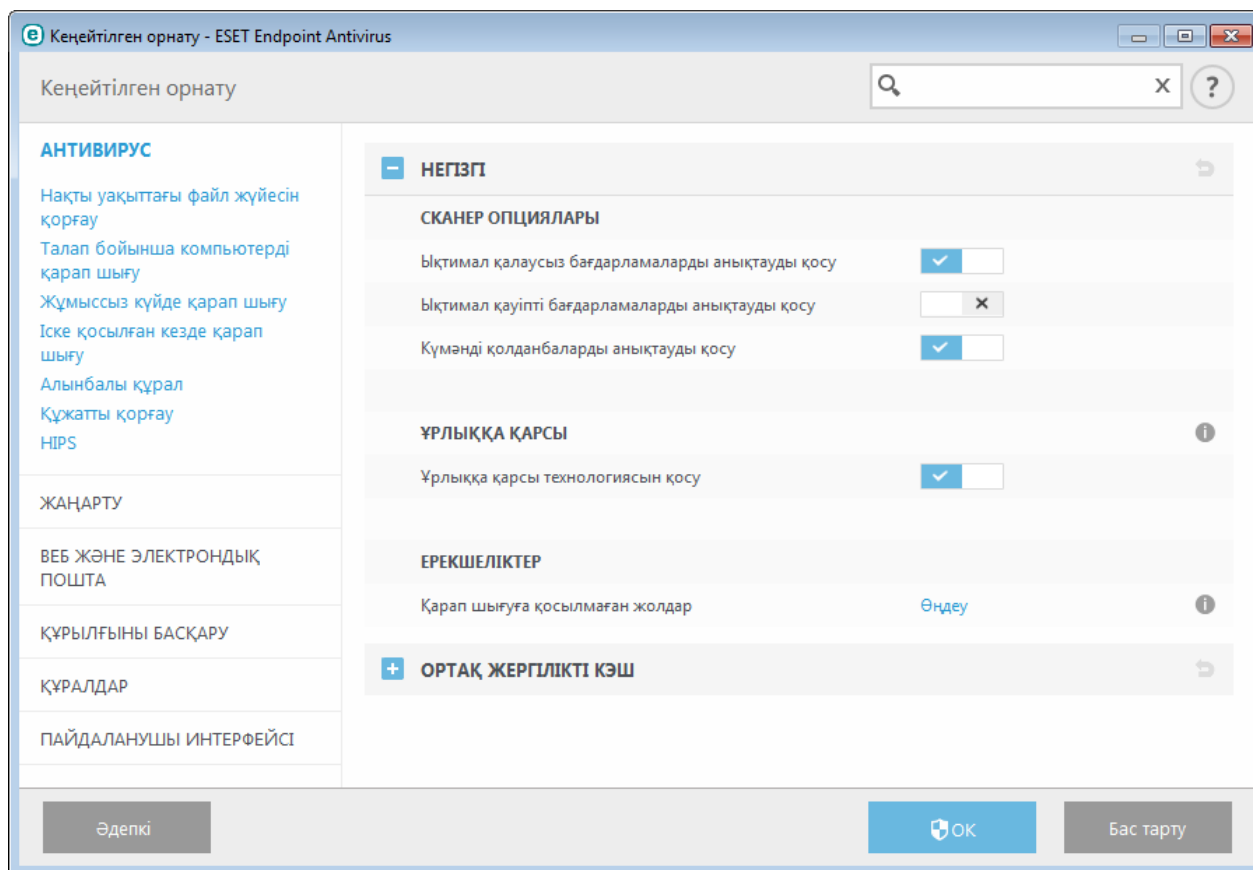
ESET өнімін орнатып жатқанда төменде көрсетілгендей ықтимал қалаусыз қолданбаларды анықтауды қосу-қоспау туралы шешім қабылдай аласыз:



 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 бағдарлама веб-браузердің басты бетіне және іздеу параметрлеріне өзгертулер енгізуі мүмкін. Сондай-ақ, файл-хостинг веб-сайттары көбінесе бағдарлама жеткізушісіне немесе жүктеуді алушыға өзгертулер жасалғаны туралы хабарламайды және өзгертуден оңай бас тартуға мүмкіндік бермейді. 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.

**ESET Live Grid** - ESET репутация технологиясының арқасында анықтау және қарап шығу жылдамдығын жақсарту үшін қарап шығылған файлдар туралы ақпарат бұлттағы [ESET Live Grid](#) қызметінен алынған деректерге қатысты тексеріледі.

## Тазалау

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

**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 (Стандартты 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.

## Ерекш өліктер

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.

## Ш ектеулер

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

### Нысан параметрлері

**Нысанның ең үлкен өлш өмі** - 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 шығудың ең ұзақ уақытының 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 өлш өмі** - Бұл опция қарап шығылуы қажет мұрағаттарда (бөлініп алынған кезде) қамтылған файлдар үшін ең үлкен өлшемді көрсету мүмкіндігін береді. Әдепкі мәні: *шексіз*.

**ЕСКЕРТПЕ:** Біз әдепкі мөндерді өзгертуді ұсынбаймыз; қалыпты жағдайда оларды өзгертудің еш негізі жоқ.

### 3.8.1.13.1 Ерекшеліктер

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

Әдепкі бойынша, барлық файлдар қарап шығылады. Қарап шығуға қосылмаған файлдар тізіміне кез келген кеңейтімді қосуға болады.

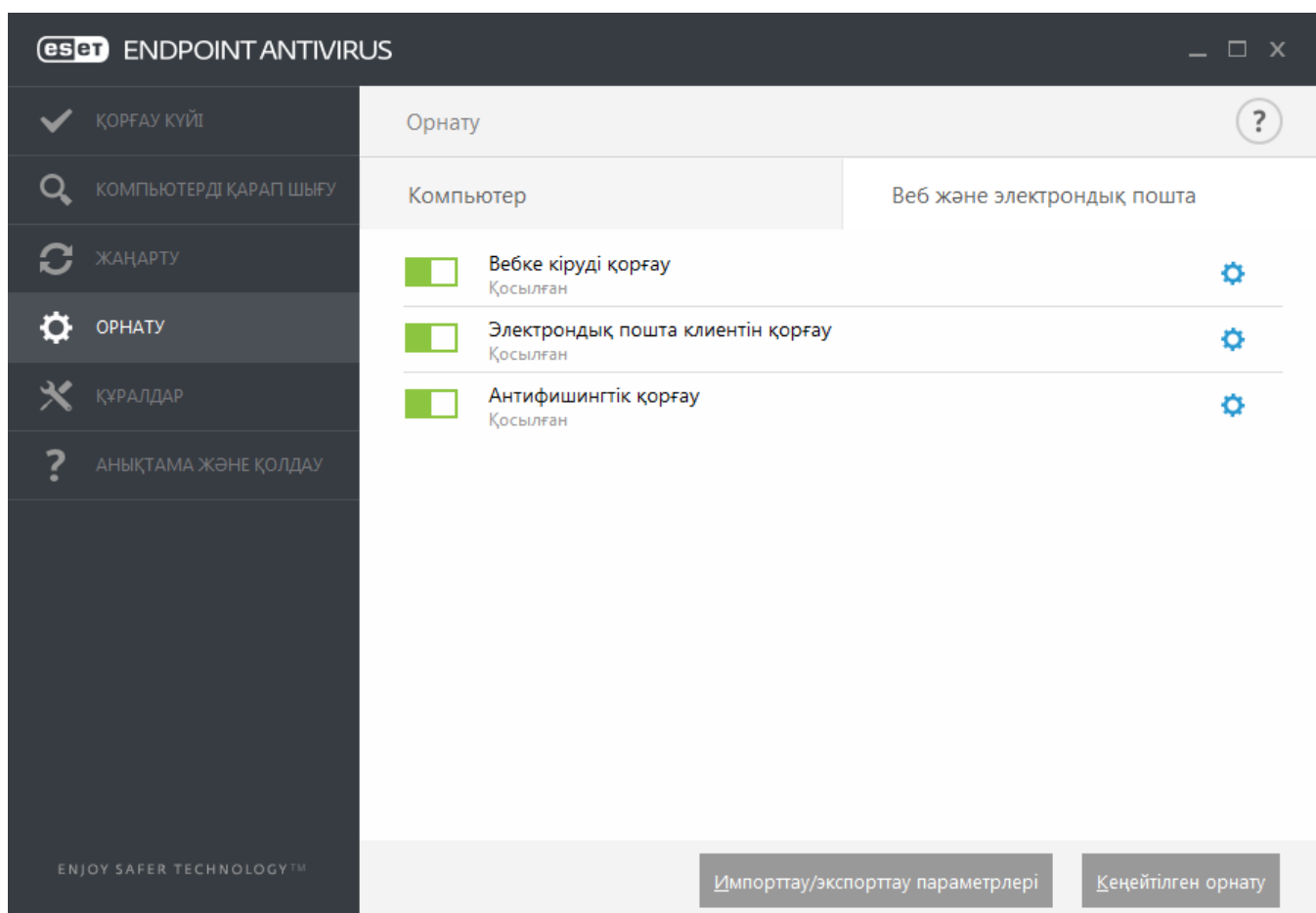
Кейде белгілі бір файл түрлерін қарап шығу кеңейтімдерді пайдаланатын бағдарламаның дұрыс емес әрекетін тудырған жағдайда файлдарды қарап шығуға қоспаған дұрыс. Мысалы, Microsoft Exchange серверін пайдаланғанда .edb, .eml және .tmp кеңейтімдерін қоспауға кеңес беруге болады.

**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, **ОК** түймесін басыңыз. **Бірнеше ө мөнді өнгізу** 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 таңбалары (сұрақ белгісі) арнайы таңбаларын пайдалануға болады. Сұрақ белгісі кез келген таңбаны білдіреді.

### 3.8.2 Веб және электрондық пошта

Веб және электрондық пошта конфигурациясын **Орнату > Веб және электрондық пошта** тармағында табуға болады. Осы жерден бағдарламаның егжей-тегжейлі параметрлерін ашуға болады.




Интернетке қосылу мүмкіндігі – жеке компьютерлердегі стандартты мүмкіндік. Өкінішке орай, ол, сонымен бірге, зиянды кодты тасымалдаудың негізгі құралына айналды. Осыған байланысты, **Веб-қатынасты қорғауды** мұқият қарастыру маңызды.

**Электрондық пошта клиентін қорғау** POP3 және IMAP протоколдары арқылы алынатын электрондық пошта хабарларын бақылауды қамтамасыз етеді. Электрондық пошта клиентіне қосылмалы модульді пайдаланып, ESET Endpoint Antivirus электрондық пошта клиентінің барлық байланыстарын (POP3, IMAP, HTTP, MAPI) бақылауды

қамтамасыз етеді.

**Антифиш инттік қорғау** — құпия сөздерді және басқа құпия ақпаратты алуға тырысатын заңсыз веб-сайттардан көбірек қорғанысты қамтамасыз ететін тағы бір қорғау қабаты. Антифишингтік қорғауды **Веб және электрондық пошта** астындағы **Орнату** тақтасында табуға болады. Қосымша ақпаратты [Антифишингтік қорғау](#) бөлімінен қараңыз.

**Өшіру** - веб/электрондық пошта қорғауын веб-браузерлер және электрондық пошта клиенттері үшін өшіру үшін осы қосқышты басыңыз .

### 3.8.2.1 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) параметрлерін өңдеу үшін **Веб және электрондық пошта > SSL/TLS протоколын тексеру** тармағына өтіңіз.

**Бағдарламалық протокол мазмұнын сүзуді қосу** - протоколды сүзуді өшіру үшін пайдалануға болады. Көп ESET Endpoint 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.

**ESET қолдау қызметіне протоколды сүзу мәселелерін диагностикалау үшін қажет ақпаратты жазу** - диагностикалық деректерді кеңейтілген журналға тіркеуді қосады, мұны тек ESET қолдау қызметі сұрағанда пайдаланыңыз.

#### 3.8.2.1.1 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 себепті тигізеді, осы себепті ESET Endpoint Antivirus бағдарламасы веб-браузердің қауіпсіздігіне баса назар аударады. Желіге қатынайтын әрбір бағдарлама интернет браузері ретінде белгілене алады. Байланыс үшін протоколдарды әлдеқашан пайдаланған қолданбаларды немесе таңдалған жолдағы қолданбаны веб және электрондық пошта клиенттері тізіміне енгізуге болады.

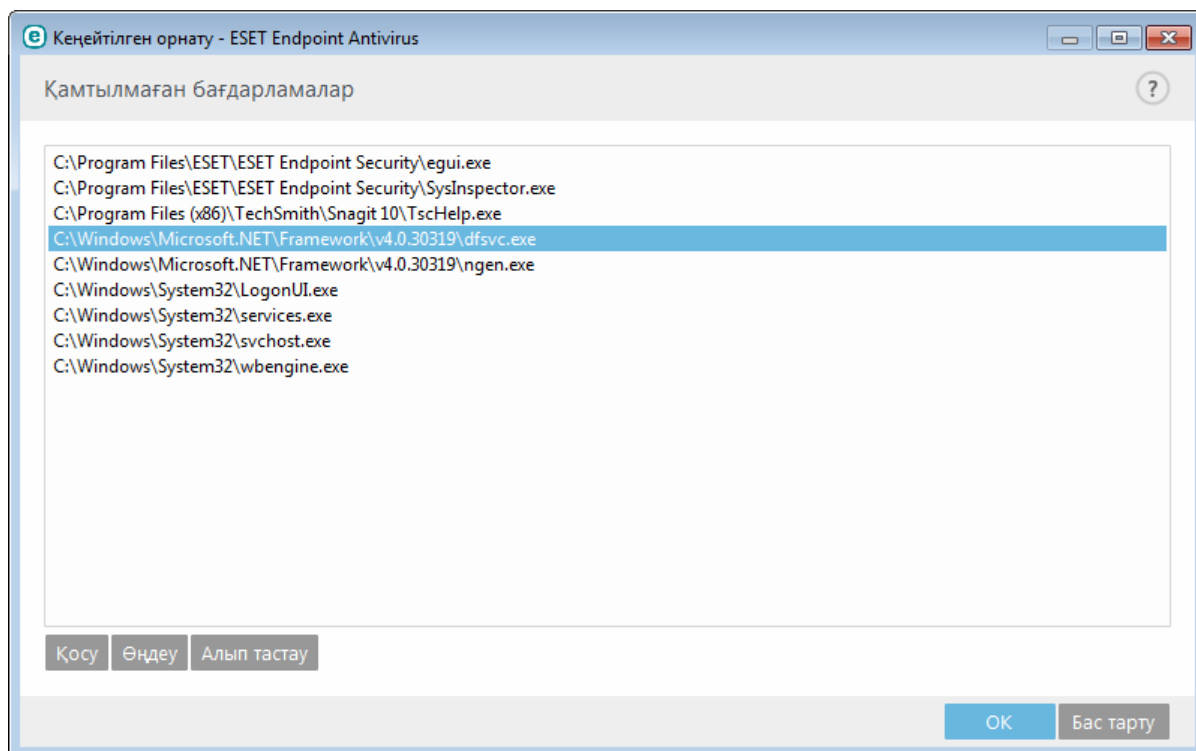
#### 3.8.2.1.2 Қамтылмаған бағдарламалар

Белгілі бір желіні пайдаланатын бағдарламалардың қосылымдарын мазмұнды сүзуге қоспау үшін оларды тізімде таңдаңыз. Таңдалған бағдарламалардың HTTP/POP3/IMAP байланысында қауіптердің бар-жоғы тексерілмейді. Бұл әдісті тек протокол сүзу қосылған кезде бағдарламалар дұрыс жұмыс істемейтін жағдайларда пайдалану ұсынылады.

Протоколды сүзу әлдеқашан әсер еткен бағдарламалар мен қызметтер **Қосу** түймесін қосқаннан кейін автоматты түрде көрсетіледі.

**Өңдеу** - Тізімнен таңдалған жазбаларды өңдеу.

**Алып тастау** - Тізімнен таңдалған жазбаларды алып тастайды.



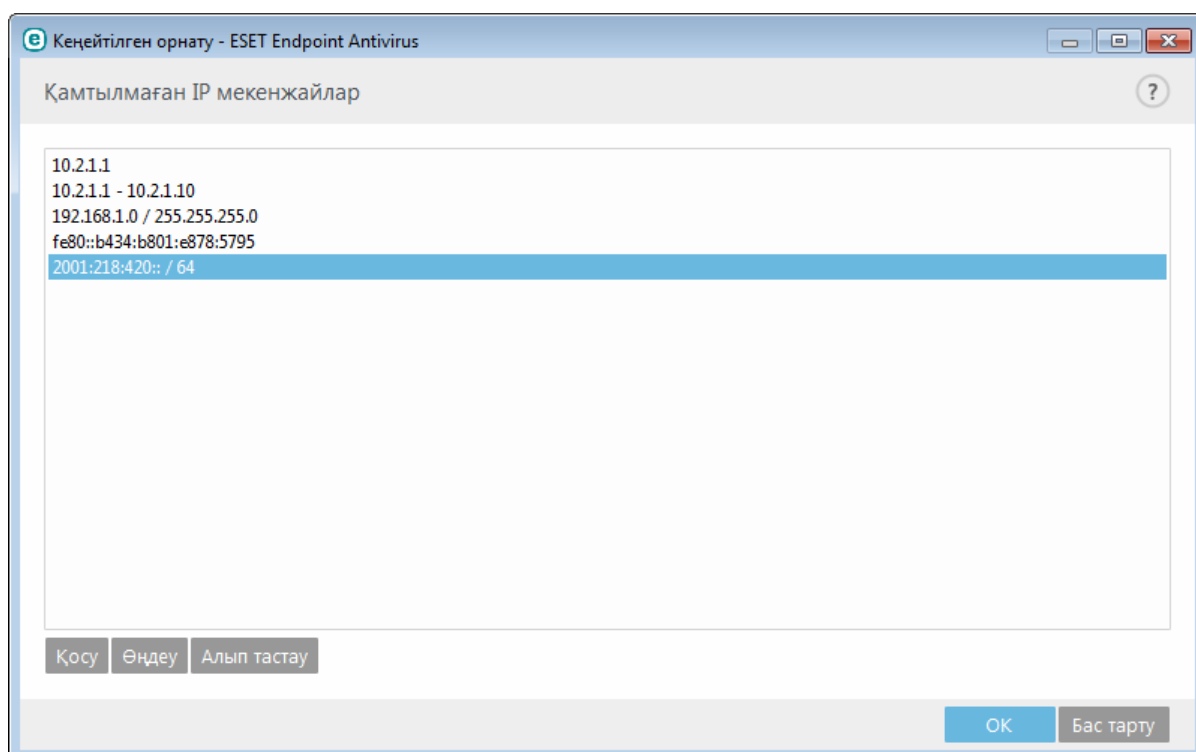
### 3.8.2.1.3 Қамтылмаған IP мекенжайлар

Бұл тізімдегі IP мекенжайлары протокол мазмұнын сүзуге қосылмайды. Таңдалған мекенжайлардың HTTP/POP3/IMAP байланысында қауіптер бар-жоғы тексерілмейді. Осы опцияны тек сенімді мекенжайларға ғана пайдалануды ұсынамыз.

**Қосу** - Ереже қолданылатын қашықтағы нүктенің IP мекенжайын/мекенжайлар ауқымын/ішкі желісін қосу үшін басыңыз.

**Өңдеу** - Тізімнен таңдалған жазбаларды өңдеу.

**Алып тастау** - Тізімнен таңдалған жазбаларды алып тастайды.



### 3.8.2.1.4 SSL/TLS протоколын тексеру

ESET Endpoint 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** - 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.

**Интерактивті режим** - егер жаңа SSL арқылы қорғалған сайтқа (белгісіз куәлігі бар) кірсеңіз, әрекет таңдау диалогтық терезесі көрсетіледі. Бұл режим қарап шығуға қосылмайтын SSL куәліктерінің тізімін жасауға рұқсат етеді.

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

#### Түбірлік куәлік

**Түбірлік куәлік** - SSL байланысы браузерде/электрондық пошта клиенттерінде дұрыс жұмыс істеуі үшін ESET жүйесіне арналған түбірлік куәлікті белгілі түбірлік куәліктер (жариялаушылар) тізіміне қосу маңызды болып табылады. **Түбір куәлікті белгілі браузерлерге қосу** опциясын қосу керек. ESET түбірлік куәлігін белгілі браузерлерге (мысалы, Opera және Firefox) автоматты түрде қосу үшін осы опцияны таңдаңыз. Жүйелік куәліктер қорын пайдаланатын браузерлерде куәлік автоматты түрде қосылады (мысалы, Internet Explorer).

Куәлікті қолдау көрсетілмейтін браузерлерге қолдану үшін **Куәлікті көру > Мәліметтер > Файлға көш іру...** 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.

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

### 3.8.2.1.4.1 Шифрланған SSL байланысы

Егер жүйе SSL протоколын қарап шығуға конфигурацияланған болса, әрекетті таңдауды ұсынатын диалогтық терезе екі жағдайда көрсетіледі:

Біріншісі, веб-сайт тексеру мүмкін емес немесе жарамсыз куәлікті пайдаланса және ESET Endpoint Antivirus осындай жағдайларда пайдаланушыдан сұрауға конфигурацияланған болса (әдепкі бойынша, тексеру мүмкін емес куәліктер үшін «иә», жарамсыздары үшін «жоқ»), диалогтық терезе қосылымға **Рұқсат ету** немесе **Блоктау** қажеттілігін сұрайды.

Екіншісі, **SSL протоколын сүзу режимі Интерактивті режимге** орнатылған болса, әр веб-сайттың диалогтық терезесі трафикті **Қарап шығу** немесе **Елемей** қажеттілігін сұрайды. Кейбір қолданбалар SSL трафигі өзгертілмегенін немесе оны ешкім тексермегенін тексереді, мұндай жағдайларда ESET Endpoint Antivirus қолданба жұмыс істеуін жалғастыруы үшін сол трафикті **Елемей** керек.

Жағдайлардың екеуінде де пайдаланушы таңдалған әрекетті есте сақтауды таңдай алады. Сақталған әрекеттер **Белгілі куәліктер тізімі** ішінде сақталады.

### 3.8.2.1.4.2 Белгілі куәліктердің тізімі

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

**Белгілі куәліктер 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 елемей үшін **Қарап шығу** немесе **Елемей** 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

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

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

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



## 3.8.2.2 Электрондық пошта клиентін қорғау

### 3.8.2.2.1 Электрондық пошта клиенттері

ESET Endpoint Antivirus бағдарламасын электрондық пошта клиенттерімен біріктіру электрондық пошта хабарларындағы зиянды кодтан белсенді қорғаудың деңгейін жоғарылатады. Егер электрондық пошта клиентіне қолдау көрсетілсе, біріктіруді ESET Endpoint Antivirus бағдарламасында қосуға болады. Біріктіру іске қосылса, ESET Endpoint Antivirus құралдар тақтасы тікелей электрондық пошта клиентіне кірістіріліп (жаңарақ Windows Live Mail нұсқаларының құралдар тақтасы кірістірілмейді), электрондық поштаны тиімдірек қорғауға мүмкіндік береді. Біріктіру параметрлері **Орнату > Кеңейтілген орнату > 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.

Электрондық пошта клиентімен жұмыс істегенде жүйе баяуласса, **Кіріс мазмұнын өзгерткеннен кейін тексеруді өшіру** опциясын таңдаңыз (тек MS Outlook). Бұл «Kerio Outlook Connector» қорынан электрондық пошта деректерін алу кезінде пайда болуы мүмкін.

#### Қарап шығарылатын электрондық пошта

**Алынған электрондық пошта хабары** - Алынған хабарларды тексеруді қосады.

**Жіберілген электрондық пошта хабары** - Жіберілген хабарларды тексеру қосады.

**Хабарды оқу** - Оқылған хабарларды тексеру қосқышы.

#### Вирус жұққан электрондық поштаға қатысты орындалатын әрекет

**Әрекет жоқ** - Егер қосылған болса, бағдарлама жұққан тіркемелерді анықтайды, бірақ электрондық поштаны ешбір әрекет жасамастан сол күйінде қалдырады.

**Электрондық поштаны жою** - Бағдарлама пайдаланушыға сүзгі(лер) туралы хабарлайды және хабарды жояды.

**Электрондық поштаны «Жойылғандар» қалтасына жылжыту** - Вирус жұққан электрондық хабарлар «Жойылғандар» қалтасына автоматты түрде жылжытылады.

**Электрондық поштаны қалтаға жылжыту** - Вирус жұққан электрондық хабарлар көрсетілген қалтаға автоматты түрде жылжытылады.

**Қалта** - Анықталған кезде вирус жұққан электрондық хабарлар жылжытылатын теңшелетін қалтаны көрсетіңіз.

**Жаңартудан кейін қарап шығуды қайталау** - Вирус қолтаңбасының дерекқоры жаңартылғаннан кейін қайта қарап шығу қосқыштары.

**Қарап шығу нәтижелерін басқа модульдерден қабылдау** - Егер осы опция таңдалған болса, электрондық поштаны қорғау модулі басқа қорғау модульдерінің қарап шығу нәтижелерін қабылдайды ((POP3, IMAP протоколдарын қарап шығу).

### 3.8.2.2.2 Электрондық пошта протоколдары

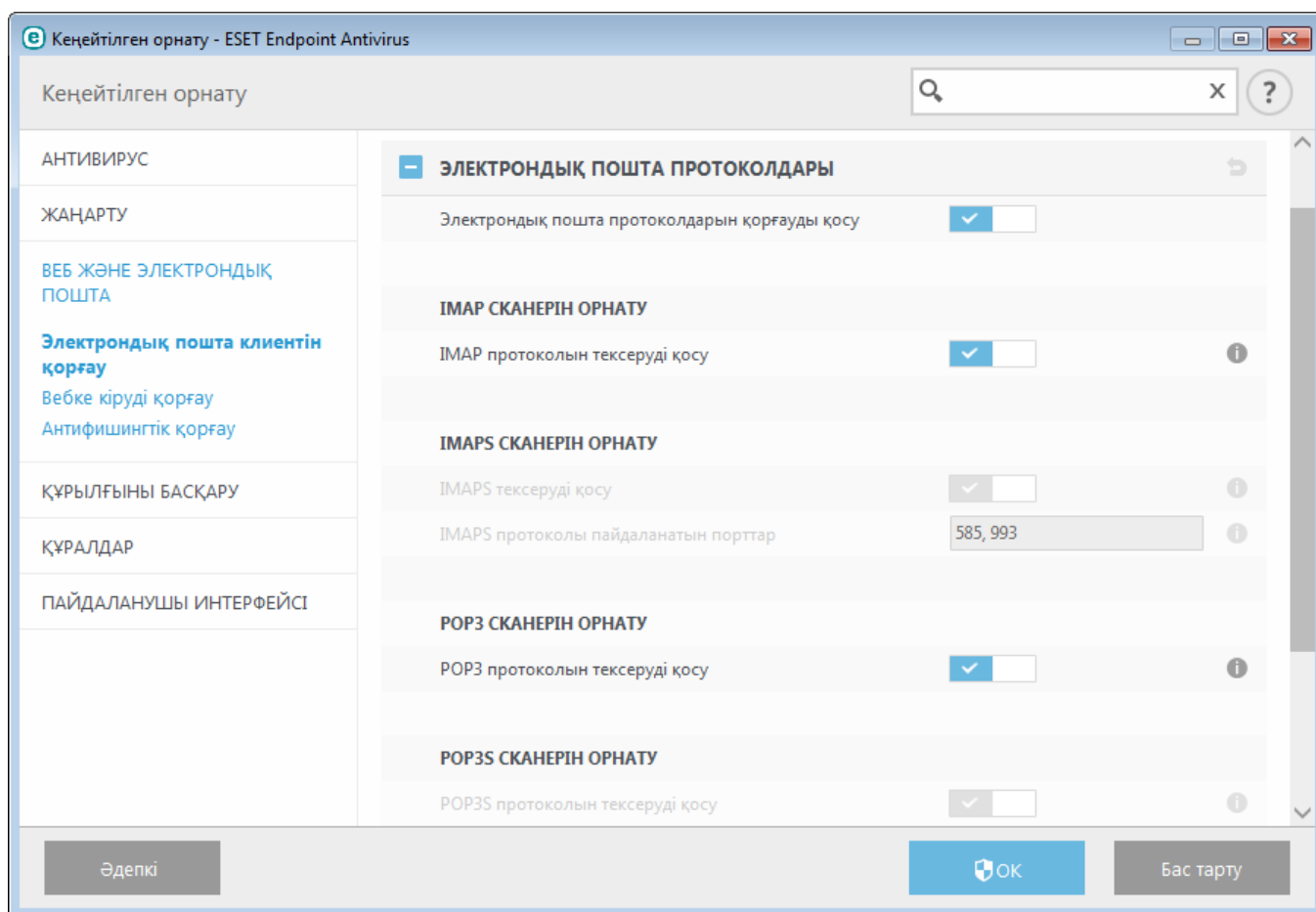
IMAP және POP3 протоколдары — электрондық пошта клиенті қолданбасында электрондық пошта хабарларын алу үшін пайдаланылатын ең кең таралған протоколдар. ESET Endpoint Antivirus осы протоколдар үшін пайдаланылатын электрондық пошта клиентіне қарамастан және электрондық пошта клиентін қайта конфигурациялау қажеттілігінсіз қамтамасыз етеді.

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 кеңейтіңіз.

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

Әдепкі параметрлер пайдаланылып жатқанда шифрланған байланыстар қарап шығылмайды. Шифрланған байланысты қарап шығуды қосу үшін «Кеңейтілген орнату» ішінде [SSL/TLS протоколын тексеру](#) тармағына өтіңіз, **Веб және электрондық пошта > SSL/TLS протоколын тексеру** тармағын басыңыз және **SSL протоколын сүзуді қосу** опциясын таңдаңыз.



### 3.8.2.2.3 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 Endpoint 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 зиянды бағдарламаларды анықтау вирус қолтаңбасының дерекқорына сәйкес келіп жатқанның өзінде 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.

**ThreatSense механизм параметрлерін реттеу** - кеңейтілген вирусты қарап шығу құралын реттеу – қарап шығу мақсаттарын, анықтау әдістерін, т.б. конфигурациялау мүмкіндігін береді. Егжей-тегжейлі вирусты қарап шығу құралын реттеу терезесін көрсету үшін басыңыз.

Электрондық пошта тексерілгеннен кейін қарап шығу нәтижелері бар хабарландыруды хабарға бекітуге болады. **Алынған және оқылған вирус жұққан электрондық пошта таның 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. Қолжетімді опциялар:

- **Еш қашан** - Барлығына қосылатын белгі хабарлары жоқ.
- **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.

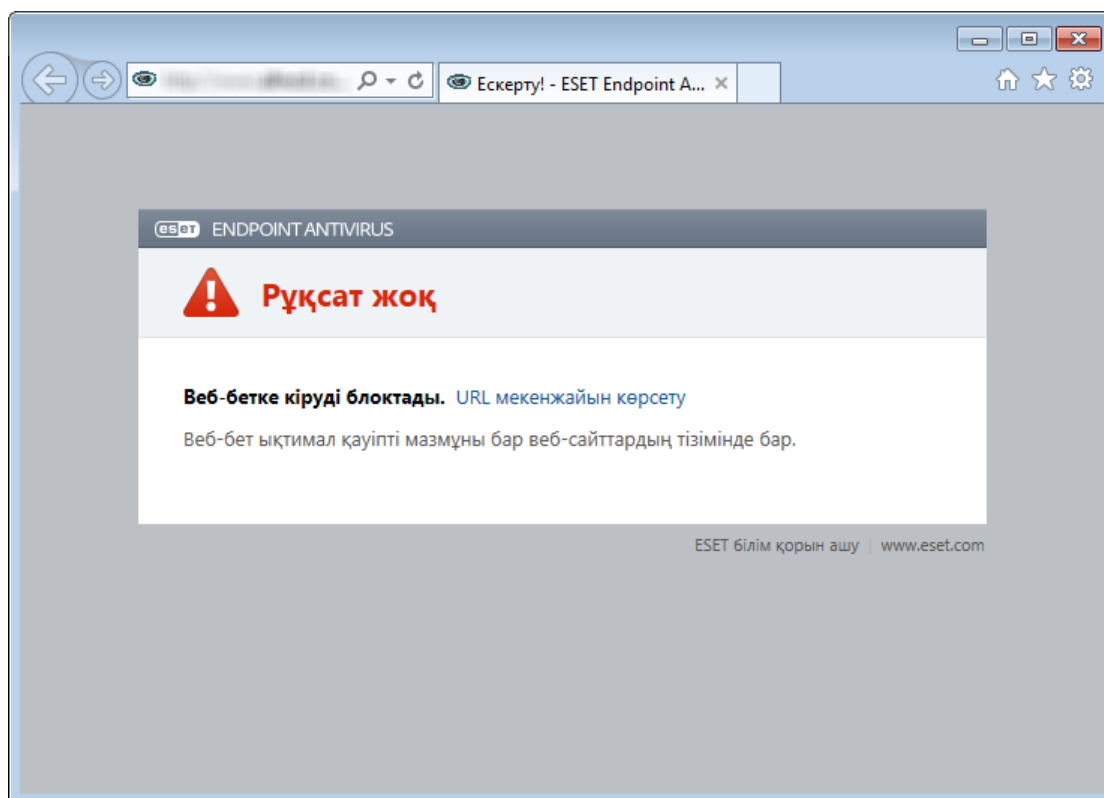
**Жіберілген вирус жұққан электрондық пошта таның тақырыбына жазба бекіту** - электрондық поштаны қорғау вирус жұққан электрондық пошта хабарының тақырыбында вирус туралы ескертуді қамтымауы керек болса, осы құсбелгіні қоймаңыз. Бұл мүмкіндік вирус жұққан электрондық пошта хабарларын қарапайым, тақырыпқа негізделген сүзуге мүмкіндік береді (егер электрондық пошта бағдарламасы қолдаса). Сондай-ақ, ол алушы үшін сенімділік деңгейін арттырады және, инфильтрация анықталса, осы электрондық пошта хабарының немесе жіберушінің қауіп деңгейі туралы құнды ақпарат береді.

**Вирус жұққан электрондық пошта таның 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.

### 3.8.2.3 Вебке кіруді қорғау

Интернетке қосылу мүмкіндігі — жеке компьютерлердің көпшілігіндегі 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 қосылған күйде қалдыру қатаң ұсынылады. Бұл опцияға ESET Endpoint Antivirus бағдарламасының негізгі терезесінен **Орнату > Веб және электрондық пошта > Веб-қатынасты қорғау** тармағына өту арқылы қатынасуға 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 механизмінің параметрлерін реттеу** - вирустарды қарап шығу құралын кеңейтілген реттеу - қарап шығатын нысандардың (электрондық хабарлар, мұрағаттар, т.б.) түрлері, веб-қатынасты қорғау үшін анықтау әдістері, т.б. сияқты параметрлерді конфигурациялауға мүмкіндік береді.

### 3.8.2.3.1 Веб-протоколдар

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

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 > HTTP сканерін реттеу** тармағында өзгертуге болады. HTTP трафигі көрсетілген порттарда барлық бағдарламалар үшін және [Веб және электрондық пошта клиенттері](#) ретінде белгіленген бағдарламалар үшін барлық порттарда бақыланады.

Сондай-ақ, ESET Endpoint Antivirus бағдарламасы HTTPS протоколын тексеруді қолдайды. HTTPS байланысы ақпаратты сервер мен клиент арасында тасымалдау үшін шифрланған арнаны пайдаланады. ESET Endpoint 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.

Әдепкі параметрлер пайдаланылып жатқанда шифрланған байланыс қарап шығылмайды. Шифрланған байланысты қарап шығуды қосу үшін «Кеңейтілген орнату» ішінде [SSL/TLS протоколын тексеру](#) тармағына өтіңіз, **Веб және электрондық пошта > SSL/TLS протоколын тексеру** тармағын басыңыз және **SSL протоколын сүзуді қосу** опциясын таңдаңыз.

### 3.8.2.3.2 URL мекенжайларын басқару

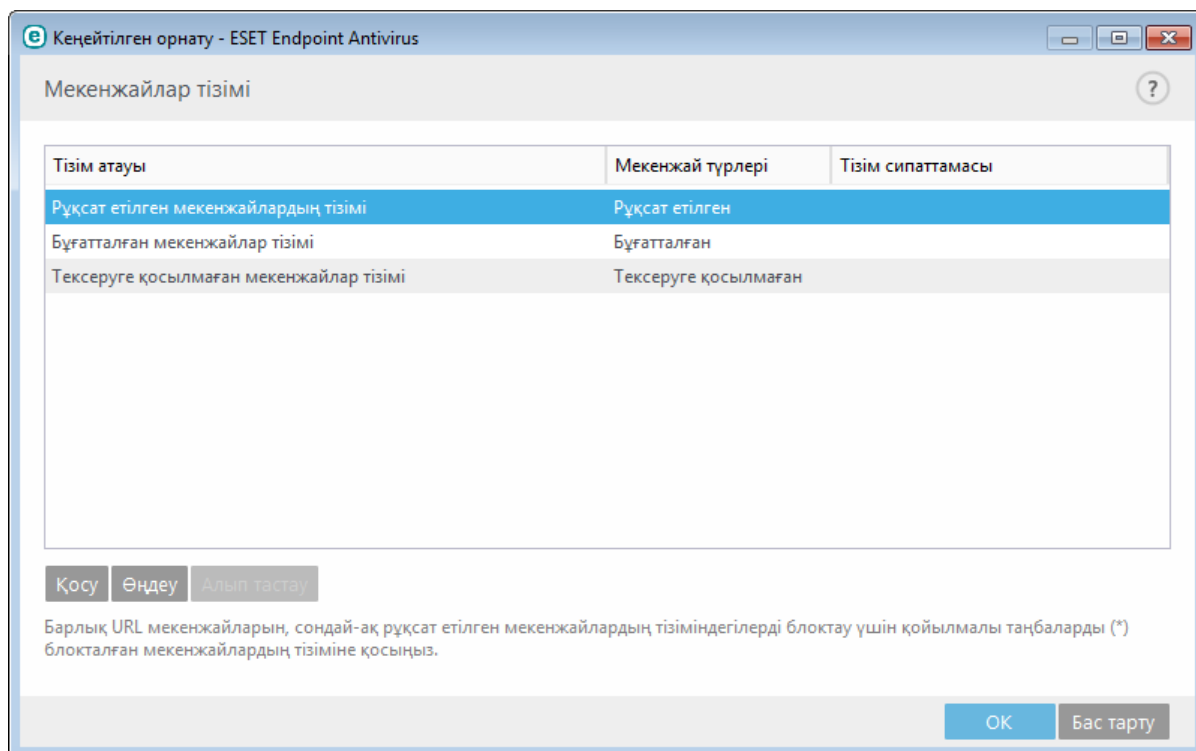
URL мекенжайларын басқару бөлімі блокталатын, рұқсат етілетін немесе тексеруге қосылмайтын HTTP мекенжайларын көрсетуге мүмкіндік береді.

**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.

Барлық тізімдерде \* (жұлдызша) және ? (сұрақ белгісі) арнайы таңбаларын пайдалануға болады. Жұлдызша кез келген санды немесе таңбаны білдіреді, ал сұрақ белгісі тек бер таңбаны білдіреді. 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 қосыңыз. Егер сіз ағымдағы тізімнен мекенжайды енгізгенде хабардар болуды қаласаңыз, **Қолданғанда хабарлау** опциясын қосыңыз.

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



**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 тізімдерде мекенжайларды қосу немесе жою үшін пайдаланыңыз.

**Жою** - бар тізімді жояды. Әдепкілері емес, тек **Қосу** көмегімен жасалған тізімдер үшін мүмкін.

### 3.8.2.4 Антифишингтік қорғау

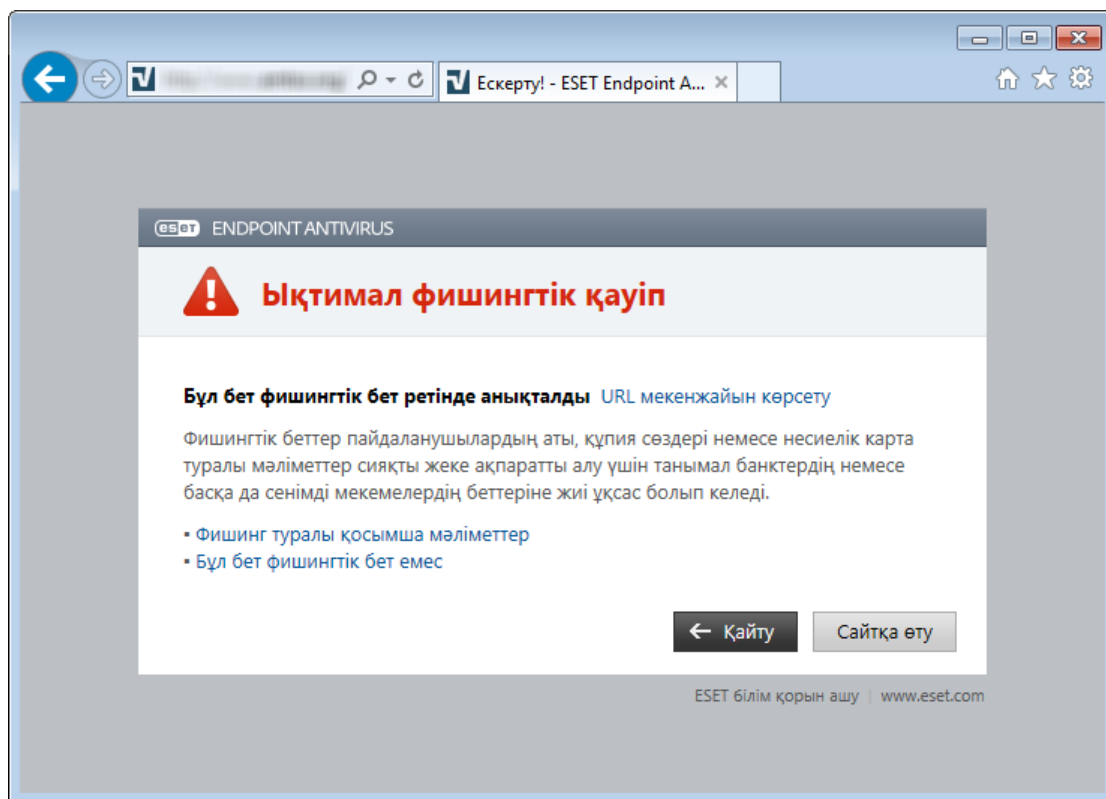
Фишинг термині қоғамдық техниканы (құпия ақпаратты алу үшін пайдаланушылардың әрекеті) пайдаланатын қылмыстық әрекетті білдіреді. Фишинг банктік есеп-шот нөмірлері, PIN-коды нөмірлері және басқалары секілді құпия деректерге кіру үшін жиі қолданылады. Осы әрекет туралы қосымша мәлімет үшін [гlossарийді](#)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

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

ESET Endpoint Antivirus бағдарламасындағы Антифишингтік қорғау туралы қосымша ақпарат алу үшін [Білім қорының мақаласына](#) кіріңіз.

#### Фишингтік веб-сайтқа кіру

Танылған фишингтік веб-сайтқа кіргенде веб-браузерде келесі диалогтық терезе көрсетіледі. Веб-сайтқа бәрібір кіргіңіз келсе, **Сайтқа кіру** 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 шарттарын біріне не бірнешеуіне сай екендігін тексеріңіз:

- тіпті веб-сайт ашылмады,
- веб-сайт қауіп түрінде қате ашылды. Бұл жағдайда [Жалған фишингтік сайт туралы есеп беруге](#) болады.

Сондай-ақ, веб-сайтты электрондық пошта арқылы жібере аласыз. Электрондық пошта хабарын [samples@eset.com](mailto: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.

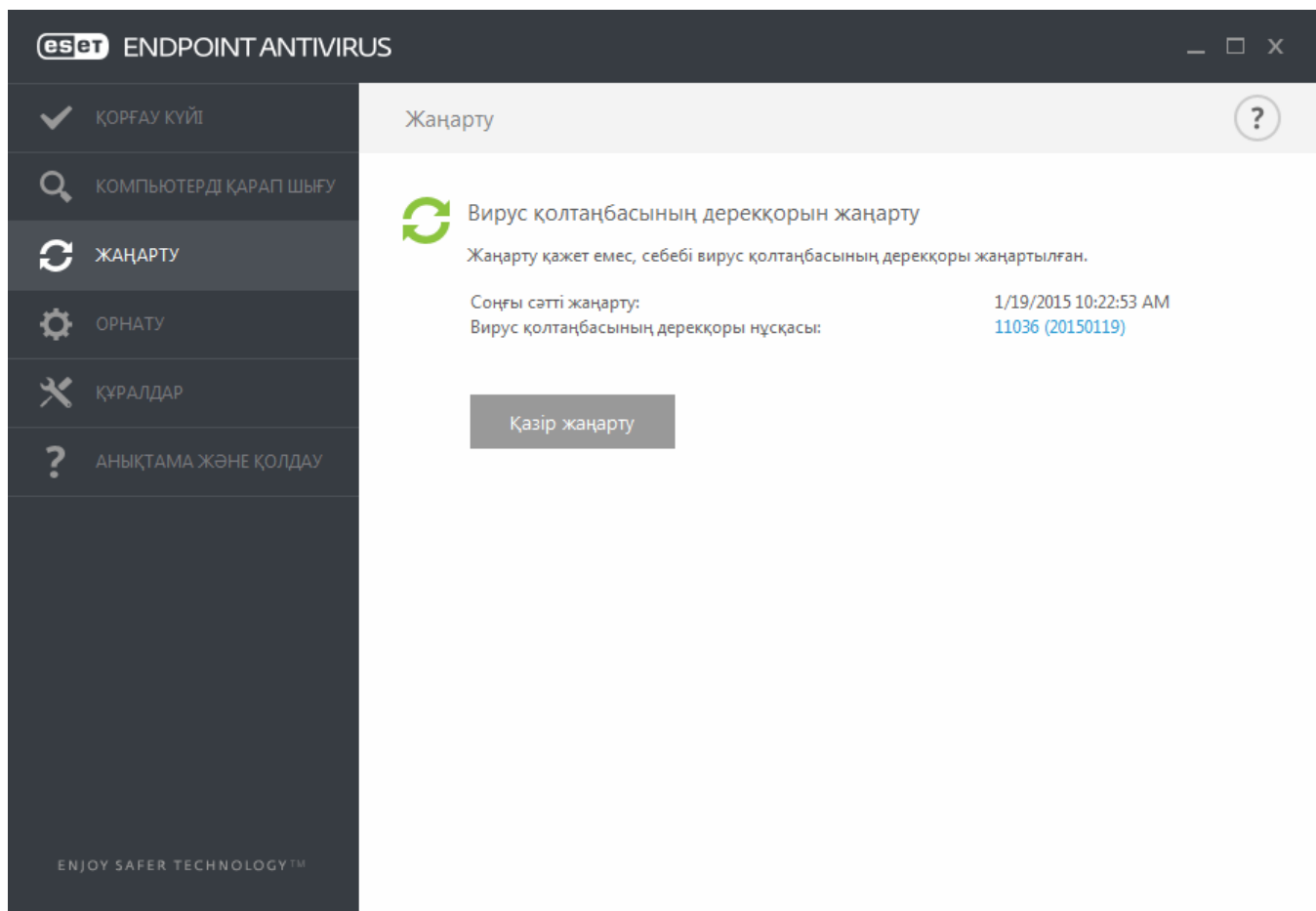
### 3.8.3 Бағдарламаны жаңарту

ESET Endpoint Antivirus бағдарламасын тұрақты түрде жаңарту – компьютерде қауіпсіздіктің ең жоғары деңгейіне жетудің ең жақсы әдісі. Жаңарту модулі бағдарлама әрдайым екі жолмен: вирус қолтаңбасының дерекқорын жаңарту және жүйелік компоненттерді жаңарту арқылы жаңартылып отыратынына кепілдік береді.

Негізгі бағдарлама терезесінде **Жаңарту** командасын таңдау арқылы ағымдағы жаңарту күйін, соның ішінде соңғы сәтті жаңартудың күні мен уақытын табуға және жаңарту керектігін не керек еместігін анықтауға болады. Сондай-ақ, негізгі терезеде вирус қолтаңбасы дерекқорының нұсқасы болады. Бұл сандық көрсеткіш – осы жаңартуға қосылған барлық қолтаңбалар тізілген ESET веб-торабына белсенді сілтеме.

Бұған қоса, жаңарту процесін қолмен таңдау опциясы **Вирус қолтаңбасының дерекқорын жаңарту** бар. Вирус қолтаңбасының дерекқорын жаңарту және бағдарлама компоненттерін жаңарту зиянды кодтан толық қорғауды жүргізудің маңызды бөліктері болып табылады. Олардың конфигурациясына және әрекетіне назар аударыңыз. Егер сіз орнату кезінде лицензия мәліметтерін енгізбесеңіз, ESET жаңарту серверлеріне қатынасу үшін жаңарту кезінде **Өнімді белсендіру** түймесін басу арқылы лицензия кілтін енгізе аласыз.

**ЕСКЕРТПЕ:** Лицензия кілтін ESET компаниясы ESET Endpoint Antivirus бағдарламасын сатып алудан кейін қамтамасыз етеді.



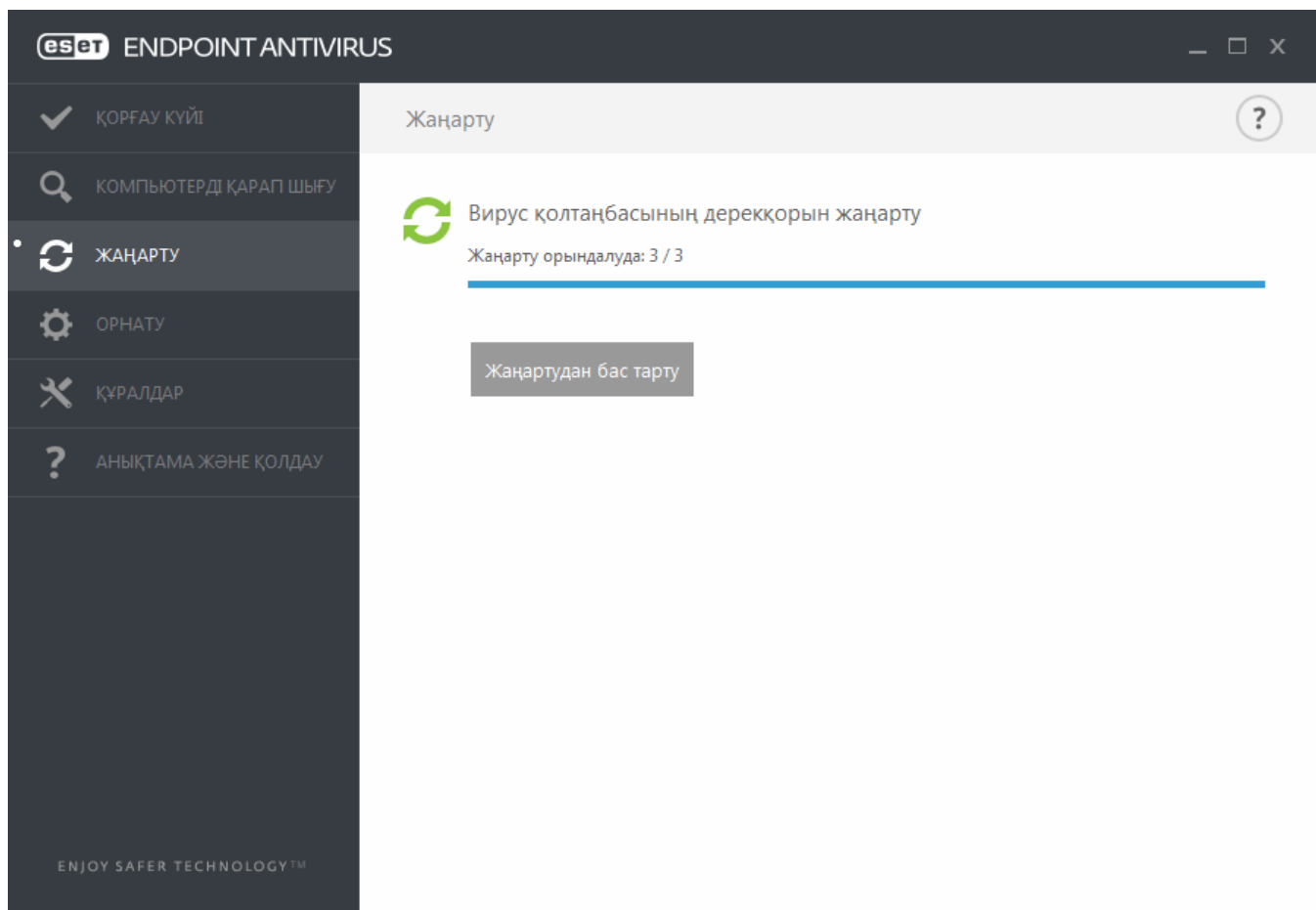
**Соңғы сәтті жаңарту** - Соңғы жаңартылған күн. Оның соңғы күнді көрсететінін тексеріңіз, яғни, вирус қолтаңбасының дерекқоры жаңа екенін тексеріңіз.

**Вирус қолтаңбасының дерекқоры нұсқасы** - Вирус қолтаңбасының дерекқорының нөмірі. Ол, сондай-ақ, ESET веб-торабына белсенді сілтеме болып табылады. Осы жаңартуға қосылған барлық қолтаңбалардың тізімін көру үшін оны басыңыз.



## Жаңарту үрдісі

**Вирус қолтаңбасының дерекқорын жаңарту** түймесін басқаннан кейін жүктеу үрдісі басталады. Жүктеудің орындалу жолағы мен жүктеуге дейін қалған уақыт көрсетіледі. Жаңартуды үзу үшін **Жаңартудан бас тарту** түймесін басыңыз.

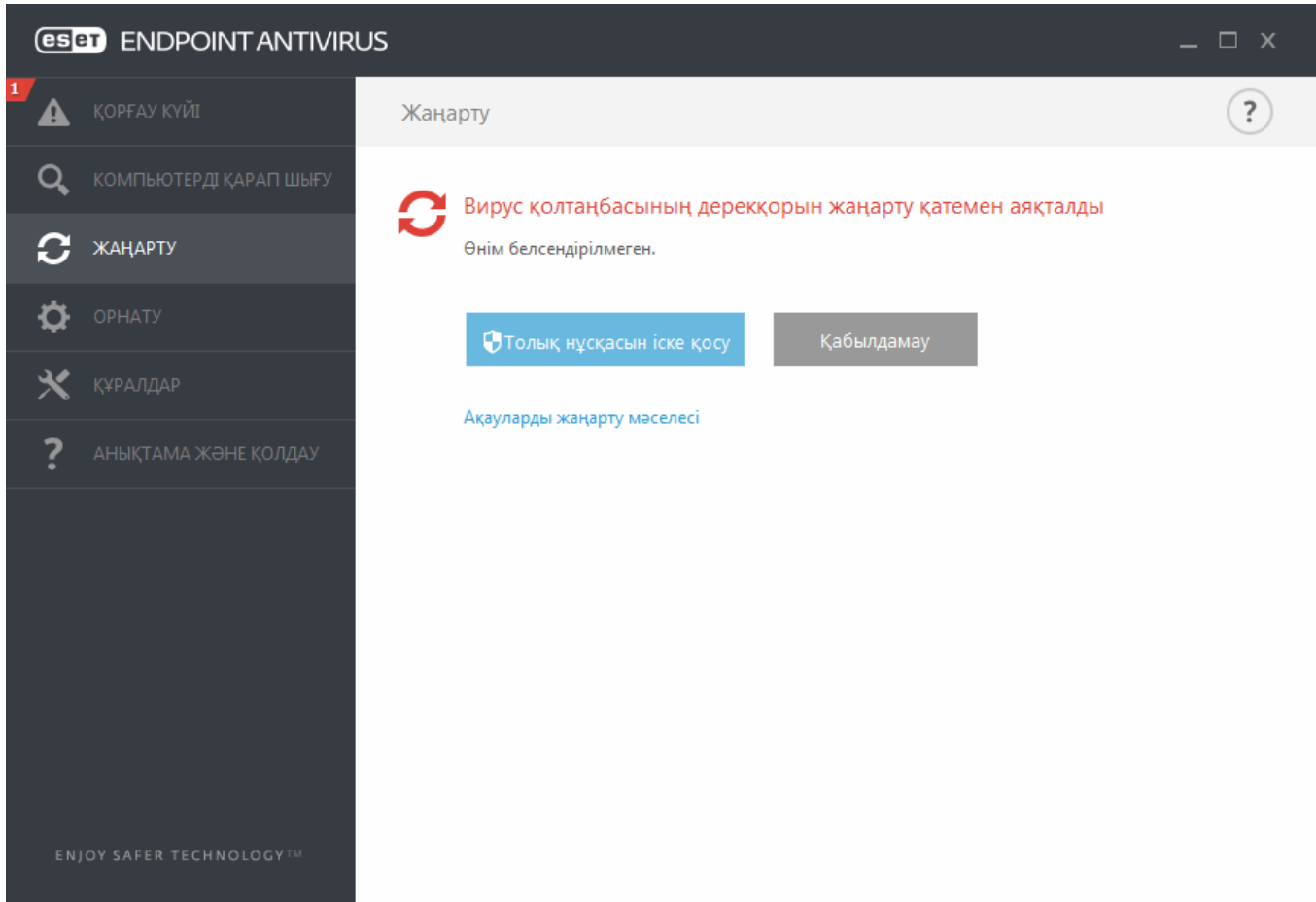


**Маңызды:** Қалыпты жағдайларда, жаңартулар тиісті түрде жүктелгенде, **Жаңарту** терезесінде **Жаңарту қажет емес, себебі орнатылған вирус қолтаңбасы жаңартылған дерекқор болып табылады** хабары пайда болады. Мұндай болмаған жағдайда, бағдарлама ескіріп және жұғу қаупі арта түседі. Вирус қолтаңбасының дерекқорын мүмкіндігінше жылдам жаңартыңыз. Әйтпесе, төмендегі хабарлардың біреуі көрсетіледі:

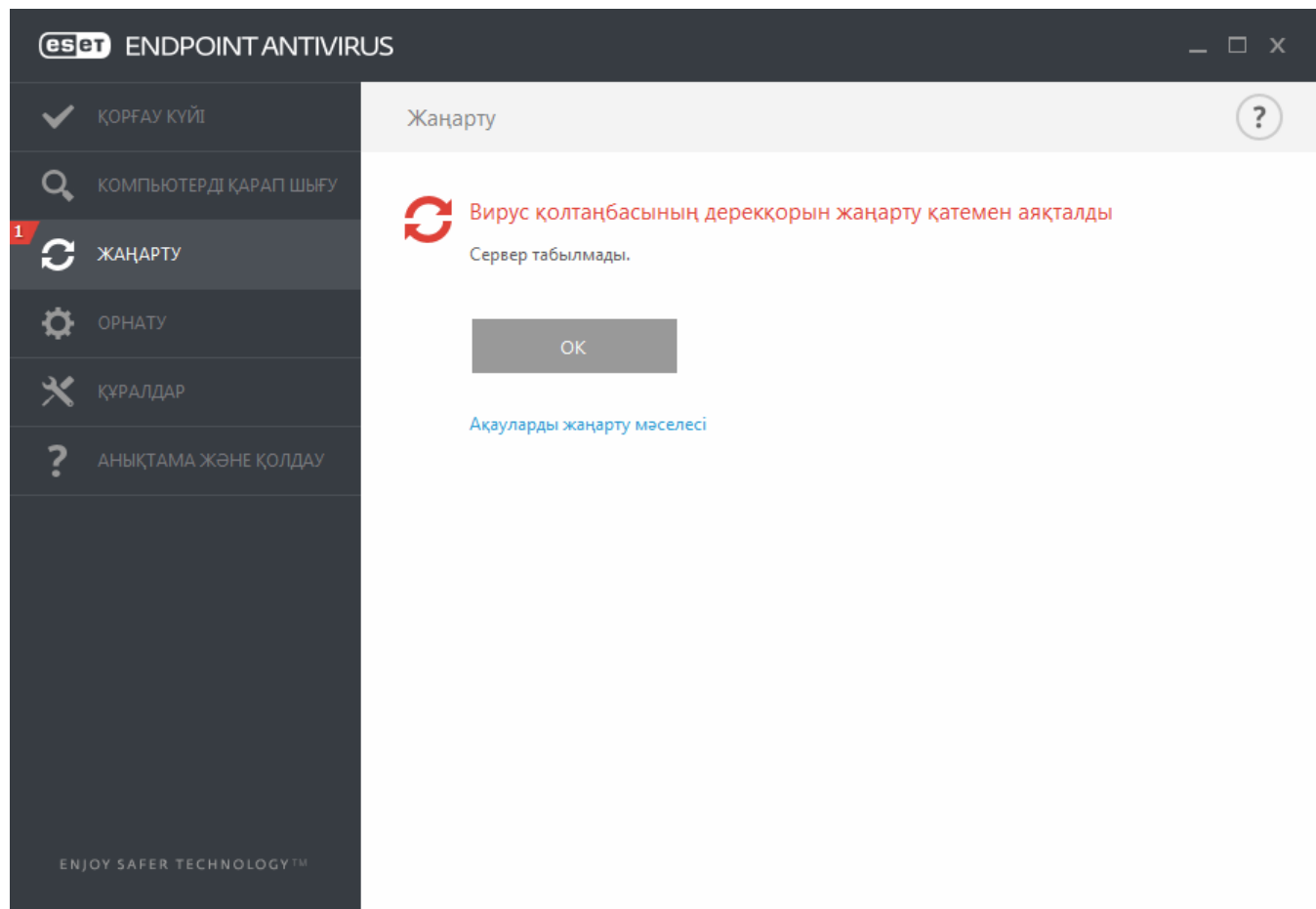
**Вирус қолтаңбасының дерекқоры ескірген** - Бұл қате вирус қолтаңбасының дерекқорын жаңартуға бірнеше сәтсіз әрекет жасалғаннан кейін шығады. Жаңарту параметрлерін тексеру ұсынылады. Бұл қатенің ең жиі себебі – дұрыс емес енгізілген аутентификациялау деректері немесе қате конфигурацияланған [қосылым параметрлері](#).

Алдыңғы хабарландыру сәтсіз жаңартулар туралы келесі екі **Вирус қолтаңбасының дерекқорын жаңарту сәтсіз болды** хабарына қатысты:

1. **Жарамсыз лицензия** - Жаңартуды орнату кезінде лицензия кілті дұрыс емес енгізілген. Аутентификациялау деректерін тексеру ұсынылады. «Кеңейтілген орнату» терезесі (негізгі мәзірде **Орнату** пәрменін, содан кейін **Кеңейтілген орнату** пәрменін басыңыз немесе пернетақтада F5 пернесін басыңыз) қосымша жаңарту опцияларын қамтиды. Жаңа лицензиялық кілтті енгізу үшін **Анықтама және қолдау** > **Лицензияны басқару** тармағын басыңыз.



2. **Жаңарту файлдарын жүктеу кезінде қате орын алды** - Қатенің ықтимал себебі – дұрыс емес [интернетке қосылым параметрлері](#). 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 мына [ESET білім қоры мақаласына](#) кіріңіз.

### 3.8.3.1 Жаңарту параметрлері

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 **Таңдалған профиль** ашылмалы мәзірінде көрсетіледі. Жаңа профиль жасау үшін **Профильдер тізімі** жанында **Өңдеу** түймесін басыңыз, содан кейін **Қосу** түймесін басып, жеке **Профиль атауы** енгізілуі керек.

Вирус қолтаңбасы дерекқорының жаңартуларын жүктеу әрекеті кезінде қиындық болса, уақытша жаңарту файлдарын/кэшті тазалау үшін **Тазалау** түймесін басыңыз.

#### Ескірген вирус қолтаңбасының дерекқоры туралы ескертулер

**Ең көп дерекқор жасын автоматты түрде орнату** - вирус қолтаңбасы дерекқоры туралы ескірген ретінде ең көбі қанша уақыттан (күндер түрінде) кейін есеп берілетінін орнатуға мүмкіндік береді. Әдепкі мән – 7.

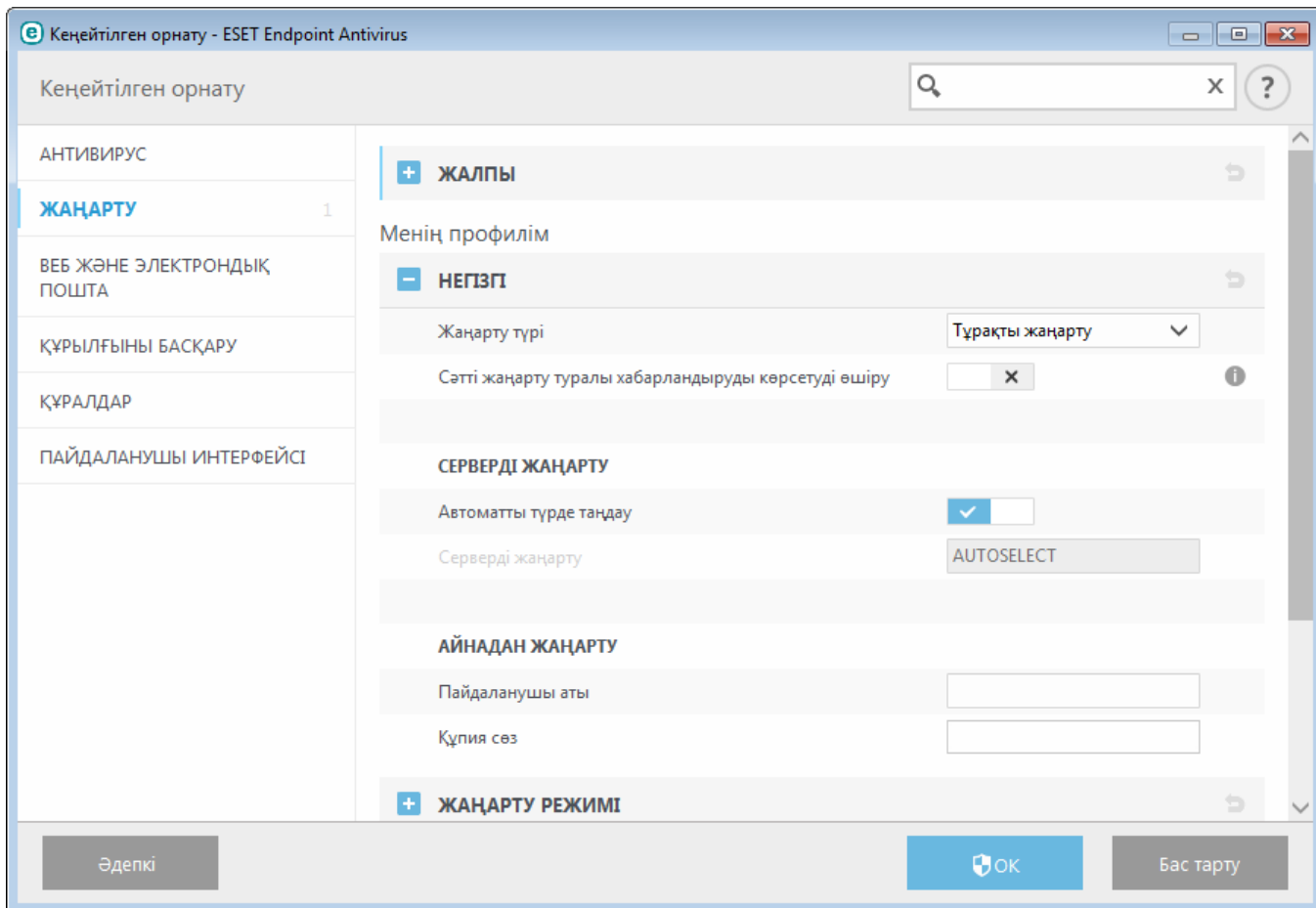
#### Қайтару

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

ESET Endpoint Antivirus бағдарламасы вирус қолтаңбасы дерекқорының лездік суреттері мен *қайтару* мүмкіндігімен

пайдалануға арналған бағдарлама модульдерін 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.

Егер **Қайтару (Кеңейтілген орнату (F5) > Жаңарту > Профиль)** түймесін бассаңыз, ашылмалы мәзірден вирус қолтаңбасы дерекқоры мен бағдарлама модулі жаңартулары кідірілетін уақыт аралығын көрсететін уақыт аралығын таңдауыңыз керек.



Жаңартулар сәйкесінше жүктелуі үшін барлық жаңарту параметрлерін дұрыс толтыру маңызды. Егер брендмауэр 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. **Көшірілген жаңарту** кезінде X сағат кешіктіру бар вирус дерекқорларының жаңа нұсқаларын қамтамасыз ететін арнайы жаңарту серверлерден жаңартуға мүмкіндік береді (яғни, дерекқорлар ағымдағы ортада сынақтан өткен және тиісінше сенімді деп есептеледі).

**Сәтті жаңарту туралы хабарландыру көрсетуді өшіру** - экранның төменгі оң жақ бұрышындағы жүйелік тақта хабарландыруын өшіреді. Толық экрандық бағдарлама немесе ойын орындалып жатқан жағдайда осы опцияны таңдау қолайлы. Көрсету режимі барлық хабарландыруларды өшіретінін ескеріңіз.

Әдепкі бойынша, **Жаңарту сервері** мәзірі АВТОТАҢДАУ опциясына орнатылады. Жаңарту сервері жаңартулар сақталатын орын болып табылады. ESET серверін пайдаланғанда әдепкі опцияны таңдалған күйде қалдыру ұсынылады.

Жергілікті HTTP серверін - сондай-ақ, айна ретінде белгілі - жаңарту серверін келесідей орнату керек:  
`http://computer_name_or_its_IP_address:2221.`

Жергілікті HTTP серверін SSL арқылы пайдаланғанда - жаңарту серверін келесідей орнату керек:  
`http://computer_name_or_its_IP_address:2221.`

Жергілікті ортақ қалтаны пайдаланғанда - жаңарту серверін келесідей орнату керек:  
`\\компьютер атауы немесе оның IP_мекенжайы\ортақ қалта`

### Айнадан жаңарту

Жаңарту серверлерінің түпнұсқалық растамасы сатып алудан кейін жасалған және сізге жіберілген **Лицензия кілтiне** негізделеді. Жергілікті айна серверді пайдаланғанда клиенттер жаңартулар алмай тұрып айна серверіне кіруіне арналған тіркелгі деректерін анықтауға болады. Әдепкі бойынша, тексеру қажет емес және **Пайдаланушы аты** және **Құпия сөз** өрістері бос қалады.

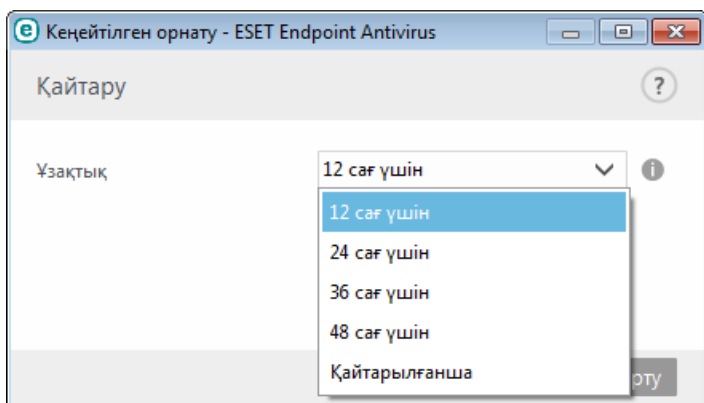
#### 3.8.3.1.1 Жаңарту профильдері

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

**Таңдалған профиль** ашылмалы мәзірі ағымдағы таңдалған профильді көрсетеді және **Менің профилім** күйіне әдепкіше орнатылған. Жаңа профиль жасау үшін **Профильдер тізімі** жанында **Өңдеу** түймесін басыңыз, содан кейін **Қосу** түймесін басып, жеке **Профиль атауы** енгізілуі керек.

#### 3.8.3.1.2 Қайтаруды жаңарту

Егер **Қайтару (Көңейтілген орнату (F5) > Жаңарту > Профиль)** түймесін бассаңыз, ашылмалы мәзірден вирус қолтаңбасы дерекқоры мен бағдарлама модулі жаңартулары кідірілетін уақыт аралығын көрсететін уақыт аралығын таңдауыңыз 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.

Вирус қолтаңбасының дерекқор нұсқасы ең ескі қол жетімді нұсқаға дейін төмендетіледі және жергілікті компьютердің файл жүйесінде лездік сурет түрінде сақталады.

**Мысал:** 10646 саны вирус қолтаңбасы дерекқорының ең соңғы нұсқасы болып табылсын. 10645 және 10643 вирус қолтаңбасы дерекқорының лездік суреттері ретінде сақталған. Назар аударыңыз, мысалы, компьютер өшірілгендіктен және 10644-тан бұрын жүктелген соңғы жаңарту қол жетімді болғандықтан 10644 қол жетімді емес. Егер **Жергілікті сақталған лездік лездік суреттердің саны** өрісі 2 санына орнатылған болса және сіз **Қайтару** түймесін бассаңыз, вирус қолтаңбасы дерекқоры (бағдарлама модульдерін қоса) 10643 нұсқасына дейін қалпына келтіріледі. Бұл процесс біраз уақыт алуы мүмкін. Вирус қолтаңбасының дерекқор нұсқасы **Жаңарту** бөлімінен ESET Endpoint Antivirus бағдарламасының негізгі мәзір терезесінен төмендетілгеніне көз жеткізіңіз.

### 3.8.3.1.3 Жаңарту режимі

**Жаңарту режимі** қойындысы бағдарлама компоненттерін жаңартуға қатысты опцияларды қамтиды. Жаңа бағдарлама компоненттерін жаңартуы қол жетімді болғанда, бағдарлама өз тәртібін алдын ала анықтау мүмкіндігін береді.

Бағдарлама компонентін жаңартулары жаңа мүмкіндіктер береді немесе алдыңғы нұсқалардан қалған мүмкіндіктерді өзгертеді. Бұл пайдаланушының араласуынсыз автоматты түрде орындалады немесе хабарландырылуды таңдауыңызға болады. Бағдарлама компонентін жаңарту орнатылғаннан кейін қайта іске қосу қажет болуы мүмкін. **Бағдарлама компоненттерін жаңарту** бөлімінде үш опция қол жетімді:

- **Бағдарлама компоненттерін жүктеу алдында сұрау** - Әдепкі опция. Қол жетімді болғанда бағдарлама компоненттерін жаңартуларды растау немесе бас тарту сұралады.
- **Бағдарлама компоненттерін әрдайым жаңарту** - Бағдарлама компоненттерін жаңарту жүктеліп, автоматты түрде орнатылады. Компьютерді қайта іске қосу қажет етілуі мүмкіндігін естен шығармаңыз.
- **Бағдарлама компоненттерін еш қашан жаңартпау** - Бағдарлама компоненттерін жаңарту мүлде орнатылмайды. Серверлер әдетте тек пайдаланылу барысында іске қосыла алатындықтан, бұл параметр серверді орнатуларына үйлесімді болып табылады.

**ЕСКЕРТПЕ:** Ең тиісті опцияны таңдау параметрлер қолданылатын жұмыс станциясына байланысты. Жұмыс станциялары мен серверлердің арасында айырмашылық болатынын ұмытпаңыз, мысалы бағдарламаны жаңартқаннан кейін серверді автоматты түрде қайта қайта іске қосу күрделі зақым келтіруі мүмкін.

**Жаңартуды жүктеу алдында сұрау** опциясына құсбелгі қойылған болса, жаңа жаңарту қол жетімді болғанда хабарландыру көрсетіледі.

Жаңарту файлының өлшемі **Жаңарту файлы (КБ) үлкенірек болғанда сұрау** өрісінде көрсетілген мәннен үлкенірек болса, бағдарлама хабарландыруды көрсетеді.

### 3.8.3.1.4 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** опциясы «Кеңейтілген орнату» тармағының **Құралдар > Прокси сервер** тармағында көрсетілген прокси сервер конфигурациясы опцияларын пайдаланады.

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

**Прокси сервер арқылы қосылу** опциясын келесі жағдайларда таңдау керек:

- Прокси серверді ESET Endpoint Antivirus бағдарламасын жаңарту үшін пайдалану керек, ол ғаламдық параметрлерде көрсетілген прокси серверден (**Құралдар > Прокси сервер**) басқа. Солай болса, параметрлерді мына жерде көрсету керек: **Прокси сервер** мекенжайы, байланыс **Порт** (әдепкі бойынша, 3128), оған қоса, қажет болса, прокси-сервер үшін **Пайдаланушы аты** және **Құпия сөз**.
- Прокси сервер параметрлері ғаламдық деңгейде орнатылмаған, бірақ ESET Endpoint 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 жеткізушісіңіз (ISP) өзгертсеңіз), осы терезеде тізімделген HTTP қатынас модулі параметрлерінің дұрыс екенін тексеріңіз. Кері жағдайда бағдарлама жаңарту серверіне қосыла алмайды.

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

**ЕСКЕРТПЕ:** **Пайдаланушы аты** және **Құпия сөз** сияқты түпнұсқалық растамасы деректері прокси серверге қатынасуға арналған. Егер пайдаланушы аты мен құпия сөз қажет болған жағдайда осы өрістерді толтырыңыз. Бұл өрістер ESET Endpoint Antivirus бағдарламасының пайдаланушы атына/құпия сөзіне арналмағандығын және прокси сервер арқылы интернетке кіру үшін құпия сөз керек екенін білсеңіз ғана толтыру керек екенін ескеріңіз.

### 3.8.3.1.5 Жергілікті желіге былайша қосылу

the Windows NT операциялық жүйесі орнатылған жергілікті серверден жаңартқанда түпнұсқалық растамасы әдепкі бойынша әр желілік қосылым үшін талап етіледі.

Мұндай есептік жазбаны теңшеу үшін **Жергілікті пайдаланушы түрі** ашылмалы мәзірінен таңдаңыз:

- **Жүйелік есептік жазба (әдепкі),**
- **Ағымдағы пайдаланушы,**
- **Көрсетілген пайдаланушы.**

Түпнұсқалық растама үшін жүйелік есептік жазбаны пайдалану үшін **Жүйелік есептік жазба (әдепкі)** опциясын таңдаңыз. Әдетте, егер негізгі жаңарту параметрлері бөлігінде түпнұсқалық растама деректері жоқ болса, мұндай түпнұсқалық растама орындалмайды.

Бағдарламаның қазір кірген пайдаланушылық есептік жазбаны пайдаланып түпнұсқалықты растауын қамтамасыз ету үшін **Ағымдағы пайдаланушы** опциясын таңдаңыз. Осы шешімнің бірде-бір кедергісі – егер пайдаланушы кірмеген болса, бағдарлама жаңарту серверіне қосыла алмайды.

Түпнұсқалық растамада белгіленген пайдаланушы жазбасын пайдалануды қаласаңыз, **Көрсетілген пайдаланушы** тармағын таңдаңыз. Әдепкі жүйенің жазбасы сәтсіз болғанда осы әдісті пайдаланыңыз. Арнайы пайдаланушының есептік жазбасы жергілікті сервердегі жаңарту файлдары каталогына қатынасы болуы керек. Кері жағдайда бағдарлама қосылымды орната алмайды, жаңартуларды қотара алмайды.

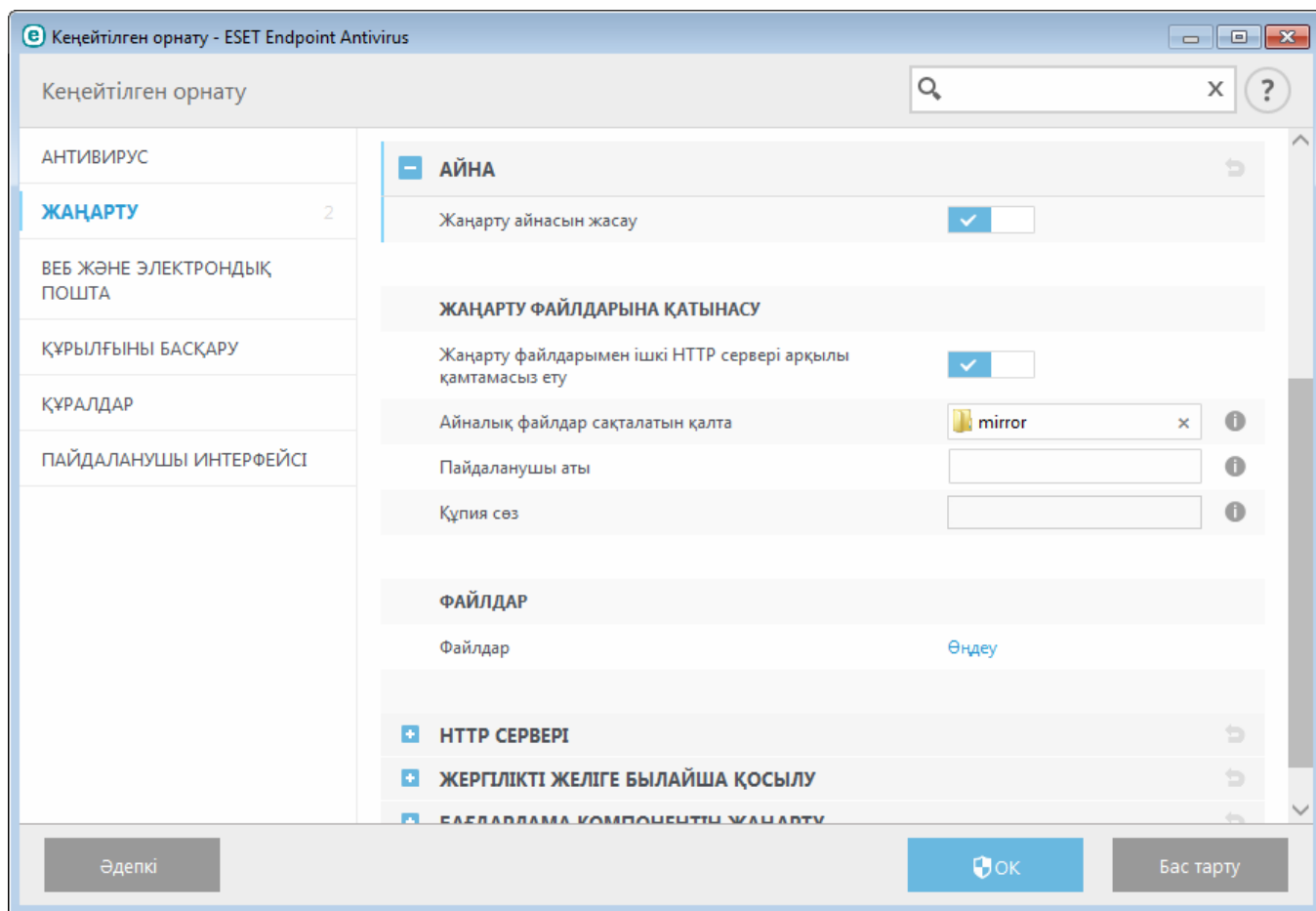
**Ескерту:** **Ағымдағы пайдаланушы** немесе **Көрсетілген пайдаланушы** опциясы таңдалғанда, бағдарлама мәліметтерін қалаған пайдаланушыға өзгерткенде қате болуы мүмкін. Негізгі жаңарту параметрлері бөлігінде LAN аутентификация деректерін енгізуді ұсынамыз. Бұл жаңарту параметрлері бөлігінде түпнұсқалық деректер келесідегідей енгізілуі тиіс: *domain\_name\user* (егер бұл жұмыс тобы болса, *workgroup\_name\name* енгізіңіз) және құпиясөз. Жергілікті серверінің HTTP нұсқасынан жаңартқанда түпнұсқалықты анықтау қажет емес.

Сервер байланысы жаңартулар жүктелгеннен кейін де белсенді болып қалса, **Жаңартудан кейін серверден ажырату** опциясын таңдаңыз.

### 3.8.3.1.6 Айна

ESET Endpoint Antivirus сізге желідегі басқа жұмыс станцияларды жаңарту үшін пайдалануға болатын жаңарту файлдарының көшірмелерін жасауға мүмкіндік береді. «*Айнаны*», яғни жаңарту файлдарының көшірмесін жергілікті желі ортасында жасау ыңғайлы, өйткені жаңарту файлдарын жеткізушінің жаңарту серверінен әр жұмыс станциясы арқылы қайталап жүктеу қажет емес. Жаңартулар жергілікті айна серверіне жүктеледі, содан кейін барлық жұмыс станцияларына таратылады, осылайша ықтимал желі трафигінің шамадан тыс жүктелуіне жол бермейді. Клиенттік жұмыс станцияларын айнадан жаңарту желінің жүктеу теңдестігін оңтайландырады және интернетке қосылу тармақтарын сақтайды.

Жергілікті айна сервері үшін конфигурация опцияларына «Кеңейтілген орнату» ішінде **Жаңарту** астында қатынасуға болады. «Кеңейтілген орнату» бөліміне қатынасу үшін **F5** пернесін басыңыз, **Жаңарту** түймесін басыңыз және **Айна** қойындысын таңдаңыз.



Клиенттік жұмыс станциясында айнаны жасау үшін **Жаңарту айнасын жасау** параметрін қосыңыз. Бұл опцияны қосу басқа айна конфигурациясы опцияларын іске қосады, мысалы, жаңарту файлдарына қатынасу жолы және айна файлдардың жаңарту жолы.

### Жаңарту файлдарына қатынасу

**Жаңарту файлдарын ішкі HTTP сервері арқылы қамтамасыз ету** - қосылған болса, жаңарту файлдарына HTTP арқылы қатынасуға болады, тіркелгі деректері қажет болмайды.

**ЕСКЕРТПЕ:** Windows XP жүйесі HTTP серверін пайдалану үшін 2 немесе одан кейінгі жаңарту бумасын қажет етеді.

Айна серверіне қатынасу әдістері [Айнадан жаңарту](#) бөлімінде егжей-тегжейлі сипатталады. Айнаға қатынасудың екі негізгі әдісі бар — жаңарту файлдары бар қалтаны ортақ желілік қалта ретінде көрсетуге болады немесе клиенттер HTTP серверінде орналасқан айнаға қатынасуға болады.

Айна үшін жаңарту файлдарын сақтауға арналған қалта **Айна файлдар сақталатын қалта** бөлімінде анықталады. Жергілікті компьютердегі қалтаға немесе ортақ желілік қалтаға өту үшін **Қалта** түймесін басыңыз. Егер көрсетілген қалта үшін түпнұсқалықты растау қажет болса, **Пайдаланушы аты** және **Құпия сөз** өрістерінде түпнұсқалықты растау деректерін енгізу керек. Егер таңдалған мақсатты қалта Windows NT/2000/XP амалдық жүйесі орнатылған желілік дискіде орналасқан болса, көрсетілген пайдаланушы аты мен құпия сөз таңдалған қалталар үшін артықшылықтарға ие болуы тиіс. Пайдаланушы аты мен құпия сөзді *Домен/пайдаланушы* немесе *Жұмыс тобы/пайдаланушы* пішімінде енгізу керек. Сәйкес құпиясөзді енгізуді ұмытпаңыз.

**Файлдар** - айнаны теңшеп жатқанда жүктеу керек жаңартулардың тіл нұсқаларын көрсетуге болады. Таңдалған тілдерді пайдаланушы теңшеген айна сервері қолдауы керек.

### HTTP сервері

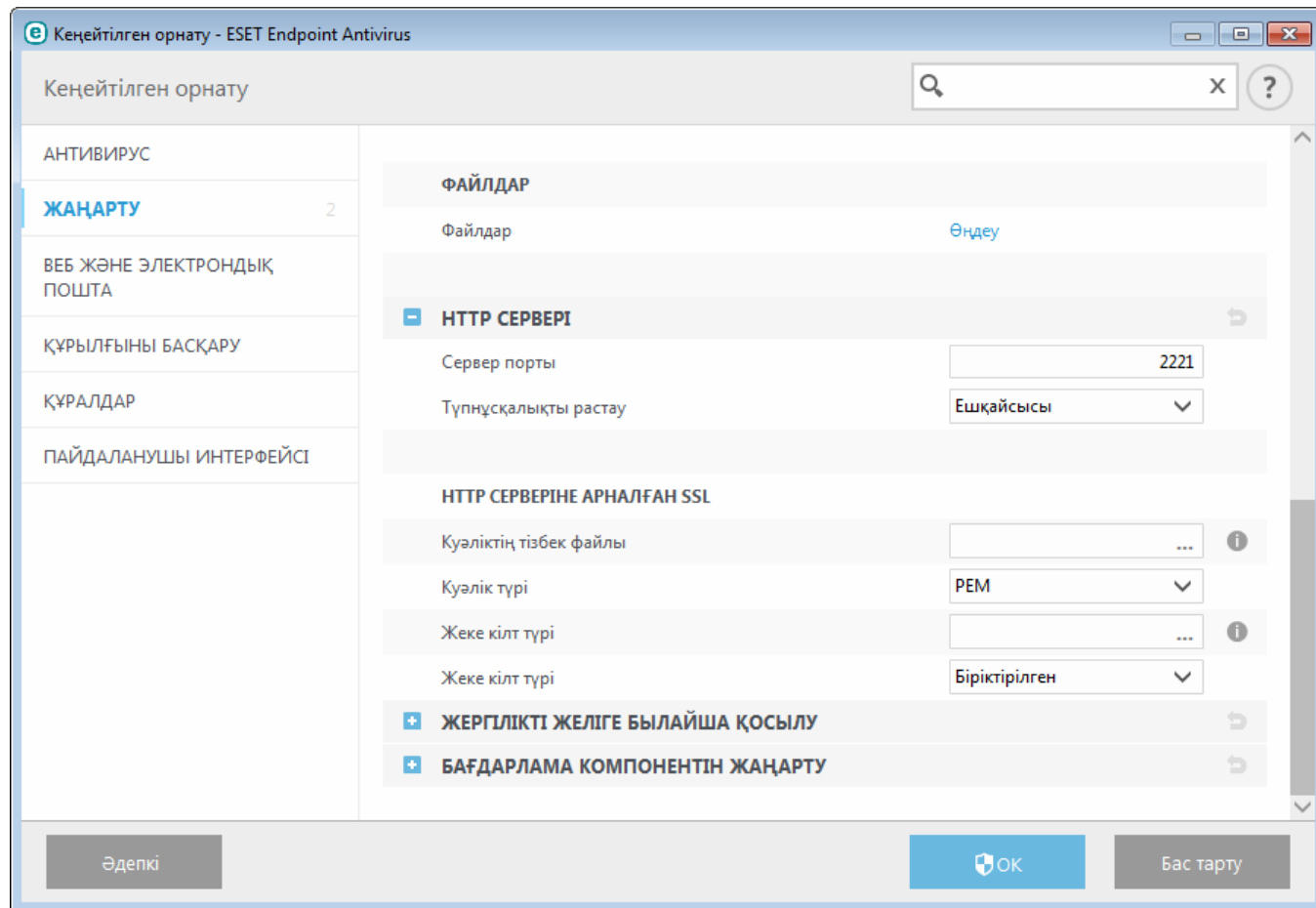
**Сервер порты** - әдепкі бойынша сервер порты 2221 деп орнатылады.

**Түпнұсқалық растама** - жаңарту файлдарына қатынасу үшін пайдаланылатын түпнұсқалықты растау әдісін анықтайды. Мына опциялар қол жетімді: **Еш қандай**, **Негізгі** және **NTLM**. Негізгі пайдаланушы атымен және құпиясөзбен аутентификациялаумен бірге «base64» кодтауды пайдалану үшін **Негізгі** опциясын таңдаңыз. **NTLM** опциясы қауіпсіз кодтау әдісін пайдаланады. Түпнұсқалық растамасы үшін пайдаланушы жұмыс станцияларында



жасаған ортақ жаңарту файлдары пайдаланылады. Әдепкі параметр – **Еш қандай**, ол аутентификациялау қажеттілігінсіз жаңарту файлдарына қатынасты береді.

**Куәліктің тізбек файлын** бекітіңіз немесе HTTPS (SSL) қолдауы бар HTTP серверін іске қосқыңыз келсе, өздігінен қол қойылатын куәлікті жасаңыз. Келесі куәлік түрлері қол жетімді: ASN, PEM және PFX. Қосымша қауіпсіздік үшін жаңарту файлдарын жүктеу үшін HTTPS протоколын пайдалануға болады. Осы протоколды пайдалану арқылы кіру тіркелгі деректерін және деректерді тасымалдауды аңғару мүмкін емес дерлік. **Құпия кілт түрі** опциясы әдепкі бойынша **Біріктірілген** параметріне орнатылған (сондықтан, **Құпия кілт файлы** опциясы әдепкі бойынша өшірулі болады). Яғни, құпия кілт — таңдалған куәлік тізбегі файлының бөлігі.



#### – Жергілікті желіге былайша а қосылу

**Жергілікті пайдаланушы түрі** - **Жүйелік есептік жазба (әдепкі)**, **Ағымдағы пайдаланушы** және **Көрсетілген пайдаланушы** параметрлері сәйкес ашылмалы мәзірлерінде көрсетіледі. **Пайдаланушы аты** және **Құпия сөз** параметрлері міндетті емес болып табылады. Сондай-ақ, [Жергілікті желіге былайша қосылу](#) бөлімін қараңыз.

Сервер байланысы жаңартулар жүктелгеннен кейін де белсенді болып қалса, **Жаңартудан кейін серверден ажырату** опциясын таңдаңыз.

#### – Бағдарлама компоненттерін жаңарту

**Компоненттерді автоматты түрде жаңарту** - жаңа мүмкіндіктерді және бар мүмкіндіктердің жаңартуларын орнатуға мүмкіндік береді. Жаңарту пайдаланушының араласуынсыз автоматты түрде орындалады немесе хабарландырылуды таңдауыңызға болады. Бағдарлама компонентін жаңарту орнатылғаннан кейін қайта іске қосу қажет болуы мүмкін.

**Компоненттерді қазір жаңарту** - бағдарлама компоненттерін соңғы нұсқаға жаңартады.

### 3.8.3.1.6.1 Айнадан жаңарту

Негізінен клиенттер жаңарту файлдарын жүктей алатын репозиторий болып табылатын айнаны теңшеудің екі негізгі әдісі бар. Жаңарту файлдары бар қалтаны ортақ желілік қалта немесе HTTP сервері ретінде көрсетуге болады.

#### Айнаға ішкі HTTP серверін пайдаланып қатынасу

Бұл конфигурация – әдепкі, ол алдын ала анықталған бағдарлама конфигурациясында көрсетілген. HTTP серверін пайдаланып айнаға қатынасуға рұқсат ету үшін **Кеңейтілген орнату > Жаңарту > Айна** тармағына өтіп, **Жаңарту айнасын жасау** опциясын таңдаңыз.

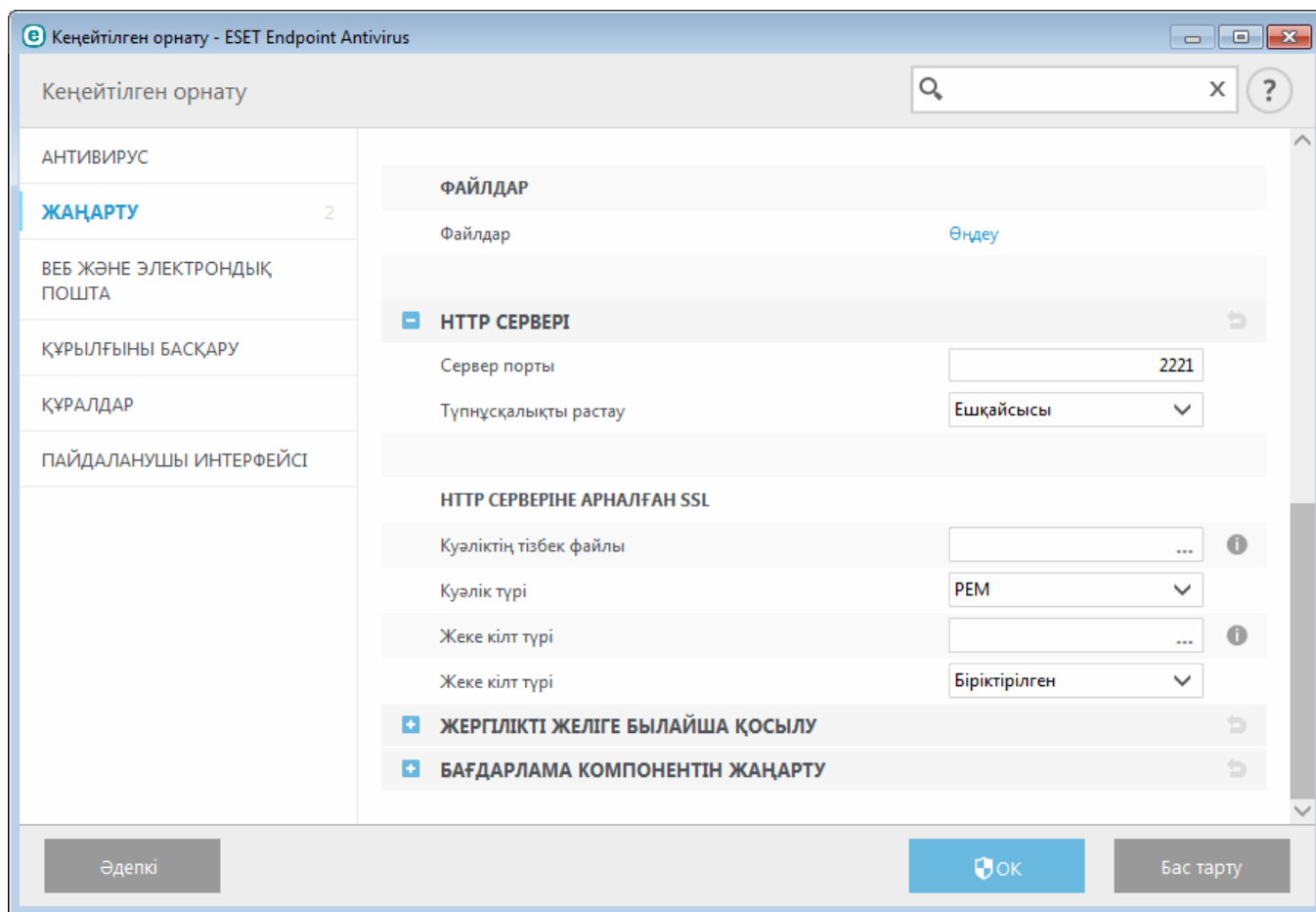
**Айна** қойындысының **HTTP сервері** бөлімінде HTTP сервері тыңдайтын **Сервер портын**, сонымен бірге HTTP сервері пайдаланаатын **Түпнұсқалық растама** түрін көрсетуге болады. Әдепкі бойынша, сервер порты **2221** деп орнатылады. **Түпнұсқалық растама** опциясы жаңарту файлдарына қатынасу үшін пайдаланылатын түпнұсқалықты растау әдісін анықтайды. Мына опциялар қол жетімді: **Еш қандай**, **Негізгі** және **NTLM**. Негізгі пайдаланушы атымен және құпиясөзбен аутентификациялаумен бірге «base64» кодтауды пайдалану үшін **Негізгі** опциясын таңдаңыз. **NTLM** опциясы қауіпсіз кодтау әдісін пайдаланады. Түпнұсқалық растамасы үшін пайдаланушы жұмыс станцияларында жасаған ортақ жаңарту файлдары пайдаланылады. Әдепкі параметр – **Еш қандай**, ол түпнұсқалықты растау қажеттілігінсіз жаңарту файлдарына қатынасты береді.

**Ескерту:** Егер жаңарту файлдарына «HTTP» сервері арқылы кіруге рұқсат еткіңіз келсе, «Айна» қалтасы дәл оны жасайтын ESET Endpoint Antivirus бағдарлама орналасқан компьютерде болуы керек.

#### HTTP серверіне арналған SSL

**Куәліктің тізбек файлын** бекітіңіз немесе HTTPS (SSL) қолдауы бар HTTP серверін іске қосқыңыз келсе, өздігінен қол қойылатын куәлікті жасаңыз. Келесі куәлік түрлері қол жетімді: **PEM**, **PFX** және **ASN**. Қосымша қауіпсіздік үшін жаңарту файлдарын жүктеу үшін HTTPS протоколын пайдалануға болады. Осы протоколды пайдалану арқылы кіру тіркелгі деректерін және деректерді тасымалдауды аңғару мүмкін емес дерлік. **Жеке кілт түрі** әдепкі бойынша **Біріктірілген** күйіне орнатылады, яғни жеке кілт таңдалған куәлік тізбегі файлының бөлігі болып табылады.

**ЕСКЕРТПЕ:** Айнадан вирус қолтаңбасы дерекқорын жаңартудың бірнеше сәтсіз әрекетінен кейін басты мәзірде «Жаңарту» тақтасында **Жарамсыз пайдаланушы аты және/немесе құпия сөз** қатесі көрсетіледі. **Кеңейтілген орнату > Жаңарту > Айна** тармағына өту және пайдаланушы аты мен құпия сөзді тексеру ұсынылады. Осы қатенің ең жиі кездесетін себебі — дұрыс емес енгізілген аутентификация деректері.



Айна сервер конфигурацияланғаннан кейін клиенттік жұмыс станцияларында жаңа жаңарту серверін қосу керек. Мұны істеу үшін төмендегі қадамдарды орындаңыз:

- **Keңейтілген орнату** (F5) тармағына өтіп, **Жаңарту** > **Негізгі** тармағын басыңыз.
- **Автоматты түрде таңдау** параметрінен таңдауды алыңыз және келесі пішімдердің біреуін пайдаланып **Серверді жаңарту** өрісіне жаңа серверді қосыңыз:  
`http://IP_address_of_your_server:2221`  
`https://IP_address_of_your_server:2221` (SSL пайдаланылса)

#### Айнаға жүйелік ортақ қалта арқылы қатынасу

Алдымен, жергілікті немесе желі құрылғысында ортақ қалта жасалуы қажет. «Айна» үшін қалтаны жасап жатқанда, жаңарту файлдарын қалтаға сақтайтын пайдаланушыларға «жазу» қатынасу рұқсатын, ал «Айна» қалтасынан ESET Endpoint Antivirus бағдарламасын жаңартатын барлық пайдаланушыларға «оқу» қатынасу рұқсатын беру керек.

Содан кейін **Keңейтілген орнату** > **Жаңарту** > **Айна** қойындысында **Ішкі НТТР сервері арқылы жаңарту файлдарын қамтамасыз ету** опциясын өшіру арқылы айнаға қатынасты теңшеңіз. Бағдарлама орнату бумасында бұл опция әдепкі мәні бойынша қосылады.

Егер ортақ қалта желідегі басқа компьютерде орналасқан болса, басқа компьютерге кіру үшін аутентификация деректерін енгізу керек. Түпнұсқалық растама деректерін енгізу үшін ESET Endpoint Antivirus **Keңейтілген орнату** (F5) тармағын ашып, **Жаңарту** > **Жергілікті желіге былайша қосылу** тармағын басыңыз. Бұл параметр дәл жаңарту параметріндей, [Жергілікті желіге былайша қосылу](#) бөлімінде сипатталған.

Айнаны конфигурациялау аяқталғаннан кейін клиенттік жұмыс станцияларында төмендегі қадамдарды пайдаланып `\\UNC\PATH` жаңарту сервері ретінде орнатыңыз:

1. ESET Endpoint Antivirus **Keңейтілген орнату** тармағын ашып, **Жаңарту** > **Негізгі** тармағын басыңыз.
2. **Жаңарту сервері** өрісін басып, жаңа серверді `\\UNC\PATH` пішімін пайдаланып қосыңыз.

**ЕСКЕРТПЕ:** Дұрыс қызмет етуі үшін айна қалтасына жолды UNC жолы ретінде көрсету керек. Көрсетілген дискілердегі жаңартулар жұмыс істемеуі мүмкін.

Соңғы бөлім бағдарлама компоненттерін (PCUs) басқарады. Әдепкі бойынша жүктелген бағдарлама компоненттері жергілікті айнаға көшірілуге дайын. Егер **Бағдарлама компонентін жаңарту** құсбелгісі таңдалған болса, **Жаңарту**

түймесін басудың қажеті жоқ, өйткені файлдар қол жетімді болған кезде автоматты түрде жергілікті айнаға көшіріледі. Бағдарлама компоненттерін жаңарту туралы толық мәлімет алу үшін [Жаңарту режимі](#) бөлімін қараңыз.

### 3.8.3.1.6.2 Айна жаңарту ақаулықтарын жою

Көбінесе айна серверден жаңарту кезіндегі қиындықтар мына мәселелердің бірі не бірнешеуі себепті туындайды: Айна қалта параметрлерін дұрыс сипаттамау, Айна қалтадағы дұрыс емес түпнұсқалық растама деректері, айна файлдарды айнадан жүктейтін жергілікті жұмыс стансалардағы дұрыс емес конфигурация немесе жоғарыдағы себептердің тіркесімі. Төменде Айнадан жаңарту кезінде келіп шығуы мүмкін өте жиі кездесетін ақаулықтардың қысқаша сипаттамасы ұсынылады:

**ESET Endpoint Antivirus Айна серверге қосылуға қатысты қате туралы есеп береді** - жергілікті жұмыс стансалары жаңартуларды жүктеп алатын жаңарту серверінің (айна қалтадағы желінің жолы) қате сипаттамасы себеп болатын сияқты. Қалтаны тексеру үшін Windows **Бастау** мәзірін, **Іске қосу** түймесін басып, қалта атын енгізіңіз де, **ОК** түймесін басыңыз. Қалтаның мазмұны көрсетілуі керек.

**ESET Endpoint Antivirus пайдаланушы аты мен құпиясөзді қажет етеді** - Жаңарту бөлімінде қате түпнұсқалық растама деректерімен (пайдаланушы аты және құпиясөз) туындайтынға ұқсайды. Пайдаланушы аты мен құпиясөз бағдарлама өзін жаңартатын жаңарту серверіне қатынастыру үшін пайдаланылады. Түпнұсқалық растама деректерінің дұрыс екеніне және дұрыс пішімде енгізілгеніне көз жеткізіңіз. Мысалы, *Домен/Пайдаланушы аты* немесе *Жұмыс тобы/Пайдаланушы аты*, сонымен қатар, сәйкес құпиясөздер. Егер Айна сервер "Барлығына" қолжетімді болса да, кез келген пайдаланушының кіруіне рұқсат берілмейтінін ұмытпаңыз. "Барлығы" қандай да бір авторизацияланбаған пайдаланушыны білдірмейді, ол қалтаның барлық домен пайдаланушыларына қолжетімді екінін білдіреді. Нәтижесінде қалта "Барлығына" қолжетімді болса, домен пайдаланушысының аты мен құпиясөз жаңарту параметрлері бөлімінде бәрібір енгізілуі керек.

**ESET Endpoint Antivirus Айна серверге қосылуға қатысты қате туралы есеп береді** - айнаның HTTP нұсқасына қатынасу үшін анықталған порттағы байланыс бұғатталған.

### 3.8.3.2 Жаңарту тапсырмаларын жасау туралы

Негізгі мәзірден **Жаңарту** түймешігін басқаннан кейін көрсетілетін негізгі терезеден **Вирус қолтаңбасының дерекқорын жаңарту** тармағын басу арқылы жаңартуларды бастауға болады.

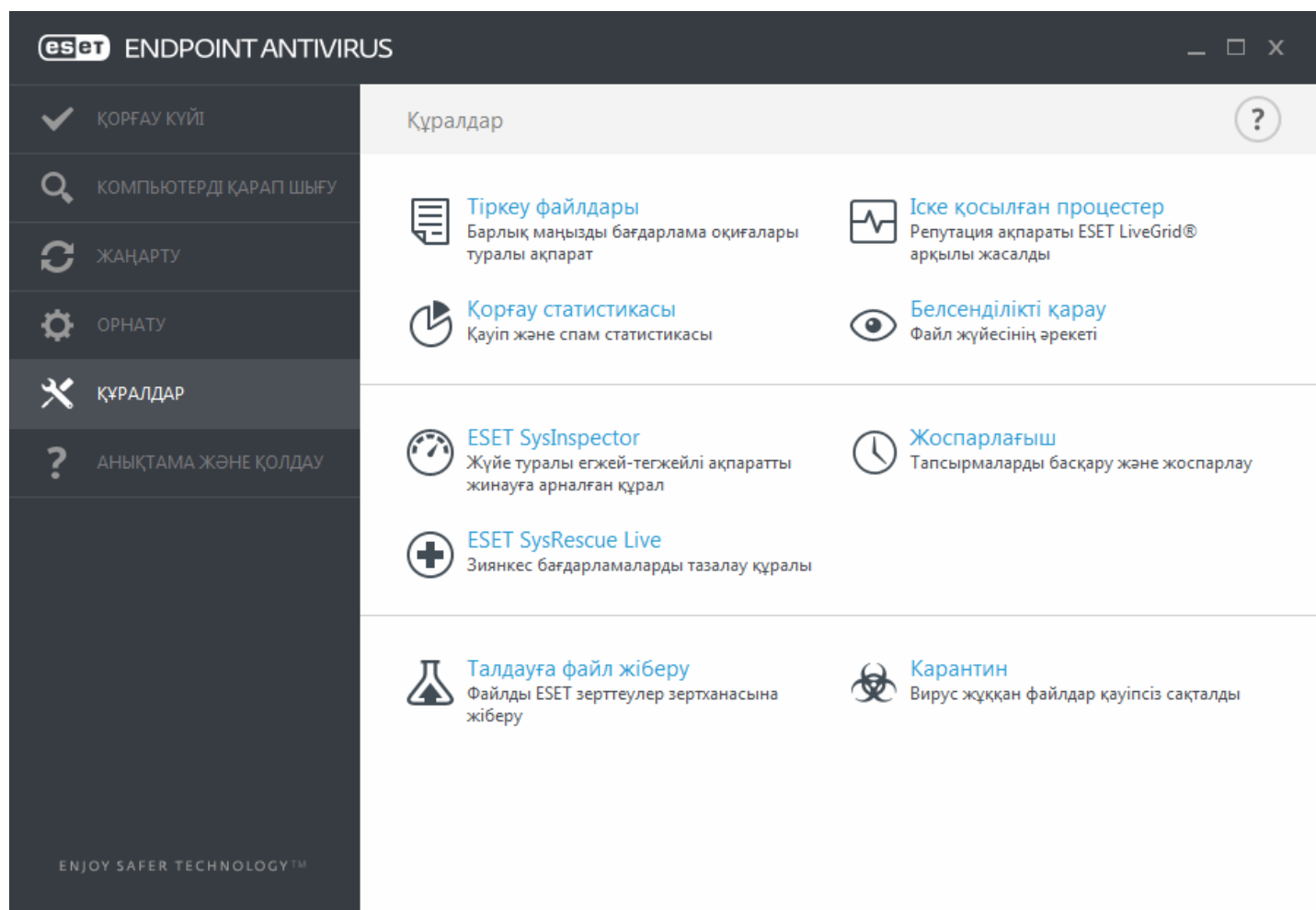
Сондай-ақ, жаңартуларды жоспарланған тапсырмалар ретінде орындауға болады. Жоспарланған тапсырманы конфигурациялау үшін **Құралдар > Жоспарлағыш** тармағын таңдаңыз. Әдепкі бойынша, ESET Endpoint Antivirus бағдарламасында келесі тапсырмалар іске қосылады:

- **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 конфигурациямен жасай алады. Жаңарту тапсырмаларын жасау және конфигурациялау туралы қосымша мәліметтер алу үшін [Жоспарлағыш](#) бөлімін қараңыз.

### 3.8.4 Құралдар

**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 Live Grid ESET Endpoint Antivirus бағдарламасында қосұлы болса)
- [Жоспарлағыш](#)
- [Карантин](#)
- [ESET SysInspector](#)

**Үлгіні талдауға жіберу** - күдікті файлды талдау үшін ESET вирус зертханасына жіберуге мүмкіндік береді. Осы опцияны басқаннан кейін шыққан диалогтық терезе [Файлдарды талдауға жіберу](#) бөлімінде сипатталған.

**ESET SysRescue** - Сізді ESET SysRescue Live бетіне қайта бағыттайды. Бұл бетте Microsoft Windows операциялық жүйелеріне арналған ESET SysRescue Live кескінін немесе Live CD/USB Creator бағдарламасын жүктеуге болады.

### 3.8.4.1 Журнал файлдары

Журнал файлдары орын алған барлық маңызды бағдарлама оқиғалары туралы ақпаратты қамтиды және анықталған қауіптерді шолуды қамтамасыз етеді. Журналдар жүйені талдауда, қауіптерді анықтауда және ақаулықтарды жоюда маңызды құрал ретінде қызмет етеді. Журналға жазу пайдаланушының араласуынсыз фонда белсенді орындалады. Ақпарат ағымдағы журнал көбею параметрлері негізінде жазылады. Мәтіндік хабарларды және журналдарды тікелей ESET Endpoint Antivirus ортасында көруге болады. Сондай-ақ, журнал файлдарын мұрағаттауға болады.

Тіркеу файлдарына негізгі мәзір терезесінде **Құралдар > Тіркеу файлдары** тармағына өтіп қатынасуға болады. Ашылмалы мәзірінен **Журнал** керекті журналды таңдаңыз. Келесі тіркеулерге қол жетімді:

- **Анықталған қауіптер** - қауіптер журналы ESET Endpoint Antivirus модульдері анықтаған инфильтрациялар туралы толық ақпаратты ұсынады. Бұл ақпарат анықтау уақытын, инфильтрация атауын, орнын, орындалған әрекетті және инфильтрация анықталған уақытта кірген пайдаланушы атын қамтиды. Мазмұнын бөлек терезеде мәліметтерін көрсету үшін журнал жазбасын екі рет басыңыз.
- **Оқиғалар** - ESET Endpoint Antivirus бағдарламасы орындаған барлық маңызды әрекеттер оқиғалар журналдарында жазылады. Оқиғалар журналының құрамында бағдарламада орын алған оқиғалар мен қателер туралы ақпарат бар. Ол жүйелік әкімшілер мен пайдаланушылар мәселелерін шешуге арналған. Осында табылатын ақпарат бағдарламада орын алатын ақаудың шешімін табуыңызға жиі көмектеседі.
- **Компьютерді қарап шығу** - қарап шығудың барлық нәтижелері осы терезеде 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 нақты ережелердің жазбаларын қамтиды. Протокол әрекетті шақырған бағдарламаны, нәтижені (ережеге рұқсат етілгенін немесе тыйым салынғанын) және жасалған ереженің атауын көрсетеді.
- **Сүзілген веб-сайттар** - Осы тізім - [Вебке кіруді қорғау](#) функциясы блоктаған веб-сайттардың тізімін көруге пайдалы. Осы журналдарда уақытты, URL-мекенжайын, пайдаланушыны және нақты веб-сайтқа байланысты ашқан бағдарламаны көруге болады.
- **Құрылғы басқару** - Компьютерге қосылған алынбалы медиа немесе құрылғылар жазбасын қамтиды. Тек құрылғыны басқару ережесі бар құрылғылар ғана журнал файлына жазылады. Егер ереже қосылған құрылғыға сәйкес келмесе, қосылған құрылғыға арналған тіркеу жазбасы жасалады. Мұнда құрылғы түрі, сериялық нөмірі, жеткізу аты және медиа өлшемі (егер болса) сияқты мәліметтерді көруге болады.

Әр бөлімде, көрсетілген ақпаратты жазбаны таңдау және **Көшіру** түймесін басу арқылы аралық сақтағышқа көшіруге болады (**Ctrl + C** пернелер тіркесімі). Бірнеше жазбаны таңдау үшін **Ctrl** және **Shift** пернелерін пайдалануға болады.

Өнімді іске қосу үшін  Сүзу шарттарын анықтауға болатын **Журналды сүзу** терезесін ашу үшін **Сүзу** түймесін басыңыз.

Контекстік мәзірді нақты жазбаны тінтуірдің оң жақ түймешігімен басу арқылы көрсетуге болады. 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 опцияны басқаннан кейін [Журналда іздеу](#) терезесі нақты 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 пішіміне экспорттайды.
- **Журналды айналдыру** - **Журнал файлдары** терезесінде ескі журналдарды авто айналдыру және белсенді журналдарды көру үшін бұл опцияны қосулы қалдырыңыз.

### 3.8.4.1.1 Журналда іздеу

Журналдарда маңызды жүйелік оқиғалар туралы ақпаратты сақталады. Журналды сүзу мүмкіндігі арнайы оқиға түрі туралы жазбаларды көрсетуге мүмкіндік береді.

**Мәтінді табу** өрісіне іздеу кілтсөзін енгізіңіз. Нақты бағандарда кілтсөзді іздеу керек болса, сүзгіні **Бағандарда іздеу** ашылмалы мәзірінде өзгертіңіз.

**Жазба түрлері** - Ашылмалы мәзірден бір немесе бірнеше жазба журналы түрлерін таңдаңыз:

- **Диагностика** - Бағдарламаны және жоғарыдағы барлық жазбаларды реттеуге қажет ақпаратты журналға тіркейді.
  - **Ақпараттық** - Ақпараттық хабарларды, соның ішінде сәтті жаңарту хабарларын, сондай-ақ, барлық жоғарыдағы жазбаларды жазады.
  - **Ескертулер** - Маңызды қателерді және ескерту хабарларын жазады.
  - **Қателер** - Қателер, мысалы, «Файлды жүктеу қатесі» және маңызды қателер жазылады.
  - **Маңызды** - Тек маңызды қателерді (антивирустық қорғауды, т.б қосатын қателерді) ғана журналға жазады.
- Уақыт аралығы** - Нәтижелер қандай уақыт аралығынан кейін көрсетілетінін анықтаңыз.

**Толық сөздерді ғана салыстыру** - Дәлірек нәтижелер алу үшін нақты толық сөздерді іздеу керек болса, осы құсбелгіні қойыңыз.

**Регистрге тәуелді** - Сүзу кезінде бас немесе кіші әріптерді пайдалану маңызды болса, осы опцияны қосыңыз.

**Жоғары қарай іздеу** - құжатта жоғарырақ көрсетілетін іздеу нәтижелері бірінші көрсетіледі.

### 3.8.4.2 Прокси серверді орнату

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 Endpoint 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 Endpoint 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.

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.

### 3.8.4.3 Жоспарлағыш

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

Жоспарлағышқа ESET Endpoint 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: вирустық қолтаңба дерекқорын жаңарту, қарап шығу тапсырмасы, жүйелік жүктеу файлын тексеру және журнал жүргізу. Тапсырмаларды тікелей негізгі жоспарлағыш терезесінен қосуға немесе жоюға болады (астында **Тапсырма қосу** немесе **Жою** түймесін 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**
- **Іске қосылғанда автоматты түрде файлдарды тексеру** (пайдаланушы кіргеннен кейін)
- **Іске қосылғанда автоматты түрде файлдарды тексеру** (вирус қолтаңбасының дерекқоры сәтті жаңартылғаннан кейін)
- **Автоматты бірінші қарап шығу**

Бар жоспарланған тапсырманың (әдепкі мен пайдаланушы анықтаған) конфигурациясын өзгерту үшін тапсырманы тінтуірдің оң жақ түймесімен басып, **Өңдеу...** пәрменін таңдаңыз 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 бағдарламаларды іске қосу** - Сыртқы бағдарламаның орындалуын жоспарлайды.
- **Жұрналды реттеу** -Тіркеу файлдарында жойылған жазбалардың қалдықтары да бар. Бұл тапсырма тиімді жұмыс істеу үшін журнал файлдарындағы жазбаларды тұрақты түрде оңтайландырады.
- **Жүйені іске қосу файлын тексеру** - Жүйе іске қосылғанда немесе кіргенде іске қосылуына 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.
- **Бірінші қарап шығу** - әдепкі бойынша, орнатудан кейінгі 20 минут немесе «Компьютерді қарап шығу» қайта жүктеу төмен басымдылық тапсырмасы ретінде орындалады.
- **Жаңарту** - Вирус қолтаңбасының дерекқорын және бағдарлама модульдерін 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:

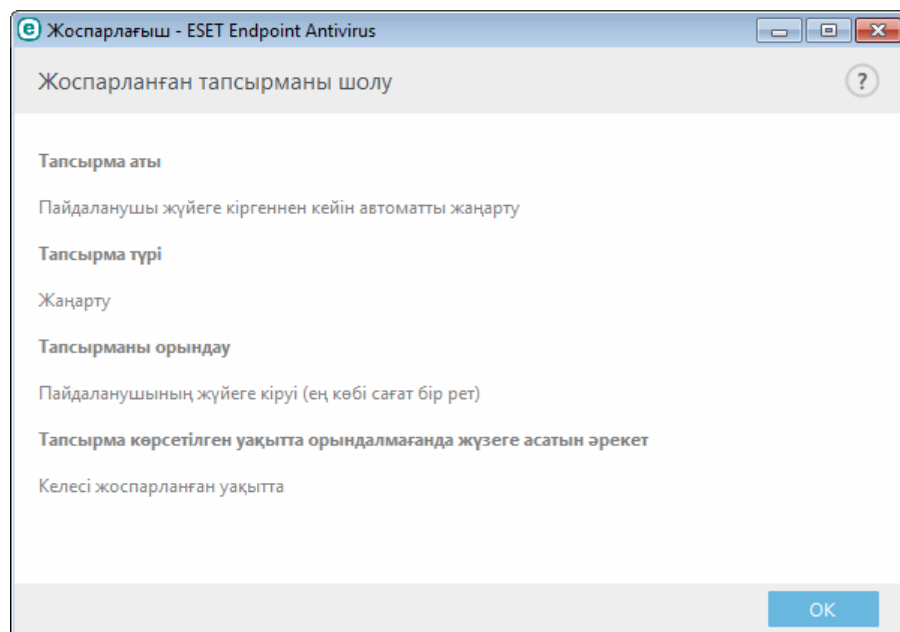
- **Бір рет** - Тапсырма алдын ала белгіленген күн мен уақытта орындалады.
- **Қайталап** - Тапсырма көрсетілген уақыт аралығында орындалады.
- **Күнделікті** - Тапсырма күн сайын көрсетілген уақытта қайталап орындалады.
- **Апта сайын** – Тапсырма таңдалған күн мен уақытта орындалады.
- **Оқиға басталған**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



#### 3.8.4.4 Қорғау статистикасы

ESET Endpoint Antivirus қорғау модульдеріне қатыссыз 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.

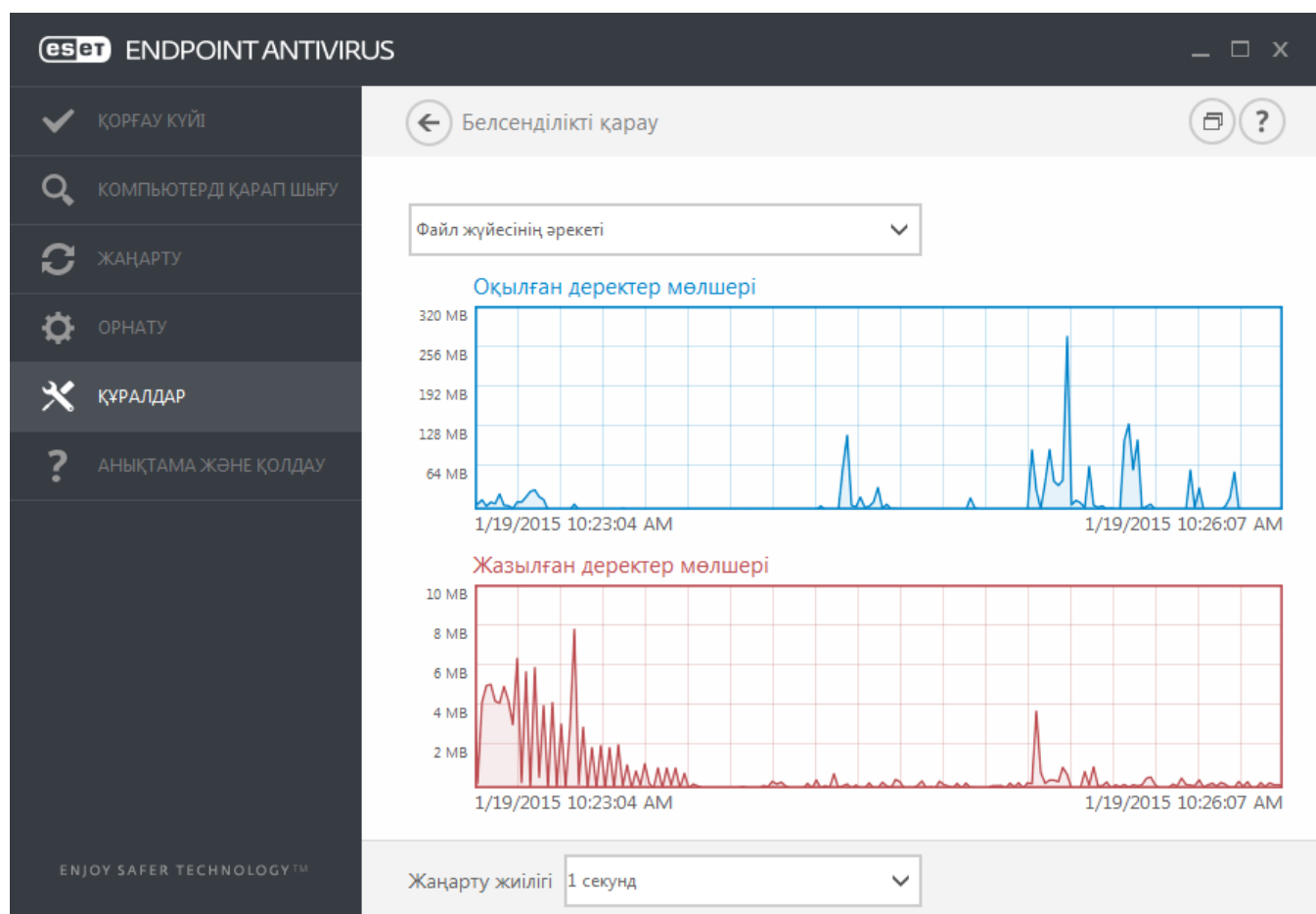
Төмендегі статистикалық графиктер қолжетімді:

- **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 графиктерінің жанында барлық қарап шығылған нысандардың санын, вирус жұққан нысандардың санын, тазаланған нысандардың санын және таза нысандардың санын көре аласыз. Статистикалық ақпаратты тазалау үшін **Ысыру** түймесін басыңыз немесе бүкіл бар деректерді тазалау және жою үшін **Барлығын ысыру** түймесін басыңыз.

### 3.8.4.5 Белсенділікті қарау

График пішінінде ағымдағы **Файл жүйесінің әрекетін** көру үшін **Құралдар > Белсенділікті қарау** тармағына өтіңіз. 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.

**Файлдық жүйесі әрекеттерінің** графигі тік осі оқылған деректердің (көк) және жазылған деректердің (қызыл) мөлшерін білдіреді. Екі мән де КБ (килобайт)/МБ/ГБ түрінде көрсетіледі. Егер сіз графиктің төменгі жағындағы шартты белгілердегі оқылған деректерді не жазылған деректерді тінтуірмен бассңыз, график сол белсенділік түріне арналған деректерді ғана көрсетеді.

### 3.8.4.6 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:

- **Ашу** - 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).
- **Барлығын жою** - Барлық журналдарды жояды.
- **Экспорттау...** - Журналды `.xml` файлға немесе қысылған `.xml` файлға экспорттайды.

### 3.8.4.7 ESET Live Grid

ESET Live Grid — бірнеше бұлтқа негізделген технологиядан тұратын озық ерте ескерту жүйесі. Ол репутация негізінде пайда болып жатқан қауіптерді анықтауға көмектеседі және ақ тізімге қосу арқылы қарап шығу өнімділігін жақсартады. Жаңа қауіп туралы ақпарат бұлтқа нақты уақытта жіберіледі, бұл ESET зиянкес бағдарламаларды зерттеу зертханасына әрқашан уақтылы жауапты және үйлесімді қорғауды қамтамасыз етуге мүмкіндік береді. Пайдаланушылар іске қосылған процестер мен файлдардың репутациясын тікелей бағдарлама интерфейсінен немесе ESET Live Grid арқылы қол жетімді қосымша ақпаратқа ие контексттік мәтіннен тексере алады. ESET Endpoint Antivirus бағдарламасын орнату кезінде келесі опциялардың біреуін таңдаңыз:

1. ESET Live Grid бағдарламасын қоспауды шеше аласыз. Бағдарламадағы функцияларды жоғалтпайсыз, бірақ кейбір жағдайларда ESET Endpoint Antivirus жаңа қауіптерге вирус сигнатуралары дерекқорын жаңартудан баяуырақ жауап беруі мүмкін.
2. ESET Live Grid 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 Live Grid бағдарламасы компьютеріңізде жаңадан анықталған қауіптер туралы ақпаратты жинайды. Бұл ақпарат қауіп пайда болған үлгісін, оның көшірмесін, жолын, файл атын, күн мен уақытын, компьютеріңізде қауіп пайда болған барысын және компьютеріңіздің амалдық жүйесі туралы ақпаратты қамтуы мүмкін.

Әдепкі бойынша, ESET Endpoint Antivirus бағдарламасы күдікті файлдарды «ESET вирус зертханасына» егжей-тегжейлі талдауға жіберуге 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 Live Grid репутация жүйесі бұлтқа негізделген ақ тізімге қосуды және қара тізімге қосуды қамтамасыз етеді. ESET Live Grid параметрлерін ашу үшін **F5** пернесін басып «Кеңейтілген орнату» тармағына кіріңіз, содан кейін **Құралдар > ESET Live Grid** тармағын кеңейтіңіз.

**ESET Live Grid репутация жүйесін қосу (ұсынылады)** - ESET Live Grid репутация жүйесі қарап шығылған файлдарды бұлттағы ақ тізімге қосылған және қара тізімге қосылған элементтердің дерекқорымен салыстыру арқылы ESET зиянкес бағдарламаларға қарсы шешімдерінің тиімділігін жақсартады.

**Анонимді статистиканы жіберу** - ESET бағдарламасына жаңадан анықталған қауіптер туралы ақпаратты жинауға рұқсат ету, мысалы, қауіп атауы, анықтау күні мен уақыты, анықтау әдісі мен байланысты метадеректер, өнім нұсқасы мен конфигурациясы, соның ішінде, жүйе туралы ақпарат.

**Файлдарды жіберу** - Қауіптерге ұқсайтын күдікті файлдар және/немесе әдеттен тыс сипаттамалары немесе мінез-құлқы бар файлдар талдау үшін ESET компаниясына 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.

**Электрондық байланыс пошта тасы (міндетті емес)** - Электрондық байланыс поштаңыз күдікті файлдармен бірге жіберіледі және талдау үшін қосымша ақпарат қажет болса олар байланыс үшін пайдаланылуы мүмкін. Қосымша ақпарат қажет болмаса, ESET компаниясынан жауап алмайтыныңызды ескеріңіз.

**Ерекш өлік** - «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 Live Grid 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.

### 3.8.4.8 Іске қосылған процестер

Іске қосылған процестер компьютерде іске қосылған бағдарламаларды немесе процестерді көрсетеді және ESET жүйесін жаңа инфильтрациялар туралы дереу және үздіксіз хабардар етіп отырады. ESET Endpoint Antivirus бағдарламасы пайдаланушыларды [ESET Live Grid](#) технологиясы қосулы күйде қорғау үшін іске қосылған процестер туралы егжей-тегжейлі ақпаратты қамтамасыз етеді.

Қа...	Процесс	PID	Пайдаланушы...	Ашылу уақыты	Бағдарлама аты
✓	smss.exe	272	██████████	1 жыл бұрын	Microsoft® Windows® ...
✓	csrss.exe	348	██████████	5 жыл бұрын	Microsoft® Windows® ...
✓	wininit.exe	384	██████████	5 жыл бұрын	Microsoft® Windows® ...
✓	winlogon.exe	436	██████████	2 жыл бұрын	Microsoft® Windows® ...
✓	services.exe	480	██████████	5 жыл бұрын	Microsoft® Windows® ...
✓	lsass.exe	488	██████████	5 жыл бұрын	Microsoft® Windows® ...
✓	lsm.exe	496	██████████	2 жыл бұрын	Microsoft® Windows® ...
✓	svchost.exe	600	██████████	5 жыл бұрын	Microsoft® Windows® ...
✓	vboxservice.exe	664	██████████	6 ай бұрын	Oracle VM VirtualBox Gu...
✓	spoolsv.exe	1132	██████████	2 жыл бұрын	Microsoft® Windows® ...
✓	filezilla_server.exe	1308	██████████	3 ай бұрын	FileZilla Server

**Жол:** c:\windows\system32\csrss.exe  
**Өлшемі:** 7.5 kB  
**Сипаты:** Client Server Runtime Process  
**Компания:** Microsoft Corporation  
**Нұсқасы:** 6.1.7600.16385 (win7\_rtm.090713-1255)  
**Өнім:** Microsoft® Windows® Operating System  
**Жасалған күні:** 7/14/2009 1:19:49 AM  
**Өзгертілген күні:** 7/14/2009 3:39:02 AM

[Мәліметтерді жасыру](#)

**Қауіп деңгейі** - Көп жағдайларда ESET Endpoint Antivirus бағдарламасы және ESET Live Grid технологиясының көмегімен 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)** – **9 - Қауіпті (қызыл)** аралығындағы қауіп деңгейі тағайындалады.

**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» тапсырмалар тақтасындағы бос аумақты тінтуірдің оң жағын басып, содан кейін «Тапсырмалар реттеушісі» түймесін басы арқылы немесе пернетақтада **Ctrl+Shift+Esc** пернелер тіркесімін басы арқылы ашуға болады.

**PID** - Windows операциялық жүйелерінде іске қосылған процестердің идентификаторы.

**ЕСКЕРТПЕ:** **Жақсы (жасыл)** ретінде белгіленген белгілі бағдарламалар анық таза (рұқсатты тізімде) және қарап шығуға қосылмайды, өйткені бұл талап бойынша компьютерді қарап шығудың жылдамдығын немесе компьютердегі нақты уақыттағы файлдық жүйені қорғауды жақсартады.

**Пайдаланушылар саны** - Осы бағдарламаны пайдаланатын пайдаланушылардың саны. Бұл ақпарат ESET Live Grid технологиясымен жиналған.

**Анықтау уақыты** - ESET Live Grid технологиясы бағдарламаны анықтағаннан бергі уақыт.

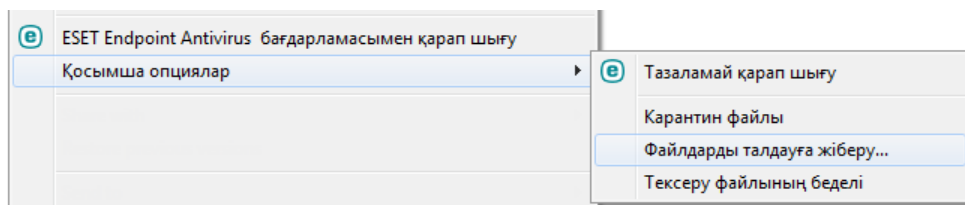
**Ескертпе:** Бағдарлама **Белгісіз (қызылт сары)** қауіпсіздік деңгейі ретінде белгіленген кезде, ол міндетті түрде зиянды бағдарлама болмайды. Әдетте бұл жай жаңа бағдарлама. Егер файлға сенімді болмасаңыз, ESET вирус зертханасына файлды жіберу үшін [файлды талдауға жіберу](#) мүмкіндігін пайдаланыңыз. Егер файл зиянкес бағдарлама болып шықса, оны анықтау келесі вирус қолтаңбасы дерекқорын жаңартулардың біріне қосылады.

**Бағдарлама аты** - Бағдарламаға немесе процеске берілген ат.

Осы бағдарламаның төменгі жағында басқанда, терезенің төменгі жағында келесі ақпарат пайда болады:

- **Жол** - бағдарламаның компьютердегі орны.
- **Өлшем** - файл өлшемі КБ (килобайт) немесе МБ (мегабайт) өлшемдерінің бірінде беріледі.
- **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 күні** - бағдарлама жасалған күн мен уақыт.
- **Өзгертілген күні** - бағдарлама өзгертілген соңғы күн мен уақыт.

**ЕСКЕРТПЕ:** Сондай-ақ, репутацияны іске қосылған бағдарламалар/процестер ретінде әрекет етпейтін файлдарда тексеруге болады- тексеру керек файлдарға белгі қойып, оларды тінтуірдің оң жақ түймесімен басыңыз да, [контекстік мәзірде](#) **Кеңейтілген параметрлер > ESET Live Grid жүйесін пайдалану арқылы файл репутациясын тексеру** тармағын таңдаңыз.



### 3.8.4.9 Үлгілерді талдауға жіберу

Үлгіні жіберу диалогтық терезесі файлды немесе сайтты ESET компаниясына талдауға жіберуге мүмкіндік береді және оны **Құралдар > Үлгіні талдауға жіберу** тармағынан табуға болады. Егер компьютеріңізден күдікті 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](mailto:samples@eset.com) мекенжайына жіберіңіз. Сипаттаушы тақырыпты пайдаланыңыз және мүмкіндігінше көп ақпарат қосыңыз (мысалы, одан жүктелген веб-сайт).

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

- файл немесе веб-сайт мүлдем анықталмайды
- файл немесе веб-сайт қауіп ретінде қате анықталған

Талдау үшін қосымша ақпарат қажет болмаса, сіз жауап алмайсыз.

**Үлгіні 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**

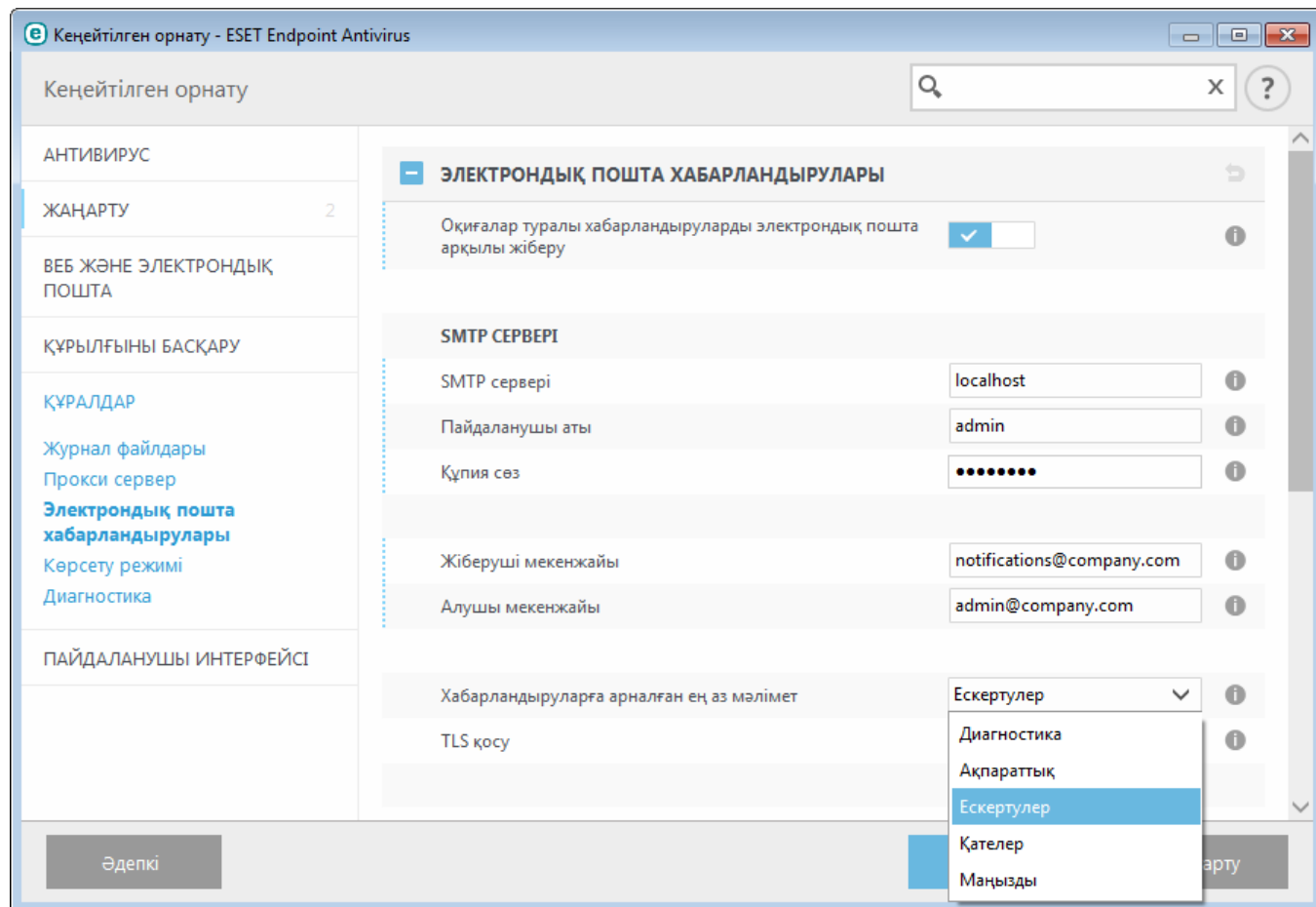
**Файл/Сайт** - Жіберу керек файлдың немесе веб-сайттың жолы.

**Байланыс электрондық пошта тасы** - Бұл байланыс электрондық поштасы ESET лабораториясына күдікті файлдармен бірге жіберіледі және талдау үшін қосымша ақпараттар қажет болса, байланысу үшін пайдаланылуы

мүмкін. Электрондық байланыс поштасын енгізу міндетті емес. Қосымша ақпарат қажет болмаса, барлық жазылымдарға жауап беруге мүмкіндік туғыза отырып, күн сайын біз серверлеріміз он мыңдаған файлдар алғанға дейін ESET компаниясынан жауап алмайсыз.

### 3.8.4.10 Электрондық пошта хабарландырулары

Таңдалған ең аз мәлімет бар оқиға орын алса, ESET Endpoint 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** - Хабарландыруларды жіберу үшін пайдаланылатын «SMTP» сервері.

**ЕСКЕРТПЕ:** TLS шифрлауы бар SMTP серверлеріне ESET Endpoint 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** - Журналдар ақпараты бағдарламаны және жоғарыдағы барлық жазбаларды реттеуге қажет.
- **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.

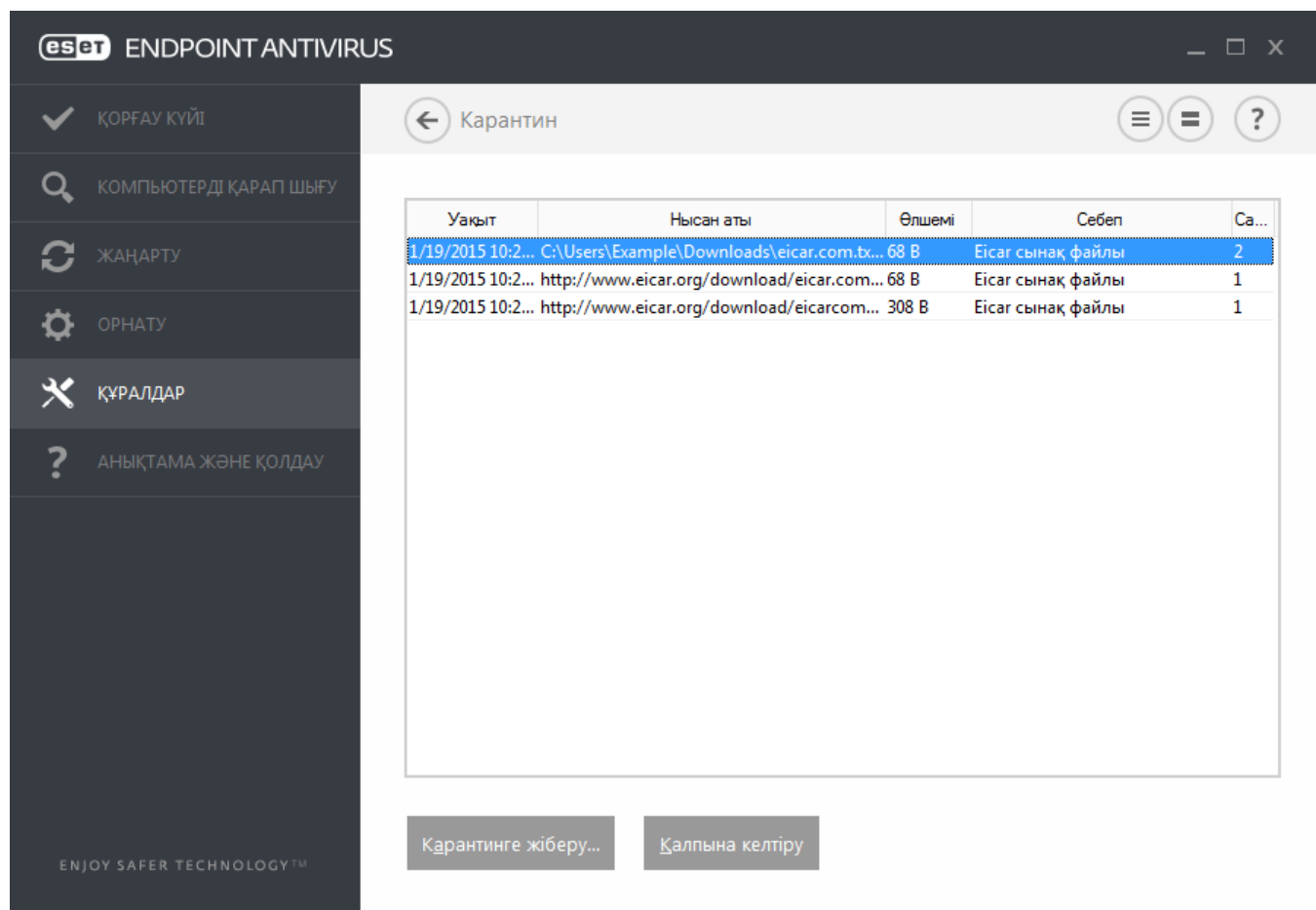
**Жергілікті өліпбилік таңбаларды пайдалану** - Электрондық поштаның хабарын Windows жүйесінің жергілікті параметрлері негізінде кодталған (мысалы, Windows-1250) ANSI таңбасына түрлендіреді. Егер бұған құсбелгі қойылмаған болса, хабар ASCII 7 битте түрлендіріліп, кодталады (мысалы, «á» таңбасы «a» таңбасына 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.

### 3.8.4.11 Карантин

Карантиннің негізгі функциясы – вирус жұққан файлдарды қауіпсіз сақтау. Файлдарды тазалау мүмкін емес болса, жою қауіпсіз емес болса немесе кеңес берілмесе немесе ESET Endpoint 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 Endpoint 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 қолмен карантинге көшіруге болады. Түпнұсқалық файл бастапқы орнына жойылады. Контекстік мәзірді де осы мақсатта пайдалануға болады; **Карантин** терезесінде тінтуірдің оң жақ түймесін басып, **Карантин** тармағын таңдаңыз.

#### Карантиннен қалпына келтіру

Сондай-ақ, карантинге қойылған файлдарды бастапқы орнына қалпына келтіруге болады. Карантинге жіберілген файлды қалпына келтіру үшін «Карантин» терезесінде тінтуірдің оң жақ түймешігін баыңыз, сөйтіп контекстік мәзірде **Қалпына келтіру** пәрменін таңдаңыз. Егер файл **ықтимал қалаусыз қолданба** ретінде белгіленген болса, **Қалпына келтіру және қарап шығуға қоспау** пәрмені де қол жетімді болады. Контекстік мәзір сонымен бірге **Қалпына келтіру...** опциясын ұсынады. Бұл опция файлды жойылған орнынан басқа орынға 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

Бағдарлама анықтамаған күдікті файлды карантинге қойсаңыз немесе файл қауіп ретінде дұрыс емес анықталған болса және кейін карантинге жіберілсе, файлды ESET вирустар зертханасына жіберіңіз. Карантинге көшірілген файлды жіберу үшін, файлды тінтуірдің оң жағымен басыңыз да, мазмұн мәзірінен **Талдауға жіберу** тармағын таңдаңыз.

### 3.8.4.12 Microsoft Windows update

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

### 3.8.5 Пайдаланушы интерфейсі

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

[Пайдаланушы интерфейсінің элементтері](#) құралын пайдаланып бағдарламаның көрінісін және пайдаланылатын әсерлерді реттеуге болады.

Қауіпсіздік бағдарламалық жасақтамасының ең жоғары қауіпсіздігін қамтамасыз ету үшін [Қатынасты реттеу](#) құралын пайдаланып кез келген рұқсат етілмеген өзгертулерді болдырмауға болады.

[Ескертулер мен хабарландырулар](#) конфигурациялау арқылы анықталған қауіп туралы ескертулер мен жүйелік хабарландырулардың әрекетін өзгертуге болады. Бұларды қажеттіліктеріңізге сай теңшеуге болады.

Кейбір хабарландыруларды көрсетпеді таңдасаңыз, олар **Пайдаланушылық интерфейс элементтері > Қолданба күйлері** тармағында көрсетіледі. Мұнда олардың күйін тексеруге немесе осы хабарландыруларды көрсетуді болдырмауға болады.

[Контекстік мәзір](#) таңдалған нысанды тінтуірдің оң жақ түймесімен басқаннан кейін көрсетіледі. Бұл құралды контекстік мәзірге ESET Endpoint Antivirus басқару элементтерін біріктіру үшін пайдаланыңыз.

[Көрсету режимі](#) – қолданбамен жұмыс істегенде қалқымалы терезелердің, жоспарланған тапсырмалардың және процессорға мен ЖЖҚ-на жүктеме түсіруі мүмкін кез келген компоненттердің үзуін қаламайтын пайдаланушылар үшін пайдалы.

### 3.8.5.1 Пайдаланушы интерфейсі элементтері

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

**Пайдаланушы интерфейсінің элементтері** бөлімінде жұмыс ортасын реттеуге болады. Төмендегі ГПИ іске қосу режимдерінен таңдау үшін **ГПИ іске қосу режимі** ашылмалы мәзірін басыңыз:

**Толық** - толық ГПИ көрсетіледі.

**Минималды** - графикалық интерфейс іске қосылған, бірақ пайдаланушыға тек хабарландырулар көрсетіледі.

**Қолмен** - хабарландырулар немесе ескертулер көрсетілмейді.

**Тыныш** - пайдаланушылық интерфейс те, хабарландырулар мен ескертулер де көрсетілмейді. Бұл режим жүйелік ресурстарды сақтау үшін қажет жағдайларда пайдалы болуы мүмкін. Тыныш режимді тек әкімші іске қоса алады.

**ЕСКЕРТПЕ:** Минималды ГПИ іске қосу режимі таңдалса және компьютер қайта іске қосылса, хабарландырулар көрсетіледі, бірақ графикалық интерфейс көрсетілмейді. Толық графикалық пайдаланушы интерфейсі режимін кері ету үшін ГПИ «Бастау» мәзірінде, **Барлық бағдарламалар > ESET > ESET Endpoint Antivirus** тармағында әкімші ретінде іске қосыңыз немесе мұны саясатты пайдаланып ESET Remote Administrator арқылы істеуге болады.

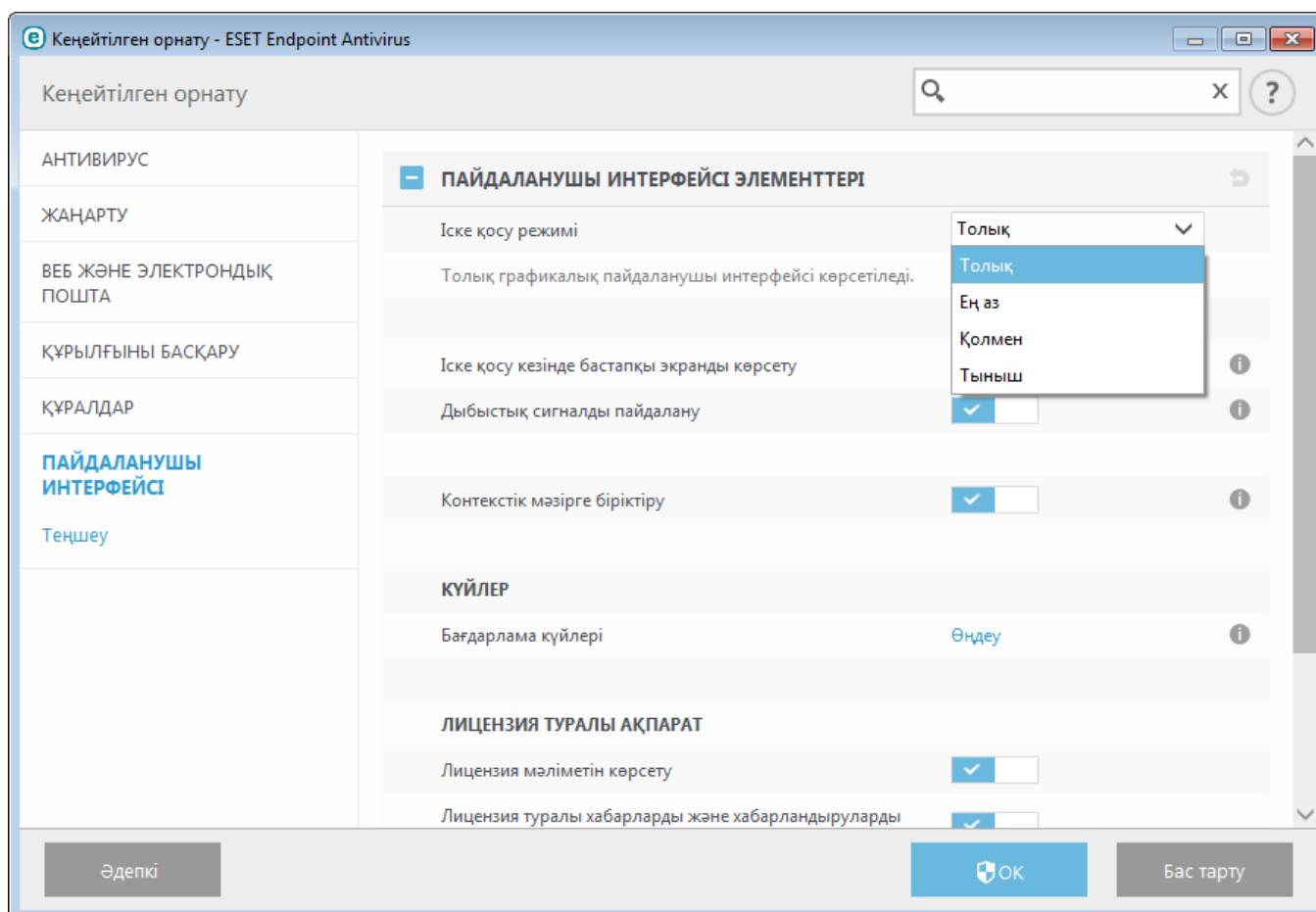
Егер ESET Endpoint Antivirus бастапқы экранын өшіргіңіз келсе, **Бастау кезінде жетілдірілген экранды көрсету** опциясын таңдаудан бас тартыңыз.

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

**Контекстік мәзірге біріктіру** - ESET Endpoint Antivirus басқару элементтерін контекстік мәзірге біріктіреді.

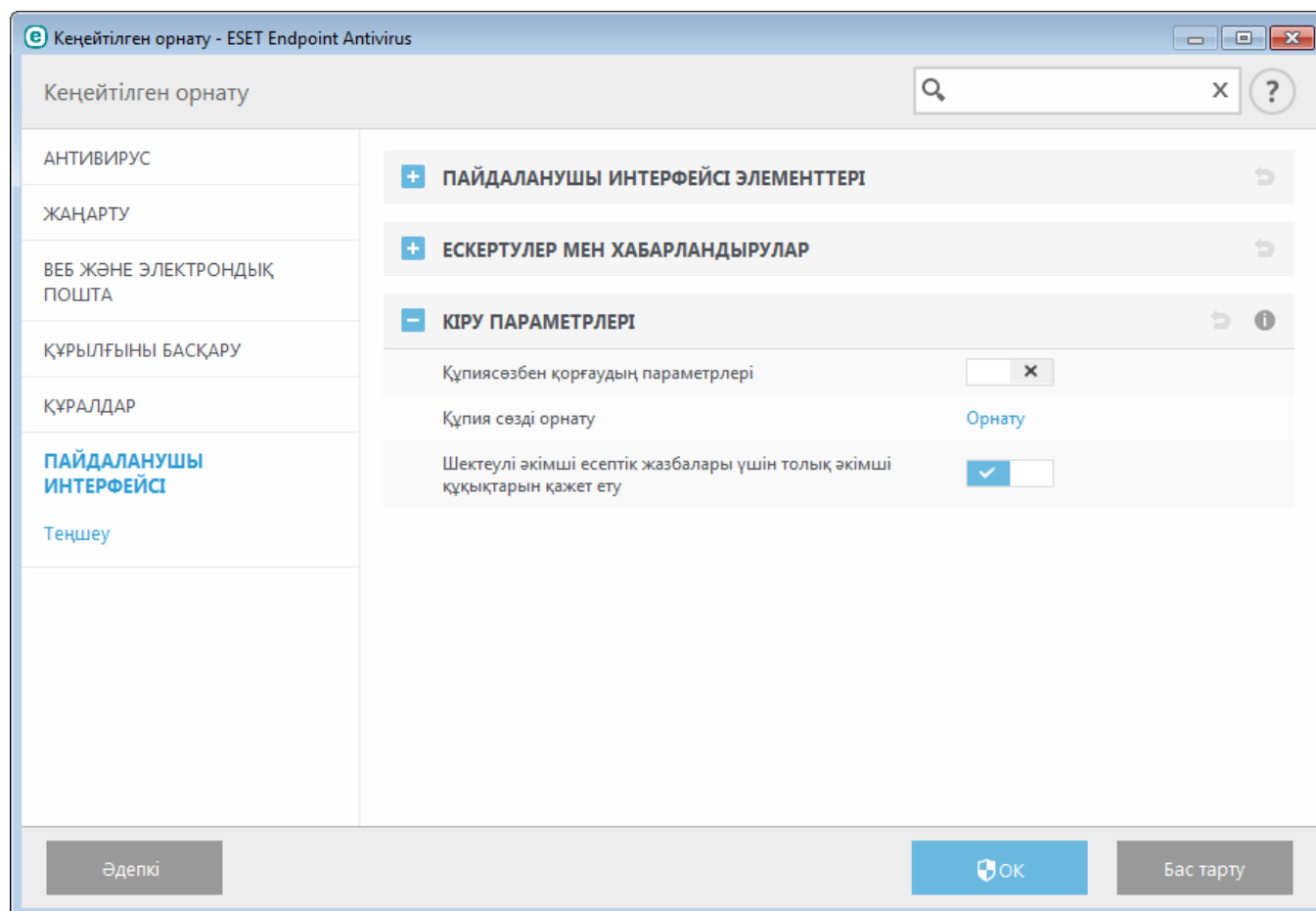
#### Күйлер

**Қолданба күйлері** - басты мәзірдегі **Қорғау күйлері** тақтасында көрсетілетін күйлерді басқару (өшіру) үшін **Өңдеу** түймесін басыңыз.



### 3.8.5.2 Кіру параметрлері

Жүйені ең жоғары қауіпсіздікпен қамтамасыз ету үшін ESET Endpoint Antivirus бағдарламасы дұрыс конфигурациялануы қажет. Кез келген орынсыз өзгерту маңызды ақпараттың жоғалуына әкелуі мүмкін. Рұқсат етілмеген өзгертулерді болдырмау үшін ESET Endpoint Antivirus бағдарламасының орнатылған параметрлерін құпиясөзбен қорғауға болады. Құпия сөзді қорғау үшін конфигурация параметрлері **Кеңейтілген орнату** (F5) ішінде, **Қатынасты реттеу** > **Пайдаланушы ылық интерфөйс** астында орналасқан.



**Құпия сөзбен қорғау параметрлері** - құпия сөз параметрлерін көрсетіңіз. «Құпия сөзді орнату» терезесін ашу үшін басыңыз.

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

**Шөктеулі әкімші есептік жазбалары үшін толық әкімші құқықтарын қажет ету** - Белгілі бір жүйелік параметрлерді (Windows Vista жүйесіндегі UAC элементіне ұқсас) өзгерту барысында әкімшінің пайдаланушы аты мен құпиясөзін енгізуге ағымдағы пайдаланушыны шақыру (егер оның әкімші құқықтары болмаса) үшін осы параметрді таңдаңыз. Өзгертулер қорғау модульдерін ажыратуды қамтиды.

Тек Windows XP үшін:

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

### 3.8.5.3 Ескертулер мен хабарландырулар

**Пайдаланушы интерфейсі** тармағындағы **Ескертулер мен хабарландырулар** бөлімі ESET Endpoint 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 мөлдірлік 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.

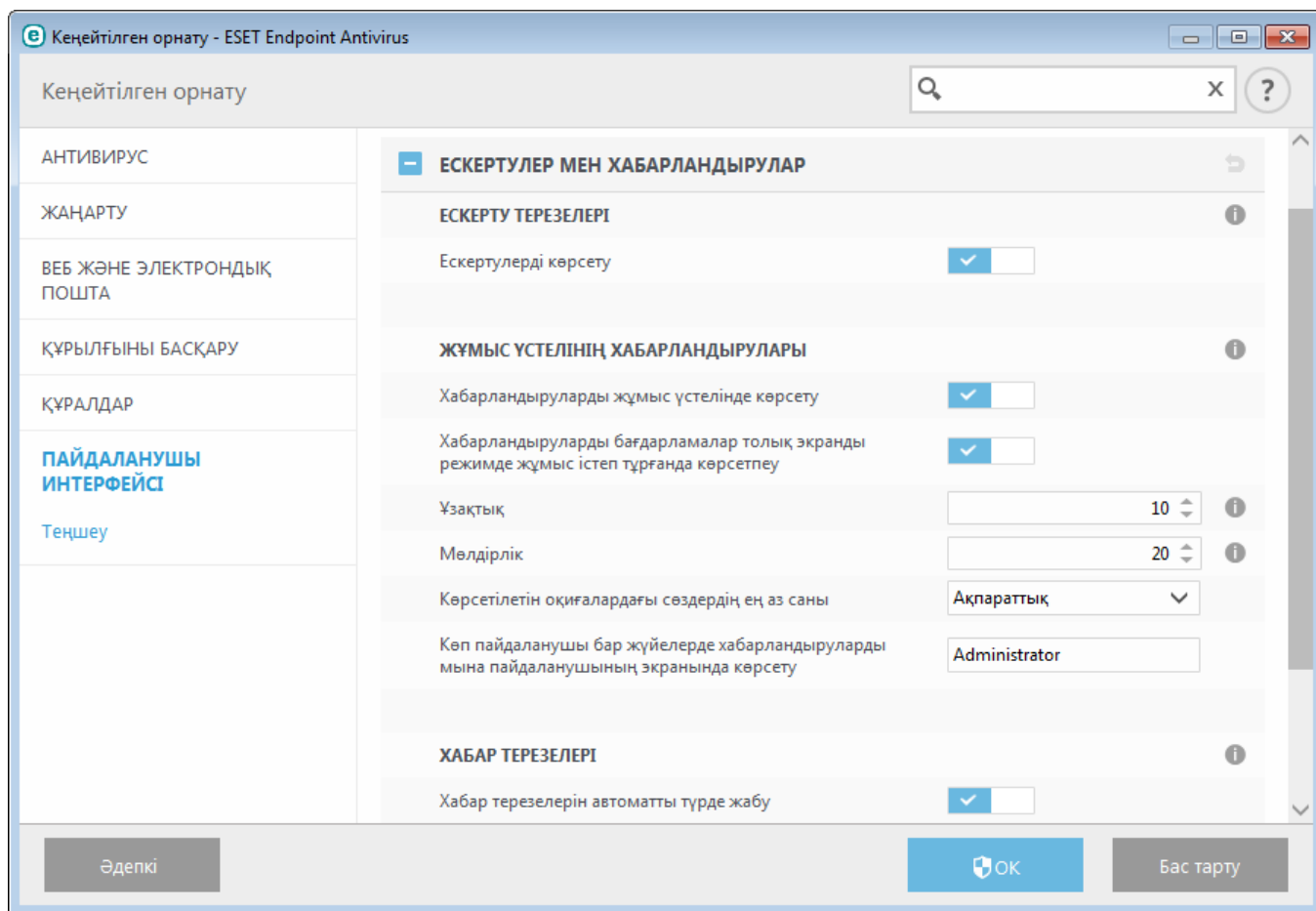
#### Жұмыс үстелінің хабарландырулары

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** қосқышын 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** - Жұрналар ақпараты бағдарламаны және жоғарыдағы барлық жазбаларды реттеуге қажет.
- **Ақпараттық** - Ақпараттық хабарларды, соның ішінде сәтті жаңарту хабарларын, сондай-ақ, барлық жоғарыдағы жазбаларды жазады.
- **Ескертулер** - Маңызды қателерді және ескерту хабарларын жазады.
- **Қателер** - Қателер, мысалы, «*Файлды жүктеу қатесі*» және маңызды қателер жазылады.
- **Күрделі** - Тек күрделі қателерді (антивирустық қорғауды, т.б.) 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.



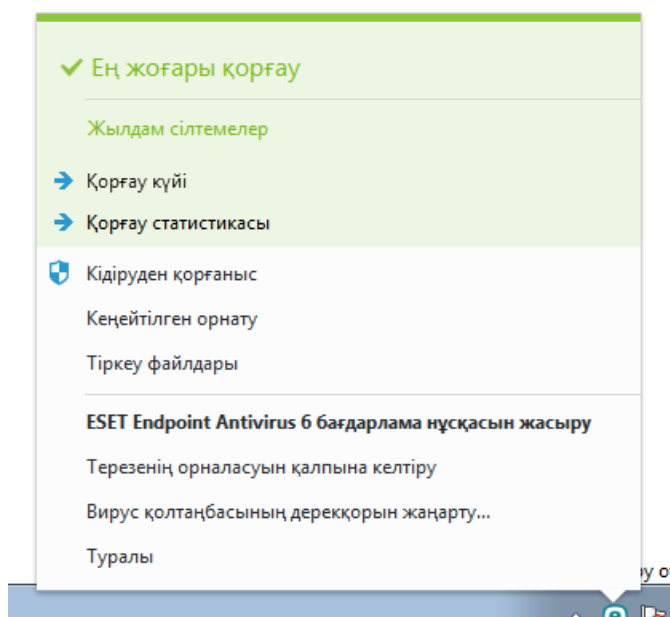
### Хабар терезелері

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** - Көрсету немесе көрсетпеді таңдауға болатын растау хабарларының тізімін көрсетеді.

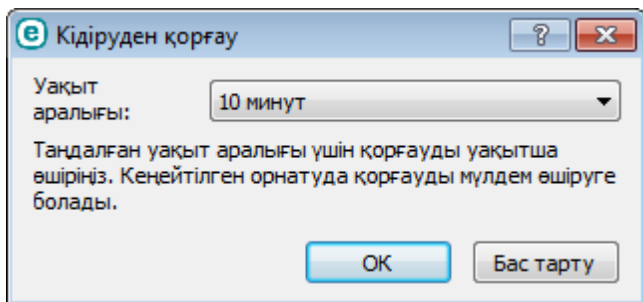
### 3.8.5.4 Жүйелік тақта белгішесі

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



**Қорғауды кідірту** - [Антивирустық және антишпиондық қорғауды](#) өшіретін растау диалогтық терезесін көрсетеді, ол

файл, веб және электрондық пошта байланысын басқару арқылы шабуылдардан қорғайды.



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

**Бүкіл желілік трафикті блоктау** - бүкіл желілік трафикті блоктайды. Оны **Бүкіл желілік трафикті блоктауды тоқтату** түймесін басу арқылы қайта қосуға болады.

**Кеңейтілген орнату** - Бұл опцияны **Кеңейтілген орнату** ағашына кіру үшін таңдаңыз. Сондай-ақ, «Кеңейтілген орнату» тармағына F5 пернесін басу немесе **Орнату > Кеңейтілген орнату** тармағына ету арқылы қатынасуға болады.

**Журнал файлдары** - [Журнал файлдары](#) орын алған барлық маңызды бағдарлама оқиғалары туралы ақпаратты қамтиды және анықталған қауіптерді шолуды береді.

**ESET Endpoint Antivirus жасыру** - ESET Endpoint Antivirus терезесін экраннан жасыру.

**Терезенің орналасуын қалпына келтіру** - ESET Endpoint Antivirus бағдарламасының терезесін экранда әдепкі өлшеміне және орнына қалпына келтіреді.

**Вирус қолтаңбасы дерекқорын жаңарту** - зиянкес кодқа қарсы қорғау деңгейін қамтамасыз ету үшін вирус қолтаңбасы дерекқорын жаңартуды бастайды.

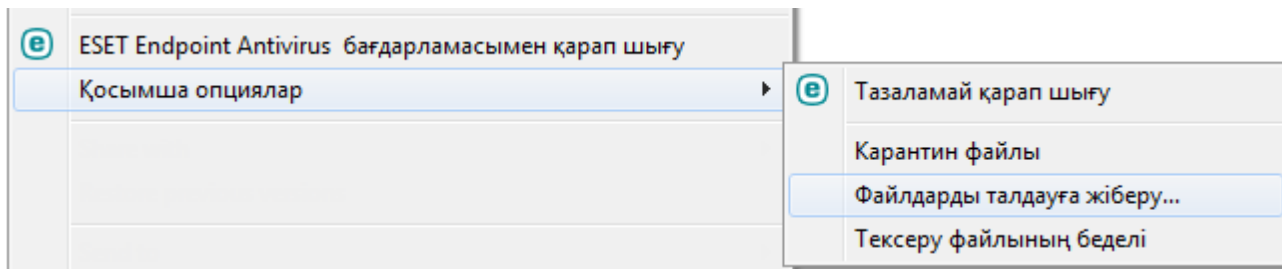
**Туралы** - жүйе туралы ақпаратты, орнатылған ESET Endpoint Antivirus нұсқасы және орнатылған бағдарлама модульдері, сонымен бірге, лицензияның мерзімі біту күні туралы мәліметтерді береді. Операциялық жүйе және жүйелік ресурстар туралы ақпаратты беттің төменгі жағында табуға болады.

### 3.8.5.5 Контекстік мәзір

Нысанды (файлды) тінтуірдің оң жақ түймесімен басқаннан кейін контекстік мәзір көрсетіледі. Мәзірде нысанға қатысты орындауға болатын барлық әрекеттер тізіледі.

ESET Endpoint Antivirus басқару элементтерін контекстік мәзірге біріктіруге болады. Осы функция үшін реттеу параметрлері «Кеңейтілген орнату» ағашында **Пайдаланушы интерфейсі > Пайдаланушы интерфейсінің элементтері** астында қол жетімді.

**Контекстік мәзірге біріктіру** - ESET Endpoint Antivirus басқару элементтерін контекстік мәзірге біріктіреді.



## 3.9 Озық пайдаланушы

### 3.9.1 Профайл реттеуші

Профиль реттеуші ESET Endpoint Antivirus бағдарламасында екі жерде пайдаланылады – **Талап бойынша компьютерді қарап шығу** бөлімінде және **Жаңарту** бөлімінде.

#### Талап бойынша 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** тармағын басыңыз, содан кейін **Профильдер тізімі** жанында **Өңдеу** түймесін басыңыз. Бар қарап шығу профильдері тізілген **Таңдалған профиль** ашылмалы мәзірі көрсетіледі. Қажеттіліктеріңізге сай қарап шығу профилін жасауда көмек алу үшін [ThreatSense механизмінің параметрлерін орнату](#) бөлімінде қарап шығуды реттеудің әр параметрінің сипаттамасын қараңыз.

**Мысал:** Жеке қарап шығу профилін жасау керек және зерделі 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 **ОК** түймесін басыңыз.

#### Жаңарту

Жаңарту параметрлері бөліміндегі профиль өңдеуші пайдаланушылардың жаңа жаңарту профильдерін жасауына мүмкіндік береді. Компьютер жаңарту серверлеріне қосылудың бірнеше жолын пайдаланғанда ғана жеке таңдамалы профильдерді (яғни, әдепкі **Менің профилім** дегеннен басқа) жасаңыз және пайдаланыңыз.

Мысалы, жергілікті желідегі жергілікті серверге (айнаға) қосылатын, бірақ жергілікті желіден ажыратылған кезде (іс сапарлар) жаңартуларды тікелей ESET жаңарту серверлерінен жүктейтін ноутбук екі профильді пайдалануы мүмкін: біріншісі жергілікті серверге, екіншісі ESET серверлеріне қосуға арналған. Осы профильдер конфигурацияланған кейін **Құралдар > Жоспарлағыш** тармағына шарлап, жаңарту тапсырмасының параметрлерін өңдеңіз. Бір профильді негізгі, ал екіншісін қосымша деп көрсетіңіз.

**Таңдалған профиль** - Қазір пайдаланылатын жаңарту профилі. Оны өзгерту үшін профильді ашылмалы мәзірден таңдаңыз.

**Профильдер тізімі** - жаңа жаңарту профильдерін жасау немесе бар жаңарту профильдерін жою.

### 3.9.2 Диагностикалар

Диагностикалар ESET процестерінің (мысалы, *ekrn*) бағдарламаның бұзылуының дамптарын қамтамасыз етеді. Бағдарлама бұзылса, дамп жасалады. Бұл әзірлеушілерге ақауларды жоюға және әр түрлі ESET Endpoint 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** - Бағдарлама неге кенет бұзылғанын 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** - Бағдарлама күтпеген жағдайда тоқтаған кезде жүйе жадының барлық мазмұнын жазады. Толық жад дамында жад дамы жиналып жатқанда орындалып жатқан процестердің деректері болуы мүмкін.

**Нысан каталогы** - бұзылу кезінде дамп жасалатын каталог.

**Диагностикалау қалтасын ашу** - осы каталогты жаңа *Windows explorer* терезесінде ашу үшін **Ашу** түймесін басыңыз.

### 3.9.3 Импорттау және экспорттау параметрлері

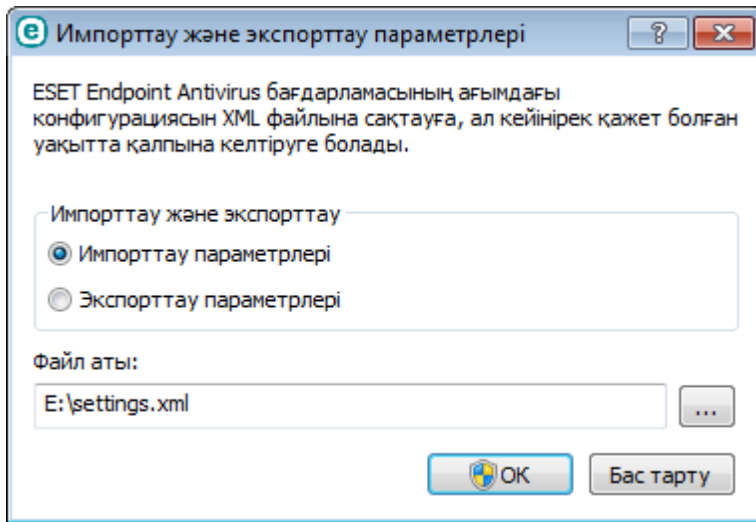
Реттелген ESET Endpoint Antivirus .xml конфигурация файлын **Орнату** мәзірінен импорттауға немесе экспорттауға болады.

Кейінгі уақытты қолдану үшін ESET Endpoint 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/экспорттау параметрлері** тармағына өтіңіз де, **Импорттау параметрлері** тармағын таңдаңыз. Конфигурацияның файл атауын енгізіңіз немесе импорттау керек конфигурацияға өту үшін ... түймешігін басыңыз.

Конфигурацияны экспорттау қадамдары осыған ұқсас. Негізгі бағдарлама терезесінде **Орнату > Импорттау/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.



### 3.9.4 Команда жолы

ESET Endpoint Antivirus бағдарламасының антивирус модулі команда жолы арқылы («ecls» командасымен) немесе бумамен («bat») қолмен қосуға болады. 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 файлының үстіне жазу (әдепкі - қосу)
/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)
/auid	әрекеттер көрсеткішін көрсету
/auto	барлық жергілікті дискілерді қарап шығу және автоматты түрде тазалау

### Қарап шығу құралының 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 бағдарламаларды қарап шығу
/no-unsafe	ықтимал қауіпті бағдарламаларды 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 әрекет жасайды (файлдарды жою алдында сізге хабарланбайды).
- rigorous - ecls.exe файлдың не екеніне қарамастан тазалауға әрекет жасамастан файлдарды жояды.
- delete - ecls.exe файлдарды тазалауға әрекет жасамастан жояды, бірақ Windows жүйелік файлдары сияқты маңызды файлдарды жоюдан ұстанады.

/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.

### 3.9.5 Жұмыссыз күйді анықтау

Жұмыссыз күйде анықтау параметрлерін **Кеңейтілген орнату** ішінде, **Антивирус > Жұмыссыз күйде қарап шығу > Жұмыссыз күйде анықтау** астында конфигурациялауға болады. Осы параметрлер мына уақытта [Жұмыссыз күйде қарап шығу](#) параметріне арналған триггерді анықтайды:

- экран суреті іске қосылған кезде,
- компьютер құлыптанды,
- пайдаланушы жүйеден шыққан кезде.

Әр түрлі жұмыссыз күйді анықтау триггерлерін қосу не өшіру үшін әр сәйкес күйдің қосқыштарын пайдаланыңыз.

### 3.9.6 ESET SysInspector

#### 3.9.6.1 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 Endpoint 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.

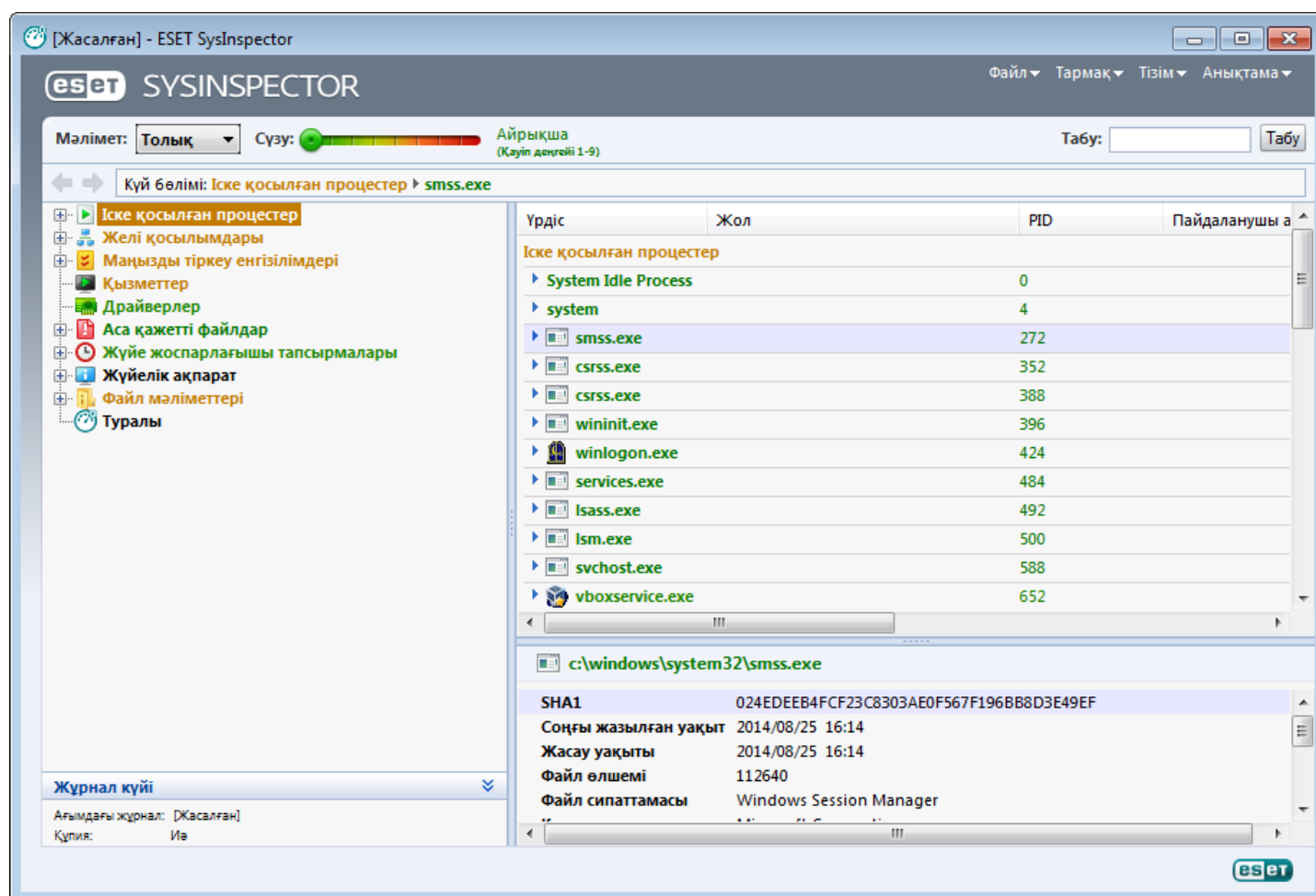
#### 3.9.6.1.1 ESET SysInspector бағдарламасын іске қосу

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 Endpoint Antivirus** түймешігін басыңыз) іске қосыңызға болады.

Бірнеше минутқа созылуы мүмкін бағдарламаның жүйені тексеруін күте тұрыңыз.

### 3.9.6.2 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.



#### 3.9.6.2.1 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 қауіп 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.

### 3.9.6.2.2 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.

**Ескөртпе:** 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.

### **Жөлілік 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 өнгізілімдері**

Жүйеге қатысты түрлі мәселелерге, мысалы іске қосылған кездегі бағдарламаларды көрсету, браузердің көмекші нысандары (ВНО), 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 айналылары, 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.

### 3.9.6.2.2.1 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

### 3.9.6.2.3 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.

Журнал күйі	
Ағымдағы журнал:	SysInspector-PETKO-PC-140922-1239-1.xml [Жүктелген]
Алдыңғы журнал:	SysInspector-PETKO-PC-140922-1239.xml [Жүктелген ZIP]
Салыстыру:	[Салыстыру нәтижесі]
Элементтердің шартты белгілерін салыстыру	
+ Қосылған элемент	☐ Тармақта қосылған элемент(тер)
– Алынып тасталған элемент	☐ Тармақта алынып тасталған элемент
⚙ Ауыстырылған файл	☐ Қосылған немесе алынып тасталған тармақтағы элемент(тер)
↕ Күй төмендетілді	☑ Тармақта ауыстырылған файл(дар)
↘ Күй арттырылды	

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:

```
SysInspector.exe current.xml previous.xml
```

### 3.9.6.3 Команда жолының параметрлері

ESET SysInspector бағдарламасы осы параметрлердің көмегімен есептер жасауды қолдайды:

<b>/gen</b>	GUI орнатусыз журналды тікелей пәрмен жолынан жасау
<b>/privacy</b>	маңызды ақпараты жоқ журнал жасау
<b>/zip</b>	шығыс журналын zip мұрағатында қысылған күйде сақтау
<b>/silent</b>	пәрмен жолынан журнал жасау кезінде өңдеу терезесін қысу
<b>/бос</b>	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.

### 3.9.6.4 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 **ОК** түймешігін басыңыз.



### 3.9.6.4.1 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.

### 3.9.6.4.2 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\khbexb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Бұл мысалда khbexb.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.

### 3.9.6.4.3 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 "%s" 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 шықыңыз 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.

### 3.9.6.5 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 есептік жазбасынан кіруге болады. Оны стандартты пайдаланушы немесе шектеулі пайдаланушы ретінде іске қосу операциялық орта туралы аз ақпарат жинауға алып келеді.

#### **ESET SysInspector бағдарламасы журнал файлы жасай ма?**

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

#### **ESET SysInspector журнал файлы қалай көруге болады?**

ESET SysInspector жасаған тіркеу файлы 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 нәліктен 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 қауіп туады. Руткитке қарсы арнайы құралсыз руткиттерді табу мүмкін емес дерлік.

#### **Нәліктен 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.

### 3.9.6.6 ESET Endpoint Antivirus ESET SysInspector бөлімі ретінде

ESET SysInspector бөлімін ESET Endpoint 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 журнал мен ескірек журналдың 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).

## 3.10 Глоссарий

### 3.10.1 Қауіптердің түрлері

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

#### 3.10.1.1 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.

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

### 3.10.1.2 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.

### 3.10.1.3 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 зиянды бағдарлама.
- **Тастаушы** - Жұққан компьютерде басқа да зиянды бағдарламалардың түрінен бас тарту мүмкіндіктері бар зиянды бағдарламалар.
- **Жүйеге жасырын кіруші** - Зиянды бағдарламалар қашықтағы шабуылдаушылармен байланысып, компьютермен қатынасып және оны басқаруға мүмкіндік береді.
- **Пернетақтық шпион** - (пернетақта тіркеуші) – пайдаланушы терген әр пернедегі әріпті жазып, ақпаратты қашықтағы шабуылдаушыларға жіберетін бағдарлама.
- **Нөмір теруші** - Зиянды бағдарламалар пайдаланушының Интернет жеткізушінің дәрежелі нөмірі арқылы қосылуына арналған. 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.

### 3.10.1.4 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 тырысқанда: 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 Endpoint Antivirus пайдаланушыларының белсенді руткиттерді анықтап, жоя алатын ұрлыққа қарсы технологиясының артықшылығы бар.

### 3.10.1.5 Жарнама бағдарламасы

Жарнама бағдарламасы дегеніміз – жарнаманы қолдайтын бағдарлама. Жарнамалық материалдарды көрсететін бағдарламалар осы санатқа жатады. Жарнама бағдарламалары жиі Интернет браузерінен автоматты түрде ішінде жарнамалары бар жаңа қалқымалы терезені ашады немесе браузердің бастапқы бетін өзгертеді. Жарнамалық бағдарлама жиі тегін бағдарламалардың ішіне салынып, жасаушыларға олардың бағдарламаларын (әдетте пайдалы) әзірлеу шығындарын жабуға мүмкіндік береді.

Жарнама бағдарламасының өзі қауіпті емес, тек жарнамалар пайдаланушылардың мазасын алады. 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. Бұл пайдаланушылар келісім бергендіктен, жарнама бағдарламалары жүйеге «заңды» жолмен жиі қатынауы ықтималдығын білдіреді. Бұл жағдайда, сақ болған жөн. Егер компьютерде жарнама бағдарламасы ретінде анықталған файл болса, оны жойған абзал, себебі оның құрамында зиянды код болу мүмкіндігі зор.

### 3.10.1.6 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.

### 3.10.1.7 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.

### 3.10.1.8 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 Endpoint Antivirus бағдарламасы осындай қауіптерді анықтау опциясын қамтамасыз етеді.

**Қауіпті 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 қауіпті ықтимал бағдарлама барын және іске қосулы екенін (және оны сіз орнатпаған болсаңыз) анықтасаңыз, желі әкімшісімен кеңесіңіз немесе ол бағдарламаны жойып тастаңыз.

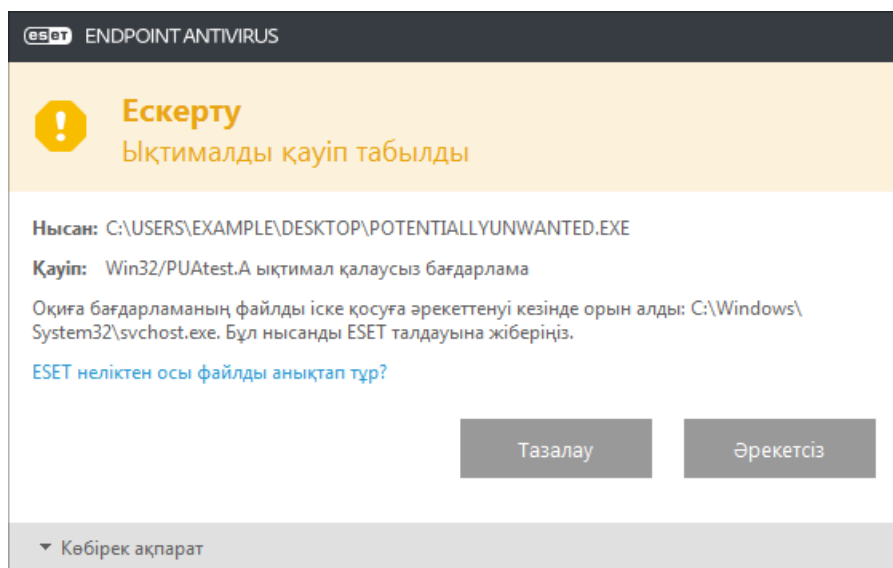
### 3.10.1.9 Ықтимал қалаусыз бағдарламалар

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.

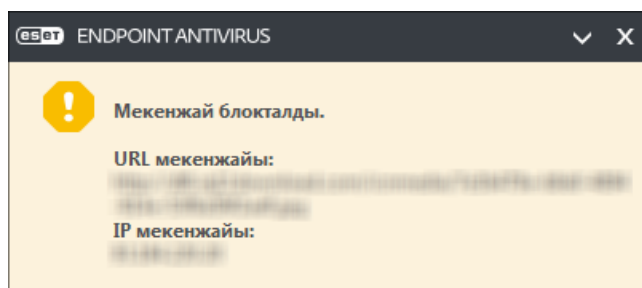
#### Ескерту - Ықтимал қауіп табылды

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. **Әрекетсіз**: бұл опция ықтимал қауіпке жүйеге кіруге рұқсат етеді.
3. Қолданбаға болашақта үзіліссіз компьютерде жұмыс істеуге рұқсат ету үшін **Қосымша ақпарат/Кеңейтілген опцияларды көрсету** тармағын басыңыз, содан кейін **Анықтауға қоспау** жанында құсбелгі қойыңыз.



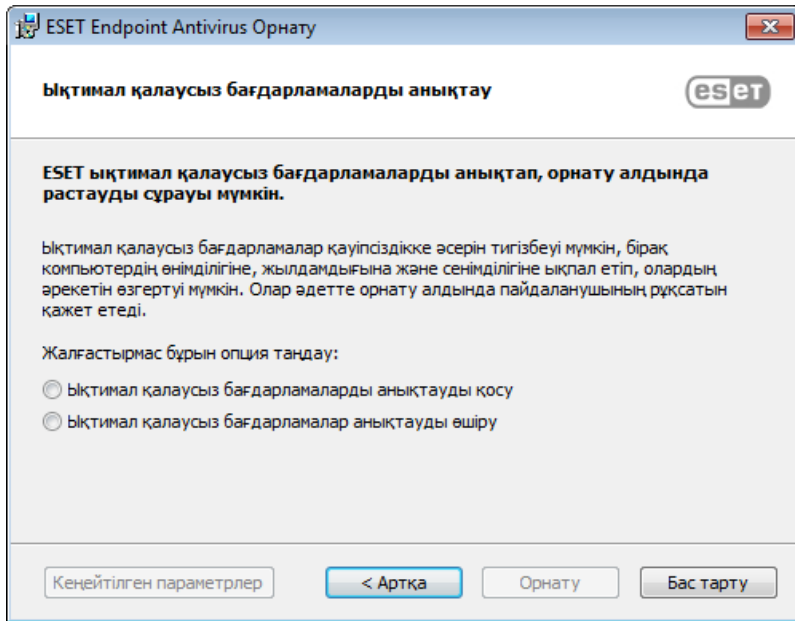
Ықтимал қалаусыз қолданба анықталса және оны тазалау мүмкін болмаса, экранның төменгі оң жақ бұрышында **Мекенжай блокталды** хабарландыру терезесі көрсетіледі. Бұл оқиға туралы қосымша ақпарат алу үшін негізгі мәзірден **Құралдар > Журнал файлдары > Сүзілген веб-сайттар** тармағына өтіңіз.






## Ықтимал қалаусыз қолданбалар - Параметрлер

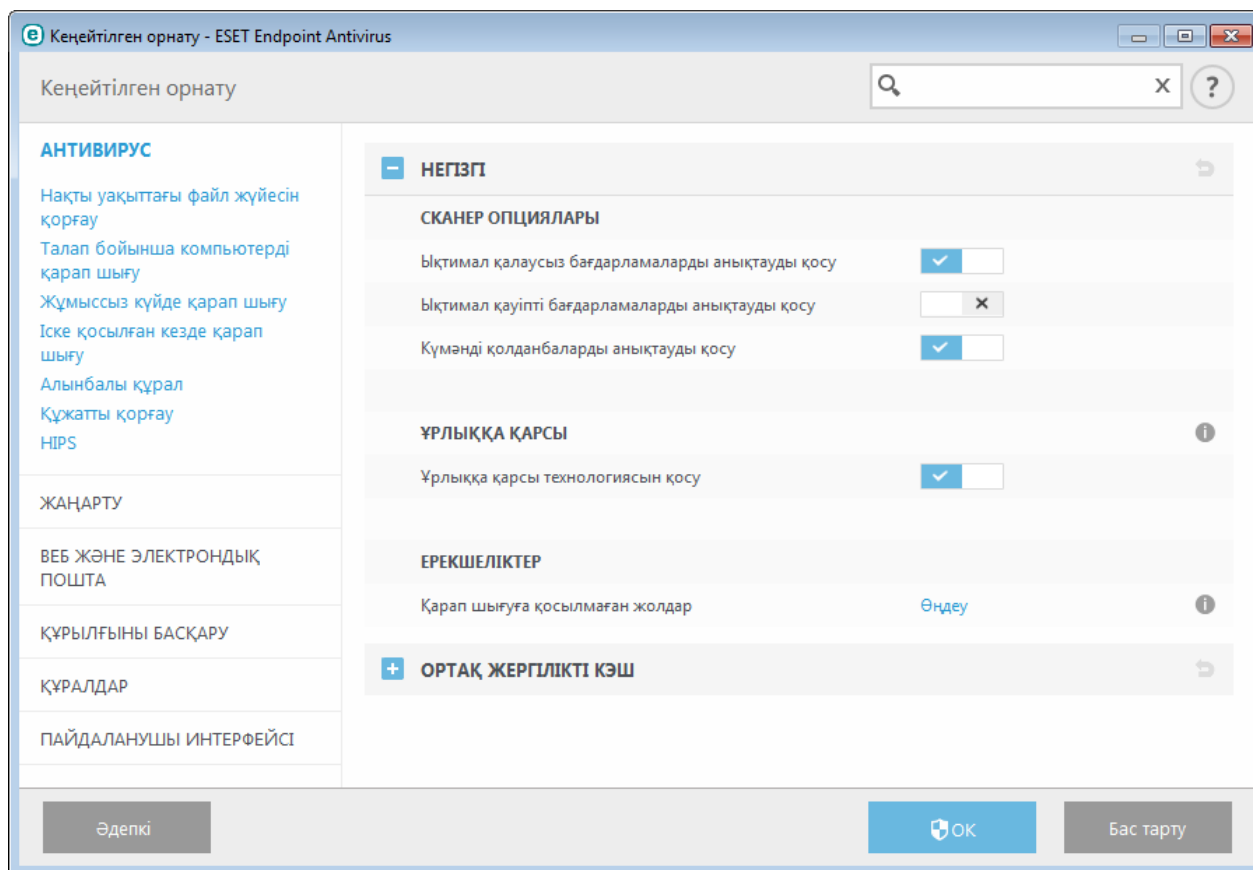
ESET өнімін орнатып жатқанда төменде көрсетілгендей ықтимал қалаусыз қолданбаларды анықтауды қосу-қоспау туралы шешім қабылдай аласыз:



 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 бағдарлама веб-браузердің басты бетіне және іздеу параметрлеріне өзгертулер енгізуі мүмкін. Сондай-ақ, файл-хостинг веб-сайттары көбінесе бағдарлама жеткізушісіне немесе жүктеуді алушыға өзгертулер жасалғаны туралы хабарламайды және өзгертуден оңай бас тартуға мүмкіндік бермейді. 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.

### 3.10.2 Электрондық пошта

Электрондық пошта – артықшылықтары көп заманауи байланыс үлгісі. Ол икемді, тез және тікелей барады, әрі 1990 жылдардың басында интернеттің дамуында шешуші рөл атқарды.

Екіншке орай, жоғары анонимдік деңгейі бар электрондық пошта мен интернетте спаминг сияқты заңсыз әрекеттерге арналған орын қалған. Спам ерікті жарнамаларды, жалған хабарларды және зиянды бағдарламалардың көбеюін 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:

- Мүмкіндігінше интернетте электрондық поштаңызды жарияламаңыз
- Электрондық поштаңыздың мекенжайын тек сенімді адамдарға беріңіз
- Ортақ бүркеншік аттарды мүмкіндігінше пайдаланбаңыз – бүркеншік аттар неғұрлым күрделі болса, қадағалау ықтималдығы соғұрлым төмен болады
- «Кіріс» қалтаңызға келген спамға жауап бермеңіз
- Интернет үлгілерін толтырғанда сақ болыңыз, әсіресе, «Иә, ақпарат алғым келеді» сияқты опциялардан сақ болыңыз.
- «Арнайы» электрондық пошта мекенжайларын пайдаланыңыз, мысалы, біреуі жұмысыңыз үшін, екіншісі достарыңызбен байланысу үшін және т.б.
- Электрондық поштаңыздың мекенжайын уақыт өте ауыстырып тұрыңыз
- Спамға қарсы шешімді пайдаланыңыз

### 3.10.2.1 Жарнамалар

Интернеттегі жарнама – жарнаманың ең қарқынды дамып келе жатқан салаларының бірі. Оның басты маркетингтік артықшылықтары – өте аз шығындар, туралық пен тиімділіктің жоғары деңгейі, сонымен бірге, хабарлар дереу 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.

### 3.10.2.2 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 өзіл немесе ойлап шығарылған әңгіме болады.

Компьютер вирусы бар жалған хабарлар алушыларға қорқыныш, сенімсіздік және күмән тудыруға тырысып, файлдарды жоятын және құпиясөздерді шығарып алатын немесе жүйесінде басқа зиянды әрекетті жүзеге асыратын "табылмайтын вирус" бар деп оларды сендіреді.

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. Көбінесе 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.

### 3.10.2.3 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 хабар 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.

### 3.10.2.4 Спам алаяқтығын анықтау

Жалпы алғанда, пошта жәшігіңізден спамды (ерікті электрондық пошта хабарлары) анықтауыңызға көмекетесетін бірнеше индикаторлар бар. Егер хабар кемінде мына шарттардың біразын орындаса, ол спам хабарға көп ұқсайды.

- Жіберуші мекенжайы контактілеріңіздің тізіміндегі ешкімге тиесілі емес.
- Сізге үлкен мөлшерде ақша ұсынылды, бірақ сіз оны алу үшін алдымен аз мөлшерде ақша жіберуіңіз қажет.
- Сізден әр түрлі алдау арқылы (деректерді тексеру, қаржылық операциялар) жеке деректеріңізді – банк есепшотының нөмірі, пайдаланушы аттары мен құпиясөздер, т.б. енгізуді сұрайды.
- Ол шет тілінде жазылған.
- Сізден қызығушылық танытпайтын өнімді сатып алуды сұрайды. Егер сіз бәрібір сатып алуға шешім қабылдасаңыз, хабар жіберушінің сенімді сатушы екеніне көз жеткізіңіз (негізгі өнім өндірушімен ақылдасыңыз).
- Кейбір сөздер спам сүзгісін алдау үшін қате жазылады. Мысалы "виагра"-ның орнына "ваигра", т. б.

### 3.10.3 ESET технологиясы

#### 3.10.3.1 Бүлдіруді блоктаушы

Бүлдіруді блоктаушы веб-браузерлер, PDF оқу құралдары, электрондық пошта клиенттері немесе MS Office компоненттері сияқты әдетте бүлдірілетін бағдарлама түрлерін күшейтуге арналған. Ол процестердің мінез-құлқында бүлдіруді көрсетуі мүмкін күдікті әрекет бар-жоғын бақылайды. Ол зиянкес файлдардың өздерін анықтауға фокусталатын әдістерден мүлде басқаша технологияны пайдалана отырпы шабуылдаушыларға бір қадам жақынырақ тағы бір қорғау қабатын қосады.

Бүлдіруді блоктаушы күдікті процесті анықтаған кезде ол процесті дереу тоқтатып, қауіп туралы деректерді жаза алады, ал олар кейін ESET Live Grid бұлт жүйесіне жіберіледі. Бұл деректертерді ESET лабораториясы өңдеп, белгісіз қауіптерден және нөлдік күн шабуылдардан (құралдар алдын ала конфигурацияланбаған жаңадан шығарылған зиянкес бағдарламалар) барлық пайдаланушыларды бұдан да жақсы қорғау үшін пайдаланады.

#### 3.10.3.2 Кеңейтілген жад сканері

Кеңейтілген жад сканері [Бүлдіруді блоктаушымен](#) бірге жұмыс істеп, шатастыру және/немесе шифрлау әрекетін пайдалану арқылы антивирустық өнімдердің анықтауын болдырмау үшін жасалған зиянкес бағдарламалардан жақсырақ қорғауды қамтамасыз етеді. Әдепкі эмуляция немесе эвристика қауіпті анықтамайтын жағдайда кеңейтілген жад сканері күдікті әрекетті анықтап және олар жүйе жадында өздерін көрсеткен кезде қауіптерді қарап шығу мүмкіндігі бар. Бұл шешімді тіпті күрделі шатастырылған зиянкес бағдарламасына қолдануға болады. Бүлдіруді блоктаушыдан ерекшелігі, бұл — орындаудан кейінгі әдіс, яғни, ол қауіпті анықтамай тұрып бір зиянкес әрекет орындалған болуы мүмкін. Дегенмен, басқа анықтау әдістері сәтсіз болған жағдайда ол қосымша қауіпсіздік қабатын ұсынады.

#### 3.10.3.3 ESET Live Grid

ThreatSense.Net® озық ерте ескерту жүйесі негізінде жасалған ESET Live Grid ESET пайдаланушылары дүние жүзінде жіберген деректерді пайдаланады және оларды ESET вирустар зертханасына жібереді. Жабайы жағдайлардан күдікті үлгілер мен метадеректерді ұсыну арқылы ESET Live Grid бағдарламасы тұтынушыларымыздың қажеттіліктеріне дереу көңіл бөлуге және ESET бағдарламасына соңғы қауіптерге дер кезінде жауап беруге мүмкіндік береді. ESET зиянкес бағдарламаларының зерттеушілері дұрыс нысанға көзделуге мүмкіндік беретін глобалдық қауіптердің дәл лездік суреті мен масштабын құрастыру ақпаратын пайдаланады. ESET Live Grid 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 санаталады. Бұл әрекет қарап шығуға едеуір оң әсерін береді.

Бұл репутация жүйесі зиянкес бағдарламалардың үлгілерін олардың қолтаңбалары пайдаланушыларға вирус қолтаңбасы дерекқоры жаңартулары арқылы күніне бірнеше рет жеткізілулеріне дейін тиімді анықтауға көмектеседі.

#### 3.10.3.4 Java бүлдірулерін блоктаушы

Java бүлдірулерін блоктаушы — бар ESET 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 әрекет жасалған Java бүлдірулерін әр түрлі қабаттарда (URL мекенжайын блоктау, файл жүктеу, т.б.) блоктау үшін сигнатуралар жасай алады.