Հակավիրուսային պաշտպանության ծրագրային միջոցների տեխնիկական պարամետրերը բավարարում են հետևյալ նշված պարամետրերը.

- հակավիրուսային պաշտպանության ծրագրային միջոցներ՝ աշխատատանքային կայանների և սերվերների համար,
- կառավարման գործիք, որը ապահովում է կապը սերվերի և պաշտպանված համակարգերի միջև,
  - կենտրոնացված կառավարման համակարգ, որը ապահովում է ծրագրերի թարմացումն և մշտադիտարկումը Windows օպերացիոն համակարգի համար,
  - կենտրոնացված կառավարման ծրագրային միջոցները պետք է ունենան WEB վահանակ՝ հաշվետվություններ ստեղծելու և կառավարելու համար;
  - Կենտրոնացված կառավարման համակարգչային ծրագիրը կարող է տեղադրվել Windows հարթակում,
  - անհայտ համակարգիչների հայտնաբերման համար գործիքների առկայություն, որոնք ավտոմատ կերպով որոնում են անձնական համակարգիչներ տեղական ցանցում, առանց դրանք ձեռքով որոնելու և ավելացնելու անհրաժեշտության,
  - Հակավիրուսային ծրագրային ապահովման հաճախորդների մասի կառավարման գործակալների տեղադրման տարբերակների առկայություն, ինչպիսիք են
    1. հեռահար կամ տեղային,
    2. տեղադրում, շարժական կրիչի կիրառմամբ, օրինակ USB,
    3. լոկալ տեղադրում,
  - Լիցենզիաներով կառավարման համար հատուկ ծրագրային գործիքների առկայություն: Դրա օգնությամբ կարելի է վերահսկել լիցենզիաները, ակտիվացված մոդուլները և լիցենզիաների հետ կապված իրադարձությունները, ինչպիսիք են դրա գործողության ժամկետի լրանալը, օգտագործումը և հավաստագրումը,
  - Արտադրանքների անվտանգության լրացուցիչ մակարդակի սպասարկում, որը ներառում է Microsoft Windows OC կառավարման տակ աշխատակայանների հակավիրուսային պաշտպանության ծրագրային միջոցների նկատմամբ պահանջներ,

- Microsoft- ի Windows- ի ընտանիքի կառավարման տակ գտնվող աշխատակայանների հակավիրուսային պաշտպանության ծրագրային միջոցները պետք է գործեն հետևյալ OC տարբերակների վրա. Microsoft Windows 10/11,
- Microsoft Windows OC ի ընտանիքի կառավարման տակ գործող աշխատակայանների հակավիրուսային պաշտպանության ծրագրային միջոցները պետք է ապահովեն հետևյալ գործառույթները՝

✓ Հակավիրուսային ծրագրային ապահովման ինտերֆեյսը պետք է ապահովի սենսորային էկրաններին և բարձր լուծմամբ էկրանների աջակցությունը,
✓ ռեզիդենտային հակավիրուսային մոնիտորինգ,
✓ հակավիրուսային ծրագրային ինտերֆեյսը ամբողջովին թաքցնելու ունակություն,
✓ հակավիրուսային սկանանավորում՝ օգտագործողի կամ ադմինիստրատորի հրամանով,
✓ պլանավորված հակավիրուսային սկանավորում,

- ✓ հակավիրուսային սկանավորում որոշակի պայմաններում,
- ✓ հակավիրուսային տվյալների բազաները թարմացնելուց հետո,
- ✓ ամեն անգամ համակարգիչը թողարկելուն պես,
- ✓ ամեն օր համակարգչի առաջին մեկնարկի ժամանակ,
- ✓ հաջողված ինտերնետ կամ VPN կապով,
- ✓ օգտատիրոջ մուտք,
- տրաֆիկի հակավիրուսային սկանավորում՝ ըստ հետևյալ արձանագրությունների. FTP, HTTP և HTTP, POP3 և POP3, ինչպես նաև IMAP և IMAP տրաֆիկը,
- պաշտպանություն դեռևս անհայտ վնասակար ծրագրերից ՝ էվրիստիկ վերլուծության հիման վրա,
- հայտերի համար ֆիլտրի ակտիվ ռեժիմ, ինչպես նաև ֆիլտրացված կամ պասիվ ռեժիմը բացառելու հնարավորություն՝ բացառված ծրագրերի համար,
- ֆիլտրում վստահելի հավելվածների համար,
- ենթատեքստային ընտրացանկից սկանավորում,
- վստահելի վեբ հասցեների ֆիլտրման անջատում,
- վստահելի IP հասցեների ֆիլտրման անջատում,
- վստահելի գործընթացները, ֆայլերը և թղթապանակները սկանավորումից բացառելու հնարավորությունը,
- ԱՀ կարգավիճակի, տեղադրված հավելվածների, ծառայությունների, ցանցային կապերի և այլնի վերաբերյալ ընդհանուր տեղեկատվությունը կենտրոնացված դիտելու ունակություն: Փոփոխություններին հետևելու և դրանք ավտոմատ կերպով համեմատելու ունակության միջոցով՝ օգտագործելով նկարներ՝ ժամանակային ընդմիջումով, ինչպես նաև փոփոխություններ կատարելու ունակությամբ, որոնք վերականգնում են համակարգի ճիշտ աշխատանքը,
- կենտրոնացված կառավարման սերվերին աշխատանքային կայանների համար հակավիրուսային լիցենզիաներ ներբեռնելու ունակություն ՝ առանց հակավիրուսային ծրագրակազմի լրացուցիչ փաթեթների, ներառյալ կառավարման գործակալների անհրաժեշտության,
- Web – էջերից ներբեռնվող վնասակար սցենարներից պաշտպանություն,
- փոստային հաճախորդների պաշտպանություն. Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail,
- սկանավորման գործընթացի արագացում այն օբյեկտների հաշվին, որոնց վիճակը նախկին ստուգումից հետո չի փոփոխվել,
- լոկալ քեշի ընդհանուր նկիրառման գործունեության առկայություն վիրտուալ միջավայարերում սկանավորման արագությունը բարձրացնելու համար,
- պաշտպանություն ֆիշինգից. պաշտպանում է գաղտնաբառերը և այլ գաղտնի տեղեկատվություն ստանալու փորձերից՝ արգելելով մուտքը վնասակար կայքեր, որոնք նման են նորմալ կայքերի,
- պաշտպանական մոդուլ՝ ցանցային հարձակումներից,
- հիշողության սկանավորման մոդուլի առկայություն, որը վերահսկում է գործընթացները և սկանավորում է վնասակար գործընթացները,

- Մոդուլի առկայություն, որը թույլ է տալիս ավտոմատ կերպով սկանավորել միացված արտաքին պահեստավորման սարքերի պարունակությունը, ինչպես նաև կիրառել ընդլայնված վերլուծություն՝ այդպիսի սարքերից ֆայլեր թողարկելու համար;
- Մոդուլի առկայություն, որը թույլ է տալիս կարգավորել մուտքի սահմանափակումները (թույլատրված չէ, միայն ընթերցում, ամբողջական մուտք, նախազգուշացում) յուրաքանչյուր օգտատիրոջ կամ օգտատերերի խմբի համար, ինչպես ըստ սարքի տեսակի (CD / DVD / Blu-Ray, USB տվյալների պահպանում, USB տպիչներ, պատկերի մշակման սարքեր, FireWire սարքերը, քարտերի ընթերցողները, քարդ-ռեդիրներ մոդեմները, LPT \ COM պորտեր, Bluetooth սարքերը), այնպես էլ ըստ տրված ատրիբուտների (արտադրող, մոդել, սերիական համար) նշում են նույն կանոնը մի քանի սարքերի համար,
- ինտեգրումը MS NAP-ի և CISCO NAC-ի հետ;
- հիշողության վթարային դամփերի ձևավորման հնարավորություն հավելվածի ձախողման դեպքում,
- վիրուսների տվյալների բազայի թարմացումները նախորդ վարկածները հետ բերելու և դրանց թարմացումները դադարեցնելու հնարավորություն,
- ինտեգրում Windows անվտանգության կենտրոնի հետ,
- Windows թարմացումների կենտրոնի հետ ինտեգրում՝ հայտնաբերված խոցելիությունները ծածկող պատչեր տեղադրելու համար՝ «ոչ անհրաժեշտ» թարմացումներից մինչև «կրիտիկական» անհրաժեշտ անհրաժեշտ թարմացումներ ընտրելով,
- Գործարկվող ֆայլերի և համակարգչային բեռնիչ տարածքների սկանավորման կարգավորում ՝ որպես առանձին առաջադրանք,
- Հավելվածի ինքնապաշտպանության տեխնոլոգիաներ, դիմումի ծառայության հեռակա չարտոնված կառավարման դեմ պաշտպանություն, ինչպես նաև գաղտնաբառով դիմումի պարամետրեր մուտքի պաշտպանություն, ինչը թույլ է տալիս խուսափել վնասակար ծրագրերից, չարամիտ կամ չորակավորված օգտատերերից,
- համակարգի ընթացիկ թարմացումների ստուգում,
- Ծրագրային ապահովման միջոցների և հակավիրուսային տվյալների բազաների թարմացում տարբեր աղբյուրներից, ինչպես հաղորդակցման ուղիներով, այնպես էլ տեղեկատվության օտարվող կրիչների վրա,
- լոգերի և հաշվետվությունների արտահանում XML, TXT, DAT, DMP ձևաչափերով,
- ամպային տեխնոլոգիայի առկայություն `անհայտ սպառնալիքների հայտնաբերման համար, հեղինակության ծառայության վրա հիմնված կիրառման վերահսկում,
- վթարների վերականգնման սկավառակներ ստեղծելու ունակություն:

Microsoft Windows OC ընտանիքի կառավարման տակ սերվերների համար հակավիրուսային պաշտպանության ծրագրային միջոցների նկատմամբ պահանջներ

Microsoft Windows օպերացիոն համակարգի ընտանիքի աշխատող սերվերային համակարգերի համար հակավիրուսային ծրագրակազմը պետք է գործի հետևյալ ՕՀ տարբերակների վրա. Microsoft Windows Hyper-V Server 2012 R2, Microsoft Windows ՕՀ ընտանիքի կառավարման տակ գործարկող ֆայլերի սերվերների հակավիրուսային պաշտպանության ծրագիրը պետք է ապահովի հետևյալ գործառույթը.

- ռեզիդենտային հակավիրուսային մոնիթորինգ,
- հակավիրուսային սկանավորում օգտագործողի կամ ադմինիստրատորի հրամանով,
- պլանավորված հակավիրուսային սկանավորում,
- հակավիրուսային սկանավորում որոշակի պայմաններում,
- տրաֆիկի հակավիրուսային սկանավորում՝ օգտագործելով հետևյալ արձանագրությունները. FTP, HTTP և HTTP, ինչպես նաև տրաֆիկի POP3 և POP3s արձանագրությունները,
- Hyper-V հակավիրուսային սկանավորում,
- պաշտպանություն դեռևս անհայտ վնասակար ծրագրերից՝ էվրիստիկ վերլուծության հիման վրա,
- թաքնված ֆայլերի / համակարգի անոմալիաների հայտնաբերում,
- առաջադրանքների մեկնարկը ժամանակացույցով և / կամ գործառնական համակարգը բեռնավորելուց անմիջապես հետո
- հակավիրուսային պլանավորման մեջ երրորդ կողմի հավելվածը թողարկելու առաջադրանք ստեղծելու ունակություն,
- պաշտպանություն վեբ-կայքերից ներբեռնված վնասակար սցենարներից,
- ինտերֆեյսի հրամանի տողից հակավիրուսային փաթեթի պարամետրերը կարգավորելու ունակություն,
- սկանավորման մոդուլների քանակը սահմանելու հնարավորություն `սկանավորման արագությունը մեծացնելու համար,
- վեբ ռեսուրսների հասանելիությունը վերահսկելու հնարավորություն `ստեղծելով արգելափակված կամ թույլատրված կայքերի ցուցակը, ինչպես նաև արգելելով բոլոր կայքերը, բացառությամբ թույլատրվածների ցուցակի մեջ նշվածները,
- հավելվածների համար ֆիլտրի ակտիվ ռեժիմ, ինչպես նաև ֆիլտրման կամ պասիվ ռեժիմին անցնելու հնարավորություն բացառված հավելվածների համար,
- ենթատեքստային ընտրացանկից սկանավորում,
- վստահելի վեբ-հասցեների ֆիլտրման անջատում,
- բազմաշերտ սկանավորում,
- ԱՀ կարգավիճակի, տեղադրված ծրագրերի, ծառայությունների, ցանցային կապերի և այլնի վերաբերյալ ընդհանուր տեղեկատվություն կենտրոնացված կերպով դիտելու ունակություն: փոփոխություններին հետևելու և դրանք ավտոմատ կերպով համեմատելու ունակության միջոցով `օգտագործելով նկարներ՝ ժամանակային ընդմիջումով, ինչպես նաև փոփոխություններ կատարելու ունակությամբ (գործընթացների և դրայվերների դադարեցում, գրանցամատյանի և համակարգային ֆայլերի ջնջում և վերականգնում), որոնք վերականգնում են համակարգի ճիշտ աշխատանքը,

- արտադրանքի միջուկը և բոլոր հիմնական մոդուլները չեն պահանջում վերաբեռնում և ակտիվ են տեղադրումից անմիջապես հետո,
- կենտրոնացված կառավարման սերվերին աշխատանքային կայանների համար հակավիրուսային լիցենզիաներ ներբեռնելու ունակություն ՝ առանց հակավիրուսային ծրագրակազմի լրացուցիչ փաթեթների, ներառյալ կառավարման գործակալների անհրաժեշտության,
- որոշակի պայմաններում կամ որոշակի ժամանակահատվածում հակավիրուսային պլանավորված արտադրության հետ կապված առաջադրանքներ ստեղծելու ունակություն,
- Web – էջերից ներբեռնվող վնասակար սցենարներից պաշտպանություն,
- փոստային հաճախորդների պաշտպանություն. Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail;
- սկանավորման գործընթացի արագացում այն օբյեկտների հաշվին, որոնց վիճակը նախկին ստուգումից հետո չի փոփոխվել,
- լոկալ քեշի ընդհանուր կիրառման գործունեության առկայություն վիրտուալ միջավայրերում սկանավորման արագությունը բարձրացնելու համար, պաշտպանություն ֆիշինգից,
- պաշտպանություն էքսփլոյթից,
- տեղեկատվության շարժական կրիչների և սարքերի (USB) արգելափակում,
- Մոդուլի առկայություն, որը թույլ է տալիս կարգավորել մուտքի սահմանափակումները (թույլատրված չէ, միայն ընթերցում, ամբողջական մուտք, նախազգուշացում) յուրաքանչյուր օգտատիրոջ կամ օգտատերերի խմբի համար, ինչպես ըստ սարքի տեսակի (CD / DVD / Blu-Ray, USB տվյալների պահպանում, USB տպիչներ, պատկերի մշակման սարքեր , FireWire սարքերը, քարտերի ընթերցողները, քարդ-ռեդիրներ մոդեմները, LPT \ COM պորտեր, Bluetooth սարքերը), այնպես էլ ըստ տրված ատրիբուտների (արտադրող, մոդել, սերիական համար) նշում են նույն կանոնը մի քանի սարքերի համար,
- ինտեգրում Windows անվտանգության կենտրոնի հետ,
- Windows թարմացումների կենտրոնի հետ ինտեգրացիա՝ հայտնաբերված խոցելիությունները ծածկող պատչեր տեղադրելու համար՝ «ոչ պարտադիր» թարմացումներից մինչև «կրիտիկական» անհրաժեշտ թարմացումներ ընտրելով,
- Windows Management Instrumentation աջակցություն,
- Գործարկվող ֆայլերի և համակարգչային բեռնիչ տարածքների սկանավորման կարգավորում ՝ որպես առանձին առաջադրանք,
- Կլաստերային համակարգերի աջակցություն հակավիրուսդային ԱՀ ավտոմատ միացման հնարավորությամբ,
- օպերացիոն համակարգի ընթացիկ թարմացումների ստուգում,
- սպասարկող սերվերների վրա տեղի ունեցող կարևոր իրադարձությունների վերաբերյալ ադմինիստրատորների տեղեկացման բազմաթիվ եղանակների առկայություն (փոստային հաղորդագրություն, բացվող պատուհանիկ, իրադարձությունների մատյանում գրանցում),

- Ծրագրային ապահովման և հակավիրուսային տվյալների բազաների թարմացում տարբեր աղբյուրներից, ինչպես հաղորդակցման ուղիներով, այնպես էլ տեղակտվության օտարվող կրիչների միջոցով,
- վնասակար կոդի նմուշները վիրուսային փորձագետներին ավտոմատ կերպով կամ ձեռքով փոխանցելու համակարգի առկայություն,
- վթարային վերականգնման սկավառակներ ստեղծելու ունակություն:

Հակավիրուսային կառավարման համակարգի նկատմամբ պահանջները

Բոլոր պաշտպանվող ռեսուրսների համար կառավարման ծրագրային միջոցները ապահովում են հետևյալ գործառնական հնարավորությունները.

- անհայտ համակարգիչների հայտնաբերման համար գործիքների առկայություն, որոնք ավտոմատ կերպով որոնում են համակարգիչներ տեղական ցանցում, առանց դրանք ձեռքով որոնելու և ավելացնելու անհրաժեշտության,
- հակավիրուսային պաշտպանության ծրագրային գործիքների, պարամետրերի, կառավարման կենտրոնացված տեղադրում / թարմացում / հեռացում,
- տեղեկատվության կենտրոնացված հավաքածու և զեկուցում հակավիրուսային պաշտպանության կարգավիճակի վերաբերյալ,
- պաշտպանված կապ սերվերի և հաճախորդի միջև,
- կենտրոնացված կառավարման ծրագրակազմը պետք է ունենա WEB վահանակ՝ զեկույցները ղեկավարելու և ստեղծելու համար,
- կենտրոնացված կառավարումը կարող է իրականացվել ցանկացած սարքից՝ Վեբ դիտարկիչի միջոցով,
- հաշվետվությունների ստեղծում տեսողական գրաֆիկական տեսքով,
- տեղեկամատյանների և հաշվետվությունների արտահանում HTML, TXT, CSV, PDF ձևաչափերով,
- շարժական սարքից անվտանգության աուդիտի հաշվառման հեռակա ստեղծելու ունակություն,
- օպերացիոն համակարգերի կամ ձեռքով ռեժիմում համապատասխան գործակալի տեղադրման փաթեթը ավտոմատ կերպով ընտրելու հնարավորություն,
- հաճախորդների համար անվտանգության քաղաքականությունների կարգավորում;
- վերջնական հաճախորդների համար հատուկ սցենարի հեռակա գործելու ունակություն, որը նախատեսված է համակարգի կրիտիկական օբյեկտներըբ ջնջելու / փոփոխելու համար,
- ԱՀ վերագործարկելու անհրաժեշտության բացակայություն հակավիրուսային պաշտպանության կառավարման համակարգը տեղադրելուց հետո,
- հակավիրուսային պաշտպանության ծրագրի և հակավիրուսային տվյալների բազաների ավտոմատացված թարմացում,
- թարմացումների տրամադրումը օգտատիրոջ աշխատանքային կայաններին դրանք ստանալուց անմիջապես հետո,
- կենտրոնացված կարանտին

- Կառավարվող համակարգիչների խմբեր ստեղծելու ունակություն ինչպես ձեռքով, այնպես էլ ավտոմատացված կերպով՝ Active Directory կառուցվածքի հիման վրա;
- Active Directory-ի հետ համաժամացման հնարավորությունը ինչպես ժամանակացույցով, այնպես էլ ձեռքով,
- հաշիվների համար սերվերի պարամետրերում կատարված փոփոխությունների աուդիտ,
- Ծրագրային ապահովման և հակավիրուսային տվյալների բազաների թարմացում տարբեր աղբյուրներից՝ ինչպես հաղորդակցման ուղիներով, այնպես էլ տեղեկատվական կրիչների միջոցով,
- տեղադրված հակավիրուսային պաշտպանության ծրագրերով աշխատանքում տեղի ունեցող իրադարձությունների մասին տեղեկացնելու մեխանիզմ և դրանց վերաբերյալ փոստով ծանուցումների բաշխումը կազմաձևելու կարողության մասին,
- վնասակար կոդի նմուշները վիրուսային փորձագետներին ավտոմատ կերպով կամ ձեռքով փոխանցելու համակարգի առկայություն,
- Դինամիկ խմբերի ստեղծման հնարավորություն, որոնցում դինամիկ կերպով կներառվեմ հաճախորդների կայանները տվյալ խմբերի պահանջներին համապատասխան,
- Վիճակագրական և դինամիկ խմբերի հետ աշխատանք,
- Ցանցի ադմինիստրատորին ծանուցելու տարբեր եղանակներ (e-mail-ով, SNMP ծուղակի կիրառմամբ),
- Սերվերի կարգավորումների և տվյալների բազային ռեզերվային պատճենների ստեղծման հնարավորություն,
- MS SQL, MySQL տվյալների բազաների աջակցություն:

Լիցենզիաների կառավարման համար հատուկ ծրագրային գործիքի առկայություն: Դրա օգնությամբ կարելի է լիցենզիաներին, ակտիվացված մոդուլներին և լիցենզիաների հետ կապված իրադարձություններին, ինչպիսիք են ժամկետի լրանալը, օգտագործումը և հավաստագրումը: Գործիքի հետ աշխատանքը տարբեր դերերի ներքո `որպես լիցենզիայի տիրոջ կամ որպես անվտանգության ադմինիստրատոր:

Հետևյալ գործողությունները կատարելու հնարավորություն,

- դիտարկել լիցենզիայի կարգավիճակը իրական ժամանակում,
- հետևել առանձին սարքեր (և միևնույն ժամանակ անջատել դրանք),
- Կարգավորել լիցենզիայի իրադարձություններին վերաբերող ծանուցումները,
- Միևնույն հաշվին նշանակել բազմաթիվ լիցենզիաներ,
- Կարգավորել ծանուցումները լիցենզիայի կարգավիճակի առավել հարմար դիտանցման համար,
- համաժամացման գործառույթի առկայությունը կենտրոնական կառավարման սերվերի հետ,
- վիրուսային սիգնատուրաների լոկալ պահեստ ստեղծելու համար հատուկ գործիքների առկայություն, առանց կենտրոնական կառավարման սերվեր օգտագործելու,
- հանգույցների վրա լիցենզիաների ապաակտիվացման հնարավորության առկայություն կառավարման սերվերում առաջադրանքների ստեղծման միջոցով,

- Վերլուծության բարձր արագություն. 5 րոպեի ընթացքում տրամադրել անհայտ նմուշների 90% -ի վերլուծություն,
- Շարժունակություն - ֆայլերը վերլուծելու հնարավորություն՝ անկախ օգտագործողների գտնվելու վայրից ՝ կորպորատիվ ցանցում կամ դրա սահմաններից դուրս,
- Կասկածելի ֆայլերը ձեռքով կամ ավտոմատ կերպով ուղարկելու հնարավորության առկայություն՝ քաղաքականության կոնֆիգուրացիայի հիման վրա,
- Անվտանգության կենտրոնի վեբ վահանակից կամ ակտիվացված ծառայության միջոցով հաճախորդի համակարգիչներից ֆայլերը ձեռքով ուղարկելու հնարավորություն,
- Անվտանգության ապահովման կենտրոնի API միջոցով ծառայության գործողությունները կառավարելու հնարավորություն,
- Մեծ ֆայլեր մինչև 64 ՄԲ ուղարկելու ունակություն,
- Ֆայլի մասին հաշվետվությունը պետք է պարունակի հետևյալ տեղեկությունները,
- Ֆայլը ուղարկող համակարգչի անունը / հասցեն,
- ֆայլը ուղարկած համակարգչում օգտատիրոջ նշումը,
- Ֆայլի անվանումը և դրա ամբողջական ուղին ուղարկողի ֆայլային համակարգում:
- Ֆայլի չափը,
- Ֆայլի կատեգորիա (ֆայլի տեսակը),
- Պարամետրերի զեկույցում առկայությունը, վիճակը և կարգավիճակ,
- Վարակված չէ. Հայտնաբերման մոդուլները չեն նշում նմուշը որպես վնասակար,
- Կասկածելի - Հայտնաբերման մոդուլը ֆայլի վարքը սահմանում է որպես կասկածելի, բայց ոչ վնասակար,
- Վնասակար - Ֆայլի պահվածքը համարվում է վնասակար,
- Անվտանգության ապահովման կենտրոնի վահանակում բոլոր փոխանցված ֆայլերի ցուցակի տրամադրմանը գործառնության առկայություն: Ուղարկված ֆայլերի ցուցակը կարելի է տեսնել վահանակների առանձնացված հատվածում,
- Անվտանգության ապահովման Կենտրոնի վահանակում նմուշների ուղարկման կարգավորումների հնարավորություն:

Հակավիրուսային բազաների թարմացման նկատմամբ պահանջները

Թարմացվող հակավիրուսային տվյալների բազաները ապահովում են հետևյալ գործառնական հնարավորությունը.

- իրականացրել է թարմացումների հայելի ստեղծելու հնարավորությունը տրաֆիկի խնայողության համար,
- թարմացումների տեսակները. Վիրուսի սիգնատուրայի տվյալների բազաների թարմացումը, ծրագրային բաղադրիչների թարմացում, միջուկի թարմացումը,
- թարմացումները կարող են տարածվել տեղեկատվության էլեկտրոնային կրիչների վրա (FDD \ CD \ DVD \ USB-drive):

Գործառնական փաստաթղթավորման պահանջներ

Հակավիրուսային պաշտպանության բոլոր ծրագրային ապահովման ապրանքների, ներառյալ կառավարման գործիքների գործառնական փաստաթղթերը պետք է ներառեն փաստաթղթեր անգլերեն կամ ռուսերեն լեզվով, ներառյալ.

- օգտատիրոջ ուղեցույց (ադմինիստրատորի),
- ադմինիստրատորի հեռահար կառավարման միջոցների ուղեցույց,
- Փաստաթղթերը, որոնք տրամադրվում են հակավիրուսային գործիքների հետ, պետք է մանրամասն նկարագրեն համապատասխան հակավիրուսային պաշտպանության միջոցի տեղադրման, կարգավորման և շահագործման գործընթացը:

Տեխնիկական աջակցության պահանջներ

Հակավիրուսային ծրագրային ապահովման տեխնիկական աջակցությունը.
Տրամադրվում է արտադրողի կողմից էլեկտրոնային փոստով, կայքով կամ հեռախոսով.

- Արտադրողի Web -կայքը ունի տեխնիկական աջակցության հատուկ բաժին, համալրվող գիտելիքների բազա և անգլալեզու, ռուսալեզու ֆորում: