ՊԵՏՈՒԹՅԱՆ ԿԱՐԻՔՆԵՐԻ ՀԱՄԱՐ ԱՊՐԱՆՔԻ ՄԱՏԱԿԱՐԱՐՄԱՆ
ՊԱՅՄԱՆԱԳԻՐ N ԳՀԱՊՁԲ-20-1/10-1

ք. Երևան

25.05.2020թ.

ՀՀ պաշտպանության նախարարությունը, ի դեմս ՀՀ ՊՆ ՆՏԱ գլխավոր վարչության պետ Ն. Յոլչյանի, որը գործում է նախարարության կանոնադրության հիման վրա՝ այսուհետ «Գնորդ», մի կողմից և «Էյչ Գրուպ» ՍՊԸ-ն, ի դեմս ընկերության տնօրեն Կ. Հարությունյանի, որը գործում է ընկերության կանոնադրության հիման վրա՝ այսուհետ «Վաճառող» մյուս կողմից, կնքեցին սույն պայմանագիրը հետևյալի մասին:

1. ՊԱՅՄԱՆԱԳՐԻ ԱՌԱՐԿԱՆ

1.1. Վաճառողը պարտավորվում է սույն պայմանագրով (այսուհետ՝ պայմանագիր) սահմանված կարգով, ծավալներով, ժամկետներում և հասցեով Գնորդին մատակարարել պայմանագրի N 1 հավելվածով՝ Տեխնիկական բնութագիր-գնման-ժամանակացուցով նախատեսված ապրանքը (այսուհետ՝ ապրանք), իսկ Գնորդը պարտավորվում է ընդունել ապրանքը և վճարել դրա համար:

2. ԿՈՂՄԵՐԻ ԻՐԱՎՈՒՆՔՆԵՐԸ ԵՎ ՊԱՐՏԱԿԱՆՈՒԹՅՈՒՆՆԵՐԸ

2.1 Գնորդն իրավունք ունի՝

2.1.1 Ապրանքը պայմանագրով սահմանված ժամկետում Վաճառողի կողմից չմատակարարելու դեպքում հրաժարվել ապրանքից, եթե մատակարարման ժամկետները խախտվել են 10 օրից ավելի:

2.1.2 Եթե հանձնվել է անպատշաճ որակի՝ պայմանագրով նախատեսված տեխնիկական բնութագրին չհամապատասխանող ապրանք՝

ա) պահանջել հատուցելու ապրանքի անպատշաճ որակի լինելու պատճառով իր կատարած ծախսերը.

բ) չընդունել ապրանքն՝ իր հայեցողությամբ սահմանելով անպատշաճ որակի ապրանքը պայմանագրին համապատասխանող որակի ապրանքով անհատույց փոխարինման ողջամիտ ժամկետ և պահանջել Վաճառողից վճարելու պայմանագրի 6.3 կետով նախատեսված տուգանքը.

գ) հրաժարվել պայմանագիրը կատարելուց և պահանջել վերադարձնելու ապրանքի համար վճարված գումարը:

2.1.3 Եթե հանձնվել է պայմանագրով որոշվածից պակաս քանակի ապրանք, ապա՝

ա) պահանջել լրացնելու ապրանքի պակաս հանձնված քանակը,

բ) հրաժարվել հանձնված ապրանքից և դրա համար վճարելուց, իսկ եթե ապրանքի համար վճարվել է, ապա պահանջել վերադարձնելու վճարված գումարը և վճարելու պայմանագրի 6.2 կետով նախատեսված տույժը:

2.1.4 Եթե հանձնվել է տեսակի պայմանի խախտմամբ ապրանք, իր ընտրությամբ՝

ա) ընդունել տեսակի վերաբերյալ պայմանին համապատասխանող ապրանքը և հրաժարվել մնացած ապրանքներից.

բ) հրաժարվել հանձնված բոլոր ապրանքներից և պահանջել վճարելու պայմանագրի 6.2 կետով նախատեսված տույժը.

գ) պահանջել տեսակի վերաբերյալ պայմանին չհամապատասխանող ապրանքի անհատույց փոխարինում պայմանագրով նախատեսված տեսակին համապատասխան ապրանքով:

2.1.5 Վաճառողի կողմից մատակարարման ժամկետների խախտման դեպքում իր հայեցողությամբ սահմանել ապրանքի մատակարարման նոր ժամկետ և պահանջել Վաճառողից վճարելու պայմանագրի 6.2 կետով նախատեսված տույժը:

2.1.6 Վաճառողից պահանջել հատուցելու վնասները, եթե Գնորդը Վաճառողի կողմից պարտավորությունը խախտելու հետևանքով պայմանագրի լուծումից հետո ողջամիտ ժամկետում այլ անձից ավելի բարձր, սակայն ողջամիտ գնով գնել է ապրանք՝ պայմանագրով նախատեսվածի փոխարեն՝ պայմանագրով սահմանված և դրա փոխարեն կնքված գործարքի գների միջև տարբերության չափով, ինչպես նաև ապրանքն այլ անձից ձեռք բերելու համար իր կատարած բոլոր անհրաժեշտ և ողջամիտ ծախսերը:

2.1.7 Միակողմանի լուծել պայմանագիրը (լրիվ կամ մասնակի), եթե Վաճառողն էականորեն խախտել է պայմանագիրը.

2.1.7.1 Վաճառողի կողմից պայմանագիրը խախտելն էական է համարվում, եթե՝

ա) մատակարարվել է անպատշաճ որակի ապրանք որը չի կարող փոխարինվել Գնորդի համար ընդունելի ժամկետում.

բ) ապրանքի մատակարարման ժամկետները խախտվել են 10 օրից ավելի,

2.1.8 Ձնհել ապրանքը և հայտնաբերված թերությունների մասին անհապաղ տեղեկացնել Վաճառողին:

2.2 Գնորդը պարտավոր է՝

2.2.1 Կատարել պայմանագրին համապատասխան մատակարարված ապրանքի ընդունումն ապահովող բոլոր անհրաժեշտ գործողությունները:

2.2.2 Վաճառողի հանձնած ապրանքից պայմանագրին համապատասխան հրաժարվելու դեպքում, ապահովել այդ ապրանքի պատասխանատու պահպանությունը և դրա մասին անհապաղ տեղեկացնել Վաճառողին:

2.2.3 Պայմանագրով նախատեսված կարգով և ժամկետներում մատակարարված ապրանքն ընդունելու դեպքում Վաճառողին վճարել վերջինիս վճարման ենթակա գումարները, իսկ վճարման ժամկետի խախտման դեպքում՝ նաև պայմանագրի 6.5 կետով նախատեսված տույժը:

2.2.4 Ապրանքի քանակի, տեսականու, որակի մասին պայմանագրի պայմանները խախտելու մասին Վաճառողին ծանուցել թերությունը հայտնաբերելուց հետո անմիջապես կամ այն բանից հետո՝ ողջամիտ ժամկետում, երբ պայմանագրի համապատասխան պայմանի խախտումը պետք է հայտնաբերված լիներ՝ ելնելով ապրանքի բնույթից և նշանակությունից:

2.2.5 Պայմանագրի 2.3.3 կետի համաձայն պայմանագրի լուծումից հետո Վաճառողին հատուցել վերջինիս պատճառված և սահմանված կարգով հիմնավորված վնասները:

2.3 Վաճառողն իրավունք ունի՝

2.3.1 Գնորդից պահանջել ընդունելու պայմանագրով նախատեսված կարգով, ծավալներով, ժամկետներում և հասցեով մատակարարված ապրանքը:

2.3.2 Գնորդից պահանջել վճարելու պայմանագրով նախատեսված կարգով, ծավալներով, ժամկետներում և հասցեով մատակարարված և Գնորդի կողմից ընդունված ապրանքի համար իրեն վճարման ենթակա գումարները:

2.3.3 Միակողմանի լուծել պայմանագիրը (լրիվ կամ մասնակի), եթե Գնորդն էականորեն խախտել է պայմանագիրը:

2.3.3.1 Գնորդի կողմից պայմանագիրը խախտելն էական է համարվում, եթե բազմիցս խախտվել են ապրանքի համար վճարելու ժամկետները:

2.3.4 Գնորդի համաձայնությամբ վաղաժամկետ մատակարարել ապրանքը:

2.4 Վաճառողը պարտավոր է՝

2.4.1 Գնորդին հանձնել ապրանքը՝ պայմանագրով նախատեսված կարգով, ծավալներով, ժամկետներում և հասցեով:

2.4.2 Ապահովել ապրանքի մատակարարումը պայմանագրի 2.1.2 կետի բ) ենթակետին և (կամ) 2.1.5 կետին համապատասխան՝ Գնորդի կողմից սահմանված ժամկետներում:

2.4.3 Գնորդին հանձնել երրորդ անձանց իրավունքներից ազատ ապրանք:

2.4.5 Գնորդին հանձնել պայմանագրով նախատեսված որակի և քանակի ապրանք՝ պայմանագրով նախատեսված ժամկետներում և հասցեով, իսկ Գնորդի պահանջով տրամադրել ապրանքի որակը հավաստող՝ ՀՀ օրենսդրությամբ սահմանված փաստաթղթեր:

2.4.6 Թերի մատակարարում թույլ տալու դեպքում, պայմանագրով նախատեսված կարգով, լրացնել թերի մատակարարվածը:

2.4.7 Հետ տանել Գնորդի կողմից պայմանագրի 2.2.2 կետին համապատասխան՝ պատասխանատու պահպանության ընդունված ապրանքը կամ ողջամիտ ժամկետում տնօրինել այն, ինչպես նաև հատուցել ապրանքը պատասխանատու պահպանության ընդունելու, այն իրացնելու կամ Վաճառողին վերադարձնելու հետ կապված անհրաժեշտ ծախսերը:

2.4.8 Պայմանագրով նախատեսված դեպքերում վճարել պայմանագրի 6.2 և 6.3 կետերով նախատեսված տույժը և տուգանքը:

2.4.9 Գնորդին հանձնել ապրանքի պատկանելիքները և համապատասխան փաստաթղթերը:

2.4.10 Պայմանագրի 2.1.7 կետի համաձայն պայմանագրի լուծումից հետո Գնորդին հատուցել վերջինիս պատճառված և սահմանված կարգով հիմնավորված վնասները:

2.4.11 Որակավորման և պայմանագրի ապահովում ներկայացրած անձը պարտավոր է ապահովումների գործողության ընթացքում լուծարման կամ սնանկացման գործընթաց սկսելու դեպքում դրա մասին նախապես գրավոր տեղեկացնել Գնորդին:

3. ՊԱՅՄԱՆԱԳՐԻ ԳԻՆԸ ԵՎ ՎՃԱՐՄԱՆ ԿԱՐԳԸ

3.1 Պայմանագրի գինը կազմում է 22 998 000 (քսաներկու միլիոն ինը հարյուր իննսունութ հազար) ՀՀ դրամ, ներառյալ ԱԱՀ-ն: Պայմանագրի գինը ներառում է պայմանագրի կատարումն ապահովելու նպատակով Վաճառողի կողմից կատարվելիք բոլոր վճարները (ծախսերը), այդ թվում՝ հարկերը, տուրքերը, փոխադրման, ապահովագրման ծախսերը, պարգևավճարները և ակնկալվող շահույթը:

Ապրանքի մատակարարման գինը կայուն է և Վաճառողն իրավունք չունի պահանջել ավելացնելու, իսկ Գնորդը նվազեցնելու այդ գինը:

3.3 Գնորդն իրեն մատակարարված ապրանքի դիմաց վճարում է ՀՀ դրամով անկանխիկ՝ դրամական միջոցները Վաճառողի հաշվարկային հաշվին փոխանցելու միջոցով: Դրամական միջոցների փոխանցումը

կատարվում է հանձման-ընդունման արձանագրության հիման վրա՝ պայմանագրի վճարման ժամանակացույցով (հավելված N 2) նախատեսված չափերով և ամիսներին: Եթե արձանագրությունը կազմվում է տվյալ ամսվա 20-ից հետո և այդ ամսում վճարման ժամանակացույցով նախատեսված են ֆինանսական միջոցներ, ապա վճարումն իրականացվում է 15 բանկային օրվա ընթացքում, բայց ոչ ուշ, քան 10.12.2020թ.:

4. ԱՊՐԱՆՔԻ ՈՐԱԿԸ ԵՎ ԵՐԱՇԽԻՔԸ

4.1 Վաճառողը երաշխավորում է մատակարարված ապրանքի որակի համապատասխանությունը պետական ստանդարտի պահանջներին:

5. ԱՊՐԱՆՔԻ ՀԱՆՁՆՈՒՄԸ ԵՎ ԸՆԴՈՒՆՈՒՄԸ

5.1 Մատակարարված ապրանքն ընդունվում է Գնորդի և Վաճառողի միջև հանձնման-ընդունման արձանագրության ստորագրմամբ: Ապրանքը Գնորդին հանձնելու փաստը ֆիքսվում է Գնորդի և Վաճառողի միջև երկկողմ հաստատված փաստաթղթով՝ նշելով փաստաթղթի կազմման ամսաթիվը:

Մինչև պայմանագրով ապրանքի մատակարարման համար նախատեսված օրը ներառյալ Վաճառողը Գնորդին է տրամադրում իր կողմից ստորագրված՝ ապրանքը Գնորդին հանձնելու փաստը ֆիքսող փաստաթուղթը (հավելված N 3.1), իսկ էլեկտրոնային գնումների armeps համակարգի միջոցով (գործողության իրականացման ձեռնարկը տեղադրված է www.procurement.am հասցեով գործող կայքի «Էլեկտրոնային գնումներ» բաժնում)՝ նաև հանձնման-ընդունման արձանագրությունը (հավելված N 3): Ընդ որում Վաճառողը հանձնման-ընդունման արձանագրությունը չի կնքում, հաստատում է էլեկտրոնային ստորագրությամբ՝ լրացնելով միայն այն սյունակները, որոնք վերաբերում են իր տվյալներին (լրացման կարգը տեղադրված է www.procurement.am հասցեով գործող կայքի «Օրենսդրություն» բաժնի «Ֆինանսների նախարարի հրամաններ» ենթաբաժնում):

5.2 Եթե մատակարարված ապրանքը համապատասխանում է պայմանագրի պայմաններին, Գնորդը պայմանագրի 5.1 կետում նշված փաստաթղթերը ստանալու օրվան հաջորդող աշխատանքային օրվանից հաշված հինգ աշխատանքային օրվա ընթացքում ստորագրում և էլեկտրոնային գնումների armeps համակարգի միջոցով Վաճառողին է տրամադրում իր կողմից ստորագրված հանձնման-ընդունման արձանագրությունը և դրա ստորագրման համար հիմք հանդիսացած դրական եզրակացությունը:

5.3 Եթե մատակարարված ապրանքը կամ դրա մի մասը չի համապատասխանում պայմանագրի պայմաններին, ապա Գնորդը չի ստորագրում հանձնման-ընդունման արձանագրությունը և պայմանագրի 5.2 կետում նշված ժամկետում էլեկտրոնային գնումների armeps համակարգի միջոցով Վաճառողին հետ է վերադարձնում հանձնման-ընդունման արձանագրությունը և դրա չստորագրման համար հիմք հանդիսացած բացասական եզրակացությունը: Սույն կետի կիրառման դեպքում Գնորդը ձեռնարկում է նման իրավիճակի համար պայմանագրով նախատեսված միջոցները և Վաճառողի նկատմամբ կիրառում է պայմանագրով նախատեսված պատասխանատվության միջոցներ:

5.4 Եթե պայմանագրի 5.2 կետով սահմանված ժամկետում Գնորդը չի ընդունում մատակարարված ապրանքը կամ չի մերժում դրա ընդունումը, ապա մատակարարված ապրանքը համարվում է ընդունված և պայմանագրի 5.2 կետով սահմանված վերջնաժամկետին հաջորդող աշխատանքային օրը Գնորդը էլեկտրոնային գնումների համակարգի միջոցով Վաճառողին է տրամադրում իր կողմից ստորագրված հանձնման-ընդունման արձանագրությունը:

6. ԿՈՂՄԵՐԻ ՊԱՏԱՍԽԱՆԱՏՎՈՒԹՅՈՒՆԸ

6.1 Վաճառողը պատասխանատվություն է կրում հանձնած ապրանքի որակի և պայմանագրով նախատեսված մատակարարման ժամկետների պահպանման համար:

6.2 Վաճառողի կողմից պայմանագրով նախատեսված ապրանքի մատակարարման ժամկետների խախտման դեպքում Վաճառողից յուրաքանչյուր ուշացված աշխատանքային օրվա համար գանձվում է տույժ՝ մատակարարման ենթակա, սակայն չմատակարարված ապրանքի գնի 0,05 (զրո ամբողջ հինգ հարյուրերրորդական) տոկոսի չափով:

6.3 Պայմանագրի 1.1 կետում նշված տեխնիկական բնութագրին չհամապատասխանող ապրանք մատակարարելու յուրաքանչյուր դեպքում Վաճառողից գանձվում է տուգանք՝ պայմանագրի գնի 0,5 (զրո ամբողջ հինգ տասնորդական) տոկոսի չափով: Ընդ որում տուգանքը հաշվարկվում է նաև ապրանքի մատակարարումը սույն պայմանագրով սահմանված ժամկետում կատարելու, սակայն պատվիրատուի կողմից այդ չընդունվելու դեպքում:

6.4 Պայմանագրի 6.2 և 6.3 կետերով նախատեսված տույժը և տուգանքը հաշվարկվում և հաշվանցվում են Վաճառողին վճարման ենթակա գումարների հետ:

6.5 Գնորդի կողմից պայմանագրի 3.3 կետով նախատեսված ժամկետի խախտման համար Գնորդի նկատմամբ յուրաքանչյուր ուշացված աշխատանքային օրվա համար հաշվարկվում է տույժ՝ վճարման ենթակա, սակայն չվճարված գումարի 0,05 (զրո ամբողջ հինգ հարյուրերրորդական) տոկոսի չափով:

6.6 Պայմանագրով չնախատեսված դեպքերում կողմերն իրենց պարտավորությունները չկատարելու կամ ոչ պատշաճ կատարելու համար պատասխանատվություն են կրում ՀՀ օրենսդրությամբ սահմանված կարգով:

6.7 Տույժերի և (կամ) տուգանքի վճարումը Կողմերին չի ազատում իրենց պայմանագրային պարտավորությունները լրիվ կատարելուց:

7. ԱՆՀԱՂԹԱՀԱՐԵԼԻ ՈՒԺԻ ԱԶԴԵՑՈՒԹՅՈՒՆԸ (ՖՈՐՍ-ՄԱԺՈՐ)

Պայմանագրով պարտավորություններն ամբողջությամբ կամ մասնակիորեն չկատարելու համար կողմերն ազատվում են պատասխանատվությունից, եթե դա եղել է անհաղթահարելի ուժի ազդեցության հետևանքով, որը ծագել է սույն պայմանագիրը կնքելուց հետո, և որը կողմերը չէին կարող կանխատեսել կամ կանխարգելել: Այդպիսի իրավիճակներ են երկրաշարժը, ջրհեղեղը, հրդեհը, պատերազմը, ռազմական և արտակարգ դրություն հայտարարելը, քաղաքական հուզումները, գործադուլները, հաղորդակցության միջոցների աշխատանքի դադարեցումը, պետական մարմինների ակտերը և այլն, որոնք անհնարին են դարձնում սույն պայմանագրով պարտավորությունների կատարումը: Եթե արտակարգ ուժի ազդեցությունը շարունակվում է 3 (երեք) ամսից ավելի, ապա կողմերից յուրաքանչյուրն իրավունք ունի լուծել պայմանագիրը՝ այդ մասին նախապես տեղյակ պահելով մյուս կողմին:

8. ԱՅԼ ՊԱՅՄԱՆՆԵՐ

8.1 Պայմանագիրն ուժի մեջ է մտնում Կողմերի ստորագրման պահից և գործում է մինչև կողմերի՝ պայմանագրով ստանձնած պարտավորությունների ողջ ծավալով կատարումը:

Պայմանագրով նախատեսված կողմերի իրավունքների և պարտականությունների կատարման պայման է հանդիսանում պայմանագիրը ՀՀ ֆինանսների նախարարության կողմից հաշվառված լինելու հանգամանքը:

8.2 Պայմանագրից ծագած՝ կողմի վճարային պարտավորությունը չի կարող դադարել այլ պայմանագրից ծագած՝ հակընդդեմ պարտավորության հաշվանցով, առանց կողմերի գրավոր և կնիքով հաստատված համաձայնության: Պայմանագրից ծագած պահանջի իրավունքը չի կարող փոխանցվել այլ անձի, առանց պարտապան կողմի գրավոր համաձայնության:

8.3 Այն դեպքում, երբ օրենքով նախատեսված կարգով օրենքի պահանջների կատարման նկատմամբ հսկողության կամ վերահսկողության կամ բողոքների քննության արդյունքում արձանագրվում է, որ պայմանագիրը կնքելու նպատակով կազմակերպված գնման գործընթացում, մինչև պայմանագրի կնքումը, Վաճառողը ներկայացրել է կեղծ փաստաթղթեր (տեղեկություններ և տվյալներ), կամ վերջինիս ընտրված մասնակից ճանաչելու մասին որոշումը չի համապատասխանում Հայաստանի Հանրապետության օրենսդրությանը, ապա այդ հիմքերն ի հայտ գալուց հետո Գնորդը միակողմանիորեն լուծում է պայմանագիրը, եթե արձանագրված խախտումները մինչև պայմանագրի կնքումը հայտնի լինելու դեպքում գնումների մասին Հայաստանի Հանրապետության օրենսդրության համաձայն հիմք կհանդիսանային պայմանագիրը չկնքելու համար: Ընդ որում, Գնորդը չի կրում պայմանագրի միակողմանի լուծման հետևանքով Վաճառողի համար առաջացող վնասների կամ բաց թողնված օգուտի ռիսկը, իսկ վերջինս պարտավոր է Հայաստանի Հանրապետության օրենքով սահմանված կարգով փոխհատուցել իր մեղքով Գնորդի կրած վնասներն այն ծավալով, որի մասով պայմանագիրը լուծվել է:

8.4 Պայմանագրի հետ կապված վեճերը ենթակա են քննության Հայաստանի Հանրապետության դատարաններում:

8.5 Պայմանագրում փոփոխություններ և լրացումներ կարող են կատարվել միայն Կողմերի փոխադարձ համաձայնությամբ՝ համաձայնագիր կնքելու միջոցով, որը կհանդիսանա պայմանագրի անբաժանելի մասը:

Արգելվում է պայմանագրում կատարել այնպիսի փոփոխություններ, որոնք հանգեցնում են գնվող ապրանքի ծավալների կամ ձեռք բերվող ապրանքի միավորի գնի կամ պայմանագրի գնի արհեստական փոփոխման:

Պայմանագրի կողմերից անկախ գործոնների ազդեցությամբ պայմանագրի փոփոխման յուրաքանչյուր դեպք սահմանում է Հայաստանի Հանրապետության կառավարությունը:

8.6 Ապրանքի մատակարարման ժամկետը կարող է երկարաձգվել մինչև պայմանագրով այդ ժամկետը լրանալը՝ Վաճառողի առաջարկության առկայության դեպքում, պայմանով, որ Գնորդի մոտ չի վերացել ապրանքի օգտագործման պահանջը, իսկ Վաճառողի առաջարկությունը ներկայացվել է ոչ ուշ, քան պայմանագրով ի սկզբանե մատակարարման համար սահմանված ժամկետը լրանալուց առնվազն 5 օրացուցային օր առաջ: Ընդ որում սույն կետով սահմանված դեպքում ապրանքի մատակարարման ժամկետը կարող է երկարաձգվել մեկ անգամ մինչև 30 օրացուցային օրով, բայց ոչ ավել քան պայմանագրով սահմանված ժամկետն է:

8.7 Պայմանագրի պատշաճ կատարման պայմաններում կողմերի (Վաճառող կամ Գնորդ) օգուտները (խնայողություններ) կամ կրած վնասները տվյալ կողմի օգուտը կամ կրած վնասն են:

Պայմանագրի կողմերի՝ երրորդ անձանց նկատմամբ պարտավորությունները՝ ներառյալ պայմանագրի կատարման շրջանակում Վաճառողի կնքած այլ գործարքները և դրանցից բխող պարտավորությունները,

դուրս են պայմանագրի կարգավորման դաշտից և չեն կարող ազդել պայմանագրի կատարման արդյունքն ընդունելու վրա: Այդ գործարքների և դրանցից բխող պարտավորությունների կատարման հետ կապված հարաբերությունները կարգավորվում են այդ գործարքների հետ կապված հարաբերությունները կարգավորող նորմերով, և դրանց համար պատասխանատու է Վաճառողը:

8.8 Պայմանագիրը չի կարող փոփոխվել կողմերի պարտավորությունների մասնակի չկատարման հետևանքով կամ ամբողջությամբ լուծվել կողմերի փոխադարձ համաձայնությամբ՝ բացառությամբ՝ Հայաստանի Հանրապետության օրենսդրությամբ սահմանված կարգով ապրանքի մատակարարման համար անհրաժեշտ ֆինանսական հատկացումների նվազեցման դեպքերի: Ընդ որում, պայմանագրի կողմերի՝ պարտավորությունների մասնակի չկատարման կամ ամբողջությամբ լուծման կողմերի փոխադարձ համաձայնությունն անհրաժեշտ է ձեռք բերել նախքան Հայաստանի Հանրապետության օրենսդրությամբ սահմանված կարգով ապրանքի մատակարարման համար անհրաժեշտ ֆինանսական հատկացումների նվազեցումը:

8.9 Վաճառողի կողմից ստանձնած պարտավորությունները չկատարելու կամ ոչ պատշաճ կատարելու հիմքով պայմանագիրն ամբողջությամբ կամ մասնակի միակողմանի լուծելու մասին ծանուցումը Գնորդը հրապարակում է www.procurement.am հասցեով գործող ինտերնետային կայքի «Պայմանագրերը միակողմանի լուծելու մասին ծանուցումներ» բաժնում նշելով հրապարակման ամսաթիվը: Վաճառողը, պայմանագիրը միակողմանի լուծելու վերաբերյալ, համարվում է պատշաճ ծանուցված՝ ծանուցումը, սույն կետով սահմանված հրապարակվելուն հաջորդող օրվանից: Պայմանագիրն ամբողջությամբ կամ մասնակի միակողմանի լուծելու մասին ծանուցումը տեղեկագրում հրապարակվելու օրը Գնորդը այն ուղարկվում է նաև Վաճառողի էլեկտրոնային փոստին:

8.10 Պայմանագրի կապակցությամբ ծագած վեճերը լուծվում են բանակցությունների միջոցով: Համաձայնություն ձեռք չբերելու դեպքում վեճերը լուծվում են դատական կարգով:

8.11 Պայմանագիրը կազմված է 17 էջից, կնքվում է երկու օրինակից, որոնք ունեն հավասարազոր իրավաբանական ուժ, յուրաքանչյուր կողմին տրվում է մեկական օրինակ: Պայմանագրի N 1, N 2, N 3 և N 3.1 հավելվածները, համարվում են պայմանագրի անբաժանելի մասը:

8.12 Պայմանագրի հետ կապված հարաբերությունների նկատմամբ կիրառվում է Հայաստանի Հանրապետության իրավունքը:

8.13 Սույն պայմանագով նախատեսված՝ Գնորդի իրավունքներն ու պարտականություններն իրականացնում է ՀՀ ՊՆ ՆՏԱ գլխավոր վարչությունը, իսկ պատասխանատու ստորաբաժանում է հանդիսանում ՀՀ ՋՈՒ կապի և ԱԿՀ վարչությունը:

9. ԿՈՂՄԵՐԻ ՀԱՍՑԵՆԵՐԸ, ԲԱՆԿԱՅԻՆ ՎԱՎԵՐԱՊԱՅՄԱՆՆԵՐԸ ԵՎ ՍՏՈՐԱԳՐՈՒԹՅՈՒՆՆԵՐԸ

ԳՆՈՐԴ	ՎԱՃԱՌՈՂ
ՀՀ պաշտպանության նախարարություն	«Էյչ Գրուպ» ՍՊԸ
ք. Երևան Բագրևանդի 5	ք. Երևան, Բաշինջաղյան 1, 13 շ., բն. 30,
ՀՀ ՖՆ գործառնական վարչություն	«Արմսվիսբանկ» ՓԲԸ
Հ/Հ 900011144079	Հ/Հ 2500010488760100
ՀՎՀՀ 02522157	ՀՀ 01254973
ՀՀ ՊՆ ՆՏԱ գլխավոր վարչության պետ	Տնօրեն
Ն. ՅՈԼՉՅԱՆ	Կ. ՀԱՐՈՒԹՅՈՒՆՅԱՆ

ՏԵԽՆԻԿԱԿԱՆ ԲՆՈՒԹԱԳԻՐ ԵՎ ԳՆՄԱՆ ԺԱՄԱՆԱԿԱՑՈՒՅՑ

հակավիրուսային համակարգչային ծրագրային արտոնագիր
2AVDR Kaspersky Total Security for Business. 1000-1499 Node 2 year Renewal License:

Ընդհանուր պահանջներ
Հակավիրուսային միջոցները պետք է ներառեն.
• Ծրագրային հակավիրուսային պաշտպանության համակարգեր Windows աշխատակայանների համար:
• Ծրագրային հակավիրուսային պաշտպանության համակարգեր աշխատակայաններիեւ Linux ֆայլերի սերվերների համար:
• Ծրագրային հակավիրուսային պաշտպանության համակարգեր ֆայլային սերվերների, ձեռնարկության մակարդակի սերվերների եւ Windows տերմինալային սերվերներիհամար:
• Հակավիրուսային պաշտպանություն և հակասպամ, Microsoft Exchange սերվերների համար:
• Linux փոստի սերվերների համար հակավիրուսային պաշտպանության եւ սպամի զտման համակարգեր:
• Linux պրոքսի սերվերների հակավիրուսայինպաշտպանության ծրագրային ապահովում:
• Կենտրոնացված կառավարման, մոնիտորինգի եւ արդիականացման համար ծրագրային ապահովում:
• Վնասակար ծրագրային ապահովման եւ հարձակումների սիգնատուրաների թարմացվող տվյալների բազաներ:
• Էկսպլուատացիոն փաստաթղթեր ռուսերեն լեզվով:

Windows- ի աշխատասեղանների համար հակավիրուսայինպաշտպանության ծրագրային ապահովմանպահանջներ
Windows- ի աշխատասեղանների համար հակավիրուսային պաշտպանության գործիքները պետք է գործեն հետեւյալ համակարգերում աշխատող համակարգիչների վրա,
Microsoft Windows 7 Professional / Enterprise /Ultimate x86 / x64;
Microsoft Windows 7 Professional / Enterprise /Ultimate SP1 և ավելի բարձր x86 / x64;
Microsoft Windows 8 Professional / Enterprise x86 / x64;
Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
Microsoft Windows 10 Pro / Enterprise x86 / x64;
Microsoft Windows Server 2012 R2 Standard x64;
Microsoft Windows Server 2012 Standard / Foundation x64;
Microsoft Small Business Server 2011 Standard x64;
Microsoft Windows Server 2008 R2 Standard / Enterprise x64 SP1;
Microsoft Windows Server 2008 Standard / Enterprise x86 / x64 SP2;
Windows- ի աշխատանքային կայանների հակավիրուսային պաշտպանության գործիքները պետք է ապահովեն հետեւյալ ֆունկցիոնալությունը.
• Հակավիրուսային սկանավորում իրական ժամանակում եւ ըստ պահանջի:
• Էվրիստիկ անալիզատոր, որը թույլ է տալիս ճանաչել եւ արգելափակել նախկինում անհայտ չարամիտ ծրագրերը:
• Գործառույթների ավտոմատ սկիզբ, ըստ ժամանակացույցի եւ / կամ օպերացիոն համակարգի բեռնվելուց անմիջապես հետո:
• RAR, ARJ, ZIP, CAB ֆորմատի արխիվներում գտնվող ֆայլերի հակավիրուսային սկանավորում եւ բուժում, այդ թվում `գաղտնաբառով պաշտպանված:
• Ամպային պաշտպանություն նոր սպառնալիքների դեմ, թույլ տալով, որ հայտը իրական ժամանակում կապ արտադրողի հատուկ ռեսուրսների հետ, ստանալով դատավճիռ `սկսվող ծրագրի կամ ֆայլի մասին:
• Էլեկտրոնային նամակագրության պաշտպանությունը վնասակար ծրագրերից, մուտքի եւ ելքի տրաֆիկի ստուգում `հետեւյալ արձանագրություններում. IMAP, SMTP, POP3, MAPI, NNTP - անկախ օգտագործվող էլփոստի կլիենտական ծրագրային ապահովումից,
• Վեբ տրաֆիկի պաշտպանություն, HTTP, FTP- ի միջոցով օգտագործողի համակարգչին հասնող օբյեկտների սկանավորում, ներառյալ էվրիստիկական վերլուծություն, վտահելի կայքերը նշելու ունակությամբ:
• Վեբ էջերից բեռնված բաններների եւ «pop-up»-ների արգելափակում:
• Ֆիշինգի սայտերի ճանաչում եւ արգելափակում:
• ICQ- ի եւ MSN- ի տրաֆիկի ստուգում, ապահովելով ինտերնետ-պեյջերների հետ աշխատելու անվտանգությունը:
• Շրագրի աննորմալ վարքագիծը որոշելու ունակություն, շնորհիվ, այդ ծրագրի գործողությունների հաջորդականության վերլուծման: Բուժման ընթացքում վնասակար ծրագրային ապահովման գործողությունները վերադարձնելու ունակությունը, ներառյալ վնասակար ծրագրերի կողմից կոդավորված ֆայլերի վերականգնումը:
• Ծրագրերի արտոնությունները սահմանափակելու ունակություն, ինչպիսիք են ռեեստրի գրելը, ֆայլերի եւ թղթապանակների հասանելիությունը: Ծրագրի ռեպուտացիայի հիման վրա սահմանափակումների մակարդակների ավտոմատ հայտնաբերում:

• BadUSB- ի հարձակումներից պաշտպանվելու մեխանիզմների առկայություն:
• Ներկառուցված Firewall, որը թույլ է տալիս սահմանել ցանցային փաթեթային կանոններ կոնկրետ արձանագրությունների (TCP, UDP) եւ պորտերի համար: Հնարավորություն ստեղծել ցանցային կանոններ հատուկ ծրագրերի համար:

• Պաշտպանություն ցանցային հարձակումներից օգտագործելով ներխուժման հայտնաբերման եւ կանխարգելման համակարգ (IDS / IPS) եւ ցանցային գործունեության կանոններ ամենատարածված ծրագրերի աշխատանքի համար, ցանկացած տեսակի համակարգչային ցանցերում, այդ թվում անլար.
• կոմպոնենտի առկայություն, որը թույլ է տալիս ստեղծել հատուկ կանոններ, որոնք արգելում են ծրագրերի տեղադրումը եւ / կամ գործարկումը: Կոմպոնենտը պետք է վերահսկի ծրագրերը, ըստ մետատվյալների, MD5 կամ sha256 checksum-ի, եւ նախանշված կատեգորիաների, տրամադրվող ծրագրային արտադրողի կողմից, ինչպես նաեւ թույ տալ բացառություններ ավելացնել որոշ Active Directory օգտագերերին:
• Վերահսկել օգտագործողի աշխատանքը արտաքին I / O սարքերով ըստ սարքի տեսակի եւ / կամ տվյալների BUS-ով, իրենց ID- ով վստահելի սարքերի ցանկը ստեղծելու ունակությամբ եւ արտաքին սարքեր օգտագործելու արտոնությունների տրամադրման հնարավորություն Active Directory- ից որոշակի օգտվողների համար:
• իրականացում անձնագիրը փորձի մոնիտորինգի է ինտերնետին, այդ թվում `բացահայտ արգելման կամ թույլտվության մատչելիության ռեսուրսների որոշակի բնույթի, ինչպես նաեւ հնարավորություն է արգելափակել որոշակի տեսակի տեղեկատվության (աուդիո, վիդեո եւ այլն): Ծրագրային ապահովումը թույլ է տալիս Ձեզ մուտք գործել ժամանակի ընդմիջումներ մոնիտորինգի համար, ինչպես նաեւ հանձնել այն միայն կոնկրետ օգտագործողներին Active Directory- ից:
• Ինտերնետի հետ աշխատանքի հսկում, ինչպես նաև ակնհայտ արգելք կամ թույլտվություն, կոնկրետ տիպի ռեսուրսների այցելելուն, ինչպես նաև կոնկրետ տիպի ինֆորմաիայի (աուդիո, վիդեո և այլ): Ծրագրային ապահովումը պիտի թույլ տա մուտքագրել կառավարման ժամանակային ինտերվալներ, ինչպես նաև աշխատացնել այն միայն որոշ Active Directory օգտատերերին:
• Արագացնել սկանավորման գործընթացը `շրջանցելով օբյեկտները, որոնց վիճակը չի փոխվել վերջին սկանից:
• Աշխատացնել հատուկ աշխատանք `հայտնաբերելու համար խոցելիությունը համակարգչում տեղադրված ծրագրերում, ինչպես նաեւ հայտնաբերված խոցելիների մասին զեկուցելու հնարավորություն:
• Համակարգչային ռեսուրսների օգտագործման ճկուն կառավարում, ֆայլի տարածքի սկանավորման ընդացքում, օգտատերի համար հարմարավետության ապահովման համար:
• Պաշտպանություն ծրագրի սերվիսի ոչ թույլատրված, հեռակա կառավորումից, ինչպես նաև ծրագրի պարամետրերին հասանելության պաշտպանություն գաղտնաբառի միջոցով, որը թույլ կտա խուսափել պաշտպանության անջատումը չարամիտ ծրագրերի կողմից, ոճրագործից կամ ոչ կվալիֆիկացված օգտատերից:
• Հնարավորություն տեղադրել միայն հակավիրուսային պաշտպանության ծրագրերի ընտրված բաղադրիչները:
• Սկավառակի ամբողջական կոդավորումը, հատուկ սկավառակային գործակալի ստեղծմամբ եւ Single Sign On տեխնոլոգիայի հետ աջակցությամբ: Անհրաժեշտ է ունենալ գործիքներ գործակալի կամ OS ֆայլերի ձախողումների դեպքում կոդավորված տվյալների վերականգնում: Պետք է իրականացվի UEFI- համակարգերի օգտագործման հնարավորություն:
• Երկաստիճան աուտենտիֆիկացիայի ապահովում ամբողջական սկավառակի կոդավորման ժամանակ:
• Ֆայլերի ճկուն կոդավորում (ըստ գտնվելու վայրի, ըստ ֆայլի տիպի, ըստ ֆայլ ստեղծող ծրագրի): Ընտրված ծրագրերին կոդավորված ֆայլերին հասանելիության սահմանափակելու մեխանիզմների առկայություն:
• Տվյալների գաղտնագրում շարժական կրիչների վրա, աշխատանքի ռեժիմի սահմանման հնարավորությամբ, որը թույլ է տալիս կոդավորել կամ ապակոդավորել ֆայլերը օրգանիզացիայի ցանցից դուրս:
• Վերոնշյալ բոլոր բաղադրիչների կենտրոնացված կառավարումը մեկ կառավարման համակարգով:

Պահանջներ, աշխատանքային կայանների եւ Linux ֆայլերի սերվերների հակավիրուսային պաշտպանության ծրագրային ապահովման համար:

Linux- ի աշխատանքային կայանների համար հակավիրուսային պաշտպանության ծրագրային ապահովումը պետք է գործածվի հետեւյալ տարբերակների օպերացիոն համակարգերով աշխատող համակարգիչների վրա.

- Red Hat® Enterprise Linux® 6.7 x86/x64
- Red Hat® Enterprise Linux® 6.8 x86/x64
- Red Hat® Enterprise Linux® 7.2 x64
- Red Hat® Enterprise Linux® 7.3 x64
- CentOS-6.7 x86/x64
- CentOS-6.8 x86/x64
- CentOS-7.2 x64
- CentOS-7.3 x64
- SUSE® Linux Enterprise Desktop 12 x64
- openSUSE® 42.2 x64
- Debian GNU/Linux 7.10 x86/x64
- Debian GNU/Linux 7.11 x86/x64
- Debian GNU/Linux 8.6 x86/x64
- Debian GNU/Linux 8.7 x86/x64

- Ubuntu 10.04 LTS x86/x64
- Ubuntu 12.04 LTS x86/x64
- Ubuntu Server 14.04 LTS x86/x64
- Ubuntu Server 16.04 LTS x86/x64
- Ubuntu Server 16.10 LTS x86/x64
- OracleLinux 7.3 x64
    - Debian GNU/Linux 7.10 x86/x64
    - Debian GNU/Linux 7.11 x86/x64
    - Debian GNU/Linux 8.6 x86/x64
    - Debian GNU/Linux 8.7 x86/x64
    - Ubuntu 10.04 LTS x86/x64
    - Ubuntu 12.04 LTS x86/x64
    - Ubuntu Server 14.04 LTS x86/x64
    - Ubuntu Server 16.04 LTS x86/x64
    - Ubuntu Server 16.10 LTS x86/x64
    - OracleLinux 7.3 x64

Linux- ի աշխատանքային կայանների հակավիրուսային ծրագրերը պետք է ապահովեն հետևյալ ֆունկցիոնալությունը:

- Մշտական հակավիրուսային մոնիտորինգ.
- Ստուգում է SMB / NFS- ի կողմից առկա ռեսուրսները
- Heuristic անալիզատոր, որը թույլ է տալիս ավելի արդյունավետ հայտնաբերել և արգելափակել նախկինում հայտնի չարամիտ ծրագրերը:
- Հակավիրուսային սկանավորում օգտագործողի կամ ադմինիստրատորի հրամաններով և ժամանակացույցով:
- Արխիվների ֆայլերի հակավիրուսային սկանավորում և բուժում:
- Գործառույթները ակտիվացնել ժամանակացույցով և / կամ օպերացիոն համակարգի բեռնվածությունից անմիջապես հետո:
- Կարանտինի մեջ կասկածելի և վնասված օբյեկտների տեղադրեք:
- HTML- ի և CSV ձևաչափերով հաշվետվությունների արտահանման և պահպանման ունակություն:
- SAMBA- ի մակարդակով ֆայլերի գործողությունները խափանելու և ստուգելու ունակությունը:
- Համակարգչային ռեսուրսների օգտագործման ճկուն կառավարում, ֆայլի տարածման սկանավորում կատարելու ժամանակ հարմարավետ Օգտվողի փորձի ապահովում:
- Ամպային պաշտպանություն նոր սպառնալիքների դեմ, թույլ տալով, որ հասանելի կլինի արտադրողի կոնկրետ կայքերում, ստանալով դատավարություն սկսվող ծրագրի կամ ֆայլի մասին:

- Վնասված օբյեկտի պատճենը պահեստում պահպանում մինչև բուժում և հեռացում, օբյեկտի պահանջով վերականգնելու համար, եթե այն տեղեկատվական արժեք ունի:
- Օգտագործման հարմարավետ գրաֆիկական ինտերֆեյսի միջոցով կառավարելու ունակություն:
- Բոլոր վերը նշված բաղադրիչների կենտրոնացված կառավարումը միասնական կառավարման համակարգով:

Պահանջներ հակավիրուսային պաշտպանության ծրագրային ապահովման համար, ֆայլային սերվերների, ձեռնարկության մակարդակի սերվերների և տերմինալային սերվերների Windows- ի համար:

Ձեռնարկությունների մակարդակի սերվերների և Windows տերմինալային սերվերների համար հակավիրուսային պաշտպանության ծրագրային ապահովումը պետք է գործածվի հետևյալ տարբերակների օպերացիոն համակարգերով աշխատող համակարգիչների վրա:

- Microsoft Windows Server 2008 Standard/Enterprise/DataCenter/Core SP1 ивыше x86/x64;
- Microsoft Windows Server 2008 R2 Core/ Standard/Enterprise/DataCenter SP1 ивыше x64;
- Microsoft Windows Server 2012 Core/Standard/Essential/DataCenter/Foundation x64;
- Microsoft Windows Server 2012 R2 Core/Standard/Essential/DataCenter/Foundation x64;
- Microsoft Windows Server 2016 Core/Standard/Datacenter/Essentials x64;
- Microsoft Windows Storage Server 2008 R2 x64;
- Microsoft Windows Storage Server 2008 R2 SP2 Standard/Workgroup x64;
- Microsoft Windows Storage Server 2012 (всередакции) x64;
- Microsoft Windows Storage Server 2012 R2 (всередакции) x64;
- Microsoft Windows Storage Server 2016 x64;
- Microsoft Windows Hyper-V Server 2008 R2 SP1 x64;
- Microsoft Windows Hyper-V Server 2012 x64;
- Microsoft Windows Hyper-V Server 2012 R2 x64;
- Microsoft Windows Hyper-V Server 2016 x64.

Տերմինալային սերվերներ:

- Microsoft Remote Desktop Services набазе Windows Server 2008;
- Microsoft Remote Desktop Services набазе Windows Server 2012;
- Microsoft Remote Desktop Services набазе Windows Server 2012 R2;
- Microsoft Remote Desktop Services набазе Windows Server 2012;
- Citrix XenApp 6.0/6.5/7.0/7.5 – 7.9;
- Citrix XenDeskTop 7.0/7.1/7.5/7.9.

Ձեռնարկությունների մակարդակի սերվերների և Windows տերմինալային սերվերների հակավիրուսային պաշտպանության ծրագրերը պետք է ապահովեն հետևյալ ֆունկցիոնալությունը:

- Տարբեր գործառույթներ իրականացնող սերվերներում հակավիրուսային սկանավորման իրականացում. Տերմինալային սերվերներ եւ տպիչ սերվերներ; Դիմումի սերվերներ եւ տիրույթի կարգավարներ; Ֆայլի սերվերներ:
- Սերվերի կլաստերի պաշտպանության համար օգտագործման ունակությունը:
- Ստուգելով պահպանվող սերվերի հետևյալ օբյեկտները, նրանց մուտք գործելիս: Ֆայլեր, երբ դրանք գրվում են և կարդացվում են; Ֆայլերի համակարգերի այլընտրանքային հոսքեր (NTFS- հոսքեր); Տեղական կոշտ սկավառակների եւ շարժական սկավառակի ռեկորդ եւ բեռնվածություն:
- Վիրուսային բռնկումների կանխարգելման միջոցով կանխարգելելով վիրուսային հարձակումների առաջացումը.
- Վարակվածից հետո վերականգնումը, հեռացնելով բոլոր ֆայլերը, որոնք կապված են համակարգի ֆայլերից և OS ռեեստրից ջնջված վնասակար օբյեկտի հետ, ինչը կանխարգելում է օպերացիոն համակարգում հնարավոր անկարգությունները.
- Ամպային պաշտպանություն նոր սպառնալիքների դեմ, թույլ տալով, որ հասանելի կլինի արտադրողի կոնկրետ կայքերում, ստանալով դատավարություն սկսվող ծրագրի կամ ֆայլի մասին:
- Կատարված ֆայլերի, սցենարների և MSI փաթեթների, ինչպես նաև DLL-մոդուլների և վարորդների գործարկման հսկողություն, որը թույլ չի տալիս չհավատարմագրված հայտերը կատարել: Մի սերվերի վրա ծրագրակազմի ընթացիկ փաթեթի վրա հիմնված ծրագրերը ավտոմատ կերպով ստեղծելու ունակություն է տալիս:
- Microsoft- ի Windows Script Technologies- ի (կամ Active Scripting) վրա ստեղծված VBScript և JScript սցենարների կատարման փորձերի շարունակական մոնիտորինգ: Ստուգել սցենարների ծրագրի կոդը և ավտոմատ կերպով արգելել այն անձանց կատարումը, որոնք վտանգավոր են ճանաչվում.
- Սարքի ցանցային ռեսուրսների հեռավոր համակարգչի հասանելիությունը արգելելու ունակությունը:
- Սերվերի ընդհանուր ցանցային թղթապանակների վրա ֆայլերի չարամտորեն կոռումպացվածության փորձեր և արգելափակող համակարգիչներ, որոնցից նման գործունեություն է կատարվում:
- Պահանջարկի սկանավորում, որը բաղկացած է մեկ ամբողջական կամ ընտրովի սկանից օբյեկտի սպառնալիքների առկայությունը սերվերում:
- Իր մոդուլների ստուգումը առանձին առաջադրանքի միջոցով հնարավորության խախտման համար:
- Կարանտինի մեջ կասկածելի և վնասված օբյեկտների տեղադրելու հնարավորություն: Կարանտինից ֆայլեր վերականգնելու ունակություն ցանցային թղթապանակների վրյա:
- Տերմինալային սերվերների պաշտպանություն, սեղանադիր ռեժիմների հրատարակում և հրատարակչական ծրագրերի աջակցություն:.
- Մաշտաբավորում հակավիրուսային աշխատանքի արդյունքի քանակի սահմանման միջոցով, բազմապատկող սերվերների օգտագործման ժամանակ սերվերի մշակման պահանջները արագացնելու համար.
- Բեռի հավասարակշռումը, կարգավորելով սերվերային ռեսուրսների բաշխումը հակավիրուսային և այլ ծրագրերի միջև 'կախված խնդիրների առաջադրանքներից. Հակավիրուսային սկանավորումները կարող են շարունակել ֆոնային.
- Վստահված գործընթացների ընտրությունը, բացառելով սկանավորելու անվտանգ գործընթացները, որոնց աշխատանքը կարող է դանդաղեցնել հակավիրուսային սկանավորման ընթացքում (տվյալների կրկնօրինակում, կոշտ սկավառակի դեֆրագրման ծրագրեր և այլն)
- Տեղական կառավարման վահանակի առկայությունը: Տեղական վահանակի միջոցով ձեռնարկության սերվերների համար այլ անվտանգության գործիքներ կապելու ունակությունը:
- Ադմինիստրատների իրավունքների բաժանումը ստանդարտ մեխանիզմների հիման վրա ՕՀ Microsoft Windows.
- Ստանդարտ սերվերային դերերի համար ներկառուցված բացառությունների առկայությունը
- Հակավիրուսային պաշտպանության միջոցառումների մասին ադմինիստրատորներին և օգտագործողներին տարբեր մեթոդներով ծանուցումներ: Simple Network Management Protocol (SNMP)-ի սպասարկում.
- Սպասարկում ReFS- ի (Resilient file system) և CSV- ի (Cluster Shared Volume).
- Կենտրոնական կառավարումը ղեկավարվում է միասնական կառավարման համակարգով:

Linux պրոքսի-սերվերների համար հակավիրուսային պաշտպանության ծրագրերի պահանջները

Linux պրոքսի-սերվերների համար հակավիրուսային պաշտպանության ծրագրերի պետք է գործեն հետևյալ օպերացիոն համակարգերով աշխատող համակարգիչներում՝

- Red Hat Enterprise Linux Server 6.2 x86/x64
- Fedora 16 x86/x64
- CentOS 5.7, 6.2 x86/x64
- SUSE Linux Enterprise Server 11 SP1 x86/x64
- Novell Open Enterprise Server 2 SP3 x86/x64
- openSUSE Linux 12.1 x86/x64
- Debian GNU/Linux 6.0.4 Squeeze x86/x64
- Mandriva Enterprise Server 5.2 x86
- Ubuntu 10.04, 12.04 LTS x86/x64
- FreeBSD 8.2, 9.0 x86/x64

Linux պրոքսի-սերվերների համար հակավիրուսային պաշտպանության ծրագրերի պետք է գործեն հետևյալ պրոքսի սերվերներում՝

- Squid 3.x

Linux պրոքսի-սերվերների համար հակավիրուսային պաշտպանության ծրագրերի պետք է ապահովեն հետևյալ ֆունկցիոնալը՝

- Կատարել օբեկտների հակավիրուսային ստուգում, փոխանցված պրոքսի-սերվերով
- Վարաքված օբեկտների բուշում և եթե բուժումը հնարավոր չէ՝ արգելել նրան հասանելիությունը
- Գտնել և բուժել բոլոր տեսակի ֆայլերի և հավելվածների մեջ
- Օգտագործել խմբային պարամետրերը՝ սահմանելու տարբեր զտիչ ընտրանքներ, կախված պահանջվող օգտագործողի օբյեկտի հասցեն և օբյեկտի հխումը (URL):
- Պահպանել աշխատանքային վիճակագրությունը, ներառյալ, տեղեկություններ հակավիրուսային սկանավորման արդյունքների և արդյունքների, կիրառման սխալների և նախազգուշացումների մասին:
- Տեղեկացնել ադմինիստրատորին վնասակար ծրագրերի մասին
- Թարմացնել հակավիրուսային տվյալների բազան ՝ինչպես արտադրողի կայքից, այնպես էլ տեղական կատալոգից:

Linux-ի փոստային սերվերների համար հակավիրուսային և սպամի զտման ծրագրային պահանջներ

Linux- ի փոստի սերվերների հակավիրուսային և սպամի զտմանծրագրային ապահովումը պետք է գործածվի հետևյալ տարբերակների օպերացիոն համակարգերով աշխատող համակարգիչների վրա

Red Hat Enterprise Linux 6.6 Server x86/x64
Red Hat Enterprise Linux 7.0 Server x64
CentOS 6.6 x86/x64
CentOS 7 x64
SUSE Linux Enterprise Server 11 SP3 x86/x64
SUSE Linux Enterprise Server 12 x64
Ubuntu Server 12.04.4 LTS x86/x64
Ubuntu Server 14.04 LTS x86/x64
Debian GNU/Linux 6.0.10 x86/x64
Debian GNU/Linux 7.7 x86/x64
FreeBSD 8.3 x86/x64
FreeBSD 9.3 x86/x64
FreeBSD 10.1 x86/x64

Linux- ի փոստի սերվերների հակավիրուսային և սպամի զտմանծրագրային ապահովումը պետք է գործեն հաջորդ սերնդի փոստային համակարգերի հետ՝

exim-4.71 և բարձր
postfix-2.5 և բարձր
qmail-1.03 և բարձր
sendmail-8.14 և բարձր

Linux- ի փոստի սերվերների հակավիրուսային և սպամի զտմանծրագրային ապահովումը պետք է հնարավորություն ունենան մատակարարվեն միասնական լուծման ձևով, որպես վիրտուալ մեքենայի պատկեր, տեղադրելու համար՝

VMware ESXi 5.5 Update 2
VMware ESXi 6.0

Հակավիրուսային պաշտպանության և սպամի ֆիլտրացիայի Linux փոստային սերվերների համար նախատեսված ծրագրային ապահովումը պետք է ապահովվի հետևյալ ֆունկցիոնալ հնարավորությունները.

Հակավիրուսային պաշպանության և սպամի ֆիլտրացիայի հնարավորությունների օգտագործումը կամայական փոստային համակարգի հետ;

Sender Policy Frameword (SPF) տեխնոլոգիայի օգնությամբ ուղարկողի IP-հասցեի ստուգումը ըստ թույլատրված դոմենների ցանկի; DKIM/DMARC տեխնոլոգիանների սպասարկում;

Իրական ժամանակի ռեժիմում բոլոր տեսակի վիրուսների, որդերի, տռոյանների և այլ վնասակար ծրագրերի փնտրում և հեռացում էլեկտրոնային փոստի նամակների և կցված ֆայլերի մեջ;

Նամակի մարմնի մեջ ֆիշինգային և վնասակար հղումների հայտնաբերման հնարավորություն;

Մոտավոր հայտնաբերման մեթոդների առկայություն;

Հաստատված ամպային սերվիսների օգտագործում;

Մուտք լինող փոստային նամակների ստուգում սպամի առկայության համար;

Պաշտպանական կոմպոնենտի առկայություն, որը թույլ է տալիս ապաարխիվացնել և հետազոտել բարդ ֆայլերը մինչ այս անհայտ սպառնալիքների հայտնաբերման համար;

Փոստային նամակների ըստ կցված ֆայլերի չափերի, անվան, տիպի հիման վրա ֆիլտրացիայի հնարավորություն;

Active Directory և Open LDAP հետ ինտեգրացիա;

SNMP պրոտոկոլով ծուղակների և ծանուցումների ուղարկման հնարավորություն;

IPv6 պրոտոկոլի հետ աշխատելու հնարավորություն;

Ուղարկողների e-mail հասցեների սեփական սև և սպիտակ ցուցակների հիման վրա նամակների ֆիլտրացիա և ֆիլտրացիայից բացառում;

Ուղարկողի ip-հասցեի ստուգում DNS-based realtime blackhole list (DNSBL) ցուցակներում;

Նամակի մարմնի մեջ SPAM URI Realtime Blocklists (SURBL) սերվիսի օգնությամբ կայքերի հասցեների և դրանց վրա հղումների ստուգում;

Գրաֆիկական ներդրումների ստուգում հայտնի սպամ նամակների սիգնատուռաների համանկման վրա;

Կասկածելի, վնասված և գաղտնաբառով պաշտպանված հայտնաբերում, նաև ֆայլերի, որոնց ստուգման ժամանակ սխալ է առաջացել;

Ընդհանուր, և սեփական կարանտինի առկայություն:
Սեփական սև և սպիտակ ցուցակների ստեղծման հնարավորություն:
Սերվերի ֆայլային համակարգի օբյեկտների հակավիրուսային ստուգման իրականացում;
Ուղարկողների և ընդունողների խմբերի համար տրված կանոնների համապատասխան փոստային տրաֆիկի մշակում:

Փոստային նամակների հոսքի լրացուցիչ ստուգում ըստ անունների և ներդրված ֆայլերի տիպերի և առանձին մշակման կանոնների կիրառում արդեն ֆիլտրած նամակների վրա;
Ներդրված ադմինիստրատորի և սպասարկման մասնագետի դերերի առկայություն;
Վնասված և վարակված օբյեկներ պարունակող նամակների մասին, ադմինիստրատորին, ուղարկողին, ստացողին ծանուցման հնարավորություն;
Amavis ինտերֆեյսով աշխատանքի հնարավորություն;
Ծրագրի աշխատանքի կառավարումը պետք է կատարվի ինչպես օպերացիոն համակարգին ներդրված հրամանների տողի օգնությամբ, այնպես էլ հատուկ վեբ-ինտերֆեյսի օգնությամբ, որը կաշխատի հետևյալ բրաուզերների հետ՝ Internet Explorer, Mozilla Firefox, Google Chrome;
Վեբ-ինտերֆեյսի օգնությամբ բոլոր ֆունկցիաների կառավարում;
Ոչ միայն միանշանակ վնասակար ծրագրերի հայտնաբերում և ոչնչացում, այլև պոտենցիալ վնասակար, ինչպիսք են: գովազդային ծրագրերը, ինֆորմացիա հավաքող ծրագրերը, վճարովի կայքերի ավտոմատ հղվող, որոնք կարող են օգտագործվել հանցագործների կողմից սեփական նպատակների համար;
PDF ֆորմատով զեկույցների ստեղծման համար նախատեսված ճկուն համակգի առկայություն;

Հակավիրուսային պաշտպանության և սպամի զտման ծրագրային միջոցների պահանջները Microsoft Exchange սերվերների համար.

Հակավիրուսային և սպամի զտման ծրագրային միջոցները Microsoft Exchange սերվերների համար պետք է գործարկվեն համակարգիչների վրա, որոնք աշխատում են օպերացիոն համակարգերի հետևյալ տարբերակների ներքո.
Microsoft Windows Server 2016;
Microsoft Windows Server 2012 R2 Standard / Datacenter;
Microsoft Windows Server 2012 Standard / Datacenter;
Microsoft Windows Small Business Server 2011 SP1 Standard;
Microsoft Windows Server 2008 R2 SP1 Standard / Enterprise / Datacenter:
Հակավիրուսային պաշտպանության և սպամի զտման ծրագրային միջոցները Microsoft Exchange սերվերների համար պետք է գործարկվեն Microsoft Exchange Server ծրագրային ապահովման հետևյալ տարբերակների հետ.

- Microsoft Exchange Server 2010 SP3;
- Microsoft Exchange Server 2013 SP1;
- Microsoft Exchange Server 2016:

Հակավիրուսային պաշտպանության և սպամի զտման ծրագրային միջոցները Microsoft Exchange սերվերների համար պետք է գործարկվեն տվյալների բազա սերվերների հետևյալ տարբերակների հետ.

- Microsoft SQL Server 2012;
- Microsoft SQL Server 2014;
- Microsoft SQL Server 2016:

Հակավիրուսային պաշտպանության ծրագրային միջոցների Microsoft Exchange սերվերների համար կառավարման վահանակը պետք է գործարկվի համակարգիչների վրա, որոնք աշխատում են օպերացիոն համակարգերի հետևյալ տարբերակների ներքո.
Microsoft Windows 10;
Microsoft Windows 8.1;
Microsoft Windows 8;
Microsoft Windows 7 SP1 Professional /Enterprise / Ultimate;
Microsoft Windows Server 2016;
Microsoft Windows Server 2012 R2 Standard / Datacenter;
Microsoft Windows Server 2012 Standard / Datacenter;
Microsoft Windows Small Business Server 2011 SP1 Standard;
Microsoft Windows Server 2008 R2 SP1 Standard / Enterprise / Datacenter:
Հակավիրուսային պաշտպանության և սպամի զտման ծրագրային միջոցները Microsoft Exchange սերվերների համար պետք է ապահովեն հետևյալ ֆունկցիոնալությունը.

- Համատեղելիություն DAG-ի հետ Microsoft Exchange-ում:
- Դերերի սպասարկում MS Exchange 2010: Edge, Hub transport, Mailbox:
- Դերերի սպասարկում MS Exchange 2013: Mailbox, Edge Transport, Client Access Server (CAS):
- Դերերի սպասարկում MS Exchange 2016: Mailbox, Edge Transport:
- Մուտքային և ելքային նամակների հոսքի մեջ, ներառյալ հավելվածները, որոնել և հեռացնել իրական ժամանակում բոլոր տեսակի վիրուսները, համակարգչային որդերը, տրոյան ծիերը և այլ վնասակար ծրագրերը:
- Microsoft Exchange սերվերի վրա պահվող հաղորդագրություններում (այդ թվում հանրային պանակներում), ներառյալ հավելվածները, որոնել և հեռացնել իրական ժամանակում բոլոր տեսակի վիրուսները, համակարգչային որդերը, տրոյան ծիերը և այլ վնասակար ծրագրերը:
- Էվրիստիկ հայտնաբերման մեթոդների առկայությունը:
- Սերվերի վրա փոստային պահեստների և հանրային պանակների ստուգում ֆոնային ռեժիմում, բոլոր օբյեկտների երաշխավորված մշակման համար, օգտագործելով հակավիրուսային տվյալների բազայի առավելագույն թարմացված տարբերակը՝ առանց զգալիորեն ավելացնելու սերվերի բեռնվածությունը:

- Վարակված ֆայլերը բուժելու ունակություն:
- Հայտնաբերելու և հեռացնելու ունակությունը ոչ միայն միանշանակ վնասակար, այլև պոտենցիալ վտանգավոր ծրագրերի, ինչպիսիք են՝ գովազդային ծրագրերը, տեղեկատվության հավաքման ծրագրերը, վճարովի կայքերի ավտոմատ կերպով հավաքագրման ծրագրերը և այլ գործիքներ, որոնք կարող են օգտագործվել հարձակվողների կողմից իրենց նպատակների համար:
- Հաղորդագրության մարմնում վնասակար և ֆիշինգային հղումներ հայտնաբերելու ունակություն:
- Վիրուսային համաճարակների ճանաչելու մեխանիզմի առկայությունը, որը թույլ է տալիս ժամանակին (ներառյալ ավտոմատ կերպով) միջոցներ ձեռնարկել փոստի սերվերի հակավիրուսային պաշտպանության ուժեղացման համար. երբ վիրուսի ակտիվությունը որոշակի շեմի է հասնում, ցանցի ադմինիստրատորը ստանում է ծանուցում էլեկտրոնային փոստով:
- Փոփոխվող հաղորդագրությունների կրկնօրինակների պահպանում ռեզերվային պահեստներում, որը թույլ է տալիս վերականգնել կարևոր տեղեկությունները օբյեկտի սխալ բուժման դեպքում: Ռեզերվային պահեստում օբյեկտ գտնելու հարմարության համար որոնման պարամետրերի լայն շրջանակ:
- Հավատարիմ ամպային ծառայությունների հետ ստուգման լրացուցիչ մակարդակ:
- Պաշտպանության բաղադրիչի առկայությունը, որը թույլ է տալիս բացել և վերլուծել բարդ ֆայլերը անոմալիաներ գտնելու կանգակգությամբ, նախկինում անհայտ սպառնալիքները արգելափակելու համար:
- Հաղորդագրության տարբեր պարամետրերի ստուգում, ինչպիսիք են ուղարկողների և ստացողների հասցեները, հաղորդագրության չափսը, ինչպես նաև հաղորդագրության վերնագրի դաշտերը:
- Հաղորդագրության զետեղում կամ զետեղումից բացառում նամակը ուղարկողի հասցեի (էլ.Փոստ և/կամ IP-հասցե) սեփական «սև» և «սպիտակ» ցուցակների մեջ առկայության հիման վրա:
- Ստուգում ուղարկողի IP-հասցեի առկայությունը DNS-based realtime blackhole list (DNSBL) ցուցակներում:
- Ուղարկողի IP-հասցեի ստուգում թույլատրված հասցեների ցանկին համապատասխանելու համար օգտագործելով Sender Policy Framework (SPF) տեխնոլոգիան:
- Ստուգում SPAM URI Realtime Block lists (SURBL) ծառայության միջոցով հասցեները և կայքերի հղումները, որոնք զետեղված են հաղորդագրության մարմնում:
- Բովանդակության զտման օգտագործում (հաղորդագրության բովանդակության վերլուծություն, ներառյալ թեմաների վերնագիրն ու կցված ֆայլերը):
- Օգտագործողների/ադմինիստրատորների դերերը օգտագործելու ունակություն անվտանգության կարգավորումները առանձնացնելու համար:
- Համակարգի տարբեր օգտագործողների կողմից անվտանգության պարամետրերի փոփոխման գրանցման/աուդիտի հնարավորությունը:
- PowerShell-ի միջոցով հաշվետվություններ ստանալը և սև/սպիտակ ցուցակների կառավարումը:
- Բովանդակության զտման օգտագործում (հաղորդագրության բովանդակության վերլուծություն, ներառյալ թեմաների վերնագիրն ու կցված ֆայլերը):
- Microsoft Office-ի ֆայլերը զտելու ունակություն, որոնք պարունակում են մակրոսներ:
- Ստուգել և ջնջել ելքային հաղորդագրությունները, որոնք սպամ են կամ պարունակում են ֆիշինգ և վնասակար հղումներ:
- Գրաֆիկական հավելվածների ստուգում՝ զանազան սպամ-հաղորդագրությունների ստորագրությունների հետ համընկնելու համար:
- Ստեղծել հաշվետվություններ պաշտպանության համակարգի շահագործման վերաբերյալ: Ավտոմատ հաշվետվությունների ուղարկման ունակպություն ադմինիստրատորներին ըստ ժամացուցակի:
- Հակավիրուսային տվյալների բազայի թարմացման ունակությոան, ինչպես նաև արտադրողի կայքերից, այնպես էլ կազմակերպության ներքին ցանցային ռեսուրսներից:
- Ֆայլերը, փոստարկղերը և հանրային պանակները սկանավորելու ունակություն ֆոնային ռեժիմում, օգտագործելով Exchange վեբ ծառայություններ:
- Մանրամասն հաշվետվություններ HTML ձևաչափով:
- Կարողություն ուղարկել հաշվետվություններ և ծանուցումներ այս էլէկտրոնային հասցեների:
- Ծրագրի մոնիտորին շնորհիվ System Center - Operations Manager.
- Ինտեգրում Active Directory-ի հետ:
- Հնարավորություն վերահսկել պաշտպանության սերվերները MMC կոնսոլով.
- Ունակություն պաշտպանության կարգավիճակի կենտրոնացված դիտման
- Ունակություն է բաշխել համակարգի ադմինիստրատորների դերերը

Կենտրոնացված կառավարման, մոնիտորինգի և թարմացման ծրագրային ապահովման պահանջները

Կենտրոնացված կառավարման, մոնիտորինգի և թարմացման ծրագրային ապահովումը պիտի գործի հետևյալ օպերացիոն համակարգի տարբերակների համար.

- Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 x86 / x64;
- Microsoft Windows 8 Professional / Enterprise x86 / x64;
- Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
- Microsoft Windows 10 Professional/Enterprise/Education x86 / x64;
- Microsoft Windows 10 RS1 x86 / x64;
- Microsoft Windows 10 RS2 x86 / x64;
- Microsoft Windows Server 2008 Foundation/Standard/Enterprise/Datacenter SP1 x86 / x64;
- Microsoft Windows Server 2008;
- Microsoft Windows Server 2008 SP1 x86 / x64;
- Microsoft Windows Server 2008 R2 Core/Foundation/Standard/Enterprise/Datacenter x64;

- Microsoft Windows Server 2008 R2 Core/Foundation/Standard/Enterprise/Datacenter SP1 x64;
- Microsoft Windows Server 2012 Core/Foundation/Standard/Enterprise/Datacenter x64;
- Microsoft Windows Server 2012 R2 Core/Essentials/Foundation/Standard/Enterprise/Datacenter x64;
- Microsoft Windows Small Business Server 2008 Standard/Premium x64;
- Microsoft Windows Small Business Server 2011 Essentials/Premium/Standard x64.

Կենտրոնացված կառավարման, մոնիտորինգի և արդիականացման համար ծրագրային ապահովումը պետք է գործածվի ԱՀԿ-ի հետևյալ տարբերակներով

- Microsoft SQL Express 2008/2008R2/2012/2014;
- Microsoft SQL Server 2008/2008R2/2012/2014/2016;
- Microsoft Azure SQL Database;
- MySQL 5.5, 5.6, 5.7 x86/x64;
- MySQL Enterprise 5.5, 5.6, 5.7 x86/x64.

Կենտրոնացված կառավարման, մոնիտորինգի և արդիականացման համար նախատեսված ծրագրերը պետք է գործեն հետևյալ տպիրթերակների վիրտուալ պլատֆորմներում.

- VMware Workstation 9.x, Workstation 10.x, 12x Pro;
- VMware vSphere 5.5, 6;
- Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 20012 R2;
- Microsoft VirtualPC 2007(6.0.156.0);
- Parallels Desktop 7,11;
- Citrix XenServer 6.1, 6.2, 6.5, 7;
- Oracle VM VirtualBox 4.0.4-70112.

Բոլոր պաշտպանված ռեսուրսների կառավարման ծրագրերը պետք է ապահովեն հետևյալ ֆունկցիոնալությունը.

- Հակավիրուսային պաշտպանության կառավարման համակարգը մեկ բաշխումից տեղադրելու հնարավորություն.
- Տեղադրման ընտրությունը պետք է կախված լինի պաշտպանված հանգույցների թվից.
- Active Directory-ից տեղեկություն ընթերցելու ունակություն, կազմակերպության տեղեկատվական համակարգչային հաշիվների և օգտվողների մասին տեղեկատվություն ստանալու համար.
- Ինտերնետային ցանցում IP- հասցեների, տանտերերի անունների, դոմեյն անունների, ենթահամեստի դիմակների միջոցով ցանցերի որոնման և հայտնաբերման ունակություն.
- Ավտոմատ տարածել օգտագործողի հաշիվներ կառավարման խմբերում, եթե ցանցում հայտնվում են նոր համակարգիչներ: Միգրացիոն կանոնների կարգավորումը կարող է լինել IP-հասցեով, ՕՀ- ի տեսակով, OU AD- ով.
- Կենտրոնացված տեղադրում, հակավիրուսային պաշտպանության ծրագրերի թարմացում և հեռացում: Կենտրոնացված կոնֆիգուրացիա, ղեկավարում, հաշվետվություն և վիճակագրական տեղեկատվություն իրենց աշխատանքի վերաբերյալ.
- Հսկիչ կենտրոնի միջոցով անհամատեղելի հայտերի կենտրոնացված հեռացում (մեխանիկական և ավտոմատ).
- Փոփոխությունների պատմությունը պահպանելու քաղաքականության և առաջադրանքների, նախորդ տարբերակները վերադառնալու ունակությունը
- Հակավիրուսային միջոցների տեղադրման տարբեր մեթոդների առկայություն. Հեռավոր տեղադրման համար 'RPC, GPO, կառավարման համակարգի գործիքներ, տեղական տեղադրման համար' ինքնուրույն տեղադրման փաթեթի ստեղծման հնարավորություն.
- Անվտանգության քաղաքականության մեջ հատուկ խթանիչների հայտնաբերման ունակություն, որոնք կանխորոշում են հակավիրուսային լուծումների կայանքներին, որոնք կախված են ՍՅ-ից, որի ներքո օգտագործողը մուտք է գործում ընթացիկ IP- հասցեին, և որի միջոցով OU- ն գտնվում է համակարգչում կամ այլ անվտանգության խմբում: Պետք է հնարավոր լինի աջակցել նման խթանիչների հիերարխիան.
- Տեղակայված ծրագրերում և օպերացիոն համակարգում օգտվողների համակարգիչների վրա խոցելիության ավտոմատացված որոնում և փակում.
- Ներբեռնվող թարմացումների փորձարկում 'կենտրոնացված կառավարման ծրագրային ապահովման միջոցով' մինչև բաժանորդային մեքենաներին բաժանումը: օգտվողների աշխատատեղերի թարմացումները ստանալուց անմիջապես հետո.
- Ցանցում վիրտուալ մեքենաների ճանաչում և դրանց միջև կիսվող խնդիրների բեռնման հավասարակշռման բաշխում այն դեպքերում, երբ այդ մեքենաները միևնույն ֆիզիկական սերվերի վրա են.
- VMware ESXi, Microsoft Hyper-V, Citrix XenServer- ի հիման վրա վիրտուալ ենթակառուցվածքների մասնագիտացված անվտանգության համակարգի պահանջարկի ավտոմատ տեղադրում .
- Կառուցել բազմաբնույթ կառավարման համակարգ, որը հնարավորություն կտա կարգավորելու ադմինիստրատորների և օպերատորների դերերը, ինչպես նաև յուրաքանչյուր մակարդակում տրամադրված հաշվետվությունների ծևերը.
- Կենտրոնացված կառավարման համար նախապես կազմաձևված օգտագործողի դերերի առկայություն: Անհրաժեշտ է ստեղծել հատուկ ռեեստրներ, օգտագործողների հաշիվների համար պարտադիր լիազորությունների սահմանում.
- Կամավոր մակարդակի կառավարման սերվերների հիերարխիայի ստեղծում և ամբողջ մակարդակի հիերարխիայի կենտրոնացված կառավարման հնարավորություն բարձր մակարդակից.
- Կառավարման սերվերների համար բազմակողմանի(multi-tenancy) աջակցություն
- Ծրագրային և հակավիրուսային տվյալների բազաների թարմացում տարբեր աղբյուրներից, ինչպես հաղորդակցման ուղիներով, այնպես էլ համակարգչային կրիչի միջոցով
- Հասանելիություն հակավիրուսային ծրագրերի ստեղծողի ամպային սպասարկուներին կառավարման սերվերի միջոցով
- Լիցենզիայի ավտոմատ բաշխումը հաճախորդի համակարգչում.
- Տեղակայված ծրագրերի և սարքավորումների գույքագրումը օգտագործողների համակարգիչների վրա.

• RDP- ի կամ ստանդարտ գործիքների միջոցով կառավարման վահանակին միանալու հնարավորություն: Օգտվողը պետք է իրազեկվի հեռավոր կապի թույլտվության մասին:
• Տեղադրված հակավիրուսային պաշտպանական ծրագրերի աշխատանքներում իրազեկման մեխանիզմի առկայություն և դրանց մասին փոստային ծանուցումների բաշխում:
• Օպերացիոն համակարգի պատկերների հետ աշխատելու գործիքների առկայությունը. ֆիզիկական կամ վիրտուալ մեքենայի վրա հիմնված թիրախային օպերացիոն համակարգի պատկեր ստեղծում, ադմինիստրատորի կողմից ընտրված համակարգչում պատկերի տեղադրում, այդ թվում՝ գորշ մետաղ: Պետք է հնարավոր լինի ավելացնել ծրագրեր նախապես ստեղծված պատկերին: Օպերացիոն համակարգի տեղադրումից հետո ծրագրային կոդի աշխատեցում կամ լրացուցիչ ծրագրեր տեղադրելու ավտոմատ ռեժիմում:
• Օպերացիոն համակարգի պատկերն բաշխվածությունից ներմուծելուունակությունը:
• Երրորդ կողմի ծրագրային ապահովման լիցենզավորման հսկողության համակարգի առկայությունը, որը թույլ է տալիս տեղեկացնել լիցենզիայի խախտման կամ լիցենզիայի գործողության ժամկետի գերազանցման մասին:
• Երրորդ կողմի ծրագրերի համար տեղադրման փաթեթների ավտոմատ ստեղծում (Adobe Reader, Mozilla Firefox, 7-zip եւ այլն) եւ այդ ծրագրային փաթեթների ավտոմատ կենտրոնական տեղադրումը համակարգիչների վրա:
• Կառավարվող շարժական սարքերում ծրագրերի կենտրոնացված տեղադրումը:
• Կառավարվող շարժական սարքերի համար վկայագրերի կենտրոնացված տեղադրում:
• Տվյալների կոդավորման հսկողության աջակցություն:
• Կառավարման համակարգում ցանցի բեռը նվազեցնելու նպատակով կազմակերպությունում ցանկացած համակարգիչ հատկանշելու ունակություն:
• Կազմակերպությունում ցանկացած համակարգիչ հայտնաբերելու ունակություն, հակավիրուսային միջոցառումների իրադարձությունները հակավիրուսային միջոցների փոխանցման կենտրոնին, ընտրված հաճախորդի համակարգչային խմբին եւ կենտրոնացված կառավարման սերվերին՝ կառավարման համակարգում ցանցի բեռը նվազեցնելու համար:
• Գրաֆիկական զեկույցների կառուցումը ինչպես հակավիրուսային պաշտպանության դեպքերում, այնպես էլ գույքագրման, լիցենզավորման եւ այլնի վերաբերյալ:
• Հասանելիություն նախապես կազմված ստանդարտ հաշվետվություններ համակարգի գործունեության վերաբերյալ:
• Արտահանման հաշվետվություններ PDF եւ XML ֆայլերով:
• Իրադարձությունները տվյալների բազայից IBM Qradar եւ HP Arcsight կամ Syslog (RFC 5424) փոխանցելու ունակություն:
• Կրկնօրինակ պահեստների և կարանտինի առարկաների կենտրոնացված կառավարում բոլոր ցանցային ռեսուրսների համար, որոնց վրա տեղադրվում է հակավիրուսային ծրագրեր:
• Կառավարման սերվերում նույնականացման համար ներքին հաշիվների ստեղծում:
• Կառավարման համակարգում ներկառուցված կառավարման համակարգի կրկնօրինակի պատճենի ստեղծում:
• Windows Failover Clustering-ի հնարավորություն:
• Windows- ի սերվերի սերտիֆիկատի հետ ինտեգրման հնարավորություն:
• Վեբ կառավարման վահանակի առկայություն:
• Օգտագործողների համար ինքնասպասարկման պորտալի առկայություն: Ինքնասպասարկման պորտալը պետք է ապահովի օգտվողներին նպատակակետին միացնելու հնարավորություն: Կառավարման գործակալի բջջային սարքի տեղադրում, բջջային սարքերի դիտում, արգելափակման հրամանները ուղարկելու, սարքի որոնման եւ օգտագործողի բջջային սարքի տվյալների վերացման մասին:
• Վիրուսային համաճարակների առաջացման հսկողության համակարգի առկայությունը:

Հակավիրուսային տվյալների բազայի թարմացման պահանջները
Թարմացվող հակավիրուսային տվյալների բազաները պետք է ապահովեն հետեւյալ ֆունկցիոնալությունը.
• Օրացուցային օրվա ընթացքում առնվազն 24 անգամ հակավիրուսային տվյալների բազաների թարմացում:
• Թարմացման բազմաթիվ եղանակներ, այդ թվում՝ կապի ուղիներով եւ օտարվող էլեկտրոնային տեղեկատվական կրիչներով:
• Էլեկտրոնային թվային ստորագրության միջոցով թարմացումների ամբողջականության եւ նույնականության ստուգում:

Գործառնական փաստաթղթերի պահանջները
Բոլոր հակավիրուսային պաշտպանության ծրագրային արտադրանքների, այդ թվում՝ կառավարման գործիքների գործառնական փաստաթղթերը պետք է ներառեն պետական ստանդարտների պահանջներին համապատասխան, ռուսերեն, ներառյալ՝
• Օգտագործողի ուղեցույց (ադմինիստրատոր):
Հակավիրուսային գործիքներով տրամադրվող փաստաթղթերը պետք է մանրամասն նկարագրեն համապատասխան հակավիրուսային պաշտպանության տեղադրումը, կազմաձեւումը եւ գործարկումը:

Տեխնիկական աջակցության պահանջներ
Հակավիրուսային ծրագրերի տեխնիկական աջակցությունը պետք է՝
• Տրամադրվի հակավիրուսային պաշտպանության մատակարարի ռուսերեն լեզվով հավաստագրված մասնագետներին եւ նրա գործընկերների սերտիֆիկացված մասնագետներին Ռուսաստանի Դաշնության տարածքում՝ հեռախոսով, էլեկտրոնային փոստով եւ ինտերնետով:

- ապարատային և ծրագրային ապահովման արտադրողի կայքը պետք է լինի ռուսերենով, ունենա հատուկ բաժին, ապարատային եւ ծրագրային ապահովման տեխնիկական աջակցության համար, համալրված գիտելիքների բազա ինչպես նաեւ ծրագրային արտադրանքի օգտագործողների համար ֆորում:

Քանակական պահանջներ

- նախատեսվող արտոնագրերի քանակը 1000 հատ՝ տարանջատված 100 խմբերի:

Ապրանքը համարվում է ծախսվող միջոց: Արտոնագիրը ուժի մեջ է սկսած մատակարարման օրից՝ առնվազն 2 տարի ժամկետով:

Ապրանքները մատակարարվելու են վաճառողի կողմից ՀՀ ՉՈՒ կապի և ԱԿՀ վարչության պահեստ՝ ք.Երևան, Քանաքեռ, Ծարավ Աղբյուրի 54:

ԳՆՄԱՆ ԺԱՄԱՆԱԿԱՑՈՒՅՑ

Գնման առարկայի						
ը/հ	անվանումը	չ/մ	քանակը	միավորի գինը (ՀՀ դրամ)	ընդհանուր գումարը (ՀՀ դրամ)	մատակարարումը 2020թ. ըստ եռամսյակների, ընդ որում՝
						2-րդ եռամսյակ
1	էլեկտրոնային պարագաներ՝ այդ թվում	դրամ	1			
	Հակավիրուսային համակարգչային ծրագրային արտոնագիր	հատ	1000	22998	22998000	1000

Հավելված N 2
N ԳՀԱՊՁԲ-20-1/10-1 պայմանագրի

ՎՃԱՐՄԱՆ ԺԱՄԱՆԱԿԱՑՈՒՅՑ*

ՀՀ դրամ

Գնման առարկայի			Նախատեսվում է ֆինանսավորել 2020թ. ըստ ամիսների, բայց ոչ ուշ, քան 10.12.2020թ., ընդ որում՝						
ը/հ	անվանումը	CPV կոդը	հունիս	հուլիս	օգոստոս	սեպտեմբեր	հոկտեմբեր	նոյեմբեր	դեկտեմբեր
1	էլեկտրոնային պարագաներ (հակավիրուսային համակարգչային ծրագրային արտոնագիր)	31711100/1	22998000	22998000	22998000	22998000	22998000	22998000	22998000

* Վճարման ենթակա գումարները ներկայացված են ամողական կարգով

ԳՆՈՐԴ

ՀՀ պաշտպանության նախարարություն

ՀՀ ՊՆ ՆՏԱ գլխավոր վարչության պետ

Ն. ՅՈԼՉՅԱՆ

ՎԱՃԱՌՈՂ

«Էյչ Գրուպ» ՍՊԸ տնօրեն

Կ. ՀԱՐՈՒԹՅՈՒՆՅԱՆ

Հավելված N 3
N ԳՀԱՊՁԲ-20-1/10-1 պայմանագրի

Պայմանագրի կողմ

_____

_____

գտնվելու վայրը _____

հհ _____

հվհհ _____

Պատվիրատու

_____

_____

գտնվելու վայրը _____

հհ_____

հվհհ_____

ԱՐՁԱՆԱԳՐՈՒԹՅՈՒՆ N
ՊԱՅՄԱՆԱԳՐԻ ԿԱՄ ԴՐԱ ՄԻ ՄԱՍԻ ԿԱՏԱՐՄԱՆ ԱՐԴՅՈՒՆՔՆԵՐԻ ՀԱՆՁՆՄԱՆ-ԸՆԴՈՒՆՄԱՆ

« » « » 20 թ.

Պայմանագրի /այսուհետ՝ Պայմանագիր/ անվանումը՝

_____

Պայմանագրի կնքման ամսաթիվը՝ «____» «_____» 20 թ.

Պայմանագրի համարը՝ _____

Պատվիրատուն և Պայմանագրի կողմը՝ հիմք ընդունելով պայմանագրի կատարման վերաբերյալ « » « » 20 թ. դրտր գրված N ___ հաշիվ ապրանքագիրը, կազմեցին սույն արձանագրությունը հետևյալի մասին.

Պայմանագրի շրջանակներում Պայմանագրի կողմը մատակարարել է հետևյալ ապրանքները՝

N	Մատակարարված ապրանքների							
	անվանումը	տեխնիկական բնութագրի համառոտ շարադրանքը	քանակական ցուցանիշը		կատարման ժամկետը		Վճարման ենթակա գումարը /հազար դրամ/	Վճարման ժամկետը /ըստ վճարման ժամանակացույցի/
			ըստ պայմանագրով հաստատված գնման ժամանակացույցի	փաստացի	ըստ պայմանագրով հաստատված գնման ժամանակացույցի	փաստացի		

Սույն արձանագրության երկկողմ հաստատման համար հիմք հանդիսացած հաշիվ ապրանքագիրը և դրական եզրակացությունը հանդիսանում են սույն արձանագրության բաղկացուցիչ մասը և կցվում են:

Ապրանքը հանձնեց

_____
ստորագրություն

_____
ազգանուն, անուն

Կ.Տ.

Ապրանքը ընդունեց

_____
ստորագրություն

_____
ազգանուն, անուն

Կ.Տ.

Հավելված N 3.1
N ԳՀԱՊՁԲ-20-1/10-1 պայմանագրի

ԱԿՏ N _____
պայմանագրի արդյունքը Գնորդին հանձնելու փաստը ֆիքսելու վերաբերյալ

Սույնով՝ արձանագրվում է, որ _____-ի (այսուհետ՝ Գնորդ) և _____
Գնորդի անվանումը Վաճառողի անվանումը
(այսուհետ՝ Վաճառող) միջև 20 թ. _____ -ին կնքված N _____
պայմանագրի կնքման ամսաթիվը պայմանագրի համարը
պայմանագրի շրջանակներում Վաճառողը 20 թ. _____-ին հանձնման-ընդունման նպատակով Գնորդին հանձնեց ստորև նշված ապրանքները.

Ապրանքի		
անվանումը	չափման միավորը	քանակը (փաստացի)

Սույն ակտը կազմված է 2 օրինակից, յուրաքանչյուր կողմին տրամադրվում է մեկական օրինակ:

ԿՈՂՄԵՐԸ

Հանձնեց

_____
ազգանուն, անուն

_____
Ստորագրություն

Ընդունեց
հայտը նախագծած ներկայացուցիչ՝

_____
ազգանուն, անուն

_____
ստորագրություն