УДК 004.75 **DOI 10.52167/1609-1817-2024-132-3-449-459**

Ж.М. Ташенова[1], Э.Н. Нурлыбаева[2], Ж.К. Абдугулова[1], Ш.А. Аманжолова[3]
[1]Л. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан
[2]Т.Қ. Жүргенев атындағы Қазақ Ұлттық өнер академиясы, Алматы, Қазақстан
[3]Құрманғазы атындағы Қазақ ұлттық консерваториясы, Алматы, Қазақстан
E-mail: zhuldyz_tm@mail.ru

WINDOWS ОПЕРАЦИЯЛЫҚ ЖҮЙЕСІНДЕГІ ҚАТЕЛІКТЕРДІ ЗЕРТТЕУ ЖӘНЕ ТАЛДАУ

Аңдатпа. Бұл мақалада 2020 жылы шыққан Windows 10 операциялық жүйеде (ОЖ) туындайтын қателіктер мен олардың алдын алу жолдары мен әдістеріне зерттеу жүргізу болып табылады. Windows операциялық жүйесінде туындайтын қателіктерді зерттеп, оларды түзеу үшін ұсыныстар жасау осы мақалада зерттеледі. Операциялық жүйе құру принциптері, қолданыстағы операциялық жүйелерде жиі кездесетін қателіктерді талдау жұмыстарын жүргізуге арналған. Windows операциялық жүйесін басқа жүйелермен саластыру және Windows операциялық жүйесінде туындайтын қателіктерді және туындау себептерін анықтау көрсетілген. Windows операциялық жүйесінде туындайтын қателіктерді жою бойынша ұсыныстар құра отырып оларды алдын алу болып табылады. Windows операциялық жүйесінде туындайтын қателіктерді зерттеу және оларды жою жолдары бойынша ұсыныстар болашақта операциялық жүйенің жаңа нұсқасында қателіктерді алдын ала жою мәселелері қарастырылды. Және де, 2020 жылы шыққан Windows 10 операциялық жүйесінде туындайтын қателіктер мен олардың алдын алу жолдары мен әдістеріне зерттеу жүргізіледі. Түзетуді қажет ететін өзекті қателіктің бірі кәсіпорындардағы домен контроллерлері Kerberos түпнұсқалығын тексеру және Kerberos билетін жаңарту мәселелеріне тап болуы мүмкіндігі болып табылады. Операциялық жүйе құру принциптеріне шолу жасалынады. Қолданыстағы операциялық жүйелерде жиі кездесетін қателіктер талданады. Windows операциялық жүйесін басқа жүйелермен саластыру жүргізіледі. Windows операциялық жүйесінде туындайтын қателіктерді және туындау себептерін анықталады. Windows операциялық жүйесінде туындайтын қателіктерді жою бойынша ұсыныстар құрылады. Сонымен қатар, windows 10 операциялық жүйесі кіріктірілген қауіпсіздік саясатын баптау бойынша ұсыныстар қосымша ақпарат ретінде келітірілді.

Түйінді сөздер. Операциялық жүйе, windows 10, қателіктер, қауіпсіздік, антивирустар, шабуылдар, Windows Defender, брандмауэр,браузерді басқару, Microsoft defender, эксплойттар.

Кіріспе.

Компьютерлік технологиялар индустриясы қазіргі әлемдегі ең прогрессивті индустрия болып саналады. Біздің планетамыздың тұрғындарының 90% жасына және кәсібіне қарамастан күн сайын гаджетті (ұялы телефон, планшет), компьютерді немесе ноутбукті пайдаланады. Жоғарыда аталған құрылғыларға енгізілген барлық аппараттық және бағдарламалық процестер операциялық жүйе (ОЖ) деп аталатын бағдарламалық жасақтама бірліктерінің жиынтығы арқылы басқарылады. Қазіргі операциялық жүйенің генезисі компьютерлік құрылғылар бағдарламалар кітапханасымен жабдықтала бастаған кезде басталды.

Қазіргі заманғы операциялық жүйелердің үлкен болуы ешбір адам бүкіл жүйені түсіне алмайтындығын білдіреді, нәтижесінде жүйені басқару бойынша қиындықтар туа

бастайды. Операциялық жүйелерде оқшаулау компоненттері жоқ. Қазіргі заманғы операциялық жүйеде ядрода орындалатын біртұтас екілік бағдарламаны құрайтын жүздеген және мыңдаған процедуралар бар. Ядро кодының миллиондаған жолдарының әрқайсысында оған байланысты емес компонент қолданатын негізгі деректер құрылымына жазу мүмкіндігі бар, бұл жүйенің құлдырауына әкелуі мүмкін [1,2].

Статкаунтер әлемдік статистикалық жұмыстар жүргізетін ұйымның зерттеулеріне сәйкес компьютерлерде қондырылған операциялық жүйелердің көшбашсы ретінде windows алға шығып отыр. Себебі, әлемнің компьютерінде орнатылған операциондық жүйелер түрлеріне қатысты статистикалық мәліметтер бойынша windows – 76,58% OS X – 18,93% және Linux – 1,62% құрап отыр [3,4].

Компьютердің өнімділігі оған орнатылған операциялық жүйенің қаншалықты тиімді жұмыс істейтініне тікелей байланысты екенін білеміз. Бұл біз қолданатын бағдарламаларды үнемі жаңартып отыру арқылы қамтамасыз етіледі. Мұндай процестерде пайдаланушының құпия деректерінің ағып кетуіне жол бермейтін және зиянды бағдарламаларды рұқсатсыз орнатуды блоктайтын жақсы құрылған ақпараттық қауіпсіздік ерекше рөл атқарады.

Танымал операциялық жүйелер мен үлкен қосымшаларда қауіпсіздік мәселелері өте жиі кездеседі десек артық айтпаймыз; көптеген бағдарламалар өздерінің жетілмегендігіне байланысты аздап әлсіздікке ие деп айтуға болады, оны біз бейресми түрде осалдық деп атаймыз. Бұл қауіпсіздік мәселелері кез келген амалдық жүйеге немесе Бағдарламалық жасақтамаға айтарлықтай әсер етеді және де олардың жұмыс жасауына кері әсерін тигізуі мүмкін.

Операциялық жүйені немесе кез келген бағдарламалық жасақтаманы қорғау - бұл үнемі тестілеуді қажет ететін үздіксіз процесс. Тәуекел мен жүйенің басымдығына байланысты қауіпсіздік жағдайын тексеру ай сайын, апта сайын немесе күн сайын жүргізілуі мүмкін.

Windows – әлемдегі ең көп сатылатын және ең танымал операциялық жүйе. Соңғы қырық жыл ішінде операциялық жүйе іскерлік есептеулерде де, тұтынушылық есептеулерде де көптеген адамдар үшін әртүрлі есептеу функцияларын орындау үшін байланыстырушы буын ретінде басты рөл атқарды. Жұмыстағы немесе үйдегі адамдардың көпшілігі Windows операциялық жүйесінің осы немесе басқа нұсқасын қандай-да бір түрде қолданды. Microsoft жүйесі MacOS және Linux операциялық жүйелерінен басқа барлық жерде бар.

Windows 10 операциялық жүйесінің соңғы нұсқасы Microsoft корпорациясының флагманы және Windows Vista және Windows 8 сияқты алдыңғы нұсқаларды толықтырды және жетілдірді. Модернизацияларына қарамастан, Windows 10 операциялық жүйесінің қателер мен проблемалар жоқ, сондықтан 2015 жылы іске қосылғаннан бері көптеген адамдар Windows 7 жүйесін 2020 жылдың 14 қаңтарында ескіргеніне қарамастан қолдана берді [5].

Енді Windows 7 қызмет ету мерзімі ағымдағы жылда аяқталған кезде, көптеген компаниялар Windows 10 операциялық жүйесіне ауыса бастады, және де көптеген мәселелермен соқтығысуда. Бұл операциялық жүйенің мөлшері, бағдарламалық жасақтаманы пайдаланатын адамдар міндетті түрде қиындықтарға тап болады. Сондықтан Windows операциялық жүйесінде туындайтын қателіктерді зерттеу мәселесі өзекті болып табылады [6].

Материалдар мен тәсілдер.

Бүгінгі таңда ақпараттық технологиялардың қарқынды дамуы мен компьютердің барлық салаларда қолдануының салдарынан өздерінің пайдалары үшін әртүрлі стандартты

емес жолдармен бағалы ақпараттарға рұқсатсыз қол жеткізгісі келеді. Бұның салдарынан осындай адамдармен күресу қажеттілігі туындады. Ақпараттық қауіпсіздікті күшейту мақсатында көптеген программалар жиынтығы құрылды. Кез келген электронды-есептеу кешенін арнайы операциялық жүйе басқаратын болғандықтан, жүйенің қауіпсіздігін қамтамасыз ету үшін ең алдымен операциялық жүйенің қауіпсіздігін қамтамасыз ету қажет.

Кез келген операциялық жүйе қандай да бір кемшіліктерге ие болады және компьютердің жұмысына абсолютті тұрақтылықты қамтамасыз етпейді. Қандай да болсын өндіруші өзінің операциялық жүйесінің қауіпсіздігін қамтамасыз етеді. Бір операциялық жүйелер жоғары деңгейде қорғау жүйелерімен қамтылған болса, кейбіреулері мүлде ондай қызметтер қарастырылмаған. Осыған орай мақалада қолданушылар арасында кең таралған Windows операциялық жүйесінде туындайтын қателіктерді зерттеу және оларды жою жолдары қарастырылатын болады [7].

Зерттеу жұмысының жоспары:

1) Операциялық жүйе құру принциптеріне шолу.

2) Қолданыстағы операциялық жүйелерде жиі кездесетін қателіктерді талдау.

3) Windows операциялық жүйесін басқа жүйелермен саластыру.

4) Windows операциялық жүйесінде туындайтын қателіктерді және туындау себептерін анықтау.

5) Windows операциялық жүйесінде туындайтын қателіктерді жою бойынша ұсыныстар құру.

Windows қауіпсіздігі - бұл операциялық жүйенің жалпы қауіпсіздік мүмкіндіктерін басқаруға арналған ыңғайлы интерфейс пен құралдарды ұсынатын Windows 10 кіріктірілген қызметі. Бұған Windows Defender кіреді, ол компьютерді вирустардан және басқа зиянды бағдарламалардан нақты уақыт режимінде қорғауды ұсынады [8].

Аталмыш, операциялық жүйе бір ерекшелігі кіріктірілген антивирустың болуы болып табылады. Бұл мақалада Windows 10 операциялық жүйесі қауіпсіздік параметрлерінен қалай бастау керектігін және дербес компьютердегі зиянды бағдарламалар мен хакерлерден қорғау үшін кіріктірілген антивирустың көмегімен күнделікті тапсырмаларды орындау қарастырылады.

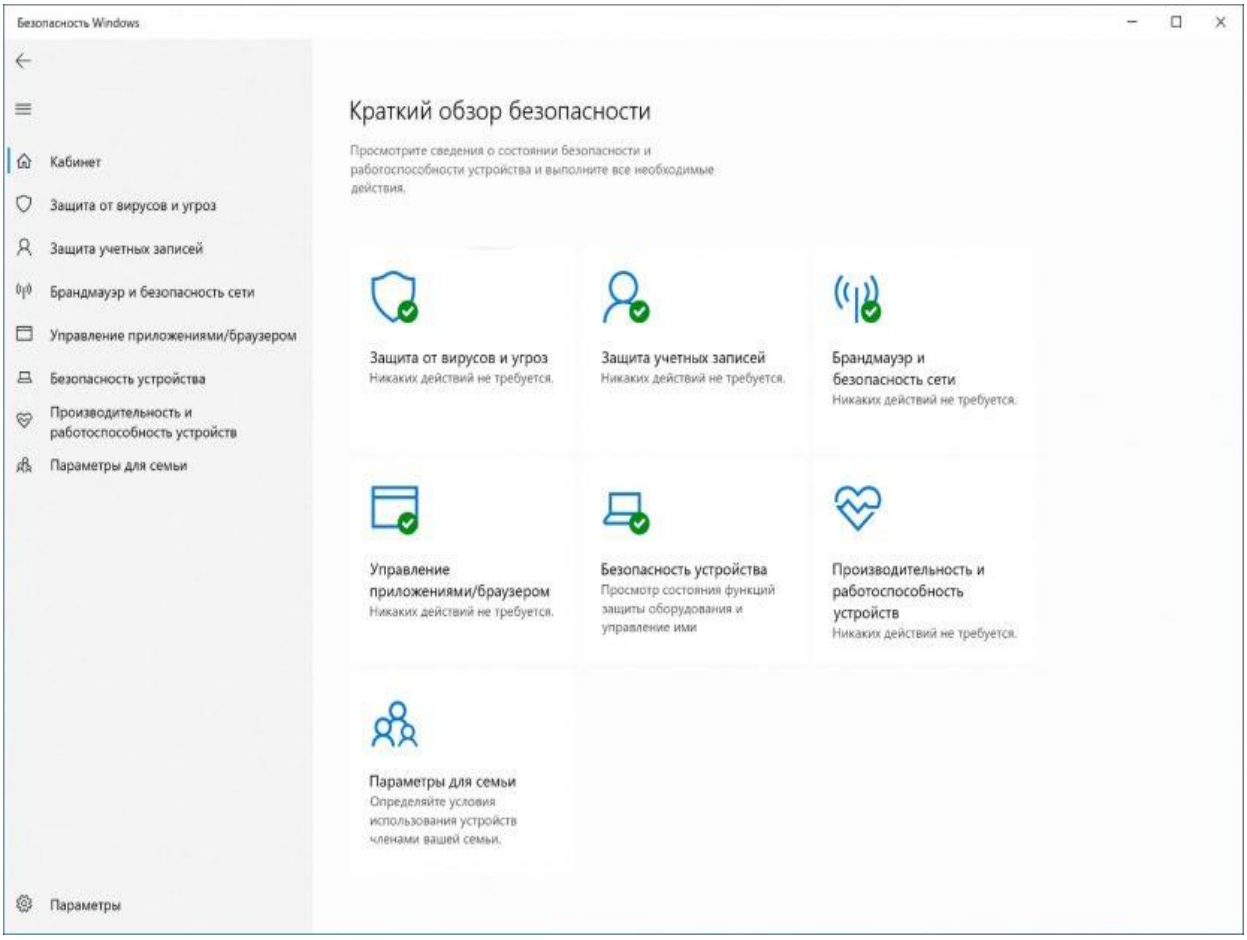
Ең алдымынен, Windows Defender мен Windows қауіпсіздігі арасындағы айырмашылықты түсіну қажет. Windows қауіпсіздігі – бұл антивирус, брандмауэр, өнімділік және басқалар сияқты қауіпсіздік мүмкіндіктерін қарау және басқару үшін бірыңғай интерфейсті ұсынатын қызмет. Ал, Windows Defender – бұл нақты уақыт режимінде зиянды бағдарламалардан, вирустардан, шпиондық бағдарламалардан және т.б. қорғауды ұсынатын кіріктірілген бағдарлама. Алайда, басқа провайдерлердің антивирусын орнату Windows Defender қызметін автоматты түрде өшіреді, бірақ Windows қауіпсіздігі қызметінің жұмысына әсер етпейді. Сол сияқты, кірістірілген антивирусты немесе брандмауэрді өшіру Windows қауіпсіздігін өшірмейді.

Нәтижелер.

Windows қауіпсіздігі – бұл қарапайым интуитивті бағдарлама. Оны Бастау мәзірінен немесе тапсырмалар тақтасындағы хабарландыру аймағындағы қалқан белгішесін екі рет басу арқылы ашуға болады [9].

Сурет 1 келтірілгендей Windows қауіпсіздігі қызметінің басты бетінде Windows 10 операциялық жүйесі әдеттегі бойынша қол жетімді барлық қорғау функцияларының қауіпсіздік күйін көруге болады. Мұнда компьютердің қауіпсіздігін қамтамасыз ету үшін жасалатын барлық әрекеттер туралы ескертулер көрсетіледі.

Тапсырмалар тақтасының хабарландыру аймағындағы қалқан белгішесі әрекетті орындау қажет болған кезде ескерту жасай алады. Егер бірнеше ескерту болса, онда тек ең маңызды ескерту көрсетіледі.



1 сурет - Windows қауіпсіздігі қызметінің интерфейсі

Windows қауіпсіздігі басқаруға болатын жеті қорғаныс аймағын қамтиды:

– вирустардан және қауіптерден қорғау – кірістірілген антивирустың параметрлерін қамтиды. Ол зиянды бағдарламалардан қорғауды бақылауға, қауіп-қатерге арналған құрылғыны сканерлеуге, оффлайн қарап шығуды іске қосуға, бағдарламалық жасақтамадан қорғаудың кеңейтілген функциясын конфигурациялауға мүмкіндік береді (2 сурет)[11];

– қолданушылардың тіркеу жазбаларын қорғау – Windows 10 операциялық жүйесі тіркеу жазбаны қорғауды талап етуге мүмкіндік береді;

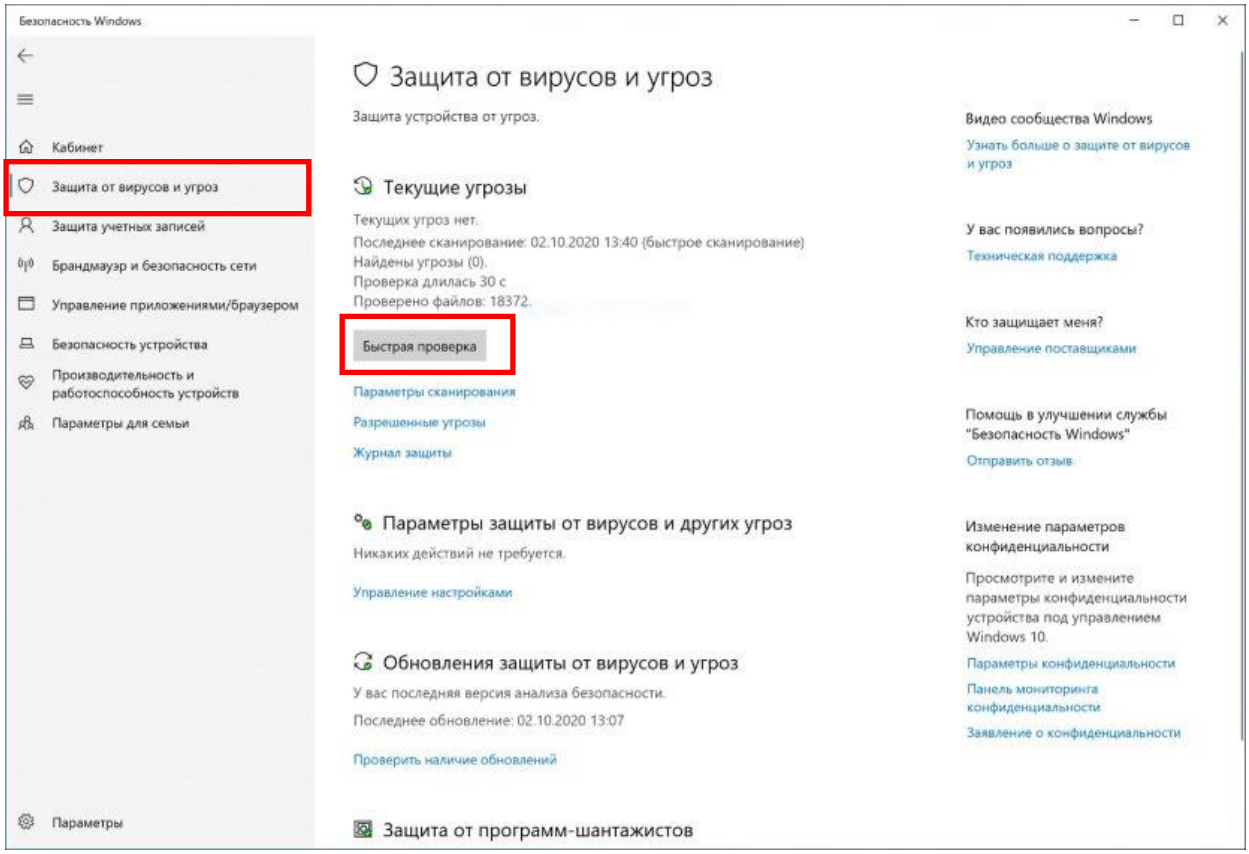
– брандмауэр және желінің қауіпсіздігі – желілік қосылымдарды бақылауға және кірістірілген брандмауэрдің әртүрлі параметрлерін реттеуге мүмкіндік береді;

– бағдарламалар мен браузерді басқару – қосымшаларда, файлдарда немесе сайттарда жасырылған зиянды кодтан қорғануға көмектеседі;

– құрылғының қауіпсіздігі – компьютерді шабуылдардан қорғау үшін ядро оқшаулау сияқты аппараттық деңгейдегі қауіпсіздік функцияларын қамтиды;

– құрылғының өнімділігі мен өнімділігі – бұл компьютердің өнімділігі туралы есеп беру мүмкіндігі;

– отбасы параметрлері – Microsoft тіркеу жазбаларын пайдаланып отбасы құрылғыларын басқаруға оңай қол жетімділікті ұсынады.



2 сурет - Вирустар мен қауіптерден қорғау қызметін қосу терезесі

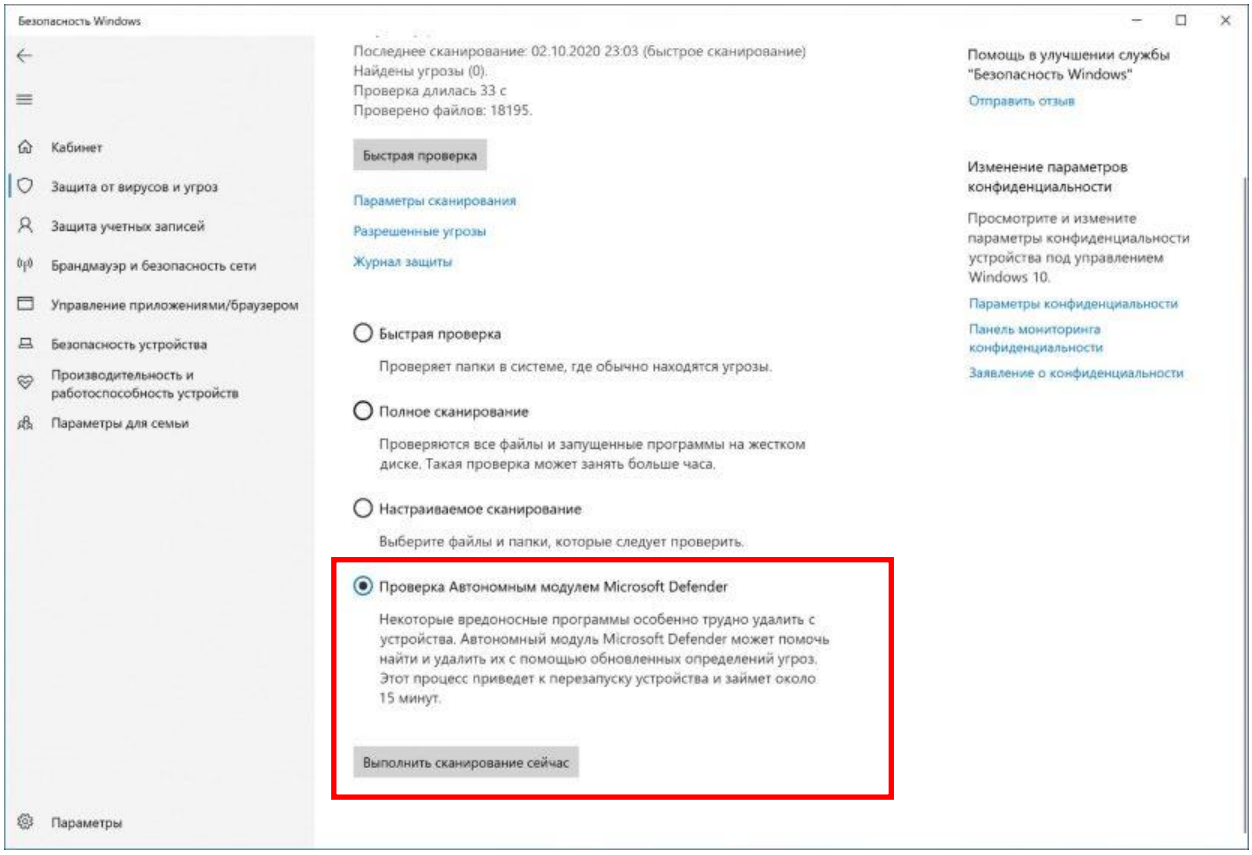
Тағы бір артықшылық, Windows 10 операциялық жүйесі зиянды бағдарламалар базасын автоматты түрде жаңартады және құрылғыны зиянды бағдарламалардан қорғау үшін үнемі тексеріп отырады. Сонымен қатар, бұл қызметтерді өз бетіменде жасауға болады. Алайда, автоматты түрдегі баптаулар қолданушылардың уақытын үнемдеп, құрылғының жұмысын оңтайландырады.

Жылдам сканерлеу қызметі бір минуттан аз уақытты алады және зиянды бағдарламалар жасырылуы мүмкін жүйенің бөліктерін ғана тексереді [12].

Windows Defender қызметінің көмегімен сканерлеуді іске қосу үшін 3-суретте қызыл түспен келтірілгендей вирустар мен қауіптен қорғау бөлімін таңдап, жылдам тексеру батырмасын басу қажет.

Осы қадамдарды орындағаннан кейін жүйені сканерлеу басталады және «ағымдағы қауіптер» бөлімінде анықталған қауіптер, сканерлеуді аяқтауға кететін уақыт және сканерленген файлдардың саны көрсетіледі. Ал, егер дербес компьютер вирус немесе қауіпті бағдарламаның әсеріне ұшыраған болса, онда толық сканерлеуді қосуға болады. Ескере кететін жайт, сканерлеудің бұл түрі дербес клмпьютердің барлық бағдарламалар мен қосымшаларын тексереді және белгілі бір уақытты алуы мүмкін.

Оффлайн модульдегі Microsoft defender қызметін қосу үшін сурет 3 келтірілген батырманы басу арқылы қосу қажет.



3 сурет - Оффлайн модульдегі Microsoft defender қызметін қосу

Кейде, дербес компьютер ауыр вируспен немесе зиянды бағдарламаның басқа түрінің әсеріне ұшырауы мүмкін, онда Windows 10 жұмыс істеп тұрған кезде антивирус оны жоймауы мүмкін. Бұл жағдайда оффлайн сканерлеу үшін Microsoft Defender бағдарламасының функциясын пайдалануға болады [13].

Оффлайн модуль функциясын қолданған кезде компьютер қалпына келтіру ортасында автоматты түрде қайта іске қосылады және Windows 10 іске қосылмас бұрын толық сканерлеуді орындайды.

Оффлайн модуль арқылы вирусты тексеруді бастау үшін келесі әрекеттерді орындау қажет:

– вирустардан және қауіптерден қорғау батырмасын басу қажет;
– «ағымдағы қауіптер» бөлімінде сканерлеу параметрлері сілтемесін басу қажет;
– Microsoft Defender дербес модулімен тексеру опциясын таңдаймыз;
– «қазір сканерлеу» батырмасын басамыз;
– ашылған терезеде тексеру батырмасын басамыз.

Осы қадамдарды орындағаннан кейін, құрылғы бүкіл компьютерді сканерлейтін Microsoft Defender антивирусының дербес модулімен қайта іске қосылады және жүктеледі. Егер зиянды код анықталса, ол автоматты түрде жойылады немесе карантинге жіберіледі [14].

Сканерлеуден кейін құрылғы Windows 10 операциялық жүйесі автоматты түрде жүктейді және сканерлеу қорытындысы бойынша есепті Windows қауіпсіздік қосымшасында көруге болады.

Кез келген операциялық жүйенің зиянды қорғау қажеттілігі бар. Оны жүзеге асыру үшін Бағдарламаны/браузерді басқару терезесінде компьютерді зиянды коды бар сайттардан, қосымшалардан және файлдардан қорғауға көмектесетін қолданбаларды

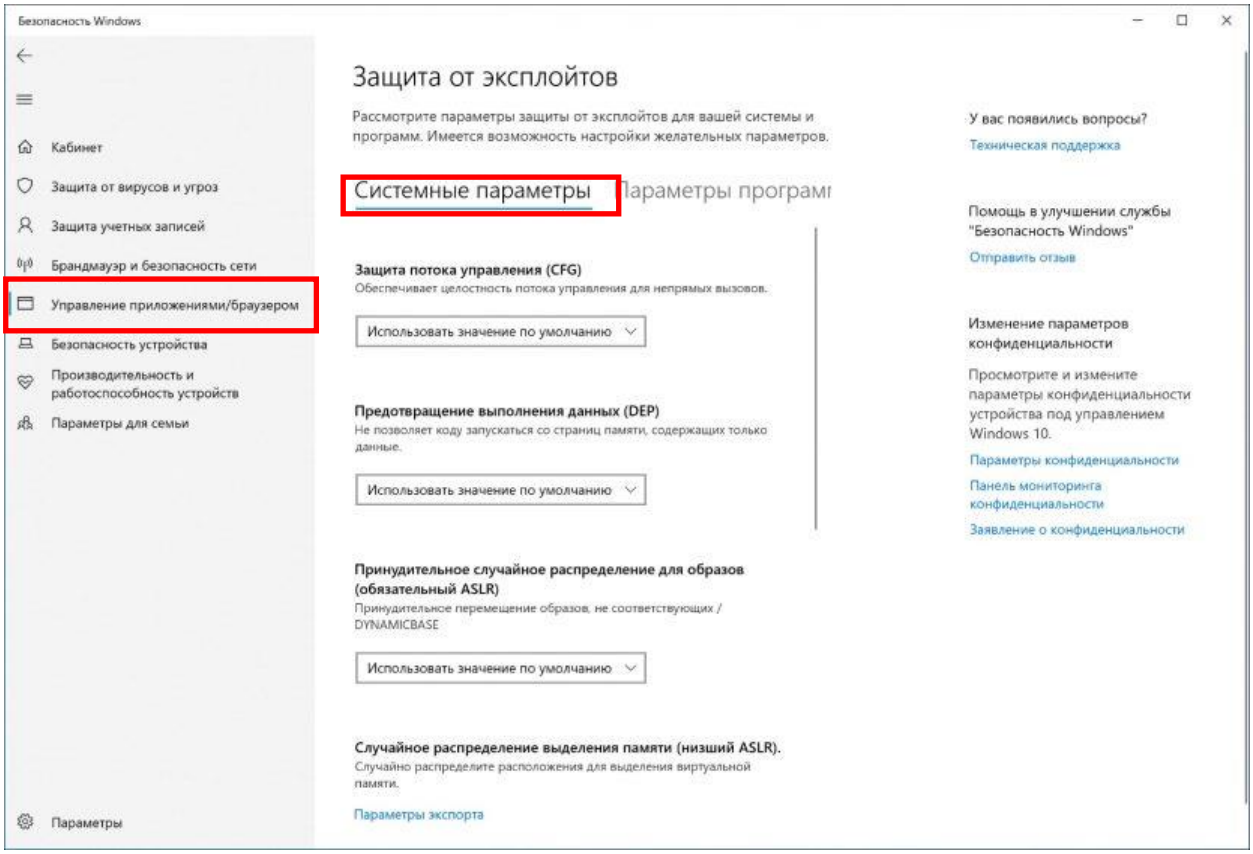
қорғау және Интернеттегі қауіпсіздік параметрлерін баптауға болады. Әдетте бұл параметрлерді әр қолданушы үнсіздік режимінде ұсынылған конфигурация ретінде қолдануы тиіс.

Сонымен қатар, windows 10 операциялық жүйесі оқшауланған қарау режимі қарастырылған. Оқшауланған қарау – бұл Windows 10 Pro, Education және Enterprise версиялы операциялық жүйесі редакторларының мүмкіндігі болып табылады. Ол Microsoft Edge браузерін аппараттық деңгейде оқшаулауға, құрылғы мен деректерді зиянды бағдарламалардан немесе нөлдік күндік шабуылдардан қорғауға арналған. Егер бұл опция қол жетімді болса, келесі қадамдарды орындау арқылы Microsoft қорғаушысындағы оның параметрлеріне қол жеткізуге болады:

– бағдарламалар мен браузерді басқару батырмасын басыңыз;
– Application Guard параметрлерін өзгерту опциясын басыңыз.

Егер, «Microsoft Defender Application Guard» компоненті «Windows компоненттерін қосу немесе өшіру» функциясы арқылы қосылған болса, жоғарыда аталған параметрлерді баптауға қол жеткізуге болады. Әдетте бұл қауіпсіздік саясаты корпоративті желілерде мекеме деңгейінде қолданылады.

Эксплойттардан қорғау – бағдарламалар мен ақаулардың санын азайтуға көмектесетін жетілдірілген мүмкіндік болып табылады. Бұл қауіпсіздік саясатын баптау үшін қосымшалар мен браузерді басқару терезесі-эксплойттардан қорғау параметрлері-жүйелік параметрлер терезесіне өту арқылы сурет 4 келтірілгендей баптау жасау қажет [15].



4 сурет - Эксплойттардан қорғау параметрлерін баптау терезесі

Қорытындылай келе, Norton, AVG, Kaspersky, Avast, Bitdefender сияқты танымал компаниялардың вирустар мен шабуылдардан қорғауға арналған шешімдерін қолдануға

болады, бірақ Windows 10 операциялық жүйесі стандартты мүмкіндіктері тез жұмыс істейтін және кез-келген басқа шешіммен бәсекеге түсе алатын қарапайым интерфейсі бар жақсы құралдар жиынтығын ұсынады.

Талқылау.

Қойылған мақсатқа жету барысында келесідей міндеттер орындалды. Атап айтқанда, зерттеу тақырыбының өзектілігін негіздеу барысында зерттеу тақырыбының заманауи ахуалы бағаланды. Яғни зерттеу объектісі ретінде алынған windows 10 операциялық жүйесі нарықтағы жағдайы статистикалық мәліметтерге сүйене отырып, бағаланды. Сонымен қатар, нарықтағы қолданысқа ие басқа операциялық жүйелермен салыстыру арқылы талдау жұмыстары жүргізілді. Зерттеу тақырыбы операциялық жүйеде кездесетін қателіктерді зерттеуге бағытталғандықтан жиі кездесетін жүйелік қателіктерге шолу жасалынды.

Зерттеу объектісі болып табылатын операциялық жүйесінде туындайтын қателіктердің маңыздылығы мен операциялық жүйе жұмысына әсері ету деңгейіне байланысты талдау жұмыстары жүргізілді. Сонымен қатар, операциялық жүйені құру барысында туындайтын шешімін таппаған қателіктерге талдау жасалынды.

Операциялық жүйеде туындайтын, жүйелік әкімші деңгейінде түзетуге келетін қателерді жою және түзету жолдары баяндалды. Сонымен қатар, windows 10 операциялық жүйесінде туындайтын қателіктерді алдын ала анықтау әдістеріде келтірілді. Кез келген қолданушы үшін операциялық жүйенің жұмыс жылдамдығы маңызды мәселе болып табылады. Сондықтанда бұл мақалада операциялық жүйе өнімділігін диагностика жасап, оны жылдамдату тәсілдері адым адыммен келтірілген болатын. Ал, операциялық жүйенің қауіпсіздік саясаты қолданушының дербес компьютермен жұмыс барысында қауіпсіз алаңсыз жұмысын қаматамасыз ету үшін қажет. Көпшілік біле бермейтін, windows 10 операциялық жүйе кіріктірілген қауіпсіздік саясатын баптау бойынша ұсыныстар қосымша ақпарат ретінде келітірлген болатын.

Қорытынды.

Мақалада 2020 жылы шыққан Windows 10 операциялық жүйесінде туындайтын қателіктер мен олардын алдын алу жолдары мен әдістеріне зерттеу жүргізілген болатын. 2020 жылы шыққан Windows 10 операциялық жүйесінде туындайтын қателіктер мен олардын алдын алу жолдары мен әдістеріне зерттеу жүргізілді. Түзетуді қажет ететін өзекті қателіктің бірі кәсіпорындардағы домен контроллерлері Kerberos түпнұсқалығын тексеру және Kerberos билетін жаңарту мәселелеріне тап болуы мүмкіндігі болып табылды. Операциялық жүйе құру принциптеріне шолу жасалынды. Қолданыстағы операциялық жүйелерде жиі кездесетін қателіктер талданды. Windows операциялық жүйесін басқа жүйелермен саластыру жүргізілді. Windows операциялық жүйесінде туындайтын қателіктерді және туындау себептерін анықталды. Windows операциялық жүйесінде туындайтын қателіктерді жою бойынша ұсыныстар құрылды. Сонымен қатар, windows 10 операциялық жүйесі кіріктірілген қауіпсіздік саясатын баптау бойынша ұсыныстар қосымша ақпарат ретінде келітірілді.

ӘДЕБИЕТТЕР

[1] Операционные системы. Теория и практика: учебное пособие/А.В.Замятин. - Томск: Изд-во Томского политехнического университета, 2012 – 263 С.

[2] Бэкон Дж., Харрис Т. Операционные системы. – СПб.: Изд-во «БХВ-Петербург», 2004. – 800 С.

[3] Дейтел Х.М., Дейтел П.Дж., Чорнес Д.Р. Операционные системы. Основы и принципы. – Изд-во «Бином-пресс», 2006. – 1024 С.

[4] Иртегов Д. Введение в операционные системы. – СПб.: Изд-во «БХВ-Петербург», 2008. – 1040 С.

[5] Стивенс У. UNIX: взаимодействие процессов. – СПб.: Питер, 2003. – 576 С.

[6] Стивенс У., Феннер Б., Рудофф Э.М. UNIX: разработка сетевых приложений. 3-е изд. – СПб.: Питер, 2007. – 1039 С.

[7] Танненбаум Э., Вудхалл А. Операционные системы. Разработка и реализация (+CD). Классика CS. 3-е изд. – СПб.: Питер, 2007. – 704 С.

[8] Скотт Мюллер. Модернизация и ремонт ПК. - М.: Изд-во Вильямс, 2011. - 1074 с.

[9] Крис Касперский. Восстановление данных. - СПб.: Изд-во БХВ-Петербург, 2007. - 352 с.

[10] Колисниченко, Денис Microsoft Windows 10. Первое знакомств. - М.: БХВ-Петербург, 2015. - 918 с.

REFERENCES*

[1] Operacionnye sistemy. Teorija i praktika: uchebnoe posobie/A.V.Zamjatin. - Tomsk: Izd-vo Tomskogo politehnicheskogo universiteta, 2012 – 263 S.

[2] Bjekon Dzh., Harris T. Operacionnye sistemy. – SPb.: Izd-vo «BHV-Peterburg», 2004. – 800 S.

[3] Dejtel H.M., Dejtel P.Dzh., Chornes D.R. Operacionnye sistemy. Osnovy i principy. – Izd-vo «Binom-press», 2006. – 1024 S.

[4] Irtegov D. Vvedenie v operacionnye sistemy. – SPb.: Izd-vo «BHV- Peterburg», 2008. – 1040 S.

[5] Stivens U. UNIX: vzaimodejstvie processov. – SPb.: Piter, 2003. – 576 S.

[6] Stivens U., Fenner B., Rudoff Je.M. UNIX: razrabotka setevyh prilozhenij. 3-e izd. – SPb.: Piter, 2007. – 1039 S.

[7] Tannenbaum Je., Vudhall A. Operacionnye sistemy. Razrabotka i realizacija (+CD). Klassika CS. 3-e izd. – SPb.: Piter, 2007. – 704 S.

[8] Skott Mjuller. Modernizacija i remont PK. - M.: Izd-vo Vil'jams, 2011. - 1074 s.

[9] Kris Kasperskij. Vosstanovlenie dannyh. - SPb.: Izd-vo BHV-Peterburg, 2007. - 352 s.

[10] Kolisnichenko, Denis Microsoft Windows 10. Pervoe znakomstv. - M.: BHV-Peterburg, 2015. - 918 c.

Zhuldyz Tashenova, PhD, acting associate docent, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan, zhuldyz_tm@mail.ru

Elmira Nurlybaeva, PhD, T. Zhurgenov Kazakh National Academy of Arts, Almaty, Kazakhstan, nuremek@mail.ru

Zhanat Abdugulova, associate professor, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan, janat_6767@mail.ru

Shirin Amanzholova, associate professor, Kazakh National Conservatory. Kurmangazy, Almaty, Kazakhstan, schirin75@mail.ru

RESEARCH AND ANALYSIS OF WINDOWS OPERATING SYSTEM ERRORS

Abstract. This article is a study of errors that occur in windows 10 operating system (os) in 2020 and ways and means to prevent them. This article examines the errors that occur in the

windows operating system and makes recommendations for their correction.The principles of creating an operating system are designed to analyze the most common errors in existing operating systems. It is shown to compare the windows operating system with other systems and to identify errors and their causes in the windows operating system. Prevent them by creating recommendations for troubleshooting errors in the windows operating system. Recommendations for researching and troubleshooting errors in the windows operating system in the future, the issues of preliminary troubleshooting in the new version of the operating system were considered. In addition, a study will be conducted on system errors of Windows 10 OS, released in 2020, and ways and methods of their prevention. One of the actual errors that need to be corrected is the possibility that domain controllers in enterprises face problems with Kerberos authentication and updating a Kerberos ticket. An overview of the principles of building an operating system is given. The most common errors in existing operating systems are analyzed. The Windows operating system is being integrated with other systems. Identifies errors and causes in the Windows operating system. Recommendations are made to eliminate errors that occur in the Windows operating system. In addition, recommendations for configuring the built-in security policy of Windows 10 were provided as additional information.

Keywords. Operating system, windows 10, errors, security, antivirus, attacks, Windows Defender, firewall, browser management, Microsoft defender, exploit.

Жулдыз Ташенова, PhD, и.о. доцент, Евразийский национальный университет им. Л. Н. Гумилева, Астана, Казахстан, zhuldyz_tm@mail.ru

Эльмира Нурлыбаева, PhD, Казахская национальная академия искусств им. Т. Жургенова, Алматы, Казахстан, nuremek@mail.ru

Жанат Абдугулова, ассоциированый профессор, Евразийский национальный университет им. Л. Н. Гумилева, Астана, Казахстан, janat_6767@mail.ru

Ширин Аманжолова, ассоциированый профессор, Казахская национальная консерватория им. Курмангазы, Алматы, Казахстан, schirin75@mail.ru

ИССЛЕДОВАНИЕ И АНАЛИЗ ОШИБОК ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS

Аннотация. Эта статья представляет собой исследование ошибок, возникающих в операционной системе (ос) windows 10, выпущенной в 2020 году, а также способов и средств их предотвращения. В этой статье рассматриваются ошибки, возникающие в операционной системе windows, и даются рекомендации по их исправлению. Принципы создания операционной системы предназначены для анализа наиболее частых ошибок в существующих операционных системах. Показано сравнение операционной системы windows с другими системами и выявление ошибок и их причин в операционной системе windows. Предотвратив их, создав рекомендации по устранению ошибок в операционной системе windows. Рекомендации по поиску и устранению ошибок в операционной системе windows в дальнейшем рассматривались вопросы предварительного устранения неполадок в новой версии операционной системы. Кроме того, будет проведено исследование системных ошибок ОС Windows 10, выпущенных в 2020 году, и способов и методов их предупреждения. Одной из актуальных ошибок, требующих исправления, является возможность того, что контроллеры домена на предприятиях сталкиваются с проблемами проверки подлинности Kerberos и обновления билета Kerberos. Дается обзор принципов построения операционной системы. Анализируются наиболее распространенные ошибки в существующих операционных системах. Выполняется интеграция операционной

системы Windows с другими системами. Выявляет ошибки и причины возникновения в операционной системе Windows. Составляются рекомендации по устранению ошибок, возникающих в операционной системе Windows. Кроме того, в качестве дополнительной информации были приведены рекомендации по настройке встроенной политики безопасности ОС windows 10.

Ключевые слова. Операционная система, windows 10, ошибки, безопасность, антивирусы, атаки, Windows Defender, брандмауэр, упраление браузерами, Microsoft defender, эксплойты.

****