ВИРУСҚА ҚАРСЫ БАҚЫЛАУДЫ ҰЙЫМДАСТЫРУ ҚАҒИДАЛАРЫ

Астана
2023 ж.

1. Терминдер мен қысқартулар

Ұйым– «Qazaq Green» ЖЭК қауымдастығы ЗТБ;

Қағидалар – вирусқа қарсы бақылауды ұйымдастыру қағидалары.

Ақпараттық қауіпсіздік жөніндегі маман – ақпараттық ресурстарды қорғауды қамтамасыз етуге және ұйымның ақпараттық қауіпсіздігін қамтамасыз етуге жауапты ұйым қызметкері;

Вирусқа қарсы – вирустардан және басқа зиянды бағдарламалардан қорғауды қамтамасыз ететін арнайы бағдарламалық қамтамасыз ету;

Компьютерлік вирус – бұл арнайы жазылған бағдарлама (яғни, орындалатын кодтың кейбір жиынтығы), ол өзін басқа бағдарламаларға «жатқыза» (оларды «жұқтырады»), олардың көшірмелерін жасай және олардың файлдарына, компьютердің жүйелік аймақтарына және т.б. ене, сонымен қатар компьютерде әр түрлі қажетсіз әрекеттерді орындай алады;

Зиянды бағдарламалық қамтамасыз ету – бұл ақпаратқа рұқсатсыз қол жеткізуге және/немесе ұйымға және/немесе ДК пайдаланушысына өзге де зиян (залал) келтіру мақсатында арналған кез келген бағдарламалық қамтамасыз ету;

Пайдаланушы – ұйымның корпоративтік есептеу желісінің жұмысына қатысатын және ұйымның ақпараттық ресурстарын пайдаланатын тұлға.

ДК – дербес компьютер.

2. Жалпы қағидалар

1. Осы қағидалар ұйымның корпоративтік есептеу желісінің ақпараттық ресурстарын компьютерлік вирустар мен зиянды бағдарламалық қамтамасыз етудің жойқын әсерінен вирусқа қарсы қорғауды ұйымдастыруға қойылатын талаптарды айқындайды; ұйым қызметкерлерінің – ұйымның корпоративтік есептеу желісінің ақпараттық ресурстарына қосылған дербес компьютерлерді пайдаланушылар, ақпараттық қауіпсіздік жөніндегі маманның жауапкершілігін белгілейді.

2. Вирусқа қарсы қорғаныстың жұмыс қабілеттілігі, тиімділігі, оны ұйымдастыруға қойылатын талаптардың орындалуын жүйелік әкімші қамтамасыз етеді.

3. Вирусқа қарсы құралдарды орнату және жаңарту

3. Вирусқа қарсы бағдарламалар:

1) ақпараттық ресурстарды вирустық инфекциялардан қорғау;

2) вирус жұқтырған файлдарды анықтау және қалпына келтіру;

3) серверлерді, әр түрлі сервистерді, пайдаланылатын тапсырмалар мен жүйелерді жаңартып отыру үшін қажет.

4. Ұйымда пайдалануға тек дербес сатып алынған лицензияланған вирусқа қарсы құралдар ғана жіберіледі.

5. Телекоммуникациялық арналар арқылы алынатын және берілетін кез келген ақпарат, сондай-ақ алынбалы жеткізгіштердегі ақпарат міндетті вирусқа қарсы бақылауға жатады.

6. Вирусқа қарсы бағдарламаларды жүйелік әкімші ұйымның барлық дербес компьютерлері мен корпоративтік есептеу желісінің серверлеріне орнатады.

7. Вирусқа қарсы құралдарды баптау мыналарды қамтамасыз етуі тиіс:

1) компьютерді қайта іске қосқан сайын (серверлер үшін – қайта іске қосқан кезде) вирусқа қарсы мониторды автоматты түрде іске қосу;

2) күннің белгілі бір уақытында компьютерде орнатылған жергілікті дискілерді толық вирусқа қарсы тексеру (сканерлеу);

3) күннің белгілі бір уақытында вирусқа қарсы базаларды жаңарту;

4) вирус жұқтырған файл вирустарын емдеу немесе емдеу мүмкін болмаған жағдайда жою;

5) web-беттерді зиянкес кодқа тексеру;

6) электрондық пошта тіркемелерін және жалпыға қолжетімді желілерден алынған файлдарды вирустардың болуын тексеру.

4. Вирусқа қарсы бақылау жүргізу тәртібі

8. Компьютерлер мен жергілікті есептеу желісін жүйелік және қолданбалы қамтамасыз етуді орнату (өзгерту) тек жүйелік әкімшінің қатысуымен жүзеге асырылуы тиіс.

9. Компьютерге орнатылатын (өзгертілетін) бағдарламалық қамтамасыз ету компьютерлік вирустардың жоқтығына тексерілуі керек. Компьютердің бағдарламалық қамтамасыз ету орнатқаннан (өзгерткеннен) кейін бірден вирусқа қарсы тексеру жүргізілуі керек.

10. Компьютерлерде (ЖЕЖ серверлерінде) вирусқа қарсы бақылау құралдарын орнатуды, баптауды, конфигурациялауды, әкімшілендіруді нақты вирусқа қарсы құралдарды қолдану жөніндегі нұсқаулықтарға сәйкес жүйелік әкімші жүзеге асырады.

11. Телекоммуникациялық арналар арқылы алынатын және берілетін кез келген ақпарат (кез келген форматтағы мәтіндік файлдар, деректер файлдары, орындалатын файлдар), сондай-ақ бөгде адамдар мен ұйымдардан алынатын

алынбалы тасығыштардан (магниттік дискілер, CD-ROM, флэш-дискілер және т.б.) ақпарат міндетті вирусқа қарсы бақылауға жатады

12.Алынбалы тасығыштардағы ақпаратты бақылау оны қолданар алдында жүргізіледі

13.Ұйымда ДК-де жұмыс істеуге уақытша жіберілген тұлғаларға тиесілі алынбалы тасығыштарға (флэш-карталар, ықшам-дискілер) ерекше назар аудару қажет (уақытша алмастыратын студент-практиканттар және т.б.). Бұл адамдардың жұмысы, әсіресе егер жұмыс жергілікті есептеу желісінің ресурстарын пайдалану арқылы жүзеге асырылса, ұйым қызметкерлерінің тікелей бақылауымен жүргізілуі керек.

14.Пайдаланушыға өзінің дербес компьютерінде:

1) вирусқа қарсы қосымшалардың баптаулары мен конфигурациясын өзгертуге;

2) кез келген вирусқар қарсы бағдарламаларды жоюға немесе қосуға;

3) вирусқар қарсы бағдарламаның дербес компьютерінде орнатылған алынбалы құралдармен алдын ала тексерусіз жұмыс істеуге;

4) электрондық пошта арқылы келген белгісіз қосымшаларды іске қосуға тыйым салынады.

15.Пайдаланушы мыналарға міндетті:

1) күн сайын жұмыс басында компьютерді жүктеу кезінде резиденттік (компьютердің жедел жадында орналасқан) вирусқа қарсы монитордың болуына көз жеткізу (міндеттер тақтасының оң жағында вирусқа қарсы қорғаныс бағдарламасының логотипі және оның үстінде осы бағдарламаның қалқымалы атауы бар белгіше болуы керек) және ол болмаған жағдайда бұл туралы жүйелік әкімшіге хабарлау.

2) ұйымның корпоративтік есептеу желісінде вирустың болуы туралы ақпараттық технологиялар қызметінен хабарлама алған кезде, сондай-ақ компьютерлік вирустың болуына күдік туындаған кезде өзінің дербес компьютерінің жергілікті дискілерін жоспардан тыс вирусқа қарсы тексеруді өз бетінше іске қосу (бағдарламалардың үлгілік емес жұмысы, графикалық және дыбыстық эффектілердің пайда болуы, деректердің бұрмалануы, файлдардың жоғалуы, жүйелік қателер туралы хабарламалардың жиі пайда болуы және т.б.);

3) қолданылатын вирусқа қарсы құралдармен емделмейтін жаңа вирус анықталған жағдайда, бұл туралы жүйелік әкімшіге дереу хабарлау.

16. Жүйелік әкімшінің міндеттері:

1) дербес компьютерлер мен серверлерде вирусқа қарсы бағдарламаларды орнату және пайдаланушыларға жүргізілген баптаулар бойынша нұсқау беру;

2) вирустардың болуына серверлер мен корпоративтік желінің жай-күйін бақылау;

3) барлық пайдаланушыларға вирустардың корпоративтік желісіне енуі туралы ескерту және вирусқа қарсы қорғау шараларын жүргізу бойынша нұсқаулар жіберу.

17.Вирусқа қарсы қорғауға жауапты жүйелік әкімші:

1) вирусқа қарсы базаларды күнделікті жаңартудың автоматты мониторингін қамтамасыз етуге;

3) аптасына кемінде бір рет вирусқа қарсы шлюздің жұмысына талдау жүргізуге;

4) вирусқа қарсы бағдарлама модульдерінің жұмыс кестесі мен тәртібін жасауға;

5) ұйымның корпоративтік желісіндегі вирусқа қарсы қорғаудың жай-күйін, сондай-ақ пайдаланушылардың осы қағидалардың талаптарын орындауын бақылауға;

6) ақпараттық қауіпсіздік жөніндегі маманға корпоративтік желі вирусын жұқтыру фактісі, вирус жұқтырған файлдың (хабарламаның) болжамды көзі, файлдағы (хабарламадағы) ақпараттың сипаты және орындалатын вирусқа қарсы іс-шаралар туралы дереу хабарлауға міндетті.

18. Күн сайын жұмыс басында компьютерді жүктеу кезінде (ЖЕЖ серверлері үшін – қайта іске қосу кезінде) автоматты режимде компьютердің жүктеу файлдарын вирусқа қарсы бақылау жүргізілуі керек.

19. Телекоммуникациялық арналар арқылы алынатын және берілетін кез келген ақпарат (кез келген форматтағы мәтіндік файлдар, деректер файлдары, орындалатын файлдар), сондай-ақ алынбалы (шығарылатын) тасымалдағыштардағы ақпарат міндетті вирусқа қарсы бақылауға жатады. Кіріс ақпаратты архивтен шығару және бақылау оны қабылдағаннан кейін немесе операциялық жүйе компьютердің жедел жадына «таза» (вирустармен ластанбаған) және жүйелік дискіні жазудан қорғалған – кез келген басқа компьютерде бастапқы жүктелген жағдайда жүргізілуі керек. Бақылау тиімділігінің ұқсас деңгейін қамтамасыз ететін кіріс ақпаратты вирусқа қарсы бақылаудың басқа әдісін қолдануға болады. Шығыс ақпаратты бақылау архивтеу және жөнелту (алынбалы тасығышқа жазу) алдында тікелей жүргізілуі тиіс.

20. Электрондық архивке орналастырылған файлдар міндетті түрде вирусқа қарсы бақылаудан өтуі тиіс.

21. Жүйелік әкімші ұйымдағы вирусқа қарсы базаларды жаңарту үшін аптасына кемінде бір рет вирусқа қарсы базалары бар репозиторийлерді ұсынуға міндетті.

22. Компьютерлік вирустармен жұқтырылған файлдарды вирусқа қарсы тексеру жүргізу кезінде жүйелік әкімші:

- жұмысты тоқтата тұруға;
- вирус жұққан ДК жергілікті желіден ажыратуға;
- вирус жұқтырған файлдарды анықтау фактісі туралы дереу хабарлауға;
- вирус жұқтырған файлдардың иесімен бірге оларды әрі қарай пайдалану қажеттілігіне талдау жасауға;
- вирус жұққан файлдарды емдеуге немесе жоюға;
- қолданылатын вирусқа қарсы құралдармен емделмейтін жаңа вирус анықталған жағдайда вирус жұқтырған файлды вирусқа қарсы БҚ өндірушісінің веб-сайтына жіберуге, вирус жұқтырған файлдарды табу фактісі бойынша вирус жұқтырған файлдың болжамды көзін (жіберуші, иесі және т.б.), вирус жұқтырған файл түрін, файлдағы ақпараттың сипатын, вирус түрін және орындалған вирусқа қарсы әрекеттерді көрсетумен қызметтік жазба жасауға міндетті.

23. Ұйымда вирусқа қарсы бақылауды ұйымдастыру үшін жауапкершілік осы қағидалардың талаптарына сәйкес жүйелік әкімшіге жүктеледі.

24. Бөлімшелерде вирусқа қарсы бақылау іс-шараларын жүргізу және қағидалардың талаптарын сақтау үшін жауапкершілік жүйелік әкімшіге жүктеледі.

5. Қағидалардың сақталуын бақылау

25. Осы қағидалардың сақталуын бақылауды ақпараттық қауіпсіздік жөніндегі маман жүзеге асырады.

26. Осы қағидалардың нормаларын бұзғаны үшін ұйымның қызметкерлеріне ақпараттық қауіпсіздік жөніндегі маманның ұсынуы бойынша тәртіптік жаза қолданылуы мүмкін.

6. Тарату

Осы қағидалармен ұйымның барлық қызметкерлері қол қоя отырып танысады (бұдан әрі - танысу парағы).

ТАНЫСУ ПАРАҒЫ

№	Тегі, аты, әкесінің аты	Лауазымы	Жеке қолы	Күні
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				