“Астана медицина университеті” АҚ
«Биостатистика курсымен информатика және математика» кафедрасы

СӨЖ - №1

ТАҚЫРЫБЫ: Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы реттеуші құқықтық қатынастар заңнамасы

Орындаған: Құдайбергенова М.О.
Қансбек Н.Ж.
Шокеманов Е.Е.
Мамандығы: Жалпы медицина
Тобы: 104 – ЖМ
Тексерген: Жунисова У.М.

Астана 2017 жыл

МАЗМҰНЫ:

КІРІСПЕ

Соңғы бірнеше онжылдықтар ішінде ақпараттық қауіпсіздік жөніндегі талаптар елеулі өзгерістерге ұшырады.

Ақпарат тасымалданатын байланыс арналары көбінесе қорғалмаған болып келеді және осы арнаға қатынас құру құқығы бар кез келген адам хабарларды қолға түсіре алады. Сондықтан тораптарда ақпаратқа айлакерлер жағынан шабуыл жасау мүмкіндігі зор.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК

Ақпараттық қауіпсіздік — мемкелеттік ақпараттық ресурстардың, сондай-ақ ақпарат саласында жеке адамның құқықтары мен қоғам мүдделері қорғалуының жай-күйі.

Ақпаратты қорғау — ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК РЕЖИМІН ҚАЛЫПТАСТЫРУ ШАРАЛАРЫ

- Заңнамалық
- Ұйымдастырушылық
- Программалық
- техникалық

Ақпараттық қауіпсіздіктің 3 жайы:

қол жеткізерлік (оңтайлық)

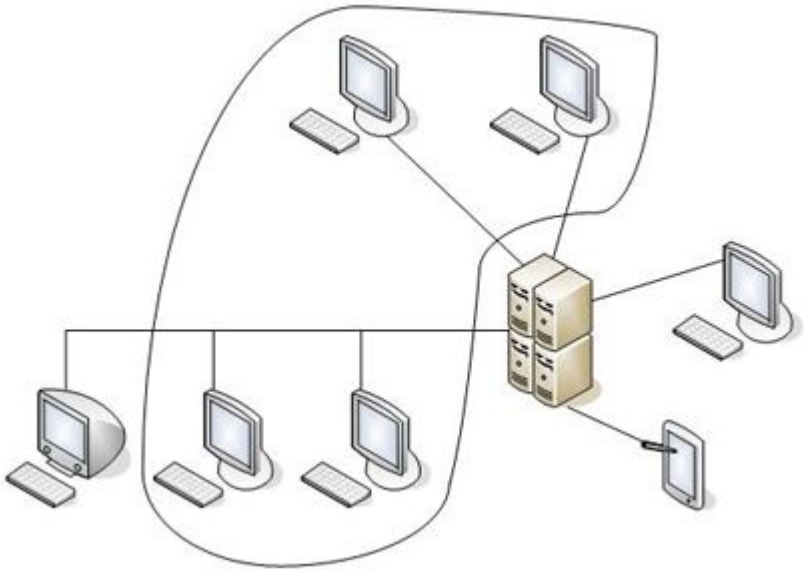
тұтастық

жасырындылық

Қол жетерлік (оңтайлық) - саналы уақыт ішінде керекті ақпараттық қызмет алуға болатын мүмкіндік.

Тұтастық - ақпараттың бұзудан және заңсыз өзгертуден қорғанылуы.

Жасырындылық - заңсыз қол жеткізуден немесе оқудан қорғау.



Қауіпсіз жүйе - белгілі бір тұлғалар немесе олардың атынан әрекет жасайтын үрдістер ғана ақпаратты оқу, жазу, құрастыру және жою құқығына ие бола алатындай етіп ақпаратқа қол жеткізуді тиісті құралдар арқылы басқаратын жүйе.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

Қауіпсіздік саясаты - мекеменің ақпаратты қалайша өңдейтінін, қорғайтынын және тарататынын анықтайтын заңдар, ережелер және тәртіп нормаларының жиыны.

Қауіпсіздік саясатының негізгі элементтері:

- қатынас құруды ерікті басқару
- объектілерді қайтадан пайдаланудың қауіпсіздігі
- қатынас құруды мәжбүрлі басқару
- қауіпсіздік таңбасы

Кепілдік - жүйенің жүзеге асырылуына көрсетілетін сенім өлшемі.

Объектінің ақпараттық қауіпсіздігін қамтамасыз етуге арналған жұмыстар кезеңі:

- 1
  - **Даяр-лық кезеңі**
- 2
  - **Ақпарат-тық қорларды түгендеу**
- 3
  - **Қатерді талдау**
- 4
  - **Қорғаныш жоспарын жүзеге асыру**

Ақпараттық қауіпсіздікке қатысты түсініктер және олардың арақатынастары

- ***Осалдық***–жүйе ішіндегі шабуыл жасауға қолайлы, шабуылға төзімсіз жер.
- ***Тәуекел*** –нақты осалдықты пайдаланып нақты шабуыл жасалады деген ықтималдық. Осының бәрін ескере келе, әрбір мекеме өзінің қаншалықты тәуекелде екенін шешу керек. Бұл шешім мекемемен қабылданған қауіпсіздік саясаты ішінде орын табу қажет.
- ***Қауіпсіздік саясаты*** – ақпараттық құндылықтар қалай өңделетінін, қорғалатынын және мекеме ішіндегі ақпараттық жүйелер арасында таратылатынын анықтайтын ережелер, директивалар және қабілеттер; қауіпсіздік сервистерін қолдануға берілетін критерийлер жиынтығы.
- ***Шабуыл*** – Ақпараттық жүйенің қауіпсіздігін бұзатын кез-келген іс-әрекет. Басқаша айтқанда осалдықтарды қолдана отырып, қауіпсіздік саясатынының бұзылуына әкеп соғатын іс-әрекеттер немесе бір-бірімен байланысқан іс-әрекеттер тізбегі.

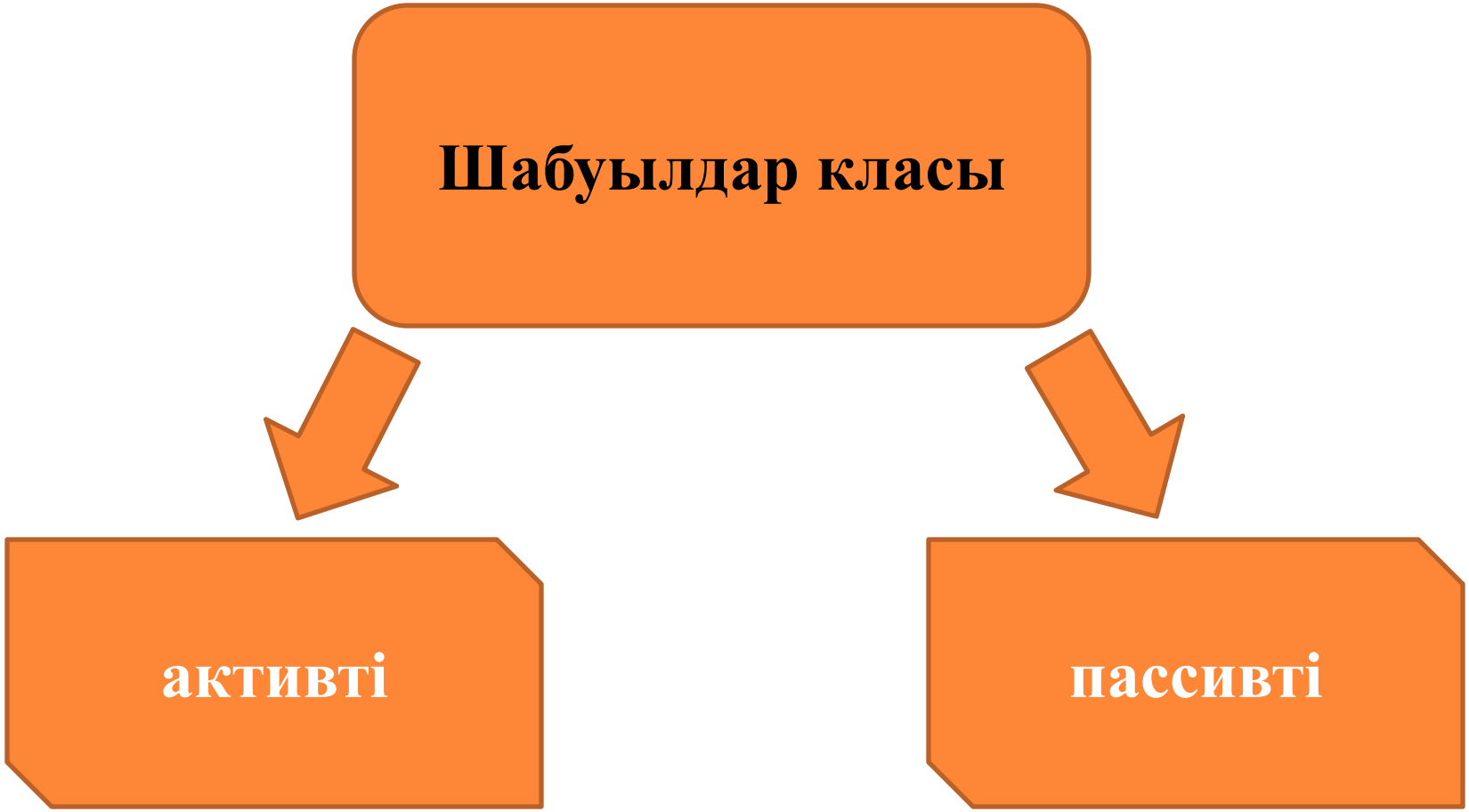
Ақпараттық құндылықтар қауіпсіздігінің негізгі бұзылушылықтары

- Ақпараттың ашылуы (жасырын-дылығының жоғалуы)
- Авторизация-сыз өзгертуі (тұтастықтың жойылуы)
- Құндылықтарға авторизация-сыз қол жетімділікті жоғалту (қол жетімділік)

Қауіпсіздік механизмі

Қауіпсіздік механизмі – шабуылды анықтайтын немесе тоқтататын бағдарламалық және/немесе аппараттық құралдар.

Желілік қауіпсіздік моделі. Желілік шабуылдар классификациясы

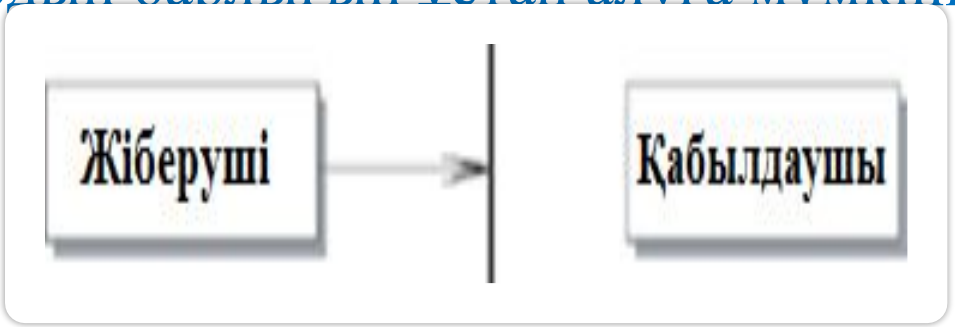


Жаудың берілген хабарламаны өзгертуге немесе ақпараттық ағын ортасына өзінің хабарламасын кіргізе алмаған кезде, мұндай шабуыл ***пассивті*** деп аталады.

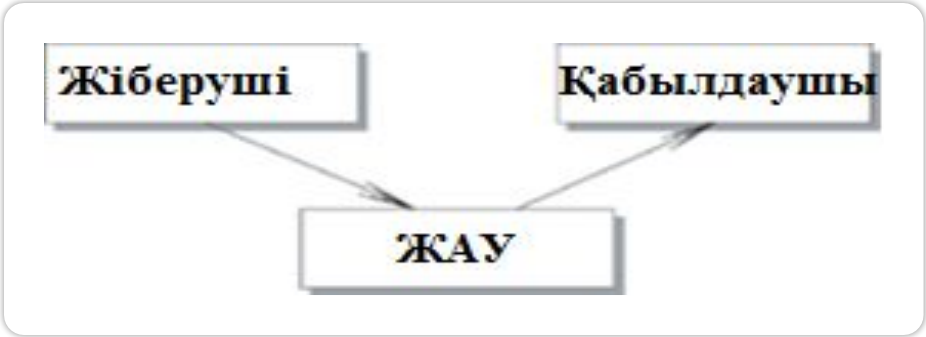
Жаудың жіберіліп отырған хабарламаны өзгертіп және де өзінің хабарламасын ортаға салуға мүмкіндігі болатын шабуыл түрін ***активті*** шабуыл деп аталады.

Активті шабуылдардың келесі түрлері бар:

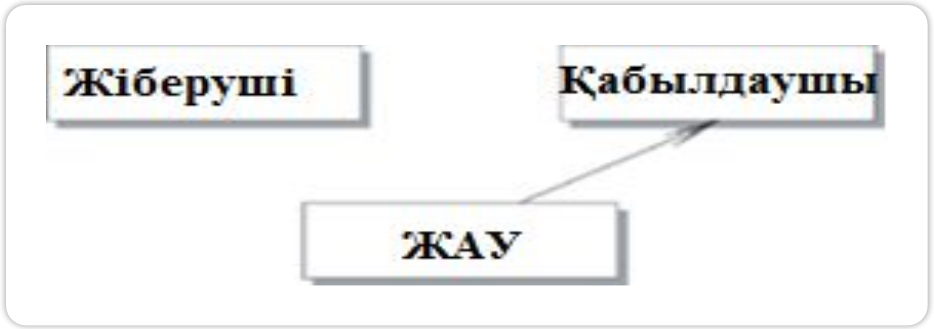
Қызмет етуден шыгып калу - **DoS-атака (Denial of Service).** Қызмет етуден шығып қалу желілік сервистердің қалыпты функционалын бұзады. Жау нақты адресатқа тиісті хабарламалардың барлығын ұстап алуға мүмкіншілігі бар.



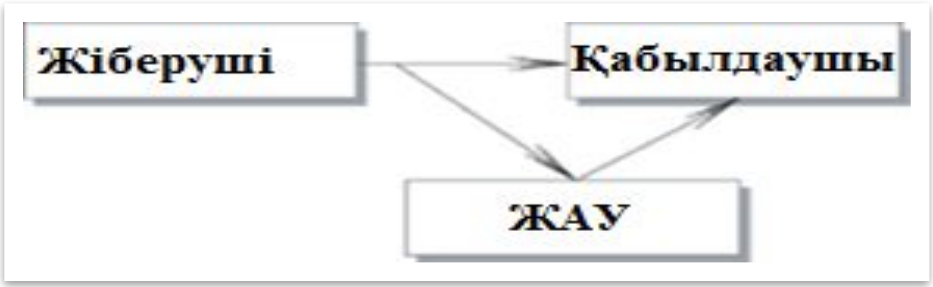
Мәліметтер ағынының модификациясы - **"man in the middle" шабуылы.** Мәліметтер ағынының модификациясы деп жіберіліп отырған хабарламаның мазмұны немесе ретінің өзгеруі.



Фальсификация (түп нұсқалықтың бұзылуы). Бір субъектінің басқа субъект ретінде көріну әрекетін айтады.



Қайта пайдалану шабуылы деп рұқсат етілмеген қол жеткізу мақсатында ары қарай жіберу ойымен мәліметтердің басып алуын replay-шабуылы деп атайды. Негізінде replay-шабуыл фальсификацияның бір түрі болып келеді, бірақ бұл рұқсат етілмеген қол жеткізуді алу үшін кең тараған шабуыл түрі болғандықтан оны жеке шабуыл түрі ретінде қарастырады.



Қауіпсіздік сервистері

Жасырындылық–жіберіліп отырған немесе сақталып отырған мәліметтерді пассивті шабуылдардан қорғау

Аутентификация– ақпараттың заңды пайдаланушыдан келуінің немесе кабылдап алушының нақты сол өзі екенінің расталуы

Тұтастық - ақпарат сақталу немесе жеткізілу барысында өзгермегеніне кепілдік беретін сервис

Қабылдамаудың жоқтығы– қабылдау алушы мен жіберуші үшін де жіберу фактісінен құтыла алмаушылығы

Рұқсат алуды басқару – коммуникациялық желілер арқылы жүйелер мен бағдарламаға рұқсат алуды шектеу және басқару мүмкіндігі

Қол жетімділік –шабуылдар нәтижесінде бір немесе бірнеше сервистің қол жетімділігі төмендеуі немесе жұмыстан шығуы

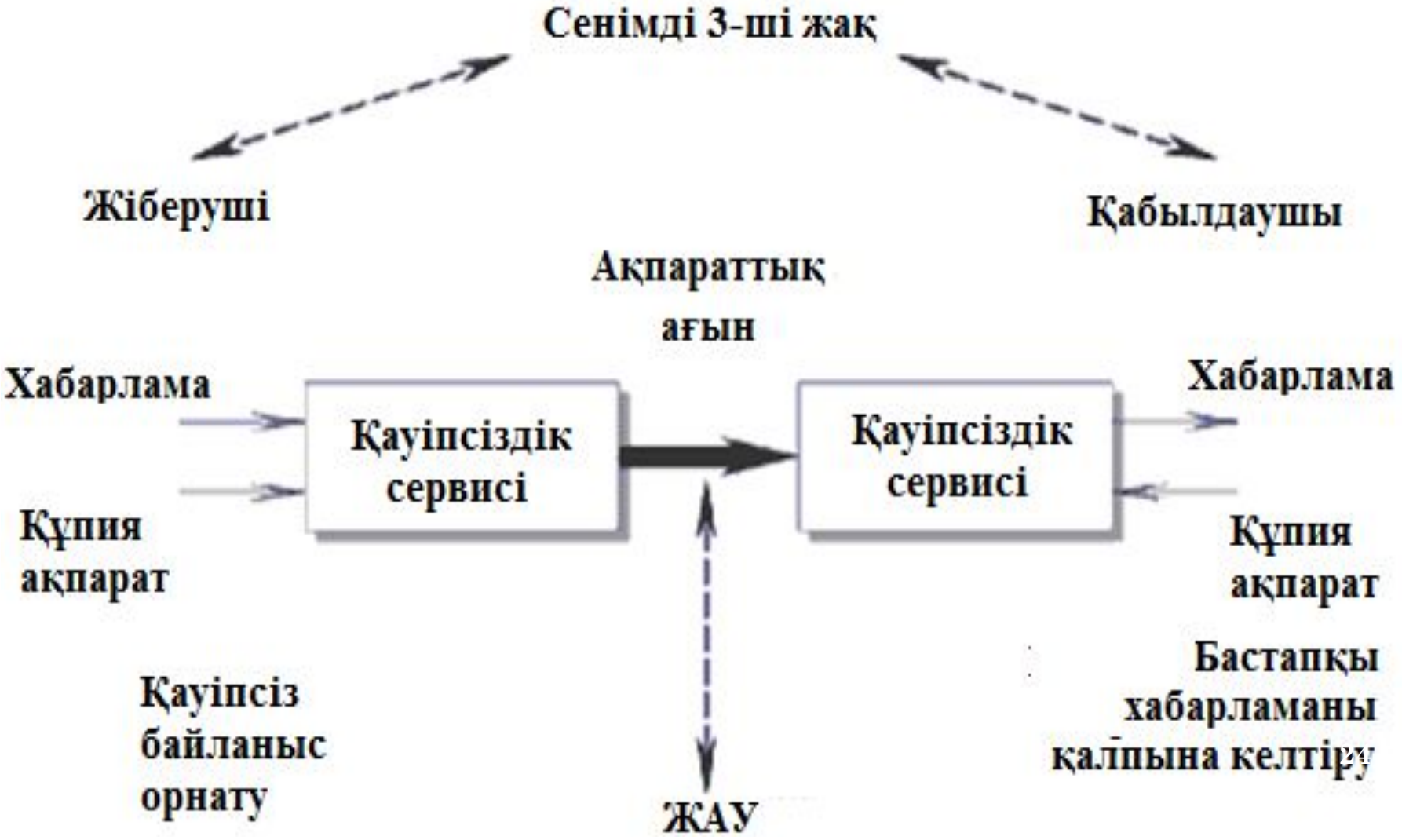
Қауіпсіздік механизмдері

Симметриялы шифрлеу алгоритмдері –шифрлеу мен дешифрлеу үшін бір ғана кілт қолданылатын және дешифлеу кілті шифрлеу кілтінен оңай алынатын шифрлеу алгоритмдері

Симметриялы емес шифрлеу алгоритмдері –шифрлеу мен дешифрлеу үшін әр-түрлі кілттер қолданылатын (ашық кілт және жабық кілт), бір кілтті біліп, екінші кілтті есептеп шығу мүмкіншілігі жоқ шифрлеу алгоритмдері

Хэш-функциялар –кіріс мәліметтер болып кез-келген ұзындықтағы хабарлама, ал шығыста –шектелген ұзындықты хабарлама шығатын функция

Желілік өзара-әрекеттесу моделі



Ақпараттық жүйе қауіпсіздігі моделі

Қазақстан Республикасының ақпараттандыру туралы заңнамасы

2-бап.

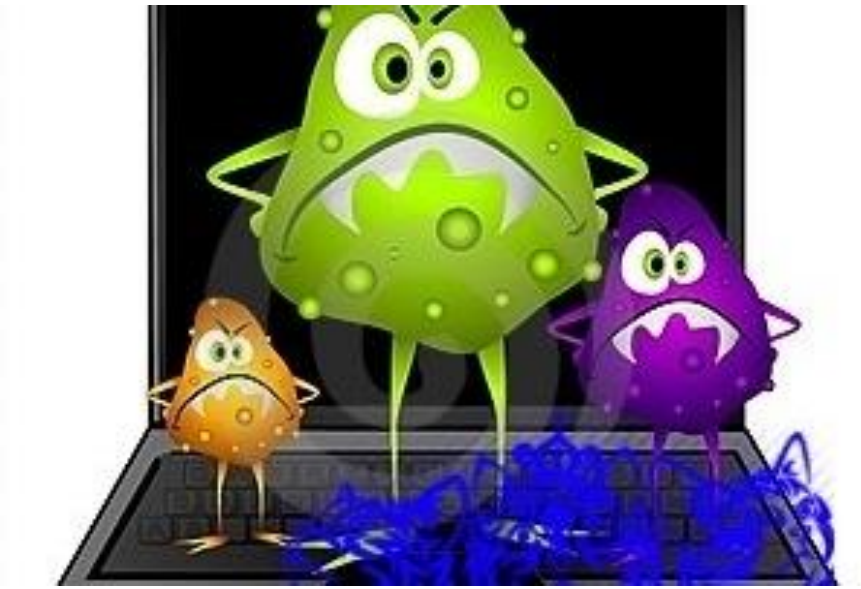
1. Қазақстан Республикасының ақпараттандыру туралы заңнамасы Қазақстан Республикасының Конституциясына негізделеді, осы Заңнан және Қазақстан Республикасының өзге де нормативтік құқықтық актілерінен тұрады.

2-тарау.
АҚПАРАТТАНДЫРУ САЛАСЫНДАҒЫ МЕМЛЕКЕТТІК РЕТТЕУ МЕН БАҚЫЛАУ

3) Қазақстан Республикасының заңнамасына сәйкес қол жеткізу шектелген электрондық ақпараттық ресурстардан басқа мемлекеттік органдардың қызметі туралы ақпаратты қамтитын электрондық ақпараттық ресурстарға еркін қол жеткізу және оларды берудің міндеттілігі (ашықтық презумпциясы);

ҚОРЫТЫНДЫ

Қорғаныштың мақсаты қатынас құруға рұқсат етілмеген арналарды ақпараттың түрін өзгертуге, ақпаратты жоғалтуға және зиян келтіруге бағытталған әсерлерден сенімді түрде сақтауды қамтамасыз ететін өзара байланысты бөгеттердің біріңғай жүйесін құру. Жүйе жұмысын қалыпты режимде көзделмеген осындай оқиғалардың біреуінің пайда болуы рұқсат етілмеген қатынас құру деп саналады.



Пайдаланылған әдебиеттер тізімі:

1. Б. Анин; «Защита компьютерной информации».
2. Қазақстан Республикасының ақпараттық қауіпсіздік тұжырымдамасы туралы
3. Қазақстан Республикасының «Ақпараттандыру туралы» Заңы 17.05.2010жыл (Әділет-Заң)

Назарларыңызға рахмет!