Тошкент ахборот технологиялари университети

3-маъруза. **Паролларни сақлаш ва паролларга бўладиган хужумлар.**

РЕЖА:

1. Паролли химоя ва уларнинг замонавий турлари.
2. Парол танлашга қўйиладиган талаблар.
3. Рақамли сертификатлар.

Парол тушунчаси

Пароллар, одатда, тизимга кириш учун калит сифатида ишлатилади, лекин улар бошқа мақсадлар учун ҳам ишлатилади:

- дискга блоклаш, маълумотларни шифрлашдаги буйруқларда;
- мос харакатлар фақатгина дастур таъминотининг қонуний эгалари ва фойдаланувчилари томонидан амалга оширилишга қатъий ишонч талаб этиладиган барча холатларда.

Ишлатиладиган парольларни қуйидаги гурухларга ажратиш мумкин:

- фойдаланувчи томонидан ўрнатиладиган пароллар;
- тизим ишлаб чиқарадиган пароллар;
- тизим ишлаб чиқарадиган мурожаат қилишнинг тасодифий кодлари;
- яримта сўз;
- таянч иборалар;
- “савол- жавоб” туридаги интерактив кетма-кетликлар;
- “қатъий пароллар”.

Парол тушунчаси

Фойдаланувчи идентификаторлари ва уларнинг пароллари ҳар бир фойдаланувчи учун ягона бўлиши керак.

Пароллар 8 та символдан кам бўлмаслиги ва машҳур номлар ёки иборалардан тузилмаслиги лозим. Ўйлаб топиладиган паролларнинг пайдо бўлишини доимий равишда махсус дастурлар ёрдамида текшириб туриш зарур. Бундай дастурларда ўйлаб топиладиган пароллар генерацияси бўйича қоидалар тўплами бўлиши лозим.

Пароллар махфий ҳолда сақланиши, яъни бошқа одамларга айтилмаслиги, дастур матнида ва ҳар - хил қоғозларда ёзилмаслиги, ҳамда ҳар 90 кунда алмаштирилиши лозим. Кўпчилик тизимлар маълум вақт ўтгач паролни мажбурий алмаштириши ва аввал фойдаланилаётган паролни йўққа чиқариши мумкин.

Фойдаланувчилар бюджети тизимга киришда 3 - та муваффақиятсиз уринишдан сўнг “қотиб қолиши”, ҳамда нотўғри киритилган пароллар номи тизим журналига киритиб қўйилиши керак.

Парол тушунчаси

Тизимга муваффақиятли кирилганда, ундан охирги марта фойдаланилган сана ва вақт акс эттирилиши лозим.

Фойдаланувчилар бюджети маълум вақт фойдаланилмагандан сўнг блокировка қилиниши шарт.

Юқори таваккалли тизимлар бир қанча кириш учун берухсат уриниб кўришлардан сўнг тизим огоҳлантириш сигналини бериши ва бу уринишларни амалга ошираётган фойдаланувчи учун сервернинг ёлғон хабарларини бериши лозим.

Чунки у тизимга қўшилган ҳолда турган вақтда, хавфсизлик администратори унинг жойлашган ўрнини аниқлашга ҳаракат қилади.

Парол турлари

Фойдаланувчи томонидан ўрнатиладиган пароллар энг кўп тарқалган гуруҳдир. Кўпчилик холатларда бундай паролни фойдаланувчининг ўзи ўрнатади, парол етарлича узун бўлиши керак. Муваффаққиятсиз паролни яратишга имкон бермайдиган усуллар бор. Масалан, тизим парол ўз ичига ёзма ва босма харфларни рақамлар билан аралашганини олишини талаб этиши мумкин; очиқдан-очиқ пароллар тизим томонидан инкор қилинади.

Тасодифий пароллар ва кодлар тизим томонидан ўрнатилади. Тизимли дастур таъминоти белгиларнинг тасодифий кетма-кетлигини тўлиқ ишлатиши мумкин. Регистр, рақам, узунликларини тасодифий танлашгача ёки ишлаб чиқарадиган жараёнларда чекланишларини ишлатиш керак.

Яримта сўз қисман фойдаланувчи, қисман тасодифий жараён томонидан яратилади. Агар фойдаланувчи енгил топиладиган парол ўйлаб топса, компьютер уни янада мураккаб тўлдиради.

“Қатъий пароллар” одатда бирорта ташқи электрон ёки механик қурилма билан бирга ишлатилади. Бу ҳолда компьютер таклифларнинг бир нечта вариантини таклиф этади, фойдаланувчи эса уларга тўғри келадиган жавобларни бериши керак. Парольларнинг бу кўриниши кўпинча бир марталик кодли тизимларда учрайди. Бир марталик кодлар ҳақиқий фойдаланувчи тизимга биринчи марта киришида ишлатилиши мумкин, кейин фойдаланувчи ўзининг паролини янада махфийроқ шахсий код билан алмаштириши керак. Тизимдан одамлар гурухи фойдаланган, лекин бунда махфийликни бузиш мумкин бўлмаган ҳолларда бир марталик кодларнинг рўйхатига мурожаат қилинади. У ёки бу фойдаланувчи вақт, сана ёки ҳафтанинг кунига мос келадиган код киритади.

Паролнинг ишончлилиги қуйидаги талабларнинг бажарилиши билан таъминланади:

- парол маълум бир узунликда бўлиши керак;
- парол ўз таркибига ҳам ёзма, ҳам босма ҳарфларни олиши керак;
- парол ўз таркибига битта ва ундан ортиқ рақамларни олиши керак;
- парол ўз таркибига битта рақамсиз ва битта алфавитсиз белгини олиши керак.

Пароллардан фойдаланишда кўплаб қонунлар ишлаб чиқилди, улардан асосийлари қуйидагилар:

- парол сифатида ҳеч қандай сўз ишлатилиши мумкин эмас;
- паролниг узунлиги 8 та белгилардан кам бўлмаслиги керак;
- бир парол турли воситаларга рухсат этиш учун ишлатилмаслиги керак;
- эски парол такроран ишлатилмаслиги керак;
- парол иложи борича тез-тез алмаштирилиши керак.

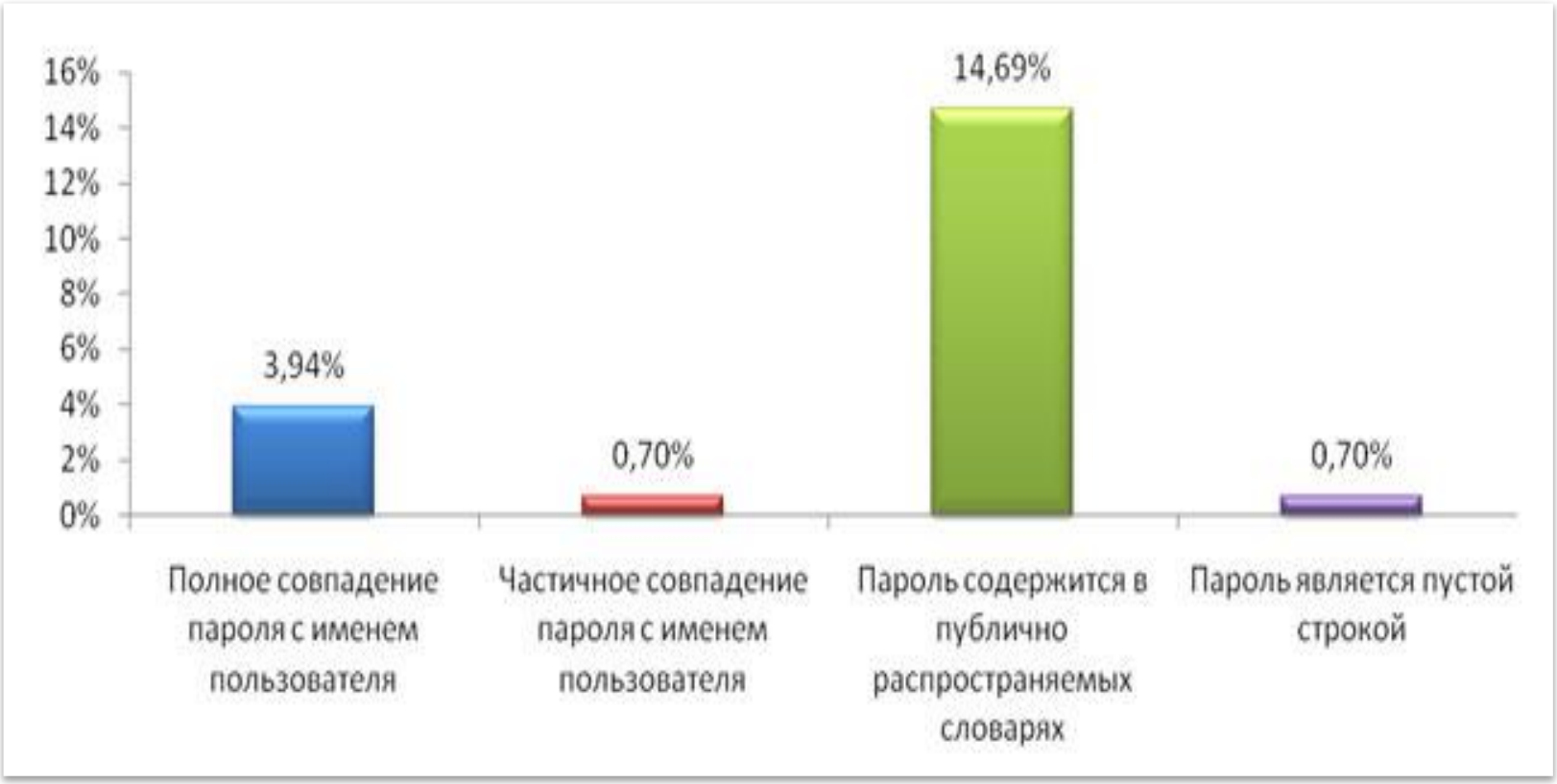
Фойдаланувчилар томонидан кўп қўлланиладиган пароллар

Пароль	Холат	Қисм, %
1234567	1	3,36%
12345678	2	1,65%
123456	3	1,02%
Бўш сатр (Пустая строка)	4	0,72%
12345	5	0,47%
7654321	6	0,31%
qweasd	7	0,27%
123	8	0,25%
qwerty	9	0,25%
123456789	10	0,23%

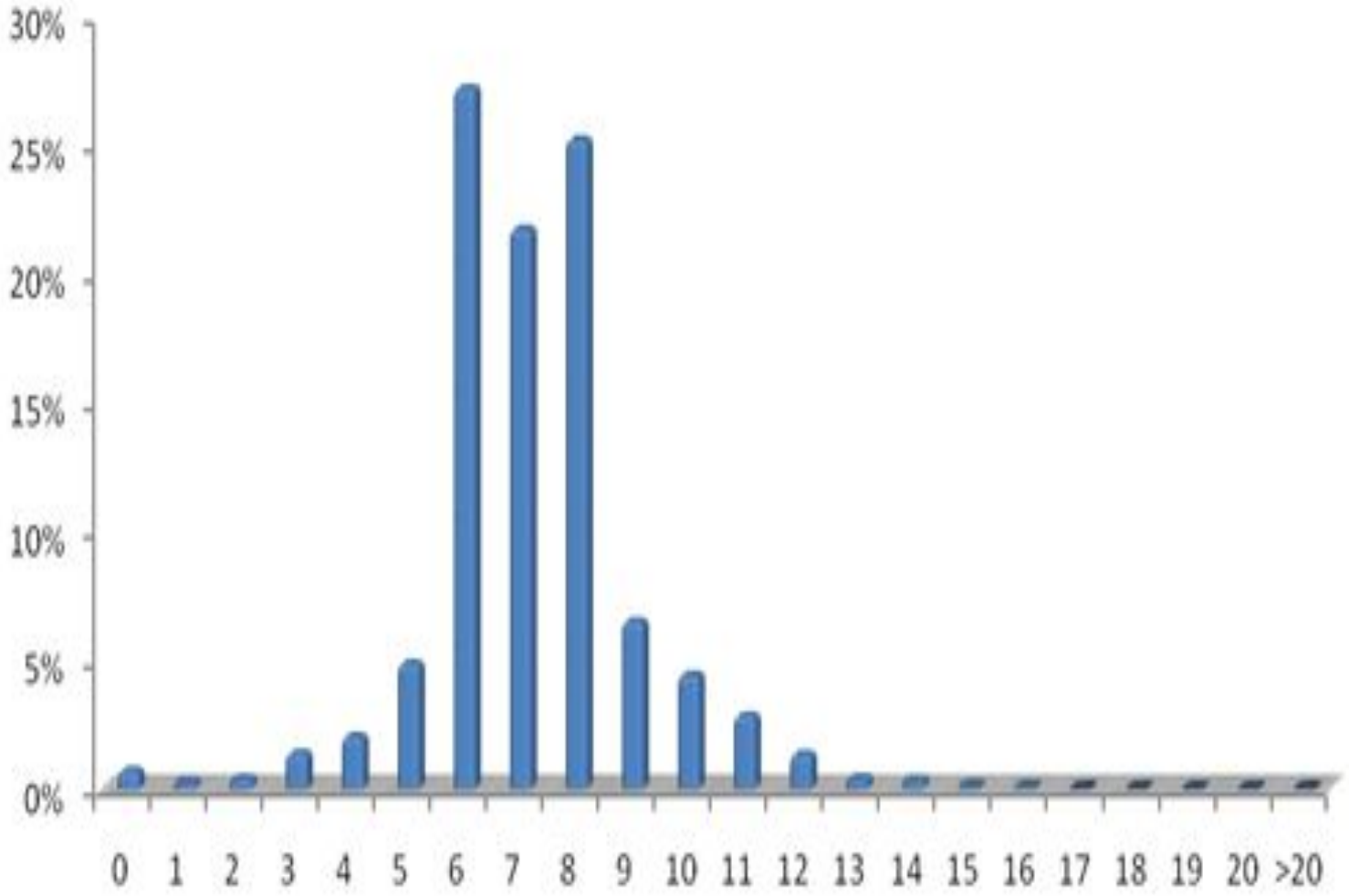
Пароллардаги қўлланиладиган белгилар тўпламларидан умумий статистика

Белгилар тўплами	Қисми, %
Фақат рақамлар (numeric)	52,73%
Кичик регистрдаги инглиз алфавити белгилари (loweralpha)	17,96%
Кичик регистрдаги инглиз алфавити белгилари ва рақамлари (loweralpha-numeric)	17,51%
Турли регистрлардаги инглиз алфавити белгилари ва рақамлари (mixalpha-numeric)	3,4%
Турли регистрлардаги инглиз алфавити белгилари (mixalpha)	1,63%
Юқори регистрдаги инглиз алфавити белгилари ва рақамлари (alpha-numeric)	1,35%
Кичик регистрдаги рус алфавити белгилари (loweralpha-rus)	1,12%

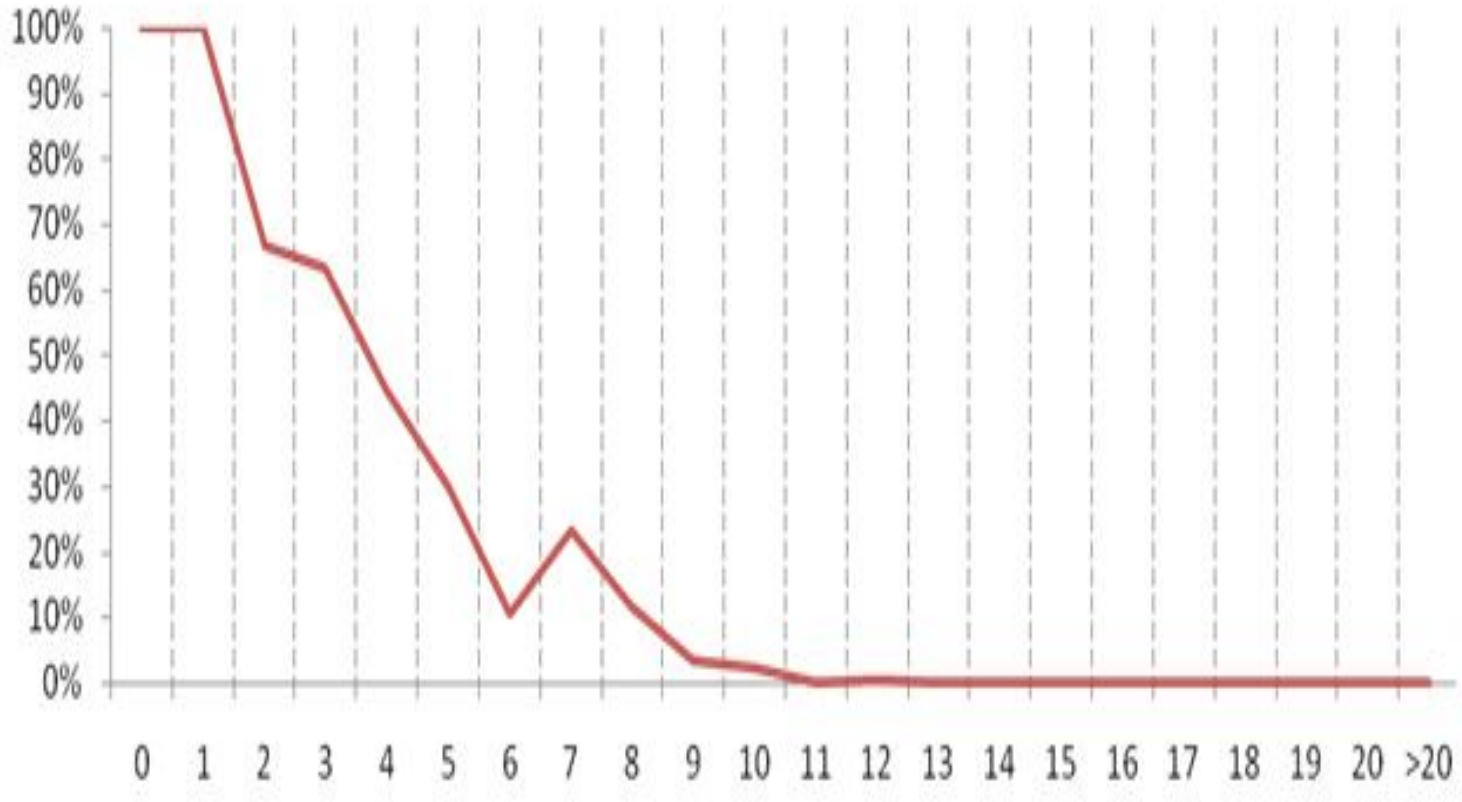
Кичик мустахкамликни пароллар бўйича умумий статистика



Фойдаланадиган паролларни узунлиги бўйича умумий статистика



Маълум узунлилик пароллар луғатидаги бузилиш эхтимоллиги



Рақамли сертификатлар

Фойдаланувчи ходимларини тасдиқлайдиган рақамли сертификатлар фойдаланувчилар сўровлари бўйича махсус ваколатли ташкилотлар бўлган сертификатлаш марказлари (***Certificate Authority*** - CA) томонидан маълум шартлар бажарилганда берилади.

Сертификатлаш марказлари сертификатни чиқариши билан сертификатда кўрсатилган очиқ калит сертификатда кўзда тутилган айнан бир субъектга тегишлилигини билдиради.

Сертификатлаш марказининг ўзига ишониш зарур ва олдиндан унинг очиқ калитини ёки ўзи имзолаган сертификатни олиши зарур.

Шуни таъкидлаш керакки, сертификатни олиш процедурасининг ўзи ҳам фойдаланувчи ҳақиқийлигини текшириш босқичини ўз ичига олади.

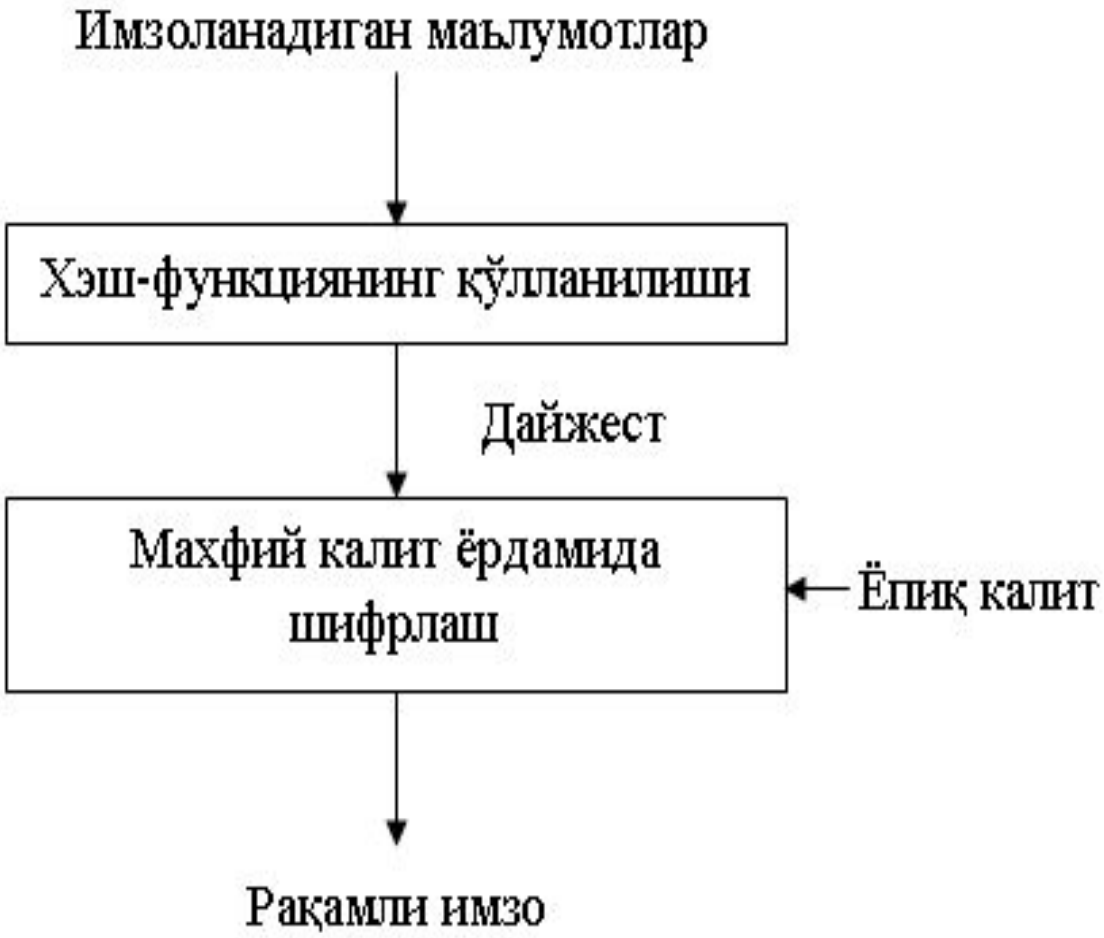
Текширувчи томон сифатида бу ерда сертификатлаш ташкилоти қатнашади. Сертификатни олиш учун мижоз CA сертификатлаш марказига унинг ходимларини тасдиқлайдиган маълумотни ва ўз очиқ калитини тақдим этиши керак. Зарур маълумотлар рўйхати олинадиган сертификат турига боғлиқ.

Сертификат қуйидаги маълумотлардан иборат бўлган шаклдан иборат:

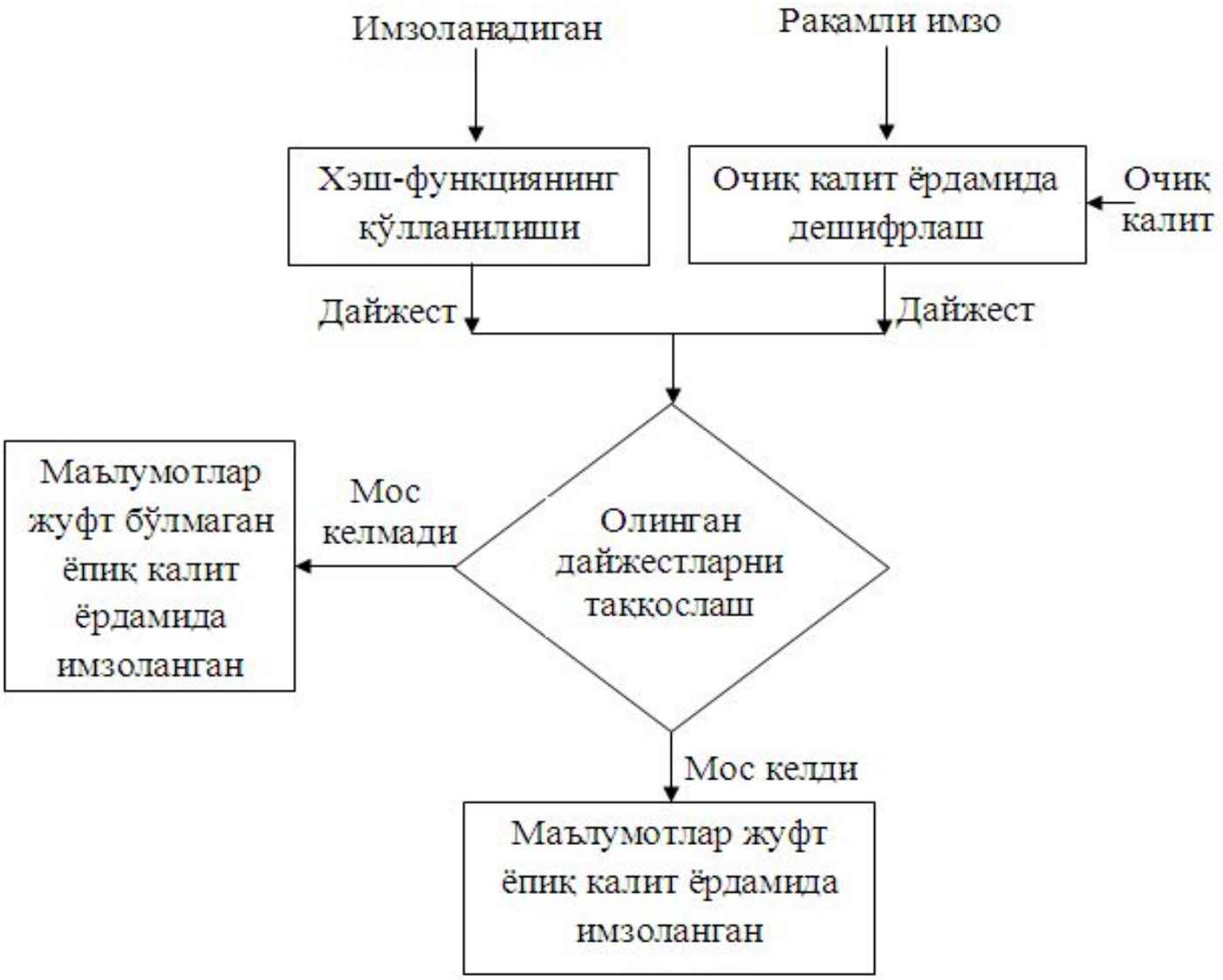
- сертификат эгасининг очиқ калити;
- сертификат эгаси ҳақидаги маълумотлар, масалан: исми-шарифи, электрон манзили, шу ходим ишлайдиган ташкилотнинг номи ва бошқалар;
- шу сертификатни берган сертификатлаштириш ташкилотининг номи;
- сертификатлаш ташкилотининг электрон имзоси бўлган сертификатдаги бу ташкилотнинг ёпиқ калит билан шифрланган маълумотлари.

Электрон имзо дастлабки маълумотларга бир томонлама ўзгартиришларни қўллаш (хэш-функция) йўли билан олинган байтлар тўплами ҳисобланади, бунинг натижасида маълум узунликдаги байтлар кетма - кетлиги олинади, кейин у сигнатурани яратадиган ходимларнинг махфий калити ёрдамида шифрланади. Ўз ёпиқ калит ёрдамида бу имзони яратган ходимлар имзо муаллифи ҳисобланади. Бу имзони фақат очиқ калит ёрдамида дешифрлаш мумкин.

Рақамли имзони яратиш алгоритми



Рақамли имзони текшириш алгоритми



Калитларни бошқариш

Калитларни бошқариш билан сертификатларни тарқатиш марказлари шуғулланади. Бундай марказга мурожаат қилган фойдаланувчи қандайдир фойдаланувчи сертификатини олиши, шунингдек, у ёки бу калит чақириб олинганганлигини текшириши мумкин.

очиқ калитлар сертификатлар билан узвий боғланган. Сертификат нафақат ходимларни тасдиқлайди, балки очиқ калитнинг тегишлилигини ҳам тасдиқлайди. Рақамли сертификат очиқ калит ва унинг эгаси ўртасидаги мувофиқликни ўрнатади ва кафолатлайди. Бу очиқ калит алмаштирилиши хавфининг олдини олади.

X.509 стандарти

X.509 стандарти орқали аниқланган сертификат энг оммавий ҳисобланади.

X.509 стандарти рақамли имзони яратишнинг турли алгоритмларидан фойдаланилишини кўзда тутади.

X.509 стандартидаги сертификатлар:

- версия ва ишлатиладиган имзони яратиш алгоритми ҳақида маълумотлар;
- идентификацион маълумотлар ва сертификатни берган ташкилот имзоси;
- сертификатнинг амал қилиш муддати;
- идентификацион маълумотлар ва унинг очиқ калитларидан иборат.

Сертификатлар орқали аутентификация қилиш бир томонлама ёки икки томонлама бўлиши мумкин.

Бир томонлама аутентификация қилишда фақат мижоз сертификати текширилади.

Икки томонлама аутентификация қилиш вақтида эса, сервер томонида мижоз сертификати, мижоз томонида сервер сертификати текширилади, бу томонларни ўзаро аутентификация қилинишини таъминлайди.

Назорат саволлари

1. Паролли химоя ва уларнинг замонавий турлари.
2. Парол танлашга қўйиладиган талаблар.
3. Рақамли сертификатлар тўғрисида тушунча беринг?
4. Сертификат нималардан ташкил топган?
5. X.509 стандартига тушунча беринг?