Ахборот хавфсизлигининг умумий тушунчалари

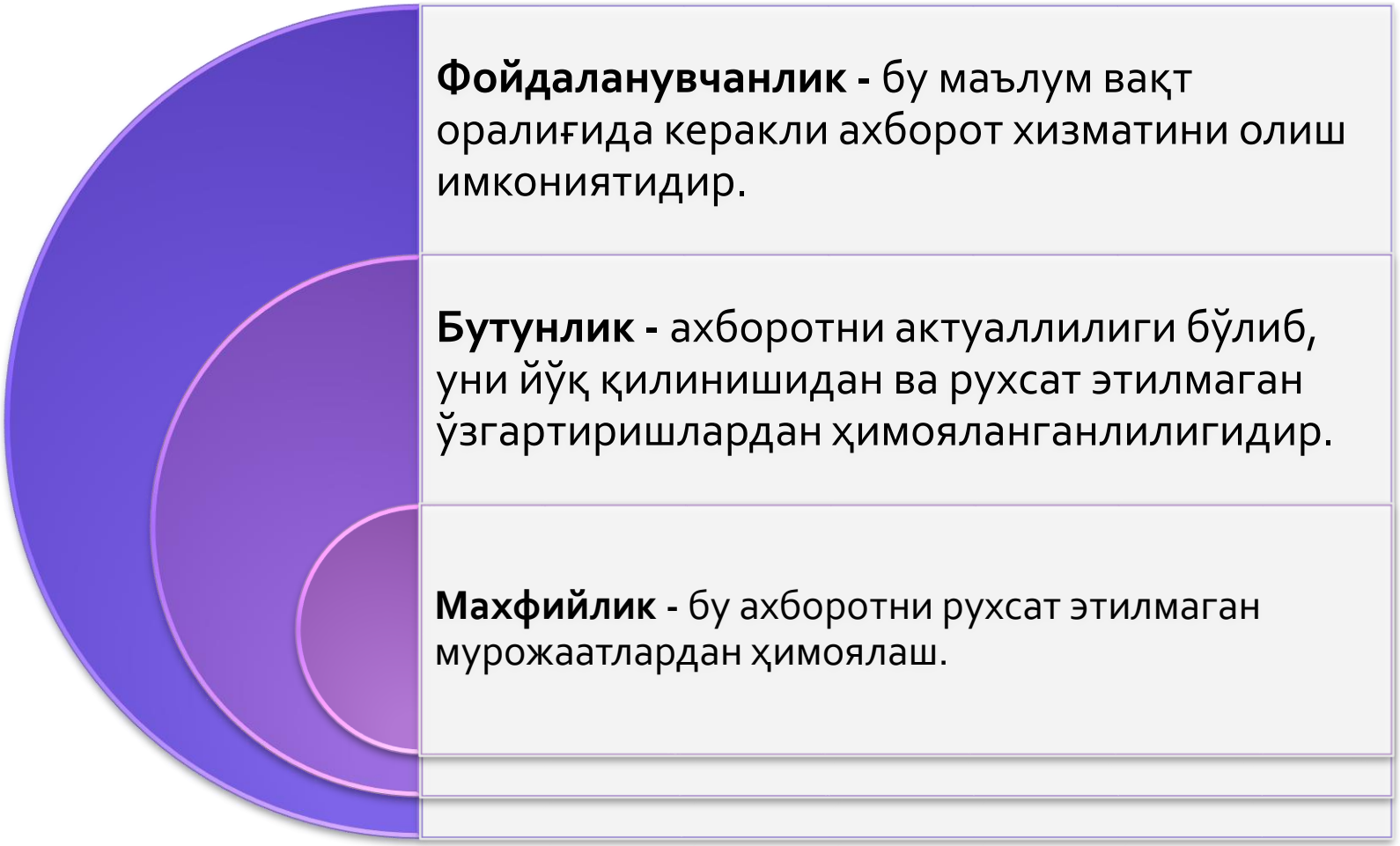
Режа:

- Ахборот хавфсизлиги тушунчаси
- Ахборотни ҳимоялашнинг асосий усуллари
- Компьютер вируслари ва антивирус ҳимоя воситалари
- Ахборот тизимларида ички ва ташқи таҳдидлар
- Ахборотларга рухсат этилмаган мурожаат

Ахборот хавфсизлиги тушунчаси

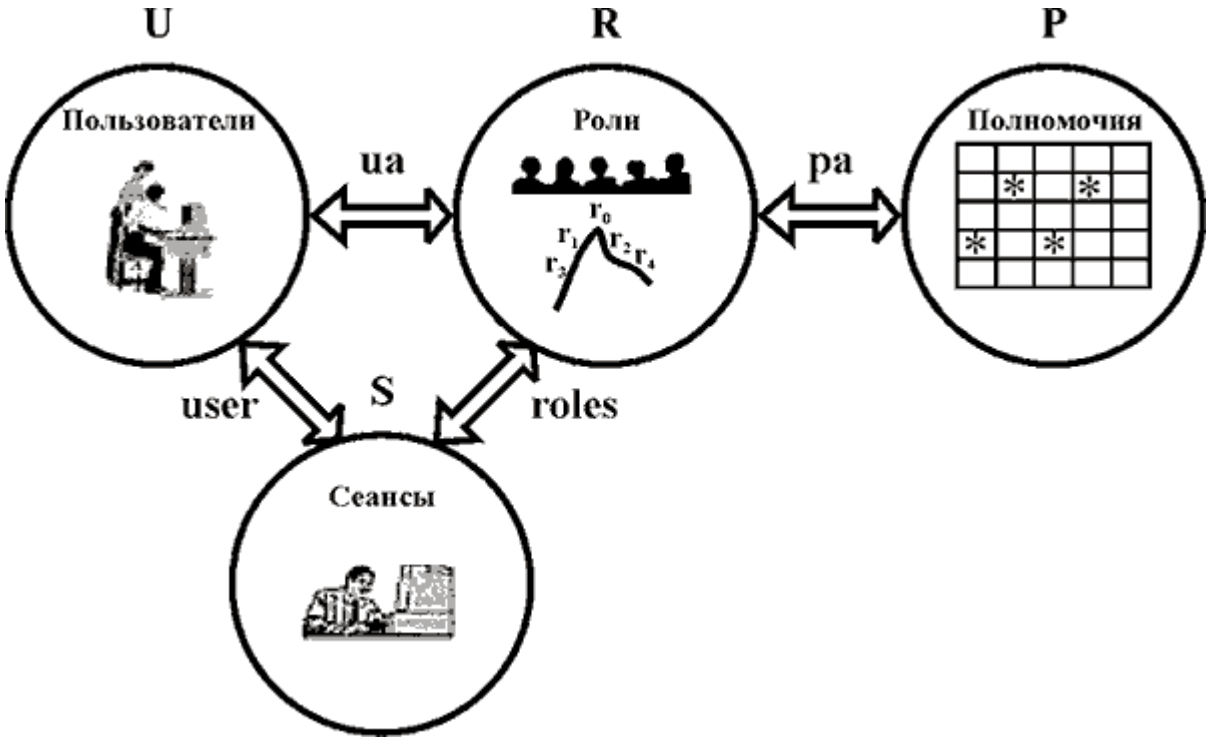
- **Ахборот хавфсизлиги (АХ)** деганда, биз тасодифий ёки олдиндан кўзланган табиий ёки сунъий характерга эга бўлган таъсирлардан, қайсики ахборот субъектларига номаъқул зиён келтирадиган, шу жумладан инфраструктурани қўллаб қувватловчи ахборот фойдаланувчиларидан ва эгаларидан ахборотни ҳимояланганлигини тушанамиз. .
- **Ахборотни ҳимоялаш** - бу ахборотни хавфсизлигини таъминлашга қаратилган комплекс чора-тадбирлар.

АХ мақсадлари



Ахборотни ҳимоялашнинг асосий усуллари

- **Рухсатларни бошқариш** — Ахборот тизимлари ва ахборот технологияларининг барча ресурсларидан фойдаланишни тартибга солиш орқали ҳимоялаш усули. Бундай усуллар, ахборотга бўлган барча рухсат этилмаган кириш имкониятларини бартараф эта олиши лозим.



Ахборотни ҳимоялашнинг асосий усуллари

Рухсатларни бошқариш қуйидаги ҳимоя функцияларини ўз ичига қамраб олади:

- фойдаланувчиларни, ходимларни ва тизим ресурсларини идентификациялаш(ҳар бир объектга шаҳсий идентификатор бериш);
- объект ёки субъектларни уларга берилган идентификатор орқали таниб олиш (ҳақиқийлигини таъминлаш);
- фойдаланиш ҳуқуқига эгалигини текшириш;
- ҳимояланган ресурсларга бўлган мурожаатларни рўйҳатга олиш;
- рухсат этилмаган киришларга уриниш ҳаракатлари бўлган вақтда сезиш (сигналли огоҳлантириш, тизимни ўчириш, тизим ишини тўҳтатиб қўйиш, сўровларга жавоб бермаслик).

Ахборотни ҳимоялашнинг асосий усуллари

- **Идентификация** субъектларга (фойдаланувчиларга, жараёнларга, маълум бир фойдаланувчи номидан ҳаракат қилувчиларга) ўзини кимлигини маълум қилиш имконини беради. **Аутентификация** орқали иккинчи томонни аслида ким эканлигини билиш имконини беради. Баъзан "аутентификация" иборасининг синоними сифатида "ҳақиқийлигини текшириш" ибораси ишлатилади.

Ахборотни ҳимоялашнинг асосий усуллари

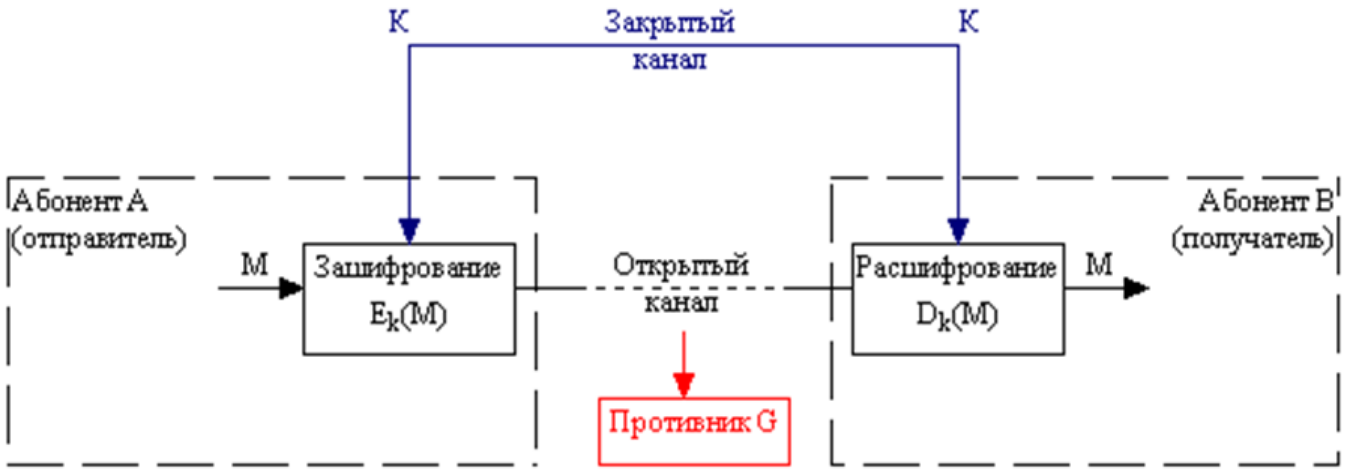
- Криптография (грекча сўзи, махфий белгилар билан ёзилган ҳат) - бу ахборотни кўзда тутилмаган фойдаланувчилардан ҳимоялаш йўлида, ахборотни ўзгартириш билан боғлиқ бўлган ғоя ва усуллар йиғиндисидир.

Ахборотни ҳимоялашнинг асосий усуллари

- Замонавий криптография тўртта катта бўлимдан иборат:

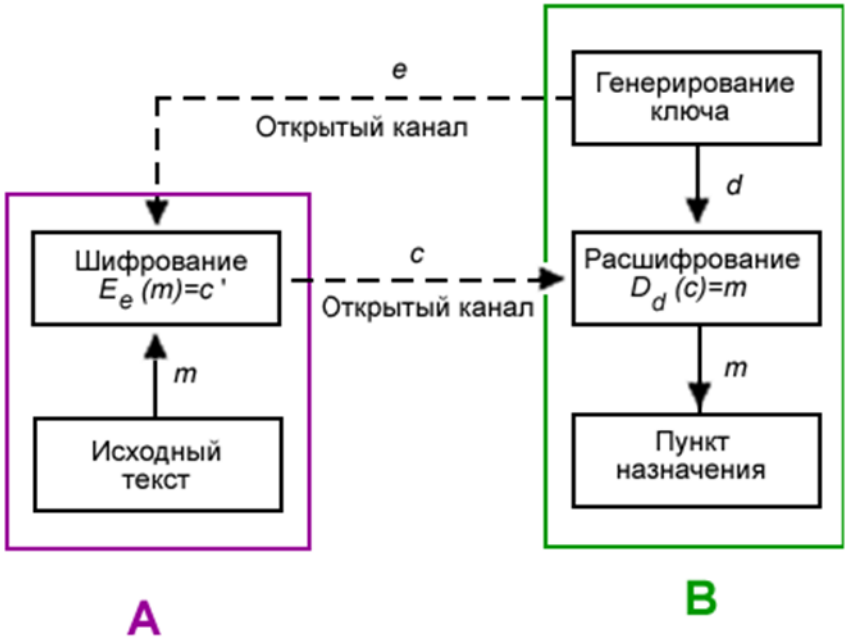
Ахборотни ҳимоялашнинг асосий усуллари

- **Симметрик криптотизимлар**, шифрлаш ва дешифрлашни битта калит орқали амалга оширувчи алгоритмларни ўз ичига олади.



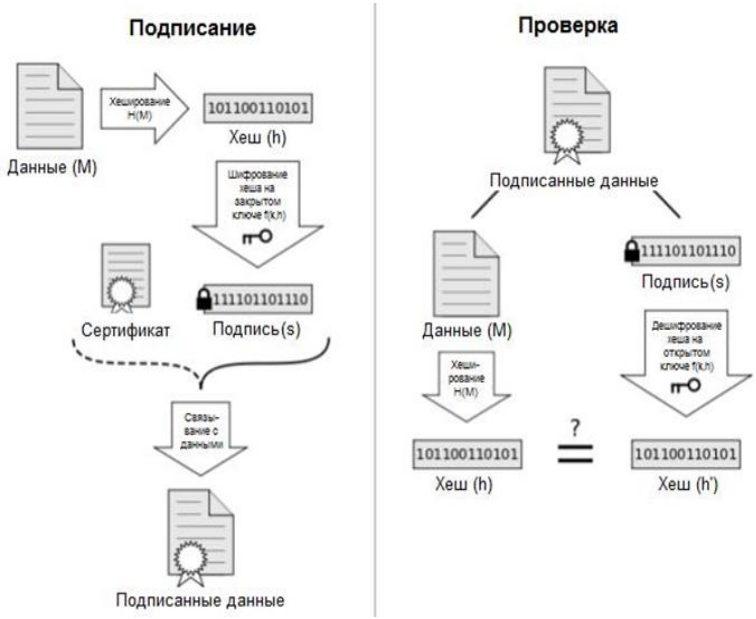
Ахборотни ҳимоялашнинг асосий усуллари

- **Очиқ калитли тизимларда** маълумотларни шифрлашда бир калит ишлатилса, дешифрлаш учун эса бошқа калит ишлатилади (шу ердан ассиметрик сўзи келиб чиқади).



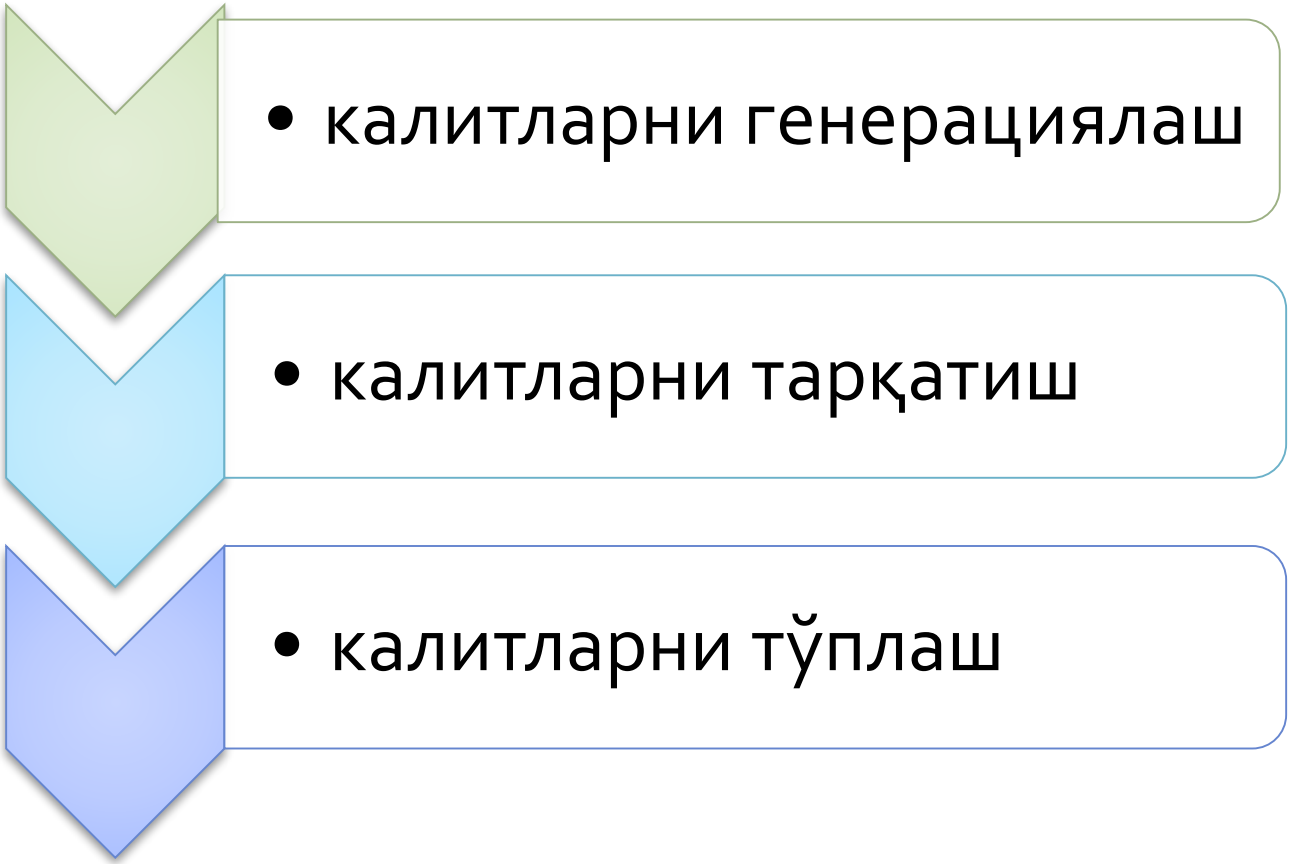
Ахборотни ҳимоялашнинг асосий усуллари

- **Электрон рақамли имзо (ЭРИ)** - электрон ҳужжатнинг реквизити бўлиб, электрон ҳужжатни қалбакисидан ҳимоялаш ва маълумот манбасини тасдиқлаш учун ишлатилади. Электрон рақамли имзо, электрон ҳужжатни криптографик ўзгартириш натижасида ҳосил бўлган символлар кетма-кетлигидан ташкил топади. ЭРИ маълумот блокига қўшилиб, маълумотни қабул қилувчига маълумот манбасини, маълумотни бутунлигини ва қалбакисидан ҳимоялаш имконини беради.



Ахборотни ҳимоялашнинг асосий усуллари

- **Калитларни бошқариш** - ахборот жараёни, ўз ичига учта элементни қамраб олади:
- :



Ахборотни ҳимоялашнинг асосий усуллари

Компьютер тизимларида аутентификация усулларидан бири – фойдаланувчи идентификаторини тизимга киритишдир, оддий халк тилида «логин» ва «парол» деган номини олган. Оддий аутентификация алгоритми қуйидагича:

- Фойдаланувчи тизимдан киришни сўров жўнатади ва шахсий идентификатор ва паролни киритади.
- Киритилган маълумотлар аутентификация серверига тушиб, эталон маълумотлар билан солиштирилади.
- Эталон маълумотлари билан бир хил бўлса, аутентификация муваффакиятли ҳисобланади, аксинча бўлса – фойдаланувчи 1 қадамга қайтарилади.

Компьютер вируслари ва антивирус ҳимоя воситалари

- **Компьютер вируси**, фойдаланувчи иштирокисиз ўзининг нусҳасини яратиш ва уларни компьютер тизими ва тармоқларининг турли объект/ресурсларига жорий қилиш имконига эга махсус ёзилган дастур ҳисобланади. Бу нусҳа остида кейинчалик тарқатиш имконини сақлаб қолади.

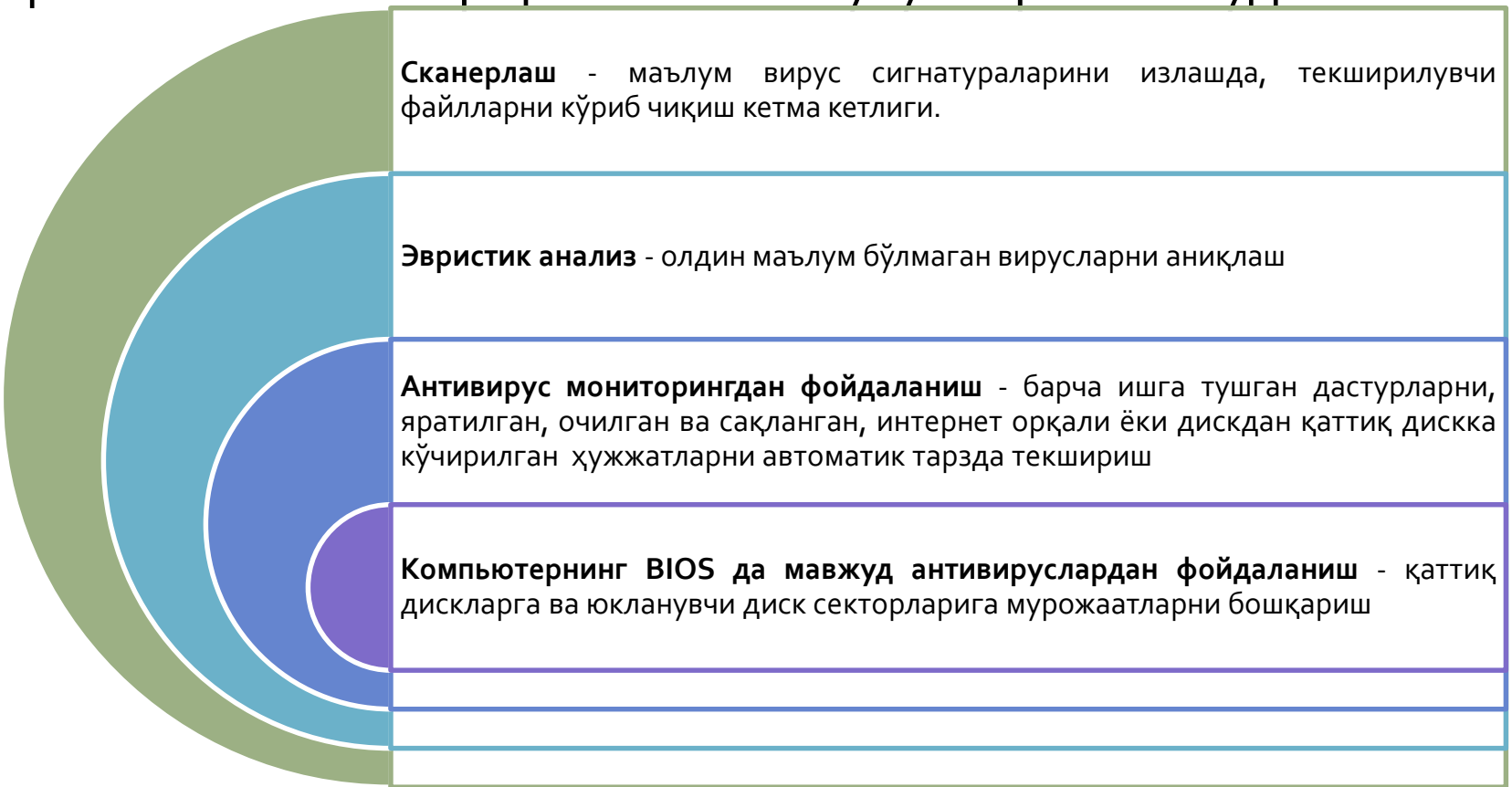
Компьютер вируслари ва антивирус ҳимоя воситалари

Вируслар класификацияси

- *вирусларнинг яшаш жойи бўйича*
- *яшаш жойини зарарлаши бўйича*
- *деструктив имкониятлари бўйича*
- *вирус алгоритмининг ўзига ҳослиги бўйича*

Компьютер вируслари ва антивирус ҳимоя воситалари

Вирусларга қарши курашишнинг асосий воситаси антивирус дастурлари бўлган ва шундай бўлиб қолмоқда, бундай антивирус дастурларининг вирусларни топиш ва ҳимоялашнинг бир қанча асосий усуллари мавжуд:



Ахборот тизимларида ички ва ташқи таҳдидлар

- **Ички таҳдидларга** ахборот хавфсизлигининг асосларини (фойдаланувчанлик, бутунлик, махфийлик) бузувчи ахборот билан боғлиқ барча амаллар киради. Шунга кўра, компаниянинг ахборот тизимини ичидан зарар етказиш бўлади.
- **Ахборот хавфсизлигининг ташқи таҳдидлар** – ахборот тизимига негатив таъсир бўлиб, унинг манбаси ташқи факторлар(табиий офатлар, кучли электромагнит нурланиш, диверсион ҳужум) ҳисобланади.

Ахборот тизимларида ички ва ташқи таҳдидлар

Ахборот технологиялар бозорида ахборот хавфсизлигини ташқи таҳдидлардан ҳимоя қилувчи дастурий таъминотнинг 4 та асосий турлари мавжуд:

антивирус дастурлари	корпоратив тармоқлар орасидаги экран	шахсий файерволлар	ҳужумларга қарши тизимлар

Компьютер тармоғига рухсат этилмаган киришлар

- **Ташкилот тармоғига рухсат этилмаган киришларнинг мақсади,** зарар етказиш (маълумотнинг йўқолиши), махфий ахборотнинг ўғирланиши ва уни ноқонуний мақсадларда ишлатишга олиб келиши мумкин.

Компьютер тармоғига рухсат этилмаган киришлар

Профессионаллар орасида рухсат этилмаган кириш усуллари қуйидагича ўзига ҳос ном олган:

- *"Очиқ жойларни топиш" усули*
- *"Шошилмаган ҳолда танлаш" усули*
- *"Компьютер абордаж" усули*
- *"Туйнук" усули*
- *"Маскарад"усули*

Эътиборингиз учун рахмат!