O‘ZBEKISTON RESPUBLIKASI
IQTISODIY TARAQQIYOT
VA KAMBAG‘ALLIKNI
QISQARTIRISH VAZIRLIGI

БТОМ-2022

BIZNES VA TADBIRKORLIK
OLIY MAKTABI

Маркетинг ва рақамли иқтисодиёт кафедраси мудири
и.ф.д., профессор, халқаро инженерлар академияси
мухбир аъзоси Кенжабаев Аман Тургунович
(atkenjabaev@mail.ru); (amankenja059@gmail.com);
Тел: +998977595931.

«Бизнес ва тадбиркорлик олий мактаби»

9-МАВЗУ: КИБЕРХАВФСИЗЛИК

Кенжабаев А.Т | *и.ф.д., профессор*

Рақамлашув ва киберхавфсизлик тушунчалари доимо ёнма-ён келади. Чунки барча тизим ва жараёнларни рақамлаштириш билан бирга, уларнинг техник жиҳатдан мукаммал ва бехато ишлашини, хавфсизлигини таъминлаш муҳим ҳисобланади. Юртимизда рақамли иқтисодиётни ривожлантиришга қанчалик эътибор қаратилаётган бўлса, киберхавфсизликни таъминлаш ҳам шунча долзарблик касб этмоқда. Ўзбекистон киберхавфсизлик глобал индексида ўзи позициясини мустаҳкамлаб бормоқда. 2017 йилда мамлакатимиз бу рейтингда 93-ўринни эгаллаган бўлса, 2018 йилда 52-ўринга кўтарилди. **«Киберхавфсизлик тўғрисида»ги Ўзбекистон Республикасининг қонуни.**Тошкент ш., 2022 йил 15 апрель,ЎРҚ-764-сон.(Қонунчилик маълумотлари миллий базаси, 16.04.2022 й., 03/22/764/0313-сон).Ушбу Қонун расмий эълон қилинган кундан эътиборан уч ой ўтгач кучга киради.

Киберхавфсизлик бўйича мутахассисларга бўлган талаб кундан кунга ортиб бормоқда.

Жорий йилнинг бошида бутун дунё бўйлаб компанияларга ушбу соҳа бўйича 3,5 миллион мутахассис ваканцияда бўлиб уларни бандлик масалалари муаммо бўлиб келмоқда.

Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан хар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.

Ахборотнинг ҳимояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатьий регламентланган динамик технологик жараёнга айтилади.

Киберхавфсизлик ҳозирда кириб келган янги тушунчалардан бири бўлиб, унга турли берилган турли таърифлар мавжуд.

Киберхавфсизлик - ҳисоблашга асосланган билим соҳаси бўлиб, бузгунчилар мавжуд бўлган шароитда амалларни кафолатлаш учун ўзида технология, инсон, ахборот ва жараённи мужассамлаштирган.

- У хавфсиз компьютер тизимларини яратиш, амалга ошириш, таҳлил қилиш ва тестлашни ўз ичига олади.
- Киберхавфсизлик таълимнинг мужассамлашган билим соҳаси бўлиб, қонуний жихатларни, сиёсатни, инсон омилини, этика ва рискларни бошқаришни ўз ичига олади.
- Тармоқ бўйича фаолият юритаётган Сшсо ташкилоти эса киберхавфсизликка қуйидагича таъриф берган: Киберхавфсизлик - тизимларни, тармоқларни ва дастурларни рақамли ҳужумлардан ҳимоялаш амалиёти.
- Ушбу киберҳужумлар одатда махфий ахборотни бошқариш, алмаштиришёки йўқ қилишни; фойдаланувчилардан пул ундиришни; ёки нормал иш фаолиятини узуб қўйишни мақсад қилади.
- Ҳозирги кунда самарали киберхавфсизлик чораларини амалга ошириш инсонларга қараганда қурилмалар сонининг кўплиги ва бузгунчилар салоҳиятини ортиши натижасида амалий томондан мураккаблашиб бормоқда.

Киберхавфсизлик кимларга керак

- **Конфиденциаллик**

— ТИЗИМ маълумоти ва ахборотига фақат ваколатга эга субъектлар фойдаланиши мумкинлигини таъминловчи қоидалар.

— Мазкур қоидалар ахборотни фақат қонуний фойдаланувчилар томонидан “ЎҚИЛИШИНИ” таъминлайди.

- **Яхлитлик (бутунлик)**

— Маълумотни аниқ ва ИШОНЧЛИ эканлигига ИШОНЧ ҲОСИЛ ҚИЛИШ.

— ЯЪНИ, ахборотни рухсат этилмаган ўзгартиришдан ёки “ЁЗИШ” дан ҳимоялаш.

- **Фойдаланувчанлик**

— Маълумот, ахборот ва тизимдан фойдаланишнинг мумкинлиги. яъни, рухсат этилмаган “бажариш” дан ҳимоялаш.

- “Маьлумотлар хавфсизлиги” билим соҳаси маьлумотларни еақлашда, қайта ишлашда ва узатишда ҳимояни таъминлашни мақсад қилади.
- Мазкур билим соҳаси ҳимояни тўлиқ амалга отттириттт учун математик ва аналитик алгоритмлардан фойдаланишни талаб этади.
- “Даетурий таьминотлар хавфсизлиги” билим соҳаси фойдаланилаётган тизим ёки ахборот хавфсизлигини таъминловчи даетурий таьминотларни ишлаб чиқиш ва фойдаланиш жараёнига эътибор қаратади.
- “Ташкил этувчилар хавфеизлиги” билим соҳаси катта тизимларда интеграллашган ташкил этувчиларни лойиҳалаш, еотиб олиш, теетлаш, анализ қилиш ва техник хизмат кўрсатишга эътибор қаратади.
- Тизим хавфсизлиги ташкил этувчилар хавфсизлигидан фарқ қилади.
- Ташкил этувчилар хавфсизлиги улар қандай лойиҳаланганлиги, яратилганлиги, сотиб олинганлиги, бошқа таркибий қисмларга уланганлиги, қандай ишлатилганлиги ва сақланганлигига боғлиқ.
- “Алоқа хавфсизлиги” билим соҳаси ташкил этувчилар ўртасидаги алоқани ҳимоялашга этибор қаратиб, ўзида физик ва мантиқий уланишни бирлаштиради.

• “Тизим хавфсизлиги” билим соҳаси ташкил этувчилар, уланишлар ва даетурий таьминотдан иборат бўлган тизим хавфсизлигининг жиҳатларига эътибор қаратади.

— Тизим хавфсизлигини тушуниш учун нафақат, унинг таркибий қисмлари ва уланишини тушунишни, балки бутунликни ҳисобга олишни талаб қилади.

• “Инсон хавфсизлиги” билим соҳаси киберхавфсизлик билан боглиц инсон ҳатти ҳаракатларини ўрганишдан ташқари, ташкилотлар (масалан, ходим) ва шахсий ҳаёт шароитида шахсий маълумотларни ва шахсий ҳаётни ҳимоя қилишга эътибор қаратади.

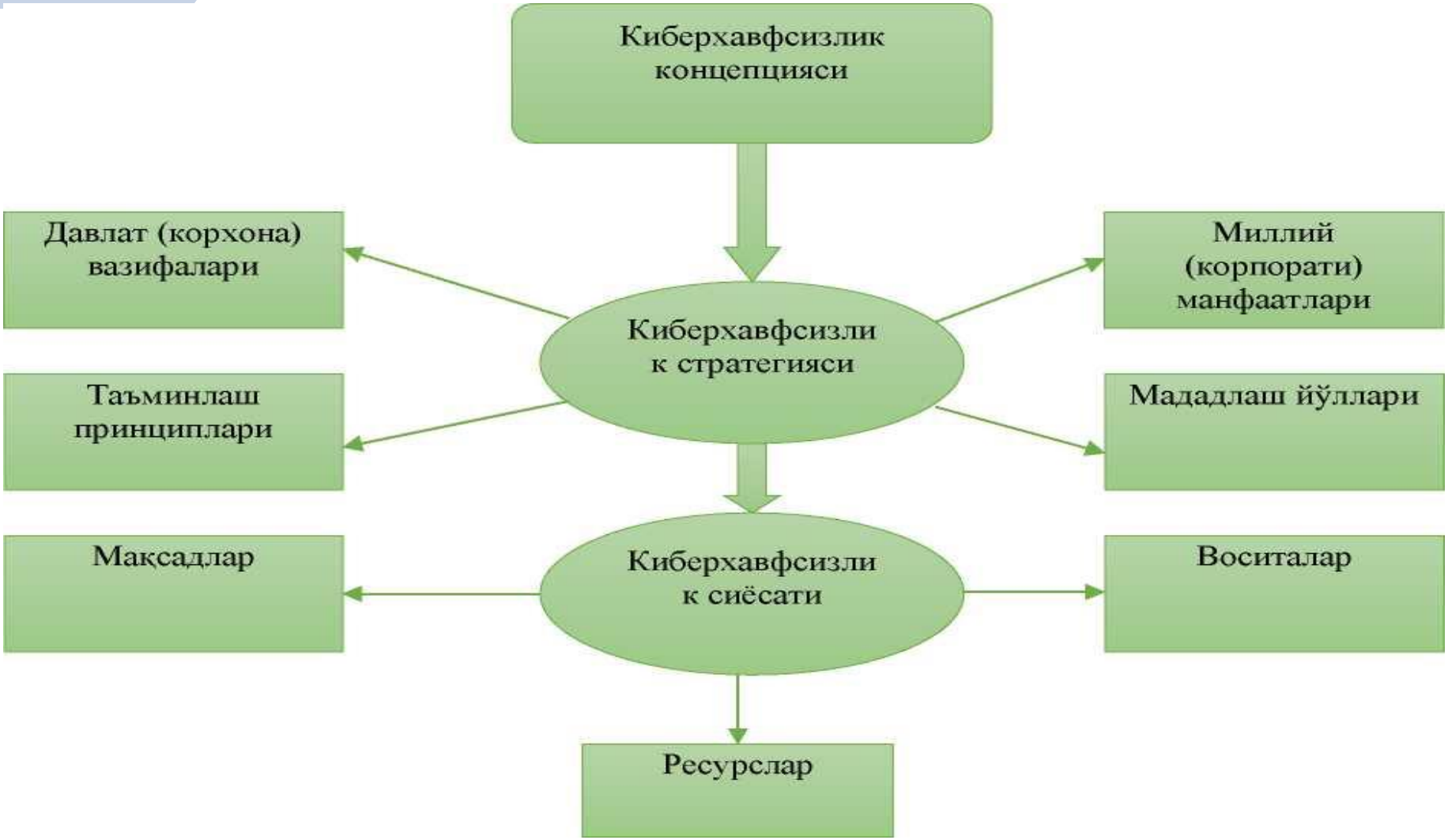
• “Ташкилот хавфсизлиги” билим соҳаси ташкилотни киберхавфсизлик таҳдидларидан ҳимоялаш ва ташкилот вазифасини муваффацциятли бажаришини мададлаш учун рискларни бошқаришга эътибор қаратади.

• “Жамоат хавфсизлиги” билим соҳаси у ёки бу даражада жамиятда таъсир кўрсатувчи киберхавфсизлик омилларига эътибор қаратади.

— Кибержиноятчилик, қонунлар, ахлоқий муносабатлар, сиёсат, шахсий ҳаёт ва уларнинг бир-бири билан муносабатлари ушбу билим соҳасидаги асосий тушунчалар.

Хавфсизлик муаммолари.

Киберхавфсизлик концепцияси - ахборот хавфсизлиги муаммосига расмий қабул қилинган қарашлар тизими ва уни замонавий тенденцияларни ҳисобга олган ҳолда ечиш йўллари. Концепцияни ишлаб чиқишни уч босқичда амалга ошириш тавсия этилади


Киберхавфсизлик концепцияси
Давлат (корхона) вазифалари
Миллий (корпорати) манфаатлари
Киберхавфсизлик стратегияси
Таъминлаш принциплари
Мададлаш йўллари
Мақсадлар
Киберхавфсизлик сиёсати
Воситалар
Ресурслар

Киберхавфсизлик сиёсати бу - ташкилотнинг мақсади ва вазифаси ҳамда хавфсизликни таъминлаш соҳасидаги чора-тадбирлар тавсифланадиган юқори сатҳли режа ҳисобланади.

У хавфсизликни таъминлашнинг барча дастурларини режалаштиради.

Ахборот хавфсизлиги сиёсати ташкилот масалаларини ечиш ҳимоясини ёки иш жараёни ҳимоясини таъминлаши шарт.

Аппарат воситалар ва дастурий таъминот иш жараёнини таъминловчи воситалар ҳисобланади ва улар хавфсизлик сиёсати томонидан қамраб олиниши шарт.

- умумий НИЗОМ;
- паролларни бошқариш сиёсати;
- фойдаланувчиларни идентификациялаш;
- фойдаланувчиларнинг ваколатлари;
- ташкилот ахборот коммуникацион тизимини компьютер вируслардан ҳимоялаш;
- тармоқ уланишларини ўрнатиш ва назоратлаш қоидалари;
- электрон почта тизими билан ишлаш бўйича хавфсизлик сиёсати қоидалари;
- ахборот коммуникацион тизимлар хавфсизлигини таъминлаш қоидалари;
- фойдаланувчиларнинг хавфсизлик сиёсатини қоидаларини бажариш бўйича мажбуриятлари ва ҳ.к.лар

РИСК номақбул воқеа - ҳодисадан келиб чиқадиган оқибатлар ва воқеа- ҳодиса юзага келиши эҳтимоллиги бирикмасини ўзида ифодалайди. Рискларни аниқлаш миқдор ёки сифат жиҳатдан рискларни тавсифлайди ва раҳбарларга қабул қилинадиган жиддийликка ёки бошқа ўрнатилган мезонларга кўра устуворликларга мувофиқ рискларни жойлаштириш имкониятини беради.

Рискни аниқлаш қуйидаги тадбирлардан иборат:

- рискларни аниқлаш;
- рискларни идентификация қилиш;
- рискларни таҳлил қилиш;
- рискларни баҳолаш.

Рискларни аниқлаш ахборот активларининг аҳамиятини белгилайди, мавжуд (ЁКИ мавжуд бўлиши мумкин) қўлланиладиган таҳдидлар ва заифликларни идентификация қилади, мавжуд бошқариш воситаларини ва уларнинг идентификация қилинган рискларга таъсирини идентификация қилади, потенциал оқибатларни аниқлайди ва НИҲОЯТ, устуворликларга мувофиқ, муайян рискларни жойлаштиради ва контекстни ўрнатишда аниқланган рискларни баҳолаш мезонлари бўйича уларни таснифлайди. РИСКНИ аниқлаш кўпинча икки (ёки ундан кўп) итерациядан фойдаланиб ўтказилади.

Компьютер ва компьютер тармоқларида компьютер хавфсизлиги инцидентларини бошкарнш ўз ичига мониторинг ва хавфсизлик ҳодиса-воқеаларини, ҳамда бу ҳодиса-воқеаларга тўғри жавобларни қайтаришни қамраб олади. Инцидентни бошқариш дастур ҳисобланиб маълум бир жараённи аниқлаб беради ва амалга оширади.

Ҳодиса - шахс ёки итттчи жараённи, жараённи, ўраб олган мухит ва тизимни нормал ҳолатини ўзгартиришни назорат этишдир.

Ҳодисанинг учта асосий тури мавжуд:

Нормал. Нормал ҳодиса критик компоненталарга таъсир қилмайди ёки кўрсатма (резолюция)ни бошланишидан олдин ўзгартиришни назорат этишни талаб қилади.

Ҳодисаларни кенгайиши ва кўпайиши (Эскалация). Ҳодисаларни кўпайиши тизимга жиддий таъсир кўрсатади ёки амалга оширилган кўрсатма (резолюция) ўзгартиришни назорат этиш жараёнини кузатишини таъминлаб бериши шарт.

Авариявий ҳодиса. Авариявий ҳодиса шахс хавфсизлиги ва соғлигига таъсир кўрсатади.
Инцидент - бу стандарт операциялар қаторига қўшилмайдиган ҳамда хизмат ҳолатини узиб қўйиш ёки хизмат сифати ёмонлашиши ҳолатларига олиб келадиган ҳар қандай ҳодисага айтилади.
Инцидентга жавоб қайтариш гуруҳи. Хавфсизлик инциденти координатори инцидентга жавоб қайтариш жараёнини бошқаради ва командани тўплаш учун жавобгар шахсдир. Координатор командани ташкил этиб, ташкил этилган команда ўз ичига инцидентни баҳоловчи ва қарор қабул қилувчи шахсларни қамраб олади.
Инцидентни тергов ҚИЛИШ - бу инцидент ҳолатини тергов қилиш ҳаракатидир. Ҳар бир инцидент тергов этишни талаб қилиши ёки унга кафиллик бериши керак бўлади. Шу билан бирга тергов қилинадиган ресурслар, ЯЪНИ тиббий воситалар, номуносиб тармоқлар ва карантин қилинган тармоқлар фавқулодда инцидентларга тез ва самарали рухсат бериш учун фойдали ҳисобланади.
Инцидентга жавоб қайтариш - бу хавфсизликни бузилиш кетма-кетлиги ёки ҳужумни бошқариш ва ечиш учун ишлаб чиқилган усулдир. Бунинг мақсади вазиятни тўғрилаш, яъни тизимни бузилишини чеклаш ва бузилган тизимни тиклаш вақти ва маблағини камайтиришдир.

Ахборот хавфсизлиги инцидентини бошқариш тизими архитектураси қуйидаги асосий компонентаналарни ўз ичига олади:

1. Интеграллашган платформа.
2. Аудит ва мониторингни аппарат-дастурий воситалари.
3. Ахборотни ҳимоялашнинг аппарат-дастурий воситалари.
4. Ахборот хавфсизлиги инцидентлари ҳақида ахборот омбори.
5. Ҳисоботларни генерациялаш воситалари ва аналитик асбоблар.
6. Воситаларни бошқариш ва интерфейсни тўғрилаш.

Интеграллашган платформа тизимнинг ядроси ҳисобланади. Бу тизим тузилишидаги ҳамма компонентаарни битта умумий функцияга боғлаб беради.

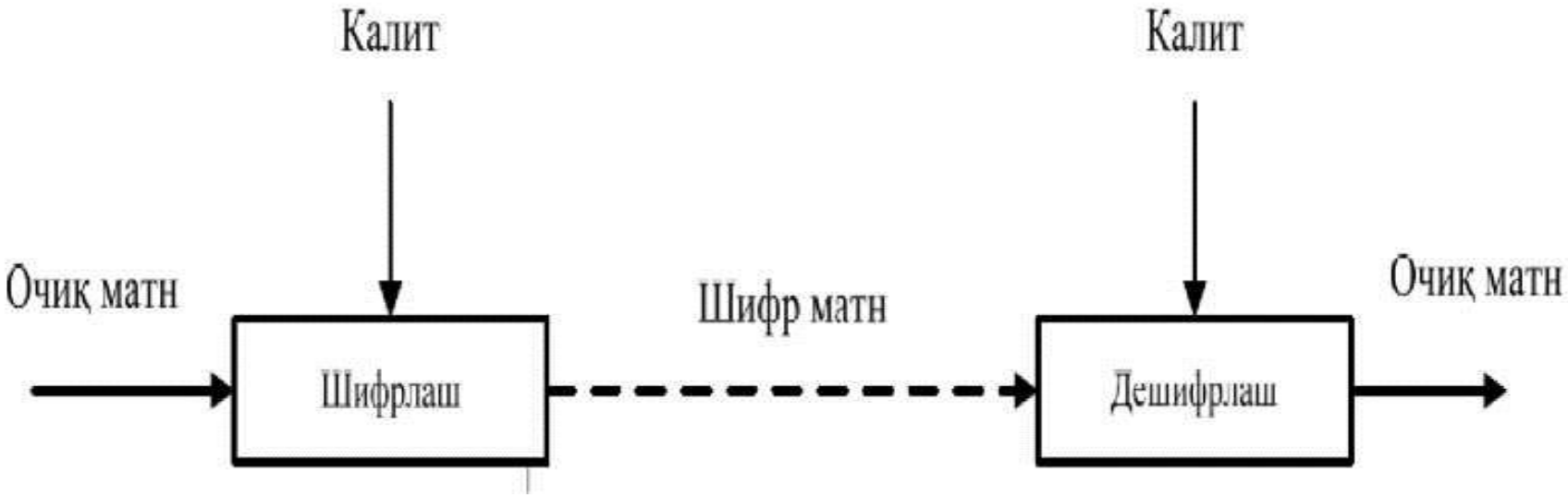
Интеграллашган платформа қўйидагилардан таркиб топган:

1. Маълумотларни йиғишни таъминловчи мониторинг ва аудит воситалари учун интерфейс.
2. Ахборот хавфсизлиги инцидентлари оқибатини локализациялаш мақсадида конфигурацияни тезкор ўзгартиришдаги ахборот ҳимояси воситалари интерфейси
3. Ҳисоботларни генерациялаш воситалари ва аналитик функциялардан фойдаланишдаги хизматлар.

Аудит ва мониторингни аппарат-дастурий воситалари - ташкилот ахборот тизимини қайта ишлаш, йиғиш ва протоколлаштиришни амалга оширувчи воситалардир. Бу воситаларга қуйидагилар киради: ўрнатилган воситалар (иловалар, операцион тизим воситалари, тармоқ қурилмалари, ҳимоя воситалари ва автоматлаштирилган тизимлар) ва махсус воситалар (аудит, хавфсизлик сканерлари, дастурий агентлар, сенсорлар, ахборот йиғувчи қурилмалар).

Аудит ва мониторингни аппарат-дастурий воситалари

Инцидентлар ахборот омбори



Криптотизимнинг “қора қути” сифатидаги кўриниши

Шифр ёки криптотизим маълумотни шифрлаш учун фойдаланилади. Ҳақиқий шифрланмаган маълумот очиқ матн деб аталиб, шифрлашнинг натижаси шифрматн деб аталади. Ҳақиқий маълумотни қайта тиклаш учун шифрматнни дешифрлаш зарур бўлади. Калит криптотизимни шифрлаш ва дешифрлаш учун созлашда фойдаланилади

Кўп ташкилот ва корхоналарда ахборот хавфсизлиги инцидентларни бошқариш жараёни қуйидагича қурилади:

- компьютер инциденти ҳақида ахборот олиш;
- қоидабузарлик аниқланган ҳолатларда қўшимча ахборот олиш;
- ҳолатни таҳлил этиш;
- сабабларни аниқлаш;
- профилактик тадбирлар ўтказиш.

Инцидентларини бошқариш жараёни самарадорлиги қўйидагиларга боғликдир:

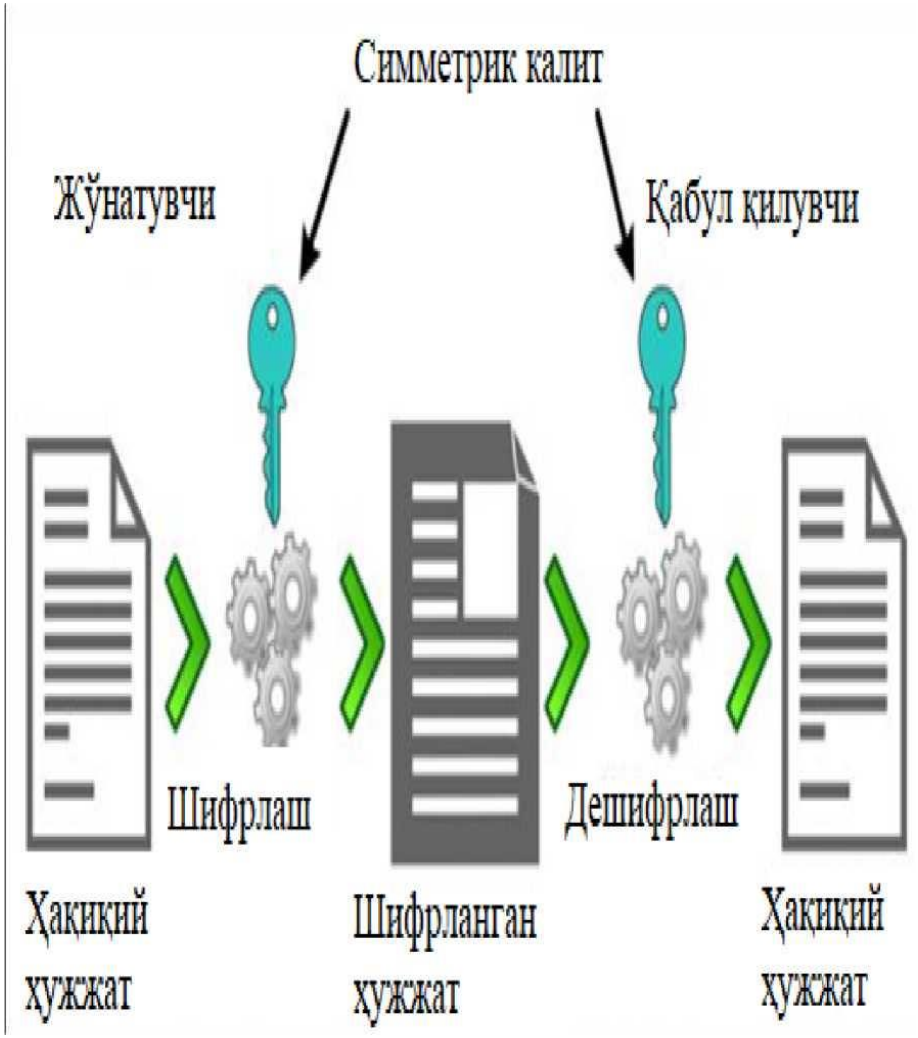
- ахборот хавфсизлиги инцидентини бошқариш жараёнида жалб этилган шахсларнинг тизимни бошқаришни яхши билиши;
- инцидент билан боғлиқ ахборотни таҳлил этиш ва олиш имкониятларнинг борлиги;
- олинган натижаларнинг ҳақиқийлиги.

Кодлаштириш деб, ахборотни бир тизимдан бошқа тизимга маълум бир белгилар ёрдамида белгиланган тартиб бўйича ўтказиш жараёнига айтилади.

Криптография деб махфий хабар мазмунини шифрлаш, ЯЪНИ маълумотларни махсус алгоритм бўйича ўзгартириб, шифрланган матнни яратиш иули билан ахборотга рухсат этилмаган киришга тўсиқ қўйиш усулига айтилади.

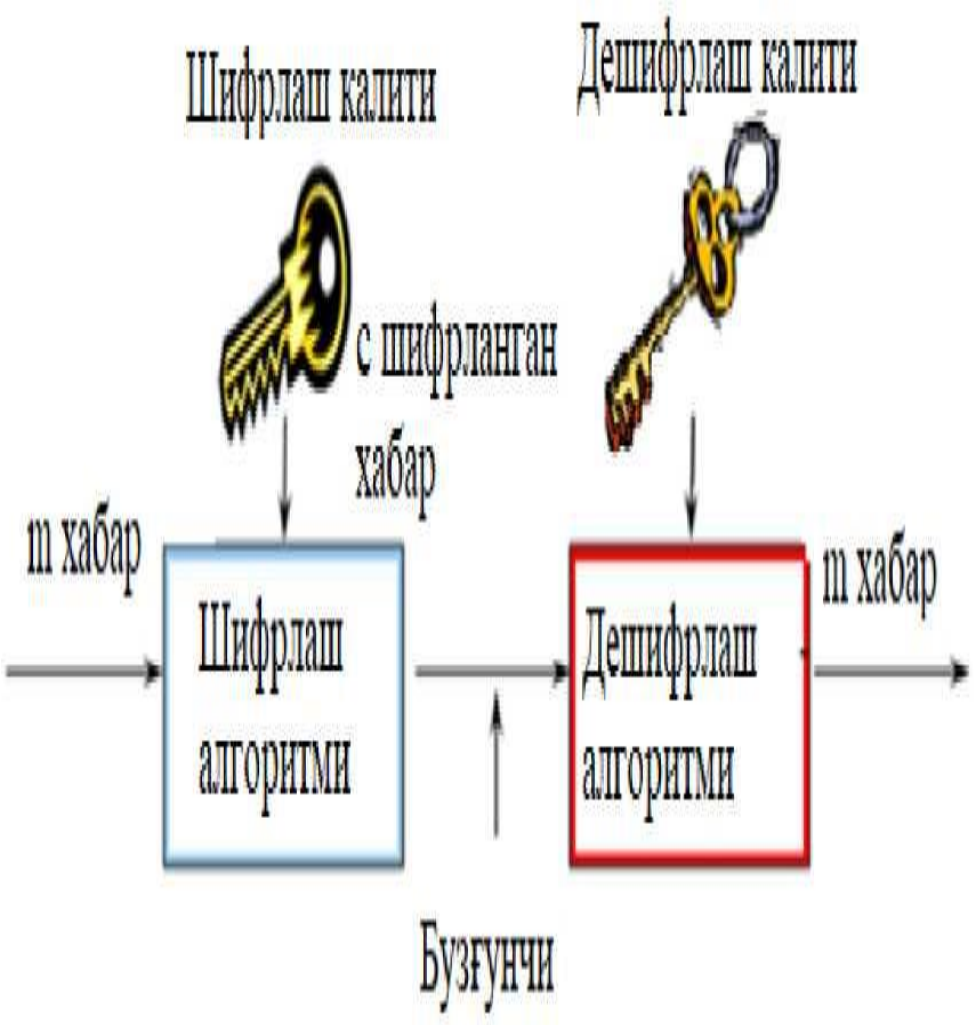
Калит- матнни шифрлаш ва шифрини очиш учун керакли ахборот.

Криптоанализ - калитни билмасдан шифрланган матнни очиш имкониятларини ўрганади.

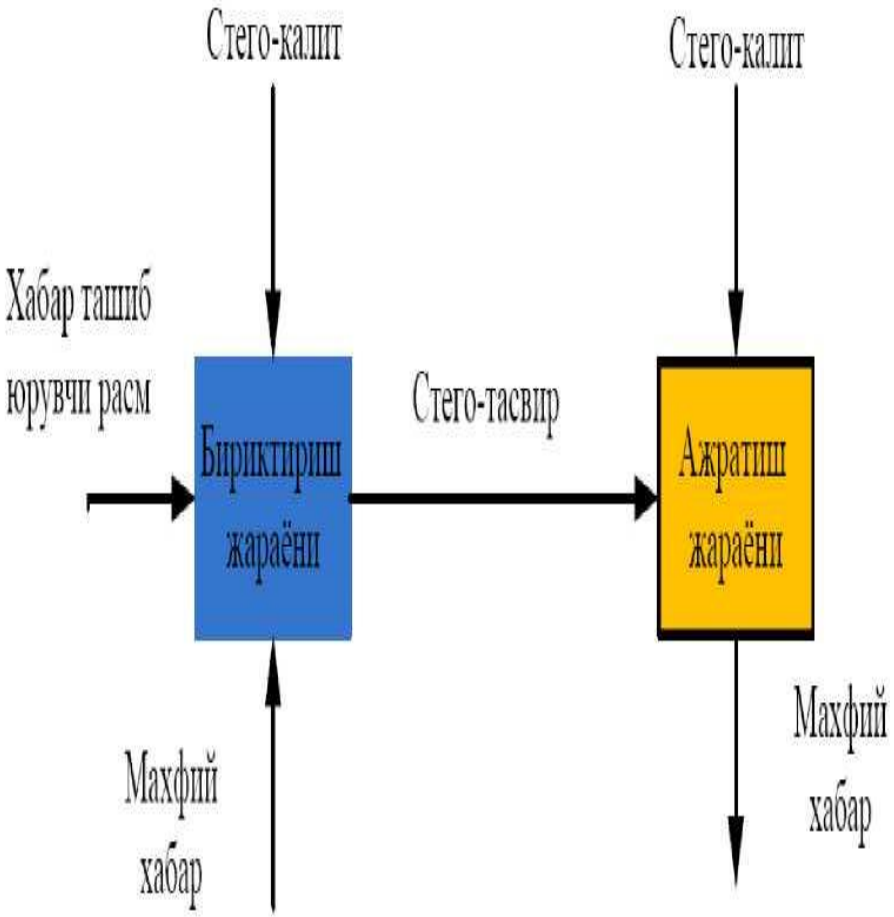


Симметрик шифрларда маълумотни шифрлаш ва дешифрлаш учун бир хил калитдан фойдаланилади

Симметрик калит



Бундан ташқари очиқ калитли (ассиметрик) криптотизимлар мавжуд бўлиб, унда шифрлаш ва дешифрлаш учун иккита калитдан фойдаланилади



2.4-расм. Стенография.

Стенанография - бу махфий хабарни сохта хабар ичига беркитиш орқали алоқани яшириш ҳисобланади. Бошқа сўз билан айтганда стеганографиянинг асосий ғояси - бу махфий маълумотларнинг мавжудлиги ҳақидаги шубҳани олдини олиш ҳисобланади

Адабиётлар ва интернет сайтлар:

1. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security
Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 |Pages: 357
2. Phillip Ferraro. Cyber Security: Everything an Executive Needs to Know.
Hardcover – July 6, 2016.
3. Ахборот хавфсизлиги бўйича ўқув-услубий мажмуа.
https://studfile.net/preview/7883185/
4. https://studfile.net/preview/7883185/page:23/

Эътиборларингиз учун рахмат!