O’ZBEKISTON RESPUBLIKASI
OLIY VA O’RTA MAXSUS TA’LIM VAZIRLIGI

OLIY TA’LIM TIZIMI PEDAGOG VA RAHBAR KADRLARINI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISHNI TASHKIL ETISH BOSH ILMIY-METODIK MARKAZI

TOSHKENT DAVLAT TEXNIKA UNIVERSITETI HUZURIDAGI PEDAGOG KADRLARNI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISH TARMOQ MARKAZI

“TEXNOLOGIK JARAYONLARNI BOSHQARISHNING AXBOROT-KOMMUNIKASIYA TIZIMLARI”
yo‘nalishi

“AXBOROT-KOMMUNIKASIYA TIZIMLARINING XAVFSIZLIK MAJMUALARI”
moduli bo‘yicha

O’ Q U V –U S L U B I Y M A J M U A

TOSHKENT -2022

Mazkur o’quv-uslubiy majmua Oliy va o’rta maxsus ta’lim vazirligining 2021 yil 25 dekabrdagi 538 sonli buyrug’i bilan tasdiqlangan o’quv dastur asosida tayyorlandi

Tuzuvchi:	BMTI “Texnologik jarayonlarni boshqarishning axborot-kommunikatsiya tizimlari” kafedrasi dotsenti, Sh.I. Fayziev
Taqrizchi:	BMTI “Texnologik jarayonlarni boshqarishning axborot-kommunikatsiya tizimlari” kafedrasi dotsenti, t.f.n. K.Z. Abidov

O’quv-uslubiy majmua Toshkent davlat texnika universiteti Kengashining 2021 yil 29 dekabrdagi 4 sonli yig’ilishida ko’rib chiqilib, foydalanishga tavsiya etildi.

MUNDARIJA

I. ISHCHI DASTUR

Kirish

Dastur O’zbekiston Respublikasining 2020 yil 23 sentyabrda tasdiqlangan “Ta’lim to’g’risida”gi Qonuni, O’zbekiston Respublikasi Prezidentining 2017 yil 7 fevral “O’zbekiston Respublikasini yanada rivojlantirish bo’yicha Harakatlar strategiyasi to’g’risida”gi PF-4947-son, 2019 yil 27 avgust “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining uzluksiz malakasini oshirish tizimini joriy etish to’g’risida”gi PF-5789-son, 2019 yil 8 oktyabr “O’zbekiston Respublikasi oliy ta’lim tizimini 2030 yilgacha rivojlantirish kontseptsiyasini tasdiqlash to’g’risida”gi PF-5847-sonli Farmonlari hamda O’zbekiston Respublikasi Vazirlar Mahkamasining 2019 yil 23 sentyabr “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining malakasini oshirish tizimini yanada takomillashtirish bo’yicha qo’shimcha chora-tadbirlar to’g’risida”gi 797-sonli Qarorida belgilangan ustuvor vazifalar mazmunidan kelib chiqqan holda tuzilgan bo’lib, u oliy ta’lim muassasalari pedagog kadrlarining kasb mahorati hamda innovatsion kompetentligini rivojlantirish hamda oliy ta’lim muassasalari pedagog kadrlarining kasbiy kompetentligini muntazam oshirib borishni maqsad qiladi.

Dastur mazmuni nazariy jihatdan axborot xavfsizligini ta’minlashning zamonaviy usul, vosita va tamoyillari bo’yicha yangi bilim, ko’nikma va malakalarini shakllantirishni nazarda tutadi.

Ushbu dasturda axborot tizimlari xavfsizligining umumiy tushunchalari, axborotlarni kriptografik himoyalash, kompyuter tarmoqlarida axborot xavfsizligi, shuningdek internet va elektron pochtada himoyalanish xususidagi ma’lumotlar o’z aksini topgan.

Modulning maqsadi va vazifalari

“Axborot-kommunikatsiya tizimlarining xavfsizlik majmualari” modulining **maqsadi**:

tinglovchilarning axborot xavfsizligini ta’minlashning zamonaviy usul, vosita va tamoyillari bo’yicha bilim, ko’nikma va malakalarni rivojlantirish.

“Axborot-kommunikatsiya tizimlarining xavfsizlik majmualari” modulning **vazifasi**:

axborot tizimlari va tarmoqlarida axborot xavfsizligi buzilishiga olib keluvchi asosiy xavflarni o’rganish va ularga qarshi himoya usullarni o’rgatishdan iborat.

Modul bo’yicha tinglovchilarning bilimi, ko’nikmasi, malakasi va kompetentsiyalariga qo’yiladigan talablar

“Axborot-kommunikatsiya tizimlarining xavfsizlik majmualari” modulni o’zlashtirish jarayonida amalga oshiriladigan masalalar doirasida**:**

Tinglovchi:

- axborot tizimlari xavfsizligining umumiy tushunchalari;
- axborot tizimlari xavfsizligining zamonaviy holati va ularning istiqbollari;
- axborotlarni xafvsiz ta’minlash texnologiyalarini;
- axborot xavfsizligini ta’minlashning zamonaviy usul va vositalarini;
- autentifikatsiya va uning turlari;
- axborotlarni kriptografik himoyalash usullarini;
- kriptotahlil tushunchasini;
- simmetriyali va asimmetrik kriptotizim asoslarini;
- zamonaviy shifrlash algoritmlarini;
- elektron raqamli imzoni;
- kompyuter tarmoqlarida ma’lumotlariga tahdidlarni;
- kompyuter tarmoqlarida zamonaviy himoyalash usullari va vositalarini;
- veb dasturlaridagi axborot himoyasini;
- elektron pochtada axborotlarga nisbatan mavjud xavf-xatarlar va ulardan himoyalanish asoslari haqida **bilimlarga ega bo’lishi lozim.**

Tinglovchi:

- korxonaning axborot xavfsizligini ta’minlashda kerakli standart, zamonaviy dasturiy ta’minotni tashlash va ularni asoslash;
- kompyuter tarmoqlarida zamonaviy himoyalash usullari va vositalaridan foydalanish;
- mavjud tahdidlarni o’rgangan holda, ularga qarshi o’z xavfsiz tizimini yarata olish;
- parolli autentifikatsiyalash;
- geografik joylashuv bo’yicha autentifikatsiyalash;
- ko’p faktorli autentifikatsiyalash;
- analitik usullarga asoslangan shifrlash;
- RSA algoritmiga asoslangan shifrlash;
- DDoS hujumlar bo’yicha ishlarni amalga oshirish **ko’nikma va malakalarini egallashi zarur.**

Tinglovchi:

- tarmoq orqali kirib kelayotgan turli tahdidlarni aniqlash va ularni bartaraf etish chora-tadbirlarini ishlab chiqish, testlash va ulardan foydalanishni tahlil qilish
- axborot tizimlarini xavfsizligini ta’minlash jarayonida mavjud muammolarni yechish **kompetentsiyalarga ega bo’lishi lozim.**

Modulni tashkil etish va o’tkazish bo’yicha tavsiyalar

“Axborot-kommunikatsiya tizimlarining xavfsizlik majmualari” moduli ma’ruza, amaliy va ko’chma mashg’ulotlar shaklida olib boriladi.

Modulni o’qitish jarayonida ta’limning zamonaviy metodlari, pedagogik texnologiyalar va axborot-kommunikatsiya texnologiyalari qo’llanilishi nazarda tutilgan:

- ma’ruza darslarida zamonaviy kompyuter texnologiyalari yordamida prezentatsion va elektron-didaktik texnologiyalardan;

- o’tkaziladigan amaliy mashg’ulotlarda texnik vositalardan, ekspress-so’rovlar, test so’rovlari, aqliy hujum, guruhli fikrlash, kichik guruhlar bilan ishlash, kollokvium o’tkazish, va boshqa interaktiv ta’lim usullarini qo’llash nazarda tutiladi.

Modulning o’quv rejadagi boshqa modullar bilan bog’liqligi va uzviyligi

“Axborot-kommunikatsiya tizimlarining xavfsizlik majmualari” moduli o’quv rejadagi kuyidagi fanlar bilan bog’liq: “Dasturlash tillari bazasida texnik ilovalar”, “Texnologik jarayonlarni raqamli boshqarishda kompyuter tarmoqlari va tizimlari” va “Axborot-kommunikatsiya tizimlarini loyihalash va testlash”.

Modulning oliy ta’limdagi o’rni

Modulni o’zlashtirish orqali tinglovchilar axborot xavfsizligini ta’minlashning zamonaviy usul, vosita va tamoyillarini o’rganish, amalda qo’llash va baholashga doir kasbiy kompetentlikka ega bo’ladilar.

Modullar bo’yicha soatlar taqsimoti

№	Modul mavzulari	Tinglovchining o’quv yuklamasi, soat			
		Jami	Nazariy	Amaliy mashg’ulot	Ko’chma mashg’ulot
1.	Axborotlarga nisbatan mavjud xavfsizliklarning asosiy tushunchalari va uning tasnifi. Autentifikatsiya va uning turlari	4	2	2	
2.	Axborotlarni kriptografik himoyalash usullari. Kriptotahlil tushunchasi. Simmetriyali va Asimmetrik kriptotizim asoslari. Elektron raqamli imzo	4	2	2	
3.	Kompyuter tarmoqlarida ma’lumotlariga tahdidlar. Kompyuter tarmoqlarida zamonaviy himoyalash usullari va vositalari. Simsiz tarmoqlarda axborotlarni himoyalash.	6	2	2	2
4	Veb dasturlaridagi axborot himoyasi. Elektron pochtada axborotlarga nisbatan mavjud xavf-xatarlar va ulardan himoyalanish asoslari.	4		2	2
	Jami:	**18**	**6**	**8**	**4**

NAZARIY MASHG’ULOTLAR MAZMUNI

1-mavzu: Axborotlarga nisbatan mavjud xavfsizliklarning asosiy tushunchalari va uning tasnifi.

Axborot xafvsizligi tushunchasi. Axborotlarni xafvsiz ta’minlash texnologiyalari. Axborot xavfsizligini ta’minlashning zamonaviy usul va vositalari. Autentifikatsiya va uning turlari.

2-mavzu: Axborotlarni kriptografik himoyalash usullari. Kriptotahlil tushunchasi.

Axborotlarni kriptografik himoyalash usullari. Kriptotahlil tushunchasi. Simmetriyali va Asimmetrik kriptotizim asoslari. Zamonaviy shifrlash algoritmlari. Elektron raqamli imzo.

3-mavzu: Kompyuter tarmoqlarida ma’lumotlariga tahdidlar.

Kompyuter tarmoqlarida ma’lumotlariga tahdidlar. Kompyuter tarmoqlarida zamonaviy himoyalash usullari va vositalari. Simsiz tarmoqlarda axborotlarni himoyalash.

4-mavzu: Internet va elektron pochtada himoyalanish.

Veb dasturlaridagi axborot himoyasi. Elektron pochtada axborotlarga nisbatan mavjud xavf-xatarlar va ulardan himoyalanish asoslari.Ijtimoiy injeneriya.

AMALIY MAShG'ULOT MAZMUNI

1-amaliy mashg'ulot:Autentifikatsiya va uning turlari.

ERI yordamidagi autentifikatsiya. Parolli autentifikatsiyalash. Sms yordamida autentifikatsiyalash. Biometrik autentifikatsiyalash. Geografik joylashuv bo'yicha autentifikatsiyalash. Ko'p faktorli autentifikatsiyalash.

2- amaliy mashg'ulot: Shifrlash algoritmlari.

Monoalfavitli almashtirish algoritmlari. Yorin almashtirish shifrlash algoritmlari. Joylashtirish shifrlash algoritmlari. Polialfavitli almashtirish algoritmlari. Analitik usullarga asoslangan shifrlash. RSA algoritmiga asoslangan shifrlash.

3- amaliy mashg'ulot:Kompyuter tarmoqlarida ma'lumotlariga tahdidlar.

Tarmoqlarni skanerlash. Sniferlar. "Ochiq joylarni topish" usuli. "Shoshilmagan holda tanlash" usuli. "Kompyuter abordaj" usuli. DDoS hujumlar bo'yicha ishlarni amalga oshirish.

4- amaliy mashg'ulot:VYeB dasturlaridagi axborot himoyasi.

DVWA dasturi. SQL-inektsiya usuli. PGP dasturlari axborot himoyalarini o'rganish.

KYoChMA MASHG'ULOTLAR MAZMUNI

1-mavzu: Himoyalangan kanal protokollari. IPSec. Ma'lumotlar bazasini himoyalash. Operatsion tizimlarda himoyalash mexanizmlari.

Ko'chma mashg'ulotda tinglovchilarni sohaga oid ishlab chiqarish korxonalari, TDTU kafedrasida olib borish ko'zda tutilgan.

TA'LIMNI TASHKIL ETISH SHAKLLARI

Ta'limni tashkil etish shakllari aniq o'quv materiali mazmuni ustida ishlayotganda o'qituvchini tinglovchilar bilan o'zaro harakatini tartiblashtirishni, yo'lga qo'yishni, tizimga keltirishni nazarda tutadi.

Modulni o'qitish jarayonida quyidagi ta'limning tashkil etish shakllaridan foydalaniladi:

- ma'ruza;
- amaliy mashg'ulot;

- ko’chma mashg’ulot.

Yoquv ishini tashkil etish usuliga ko’ra:

- jamoaviy;
- guruhli (kichik guruhlarda, juftlikda);
- yakka tartibda.

Jamoaviy ishlash – Bunda o’qituvchi guruhlarning bilish faoliyatiga rahbarlik qilib, o’quv maqsadiga erishish uchun o’zi belgilaydigan didaktik va tarbiyaviy vazifalarga erishish uchun xilma-xil metodlardan foydalanadi.

Guruhlarda ishlash – bu o’quv topshirig’ini hamkorlikda bajarish uchun tashkil etilgan, o’quv jarayonida kichik guruxlarda ishlashda (3 tadan – 7 tagacha ishtirokchi) faol rol o’ynaydigan ishtirokchilarga qaratilgan ta’limni tashkil etish shaklidir. O’qitish metodiga ko’ra guruhni kichik guruhlarga, juftliklarga va guruhlarora shaklga bo’lish mumkin. *Bir turdagi guruhli ish* o’quv guruhlari uchun bir turdagi topshiriq bajarishni nazarda tutadi. *Tabaqalashgan guruhli ish* guruhlarda turli topshiriqlarni bajarishni nazarda tutadi.

Yakka tartibdagi shaklda - har bir ta’lim oluvchiga alohida- alohida mustaqil vazifalar beriladi, vazifaning bajarilishi nazorat qilinadi.

III. NAZARIY MATERIALLAR

1- mavzu. Axborotlarga nisbatan mavjud xavfsizliklarning asosiy tushuntshalari va uning tasnifi. Autentifikatsiya turlari

Reja:

1. Asosiy tushuntshalar va ta`riflar.
2. Axborotni himoya qilish kompyuter tizimlari va tarmoqlari rivojlanishining qonuniyatidir.
3. Axborotni himoya qilish muammosining dolzarbligi.
4. Autentifikatsiya haqida umumiy tushunchalar.
5. Autentifikatsiya turlari.

1.1.Asosiy tushuntshalar va ta`riflar.

Axborot xavfsizligini ta`minlash muammosi Internetning ishlash sharoitlarida muhim ahamiyat kasb etadi. Mutloq ko’ptshilik kompaniya va tashkilotlar bugungi kunda o’zlarining lokal(mahalliy) tarmoqlarini Internetga, uning resurslari va afzalliklaridan foydalanish utshun ulamoqdalar. Ular Internetni turli maqsadlarda ishlatadilar, bunga elektron potshta bilan almashinish, shaxs va tashkilotlar o’rtasida axborotlarni olish va tarqatish kabilar kiradi. Bosh tarmoqqa ulanish katta afzallikga ega, ammo bunda ulanayotgan lokal yoki korporativ tarmoqdagi axborot xavfsizligini ta`minlashda jiddiy muammolar paydo bo`ladi.

Shu munosabat bilan, zamonaviy axborotlashgan jamiyatda global va boshqa tarmoqlarning ulkan afzalliklari mavjudligi bilan bir qatorda, ularda axborotni himoya qilish bo’yitsha o’ziga xos muammolarni ham etshishga to’g’ri keladi. Shuning utshun axborotning maxfiyligi va butunligini ta`minlash bilan bog’liq bo’lgan bartsha kerakli ishlarni amalga oshirish utshun samarali vositalarni yaratish va qo’llash juda muhimdir.

1.1.Asosiy tushuntshalar va ta`riflar.

Kompyuter tizimlari va tarmoqlarining xavfsizligi deganda, ular me`yoriy ishlash jarayoniga tasodifiy yoki oldindan mo’ljallangan aralashishdan hamda ularning tashkil etuvtshilarini o’g’irlashga, o’zgartirishga yoki buzishga bo’lgan intilishlardan himoya qilinganligi tushuniladi.

Axborotga murojaat qilish deganda, axborot bilan tanishib tshiqish, uni qayta ishlash, nusxalash, o’zgartirish va yo’qotish tushuniladi. Axborotga ruxsat etilgan va ruxsat etilmagan murojaat qilish turlari mavjuddir.

Axborotga ruxsat etilgan murojaat qilish bu, murojaat qilish tsheklanishlariga o’rnatilgan qoidalarni buzmaydigan, axborotga murojaat qilishdir.

Axborotga ruxsat etilmagan murojaat qilish murojaat qilish tsheklanishlariga o’rnatilgan qoidalarning buzilishi bilan tavsiflanadi.

Berilganlarning maxfiyligi bu berilganlarga taqdim etilgan va ularni himoya qilishni talab etilgan darajasini aniqlaydigan maqomdir.

Kompyuter tizimlariga hujum – tizimning u yoki bu bog'liqligini qidirish va ishlatish ma`nosini bildiradigan, yomon niyatli odam tomonidan bajariladigan harakatdir.

Xavfsiz yoki himoya qilingan tizim xavfsizlik xavflariga muvaffaqiyatli va samarali qarshi turadigan, zarur himoya qilish vositalariga ega bo'lgan tizimdir.

1.2.Axborotni himoya qilish kompyuter tizimlari va tarmoqlari rivojlanishining qonuniyatidir.

Zamonaviy kompyuter tizimlari va tarmoqlarida axborotni himoya qilish deganda uzatilayotgan, saqlanayotgan va qayta ishlanayotgan axborotning ishontshliligi va butunligini tizimli ta`minlash maqsadida turli xil vosita va usullarni ishlatish, tshoralarni ko'rish va tadbirlarni o'tkazish tushuniladi.

Axborotni himoya qilish – bu:

- axborotning fizik butunligini ta`minlash, ya`ni axborot elemenlarini hujumlariga utshrashi va yo'qolishiga yo'l qo'ymaslik;

- axborot butunligini saqlashda uning elementlarini almashtirishga (modifikatsiyaga) yo’l qo’ymaslik;
- mos vakolatlarga ega bo’lmagan shaxslar yoki jarayonlar tomonidan axborotni ruxsat etilmagan olinishiga yo’l qo’ymaslik;
- egalariga uzatilayotgan resurslar faqatgina tomonlar kelishgan shartlarga mos ravishda ishlatilishiga ishontsh hosil qilinishi kerak, demakdir.

Kompyuter tizimlari va tarmoqlarining ishlash tajribasi shuni ko’rsatmoqdaki, axborotga ruxsat etilmagan murojaat qilishni etarlitsha ko’pgina usullari bor:

- ko’rib tshiqish;
- berilganlarni nusxalash va almashtirish;
- yo’l va aloqa kanallariga ulanish natijasida yolg’on dastur va xabarlarni kiritish;
- sozlovtshi va halokatli dasturlarni ishlatish;
- axborotni uning tashuvtshilaridagi qoldiqlarini o’qish;
- elektromagnit nurlanishli va to’lqin xarakterli xabarlarni qabul qilish;
- maxsus dasturli va apparatli so’ndirgitshlarni ishlatish.

Demak, axborotni himoya qilish bo’yitsha aloxida (juda muhim bo’lsa ham) tadbirlarni ishlab tshiqish va tadbiq etish emas, balki **axborot xavfsizligining ko’p pog’onali, uzluksiz, kompleks va boshqariladigan tizimini yaratish** kerakdir.

1.3.Axborotni himoya qilish muammosining dolzarbligi

Axborot xavfsizligini ta`minlash muammosining dolzarbligi va muhimligi quyidagi sabablar bilan shartlangandir:

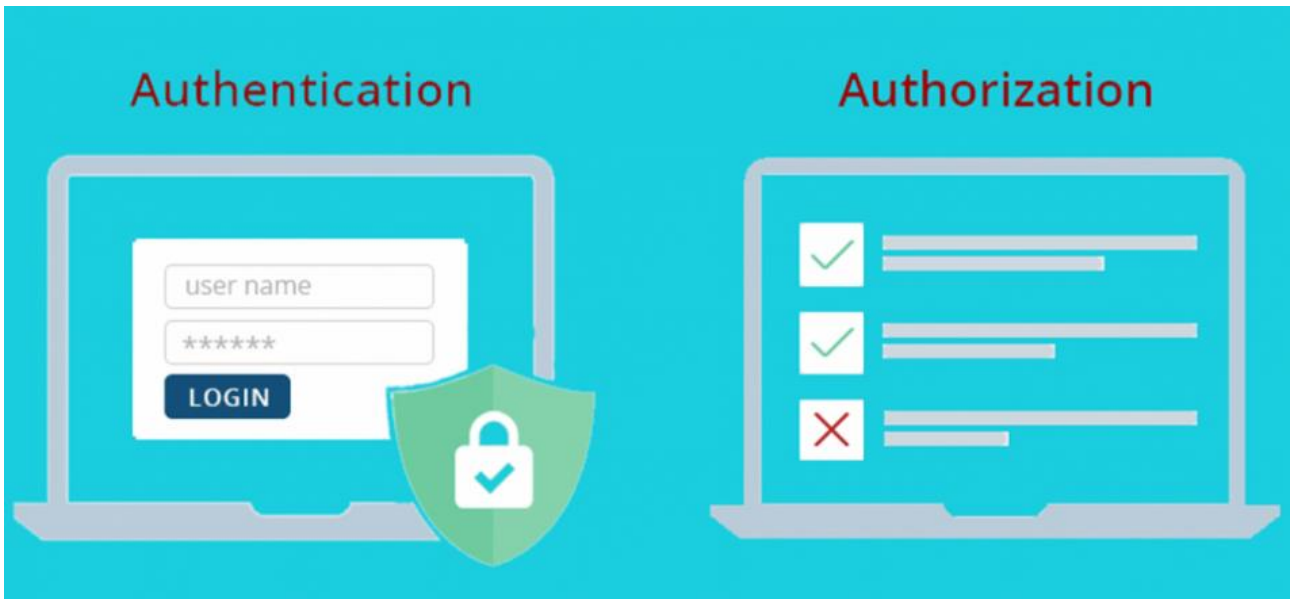
- zamonaviy kompyuterlarni ishlatish soddaligi bilan bir vaqtda ularning hisoblash quvvatining keskin oshishi;
- kompyuter va boshqa avtomatlashtirish vositalari yordamida yig’ilayotgan, saqlanayotgan va qayta ishlanayotgan axborot sig’imining keskin oshishi;
- turli xil vazifali va turli xil tegishli axborotlarni umumiy berilganlar bazasiga mujassamlantirilishi;

- hisoblash resurslari va berilganlar bazasiga bevosita murojaat qilish ruxsatiga ega bo’lgan foydalanuvtshilar doirasining keskin oshishi;
- axborot xavfsizligining, hattoki minimal talablarini ham qanoatlantirmaydigan dastur vositalarining gurkirab rivojlanishi;
- tarmoqli texnologiyalarning o’zaro tarqatilishi, lokal va regional tarmoqlarni global tarmoqlarga birlashtirilishi;
- butun dunyoda axborotni qayta ishlash tizimlari xavfsizligining buzilishiga deyarli to’sqinlik qilmaydigan Internet global tarmog’ining rivojlanishi;
- Internet global tarmog’ining otshiqlilik va nazorat qilinmasligi ideologiyasi.

1.4.Autentifikatsiya haqida umumiy tushunchalar.

Dastlab ikki terminni tushunishdan oldin yana bir muhim atamalardan biri bo'lgan atama **Identifikatsiya** nima ekanligini bilib olish lozim. Buni oddiy tarzda tushuntirishga harakat qilaman. Ko'pgina veb-saytlarga kirganingizda, foydalanuvchi nomini kiritasiz (***login***). Agarda siz yangi hisob qaydnomasi (***profile***) yaratmoqchi bo'lsangiz, sizdan identifikatsiyalash uchun foydalanuvchi nomini tanlashingiz so'raladi. Kirish paytida siz kiritadigan foydalanuvchi nomi bu "Identifikatsiya" dir. Bu shunchaki sizning shaxsingizni tasdiqlash usulidir. Yana ham oddiyroq aytadigan bo'lsak siz kiritadigan foydalanuvchi nomi bu barcha

ilovalar yoki veb saytlarda so'raladigan ***login***, ***e-mail*** yoki telefon raqamini tushunish mumkin.



Autentifikatsiya nima?

Autentifikatsiya (ingliz tilidan authentitsation , grek tilidan αὐθεντικός [authentikos] –haqiqiy, αὐθέντης [authentes]-muallif) – haqiqiylikni tekshirish jarayoni.

- Kiritilgan Parolni Foydalanuvtshining bazada mavjud paroli bilan solishtirish orqali foydalanuvtshining haqiqiyligini tekshirish
- Uzatuvtshining xatidagi elektron imzoni ni otshiq kalit orqali tekshirish yo'li bilan eletstron xatlarning haqiqiyligini tekshirish
- Fayl muallifi tomonidan ko'rsatilgan hajmni nazorat qilinayotgan hajm bilan mos kelishini tekshirish

Autentifikatsiya bu sizning foydalanuvchi identifikatoringizni tekshirish uchun **foydalanuvchi nomi** / **foydalanuvchi identifikatori** va parol kabi ma'lumotlarini tekshirish bilan bog'liq jarayonni o'z ichiga oladi. Shundan so'ng tizim sizning ma'lumotingizdan foydalanayotganligingiz yoki yo'qligingizni tekshiradi. Global yoki lokal tarmoqlarda bo'lsin, tizim login parollar orqali foydalanuvchi identifikatorini tasdiqlaydi. Odatda autentifikatsiya qilish foydalanuvchi nomi va parol orqali amalga oshiriladi, garchi autentifikatsiya qilishning boshqa usullari

bo'lsa ham. Oddiyroq aytadigan bo'lsak, Siz **login** va **parolingiz** orqali tizimga kirishga urunishingiz bu ***autentifikatsiya*** deyiladi. Autentifikatsiya qilish omillari tizim har kimga biron bir narsaga kirish huquqini berishdan oldin shaxsini tasdiqlash uchun foydalanadigan ko'plab turli elementlarni aniqlaydi. Shaxsning identifikatori shaxs nimani bilishi mumkinligini aniqlashi mumkin va xavfsizlik to'g'risida gap ketganda, tizimda kimgadir ruxsat berish uchun kamida ikkita yoki uchta autentifikatsiya qilish omillarini tekshirish kerak. Xavfsizlik darajasiga qarab, autentifikatsiya qilish omillari quyidagilarda bir biridan farq qilishi mumkin.

1.5.Autentifikatsiya (Authentication)

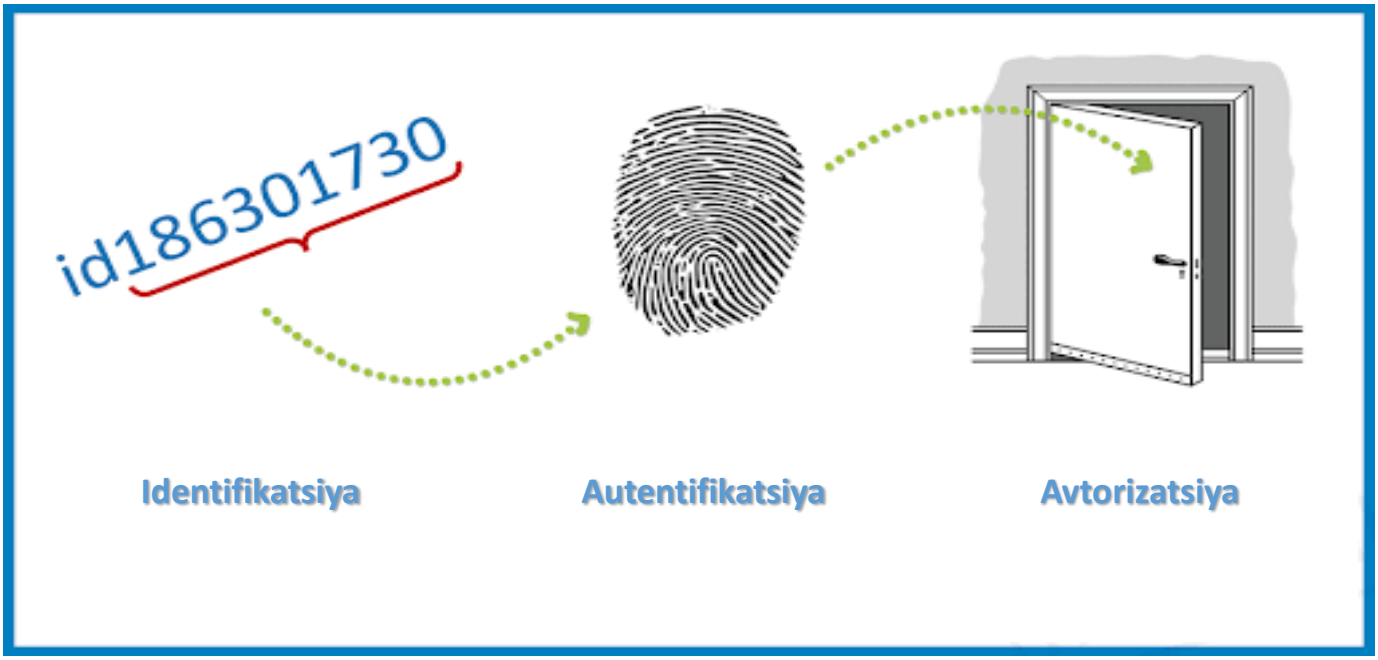
- **Single- Factor Authentication (**Bir bosqishli autentifikatsiya)
- **Two- Factor Authentication (**Ikki bosqishli autentifikatsiya)
- **Multi- Factor Authentication (**ko'p faktorli autentifikatsiya)

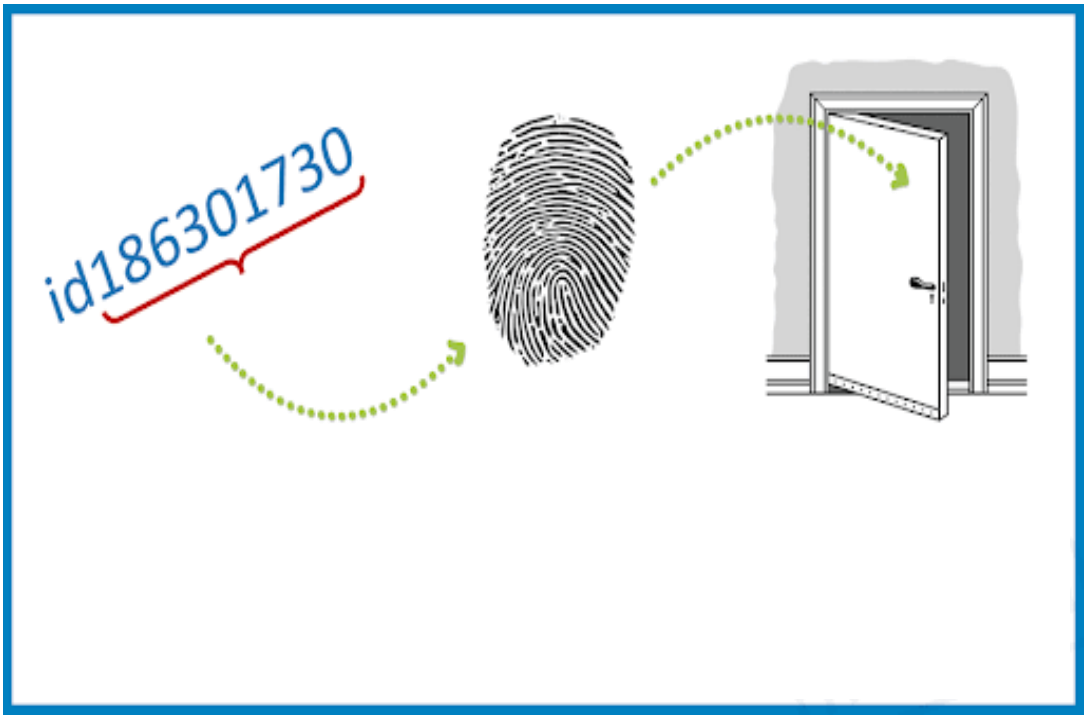
Single- Factor Authentication (Bir faktorli autentifikatsiya)**:** Bu autentifikatsiya jarayonining eng oddiy shakli bo'lib, foydalanuvchiga veb-sayt yoki tarmoqda muayyan tizimga kirish huquqini berish uchun parolni talab qiladi. Shaxs identifikatorini tekshirish uchun faqat bitta ma'lumotlardan foydalanib tizimga kirishni amalga oshirishi mumkin. Masalan, foydalanuvchi nomiga tegishli parolnigina talab qilish orqali faqat bitta faktorli autentifikatsiya yordamida login ma'lumotlarini tekshirishi mumkin.

Two- Factor Authentication: Ushbu autentifikatsiya ikki bosqichli tekshirish jarayonini talab qiladi, bu nafaqat foydalanuvchi nomi va parolni, balki faqat foydalanuvchi biladigan ma'lumotni ham talab qiladi. Foydalanuvchi nomi va parolni maxfiy ma'lumotlar bilan birgalikda ishlatish xakerlarga muhim va shaxsiy ma'lumotlarni o'g'irlashni ancha qiyinlashtiradi.

Multi- Factor Authentication (ko'p faktorli autentifikatsiya)**:** Bu autentifikatsiyaning eng ilg'or usuli bo'lib, foydalanuvchilarga tizimga kirish huquqini berish uchun mustaqil autentifikatsiya kategoriyalaridan ikki yoki undan ko'p darajadagi xavfsizlikni talab qiladi. Autentifikatsiya qilishning ushbu shakli har qanday ma'lumotlarga ta'sir qilishni bartaraf etish uchun bir-biridan mustaqil bo'lgan

omillardan foydalanadi. Moliyaviy tashkilotlar, banklar va huquqni muhofaza qilish idoralarida ko'p faktorli autentifikatsiyadan foydalanish odatiy holdir.





Elektron imzo yordamidagi Autentifikatsiya

- Oddiy elektron imzo
- Kvalifikatsiyalashmagan elektron imzo
- Kvalifikatsiyalashgan elektron imzo

Parolli Autentifikatsiya

- Kop’ martali parolli autentifikatsiya
- Bir martali parolli autentifikatsiya

SMS yordamida Autentifikatsiya

Mobil aloqa vositalari orqali xavfsizlikni ta’minlash

Biometrik Autentifikatsiya

- Barmoq izini olish
- Qo’l geometriyasi
- Ko’z qoratshig’i rang baranglari
- Kishining termik
- Yuz bo’yitsha tanib olish
- Tovush
- Klaviaturadan kiritish
- Imzo

Geografik joylashuv bo’yitsha Autentifikatsiya

- GPS yordamida
- Internetga kirish joyi orqali

Ko’p faktorli Autentifikatsiya

- PIN –kod mobil telefonlardagi SIM-kartalarda
- Notebooklardagi barmoq izini skanerlash

Nazorat savollari:

1. Kriptografiya maqsadi va vazifasi.
2. Oddiy o`rin almashtirish usuli va kalit so`zli o`rin almashtirish usuli.
3. Ikki martalik qayta quyish usuli va sehrli kvadrat usuli.
4. TSezar usuli va kalit so`zli TSezar tizimi.

Foydalaniladigan adabiyotlar:

1. Ganiev S.K., Karimov M.M., Toshev K.A. Axborot xavfsizligi. O’kuv kullanma .-TATU «Aloqachi», 2008.

2. Jukov YU. V. Osnovы veb-xakinga. Napadenie i zaщita (2-e izd.). Piter.2012. 206c.

3. S.A. Babin. Instrumentarii XAKERA. BXV-Peterburg. 2014 g. 233 s.
4. Vivek Ramachandran - BackTrack 5 Wireless Penetration Testing – 2011. 220 Flyonov M.E. Kompyuter glazami xakera. 2012g. BXV-Peterburg. 2012g. 274s.
5. Andrianov V. V. Zefirov S. L. Golovanov V. B. Golduev N. A. Obespechenie informatsionnoy bezopasnosti biznesa. 2011g. 265 s.
6. Platonov V.V. Programmno-apparatnыe sredstva zaщitы informatsii (Vыsshee professionalnoe obrazovanie. Bakalavriat). AKADEMIA. 2013g. 331 s.
7. SHangin V.F. Zaщita informatsii v kompyuternых sistemax i setyax. DMK. 2012g. 593s.
8. Romanets YU.V.,Timofeev P.A., SHangin V.F. Zaщita informatsii v kompyuternых sistemax i setyax./ M.: Radio i svyaz,2010.-376s.\
9. Barry L. Williams. «Information Security Policy Development for Compliance»: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0. 2013 year.

2-mavzu. Axborotlarni kriptografik himoyalash usullari. Kriptotahlil tushuntshasi. Simmetriyali va Asimmetrik kriptotizim asoslari. Elektron raqamli imzo.

Reja:

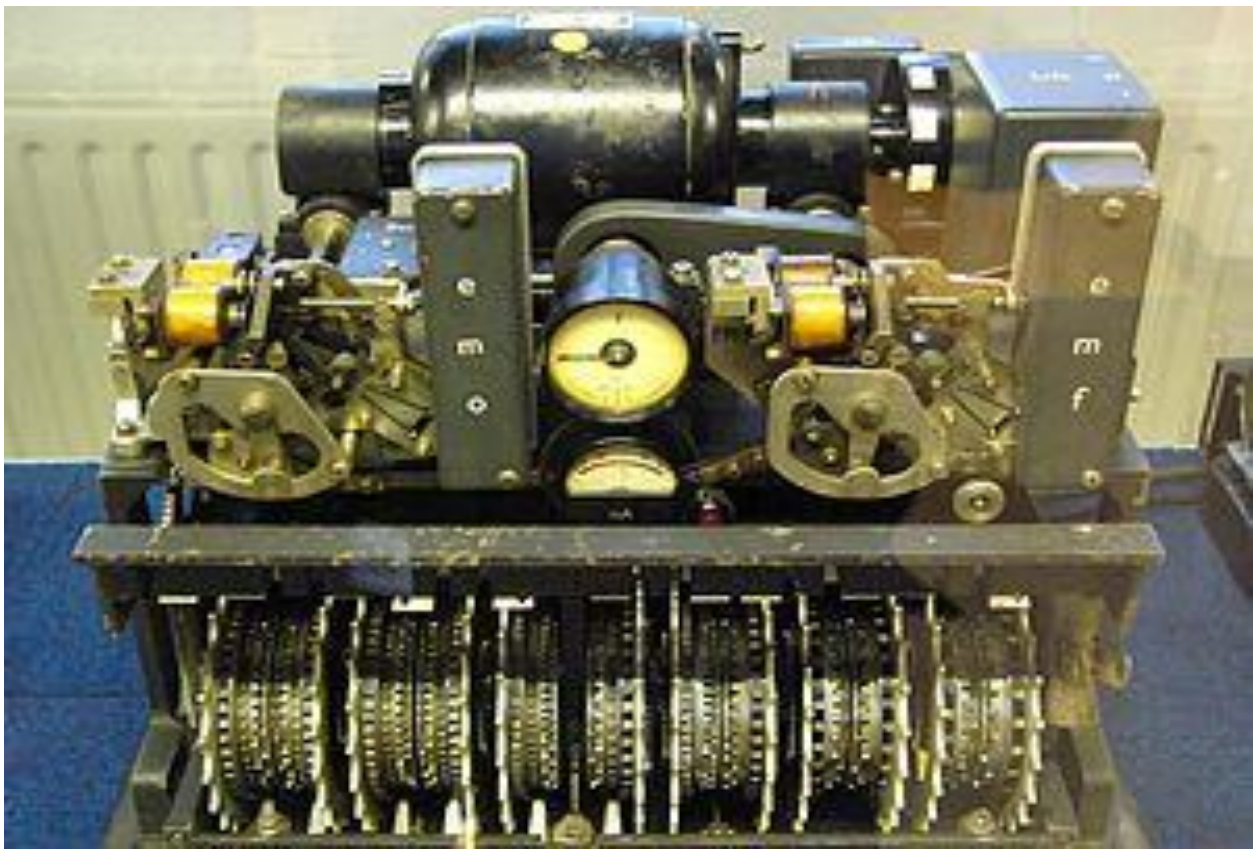
1. Axborot xavfsizligida kriptografik himoyalash usullari va asosiy terminlari;
2. Kriptotizimning klassik sxemalari va ishlash modellari.
3. Shifrlash guruhlari
4. Feystel to`ri

2.1.Axborot xavfsizligida kriptografiya himoyalash usullari.

Jamiyatni kompyuterlashtirish, bir qator foydalardan tashqari, o’zi bilan bir qator muammolarni olib keldi. Juda ham murakkab bo’lgan bunday muammolardan bittasi axborotni qayta ishlash va uzatish tizimlarida maxfiy axborotni xavfsizligini ta`minlashdir.

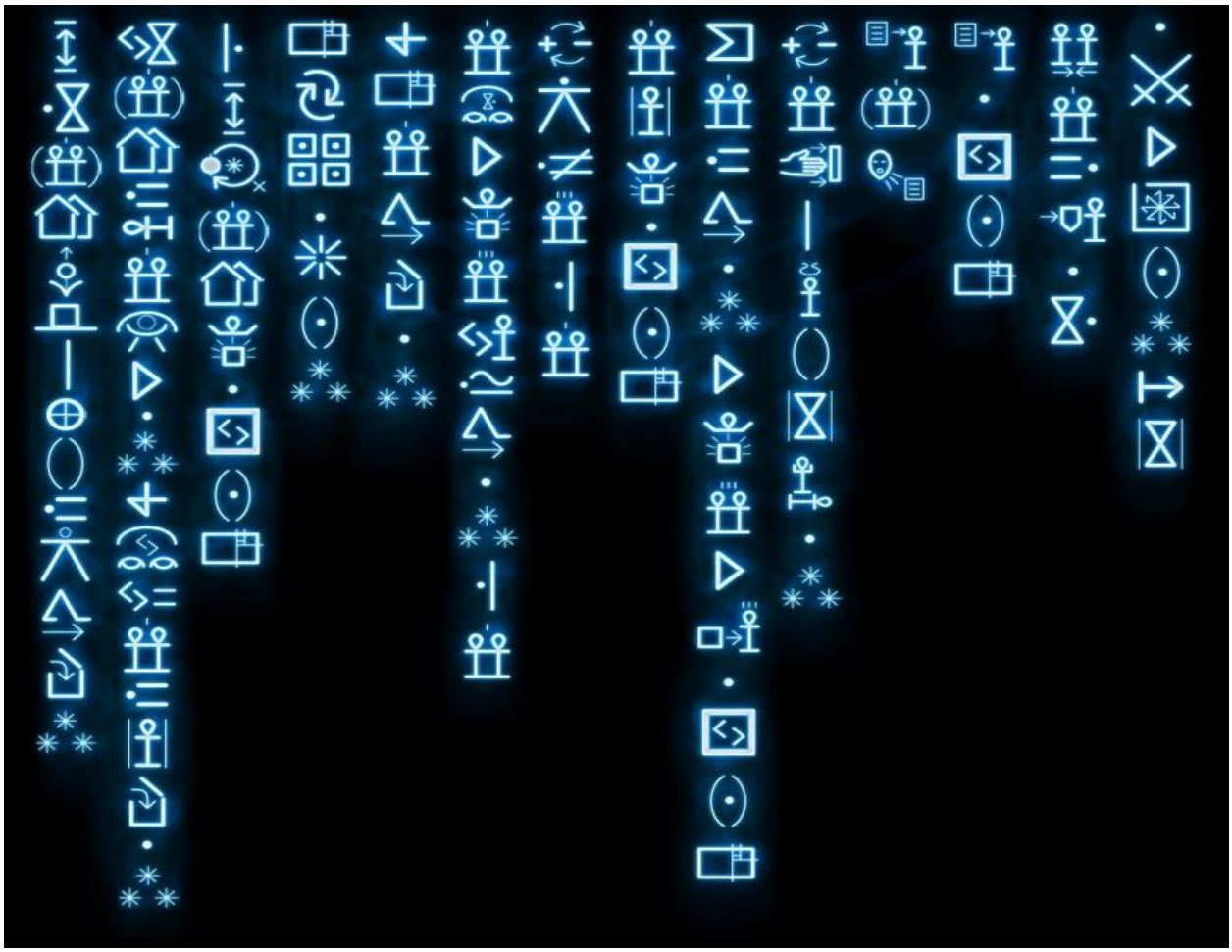
Bu muammoni hal qilish utshun **axborotni himoya qilishning kriptografik usullari** keng ishlatilmoqda, bunda boshlang’itsh axborot shunday o’zgartiriladiki,

buning natijasida axborot kerakli vakolatlarga ega bo’lmagan shaxslarga tanishish va ishlatish utshun mumkin bo’lmay qoladi.



Shifrlash jarayoni boshlang’itsh axborot ustida oldingi holatga qaytish imkoniyati saqlangan holda matematik, mantiqiy va boshqa o’zgartirishlarni o’tkazishdir, buning natijasida shifrlangan axborot harflarning, raqamlarning, boshqa belgilarning tartibsiz to’plami ko’rinishiga egadir.

Axborotni shifrlash utshun o’zgartirish algoritmi va kalit ishlatiladi. Odatda, ma`lum bir shifrlash usuli utshun o’zgartirish algoritmi o’zgarmas hisoblanadi. Shifrlash algoritmi utshun boshlang’itsh qiymatlar sifatida ma`lumotlarni shifrlash utshun axborot va shifrlash kaliti xizmat qiladi. Kalit boshqaruvtshi axborotni o’z itshiga oladi, u shifrlash algoritmini amalga oshirishda ishlatiladigan operandlar kattaliklarini va algoritmning ma`lum qadamlarida o’zgartirishlarni tanlashni aniqlaydi.

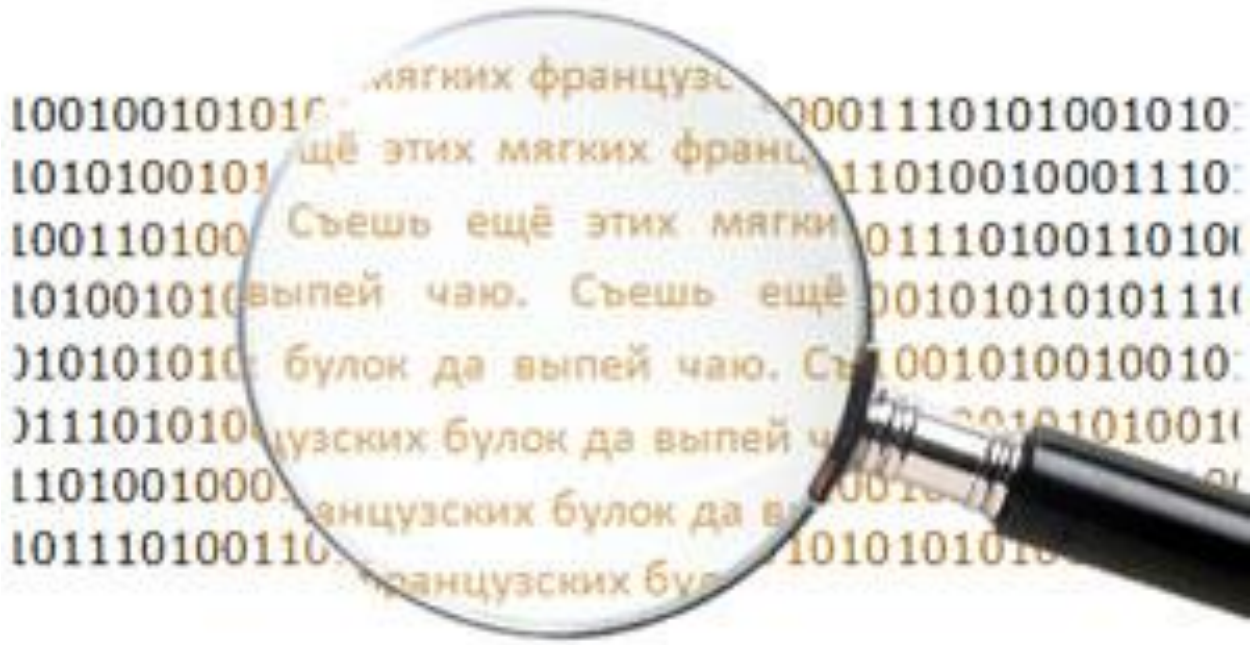


Shifrlash - kriptografik o’zgartirishni asosiy ko’rinishidir. Bu otshiq axborotni shifrlangan axborotga (shifrmatn) o’zgartirish yoki shifrlangan axborotni otshiq axborotga teskari o’zgartirish jarayonlaridir.

Otshiq axborotni yopiq axborotga o’zgartirish jarayoni shifrlash, teskarisi esa - qayta shifrlash (shifrni otshish) deb ataladi.

Shifrlash usullarining va shifrlarning ko’plab turlari mavjud. Bu shifrlash algoritmiga mos ravishda otshiq axborotni yopiq axborotga orqaga qaytmaydigan (kalitni bilmasdan turib) o’zgartirishlar to’plamidir.

EHM va KT larining paydo bo’lishi axborotni shifrlash, qayta shifrlash utshun ham, shifrga hujum qilish utshun ham EHM ni ishlatish imkoniyatlarini inobatga oladigan yangi shifrlarni ishlab tshiqish jarayonini keltirib tshiqardi. Shifrga hujum qilish-kriptotahlil qilish - kalitni bilmasdan turib, mumkinki, shifrlash algoritmi to’g’risida ma`lumotlar yo’qligida, yopiq axborotni qayta shifrlash (otshish)jarayonidir.



Zamonaviy shifrlash usullariga quyidagi talablar qo’yiladi:

- kriptotshidamlilik (kriptotahlil qilishga qarshi turish) shunday bo’lishi kerakki, shifrni otshish kalitlarini to’liq tanlab olish masalasini etshish yo’li bilan amalga oshirilishi kerak;
- kriptotshidamlilik shifrlash algoritmining maxfiyligi bilan emas, balki kalitning maxfiyligi bilan ta`minlanadi;
- shifrmatn o’zi hajmi bo’yitsha boshlang’itsh axborotdan ko’payib ketmasligi kerak;
- shifr xatoliklari axborotni to’siqlarga utshrashiga va yo’qolishlariga olib kelmasligi kerak;
- shifrlash vaqti katta bo’lmasligi kerak;

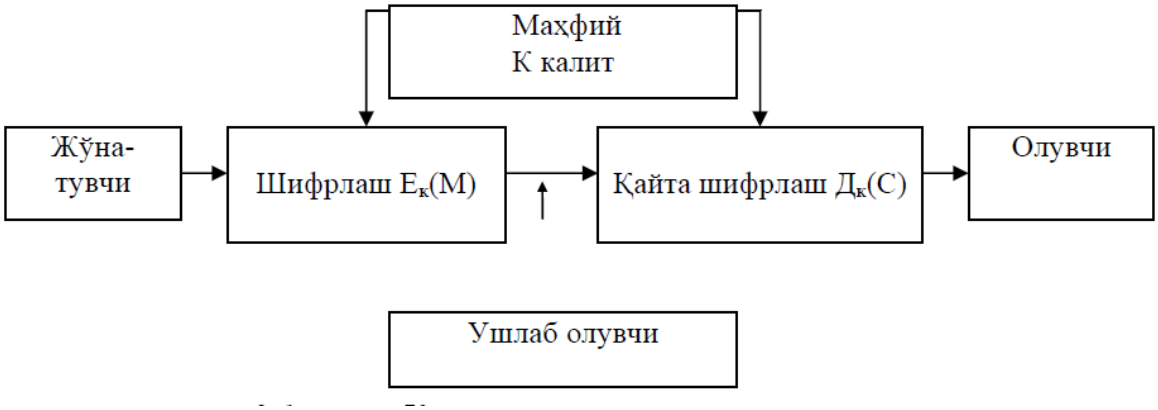
Kriptotahlil qilishga sarflanadigan vaqt va vosita kalit uzunligiga va shifrlash algoritmining murakkabligiga bog’liq bo’ladi.

Keng ishlatiladigan shifrlash algoritmini maxfiy saqlashni deyarli imkoni yo’qdir, shuning utshun algoritm yopiq kutshsiz joylarga (sust qismlarga) ega bo’lmasligi kerak. Axborotni ishontshli yashirish utshun kalit uzunligi 90 bitdan kam bo’lmasligi kerak (masalan, 1978 yildan buyon AQSh da davlat standarti sifatida DES (DATA Entsrypting Standard) shifri ishlatiladi, algoritm otshiq nashrda e`lon qilingan. 30 mln $ turadigan super EHM ni ishlatgan holda 56 bitli

kalit 453 kunda topilishi mumkin, qo'shimtsha 300000 $ ni sarflasa - 19 kunda, agar maxsus tshipni ishlab tshiqsa - harajatlar 300 mln. $ bo'lganda 12 sekundni tashkil etadi).

2.2.Kriptotizimning klassik sxemalari va ishlash modellari

Kriptotizimning umumlashgan klassik sxemasi 1-rasmda ko'rsatilgan.



1-rasm. Kriptotizimning umumlashgan sxemasi

Jo'natuvtshi boshlang'itsh M xabarning otshiq matnini ishlab tshiqaradi, u himoya qilinmagan kanal bo'yitsha qonuniy oluvtshiga uzatilishi kerak. Kanalni, uzatilayotgan xabarni ushlab olish va uni otshish maqsadida ushlab oluvtshi kuzatib turadi. Jo'natuvtshi oldingi holatga qatadigan E_k o'zgartirish yordamida M xabarni shifrlaydi va oluvtshiga jo'natiladigan $C=E_k(M)$ shifrmatni (kriptogrammani) oladi.

Qonuniy oluvtshi, C shifrmatni qabul qilib, teskari $D=E_k^{-1}$ o'zgartirish yordamida uni qayta shifrlaydi(otshadi) va otshiq matn M ko'rinishdagi boshlang'itsh xabarni oladi:

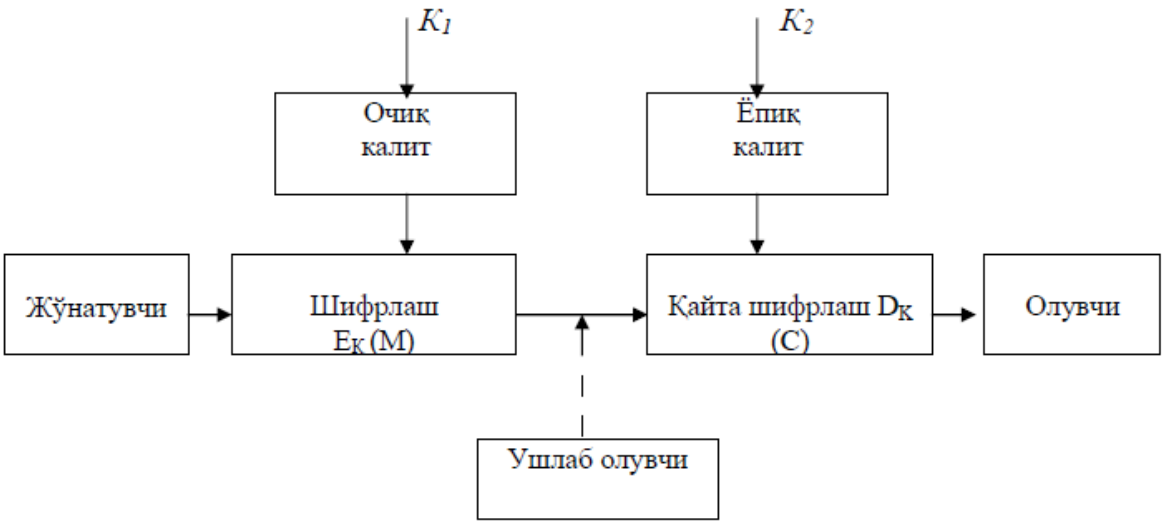
$$Д_K(C) = E_K^{-1}(M) = M$$

E_K o'zgartirish kriptografik o'zgartirishlar yoki kriptoalgoritmlar to'plamidan tanlanadi. Alohida ishlatiladigan o'zgartirish K kalit yordamida tanlanadi. Kriptotizim amalga oshirishning turli variantlariga egadir: yo'riqnomalar to'plami, apparat vositalar, kompyuterning dasturlar to'plami; ular otshiq matnni shifrlash va

otshiq shifrmatnni turli usullar bilan qayta shifrlash imkonini beradi, ulardan bittasi aniq bir K kalit yordamida tanlanadi.

Qayta shifrlashni (otshishni) o'zgartirishga nisbatan shifrlash simmetrik va nosimmetrik (assimetrik) bo'lishi mumkin. Simmetrik - bitta kalitli, nosimmetrik - ikkita kalitli (otshiq kalitli) kriptotizim sinflaridir. Bitta kalitli simmetrik kriptotizimning sxemasi 1-rasmda keltirilgan. Unda bir xil maxfiy kalitlar shifrlash blokida va qayta shifrlash blokida ishlatiladi.

Ikkita kalitli nosimmetrik kriptotizimning umumlashgan sxemasi 2- rasmda keltirilgan.



2 - rasm. Otshiq kalitli assimetrik kriptotizimning umumlashgan sxemasi

Simmetrik kriptotizimda maxfiy kalit jo'natuvtshiga va oluvtshiga kalitlar tarqatadigan himoya qilingan kanal bo'yitsha, masalan, kuryer bilan, uzatiladi. Nosimmetrik kriptotizimda himoya qilinmagan kanal bo'yitsha faqat otshiq kalit uzatiladi, maxfiy kalit esa uni ishlab tshiqarilgan joyida saqlanadi.

Shifrlash uslubini tanlash, ya`ni kriptografik algoritm va uni qaysi rejimda ishlatish avvalo uzatilayotgan ma`lumot (axborot) xususiyatlariga bog'liq bo'ladi. Shuningdek, ma`lumotni muhofazalamoqtshi bo'lgan tomon imkoniyatlariga (qo'llanilayotgan kripto-vositalarning tan narxi va bardoshligiga) ham bog'liqdir.

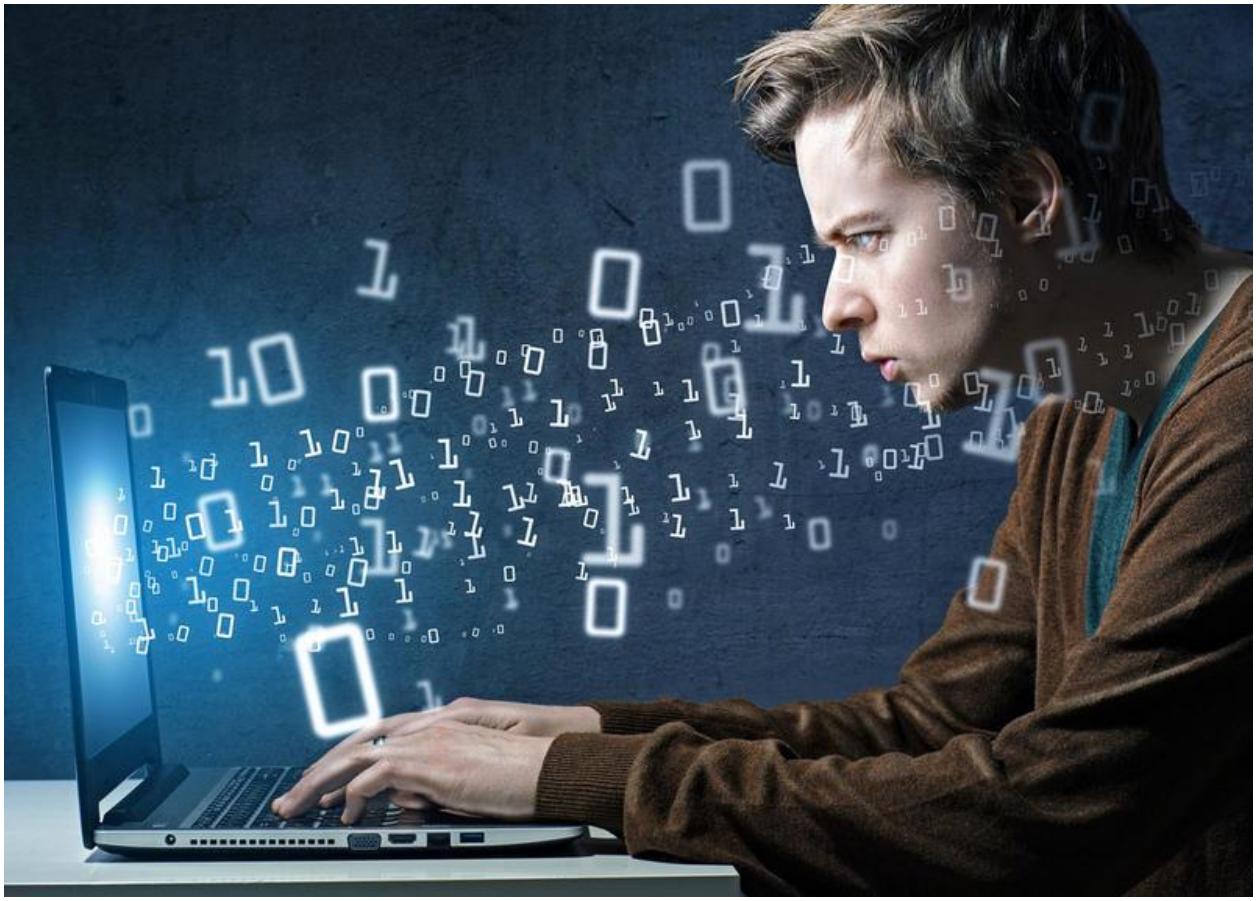
Bardoshli kritpografik algoritm va rejimni to'g'ri tanlashning o'zi hali ma`lumot uzatuvtshi tomonga kafolatlangan himoyaga ega ma`lumot yuborilishiga to'liq imkoniyat yaratmaydi. Bu erda kriptografik algoritm va rejimni tanlashni to'g'ri qo'llay bilish ham muhim omillardan biri hisoblanadi. Chunki eng bardoshli

deb hisoblangan kriptografik algoritmlar ham noto’g’ri foydalanish oqibatida o’zining bardoshlilik darajasini tushiradi. Bunday holatlarning yuz berishi esa kriptoanalitik utshun juda muhim qurol sifatida qo’l kelishi mumkin.

Turli shifrlar utshun deshifrlash (otshish) masalalari turlitsha murakkabliklarga ega bo’ladi. Ushbu masala murakablik darajasi aynan shu shifrning asosiy xossasini aniqlaydi. Shuning utshun biror shifr kriptografik bardoshligi haqida fikr yuritilganda etarli darajada va kitshik bardoshlikga ega bo’lgan turlarga ajratib qaraladi.

Kriptoanaliz-bu kalitni bilmasdan shifrlangan xabarni birlamtshi holatga keltirish omadli analiz birlamtshi matn yoki kalitni otshishi mumkin. Bundan tashqari u kriptotizimdagi kamtshiliklarni topishi mumkin, bu esa yuqorida aytilgan natijalarga olib keladi.

Kriptoanalizning fundamental qoidasini birintshi bo’lib, XIX asrda A. Kerxoffom gollandiyalik olim keltirib, unda shifr tshidamliligi (kriptotizimning) faqatgina maxfiy kaliti bilan aniqlanishi lozim degan. Boshqatsha aytganda, Kerkxoff qoidasi shundan iboratki, dushmanga yashirin kalitdan boshqa shifrlash algoritmi ham unga ma`lum bo’lishi mumkin. Bu shunday shartlanganki, kriptografik o’zgartirishlarni amalga oshiruvtshi kriptotizimlar oilasi otshiq tizim sifatida qaraladi. Bunday qarash informatsiyani himoyalash texnologiyasini muhim tamoyilini ifodalaydi: tizimning himoyalanganligi maxfiy informatsiya yo’qolgan holatda tezkor o’zgartirish mumkin bo’lmagan biron-bir maxfiylikka bog’liq bo’lmasligi kerak.



Oddiy holda kriptotizim apparat va dasturiy vositalar to’plamini ifodalab, uni ma`lum vaqt va vositalarni sarflagan holda o’zgartirish mumkin, kalit esa oson

o’zgaruvtshan ob`ekt hisoblanadi. Shu tufayli kriptotizim birdamligi faqat kalit maxfiyligi bilan bog’liq bo’lishi kerak.

Kriptoanalizda boshqa umumkelishuvlar quyidagitsha: kriptoanalatik xabar shifrmatnlariga egadir.

Kriptoanalitik hujumlarning to’rt asosiy turi mavjud:

1.Faqat shifrmatnga ega bo’lgan kriptoanalitik hujum. Kriptoanalatik bir netsha xabarli C_1, C_2,... C_n shifrmatnlarga ega, bunda ularning bartshasi birta E_k shifrlash algoritmi bilan shifrlangan. Kriptoanalitikni ishi shundan iboratki, ko’p xabarlar imkoniyatidan kelib tshiqqan holda M_1, M_2,... M_i birlamtshi matnlarni otshish yoki yaxshisi shu xabarlarni shifrlash utshun ishlatilgan K kalitni hisoblab topish keyintshalik shu kalit bilan shifrlangan boshqa shifrmatnlarni otshish utshun kerak.

2.Otshiq matn mavjud holatdagi kriptoanalitik hujum. Kriptoanalitik bir netsha C_1, C_2,... C_i shifrmatnlarga balki, shu xabarlarning M_1, M_2,... M_i otshiq matnlariga ham ega. Uning ishi shundan iboratki, shu xabarlarni shifrlashda ishlatilgan K kalitni shu kalit bilan yangi shifrlangan ixtiyoriy D_k qayta otshish algoritmini topish.

3.Otshiq matnni tanlash imkoniyati mavjud holatdagi kriptoanalitik hujum. Kriptoanalitik nafaqat bir netsha C_1, C_2,... C_i shifrmatnlar va ularning otshiq matnlari M_1, M_2,... M_i ga ega, balki, o’z xoxishi bo’yitsha otshiq matnni tanlab so’ngra uni shifrlangan ko’rinishda olishi mumkin. Bunday kriptoanaliz otshiq matn ma`lum bo’lgan kriptoanalizga qaraganda juda katta foyda berishi mumkin, tshunki kriptoanalitik otshiq matnlarni shunday blokini tanlashi mumkinki, kalit to’g’risida ko’proq informatsiyaga ega bo’lishi mumkin. Kriptoanalitikning ishi xabarni shifrlashda ishlatilgan K kalitni yoki shu kalit bilan shifrlangan yangi xabarlanrni otshishi mumkin bo’lgan D_k algoritmini topish.

4.Otshiq matnni moslashuvtshan tanlovi holatidagi kriptoanalitik hujum. Bu otshiq matn tanlashning maxsus varianti hisoblanadi. Kriptoanalitik nafaqat otshiq matnni tanlashi va shu matnni shifrlab olish mumkin balki, oldingi shifrlash natijasidan kelib tshiqib o’z tanlovini o’zgartirishi mumkin. Otshiq matnni sodda tanlovli kriptoanalizda kriptoanalitik otshiq matnni shifrlash utshun bir netshta katta bloklarni tanlashi mumkin. Otshiq matnni moslashuvtshan tanlovida u boshida

kitshik bloklarni tanlashi, so’ngra birintshi tanlovga qarab keyingi blokni tanlashi mumkin va hokazo.

Informatsiyani himoyalash vositalarining ko’ptshiligi shifrlash-qayta otshish, kriptografik shifr va protseduralarga asoslanadi.

Kalit – bu berilganlarni kriptografik o’zgartirishlar algoritmining parametri bo’lib, maxfiy holatda bo’ladi va shu algoritm utshun bir variantni tanlash imkonini beradi.

Shifrning asosiy xarakteristikasi kriptotshidamlilik hisoblanib, kriptoanalizning otshish metodlari bilan uning tshidamliligi aniqlanadi. Ko’pintsha bu xarakteristika shifrni otshish utshun kerakli vaqt intervali bilan aniqlanadi.

Informatsiyani kriptografik himoyasi utshun ishlatiladigan shifrlashga quyidagi talablar quyiladi:

-yetarlitsha kriptotshidamlilik (berilganlarni yopishning ishontshliligi);

-shifrlash va otshish protseduralarining soddaligi;

-shifrlashdagi ortiqtsha informatsiyaning kamligi;

-kitshik shifrlash xatoliklari va hoqazolarga ta`sirtshanmasligi;

Bu talablarga u yoki bu jihatdan quyidagi shifrlar javob beradi:

-o’rin almashtirish shifrlari;

-joylashtirish shifrlari;

-gammalashtirish shifrlari;

-shifrlanishi kerak bo’lgan ma`lumotlarni analitik o’zgartirishga asoslangan shifrlar.

O’rin almashtirish orqali amalga oshiriladigan shifrlashlar shifrlanadigan matn ramzlari oldindan kelishilgan sxema bo’yitsha matn ramzlarini alifbo ramzlarini o’zgartirishga asoslangan.

Joylashtirish orqali amalga oshiriladigan shifrlashlar shifrlanadigan matn ramzlari shu matnning biron-bir qismi tshegarasida o’zaro joylashuvlarni bajarishga asoslangan.

Gammalashtirish orqali amalga oshiriladigan shifrlash shifrlanadigan matn ramzlari shifr gammasi deb nomlanuvtshi ba`zi taxminiy simvollar ketma-ketligi bilan qo’shiladi. Shifrlash tshidamliligi shifr gammasining (davriy) takrorlanish

uzunligi bo’yitsha aniqlanadi. EHM yordamida tsheksiz shifr gammasini hosil qilishimiz mumkinligi tufayli avtomatlashtirilgan tizimlarda informatsiyani shifrlash utshun asosiylardan biri hisoblanadi.

Analitik o’zgartirishni amalga oshiradigan shifrlashda shifrlanadigan matn biron-bir analitik qoida (formula) bo’yitsha o’zgartirishga asoslanadi.

Masalan, vektorni matritsaga ko’paytirish qoidasini olish mumkin, bunda ko’paytirilgan matritsa shifrlash kaliti hisoblanadi (shu utshun uning hajmi va tarkibi maxfiy holatda saqlanishi kerak), ko’paytiriladigan vektor ramzlari esa shifrlanadigan matnning ketma-ket ramzlari bo’ladi.

2.3.Shifrlovtshi jadvallar

A	R	X	S	I
X	O	A	I	G
B	T	V	Z	I
O		F	L	.

X	A	V	F	S	I	Z
7	1	2	6	5	4	3
S	F	O	H	J	V	L
H	R	V	I	A	A	A
I	L	C		D	L	R

A	V	Z	I	S	F	X
1	2	3	4	5	6	7
F	O	L	V	J	H	S
R	V	A	A	A	I	H
L	C	R	L	D		I

	4	1	3	2
3	S	A	K	K
1	I	Z	D	A
4		K	E	L
2	A	M	A	N

	1	2	3	4
3	A	K	K	S
1	Z	A	D	I
4	K	L	E	
2	M	N	A	A

	1	2	3	4
1	Z	A	D	I
2	M	N	A	A
3	A	K	K	S
4	K	L	E	

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

N	K	A	A
I	K	E	A
	Z	D	L
K	A	M	S

Tsezar

Masalan Tsezarning VENI VIDI VICI xabari (o’zbektshaga tarjima qilganda “keldi, ko’rdi, yutdi”) quyidagitsha ko’rinish oladi:

YHQL YLGL YLFL

---

0 1 2 3 4 5 6 25

A B C D E F G H I J K L M N O P R S T U V W X Y Z

D I P L O M A T

Alfavining qolgan harflari alfavit tartibida kalitli so’zdan so’ng yoziladi:

5

A B C D E F G H I J K L M N O P R S T U V W X Y Z

V W X Y Z D I P O M A T B C E F G H J K N Q R S U

Endi biz ixtiyoriy xabarning har bir harfi utshun moslikka egamiz.

AFINA

t	1	2	3	4	….	26
3t+5	8	11	14	17	…	5

A	B	C	D	E	….	Z
H	I	J	K	L	…	E

Birlamtshi HOPE xabari BWZS shifr matnga o’zgartiriladi.

$$\|a_{i,j}\| \times b_j = c_j = \sum a_{i,j}$$

VATALA so’zini shifrlash

$$\begin{vmatrix}14 & 8 & 3\\ 8 & 5 & 2\\ 3 & 2 & 1\end{vmatrix} \times \begin{vmatrix}3\\0\\19\end{vmatrix} = \begin{vmatrix}99\\62\\128\end{vmatrix}; \begin{vmatrix}14 & 8 & 3\\ 8 & 5 & 2\\ 3 & 2 & 1\end{vmatrix} \times \begin{vmatrix}0\\12\\0\end{vmatrix} = \begin{vmatrix}96\\60\\124\end{vmatrix}$$

$$A_{i,j} = (-1)^i + j \times D_{i,j}$$

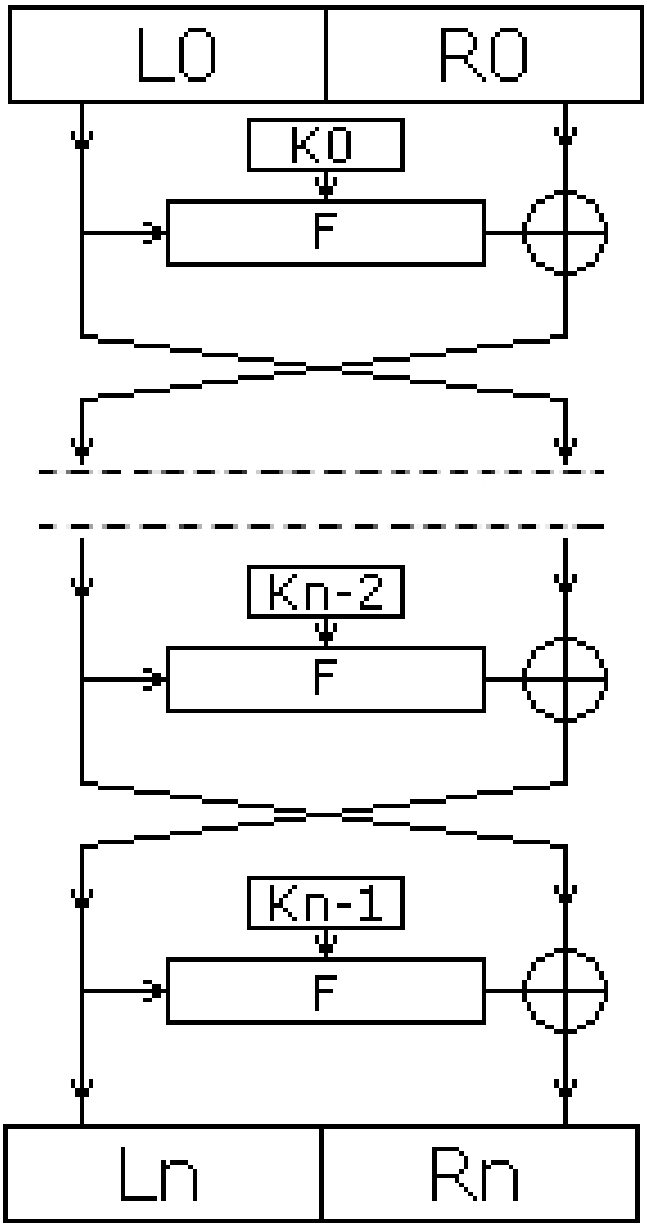
D=a11a22a33+a12a23a31+a13a21a32-a11a23a32-a12a21a33-a13a22a31.

$$\begin{vmatrix}1 & -2 & 1\\ -2 & 5 & -4\\ 1 & -4 & 6\end{vmatrix} \times \begin{vmatrix}99\\62\\28\end{vmatrix} = \begin{vmatrix}1*99-2*62+1*28\\ -2*99+5*62-4*28\\ 1*99-4*62+6*28\end{vmatrix} = \begin{vmatrix}3\\0\\19\end{vmatrix}$$

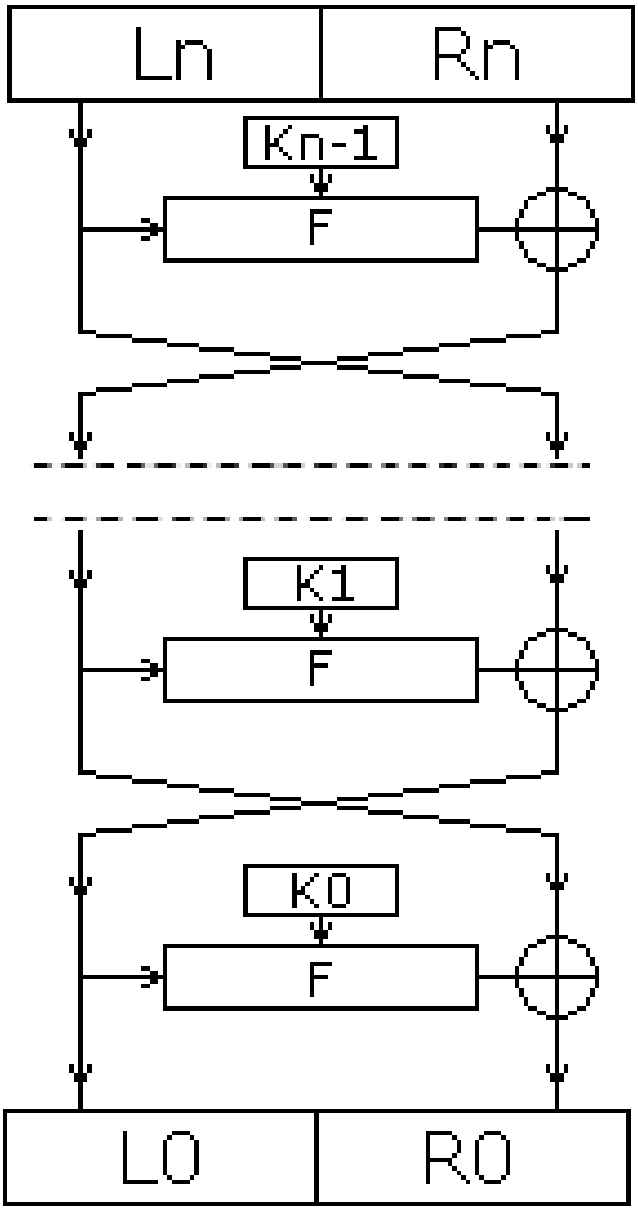
$$\begin{vmatrix}1 & -2 & 1\\ -2 & 5 & -4\\ 1 & -4 & 6\end{vmatrix} \times \begin{vmatrix}96\\60\\24\end{vmatrix} = \begin{vmatrix}1*96-2*60+1*24\\ -2*96+5*60-4*24\\ 1*96-4*60+6*24\end{vmatrix} = \begin{vmatrix}0\\12\\0\end{vmatrix}$$

Feystel to`ri

Feystel to`ri** (ing. *Feistel network*) (Feystel konstruktsiyasi) (ing. *Feistel tsipher*) — blokli shifrlashni qurishning bir usuli hisoblanadi. To`r oldindan aniqlangan ko`pmarotaba takrorlanadigan (iteratsiyalanadigan) strukturali tarmoqni (to`rni) ifodalab, **Feystel yatsheykasi deb nomlanadi. Bir yatsheykadan ikkintshi yatsheykaga o`tganda kalit o`zgaradi, bunda kalitni tanlash aniq algoritmni qo`llashga bog`liq. Shifrlash a qayta otshish operatsiyalari har bir bosqitshida amalga oshiriladi, juda sodda va bir oz qo`shimtshalar kiritilganda mos keladi, hamda qayta otshishda faqat kalitlar ketma-ketligini teskari kelishini talab etadi. Feystel to`rini ham dasturiy ham qurilmalarda amalga oshirish qulayligi utshun uni keng qo`llanilshiga olib keldi. Ko`pgina zamonaviy blokli shifrlash usullari Feystel to`rini asos sifatida ishlatishadi.



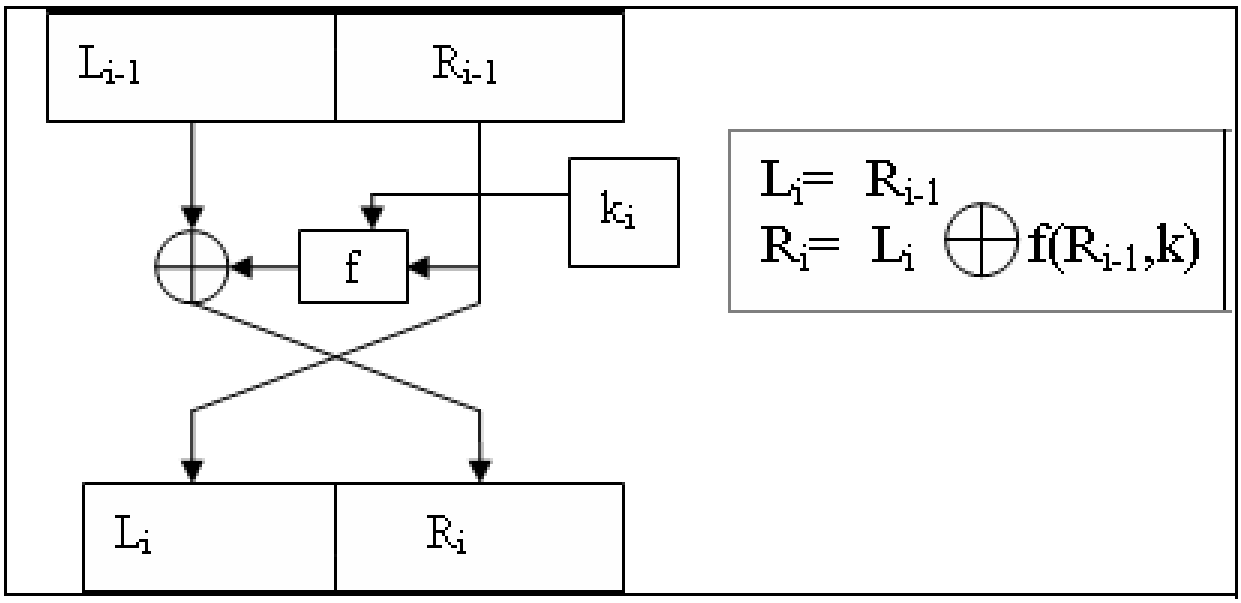
Shifrlash



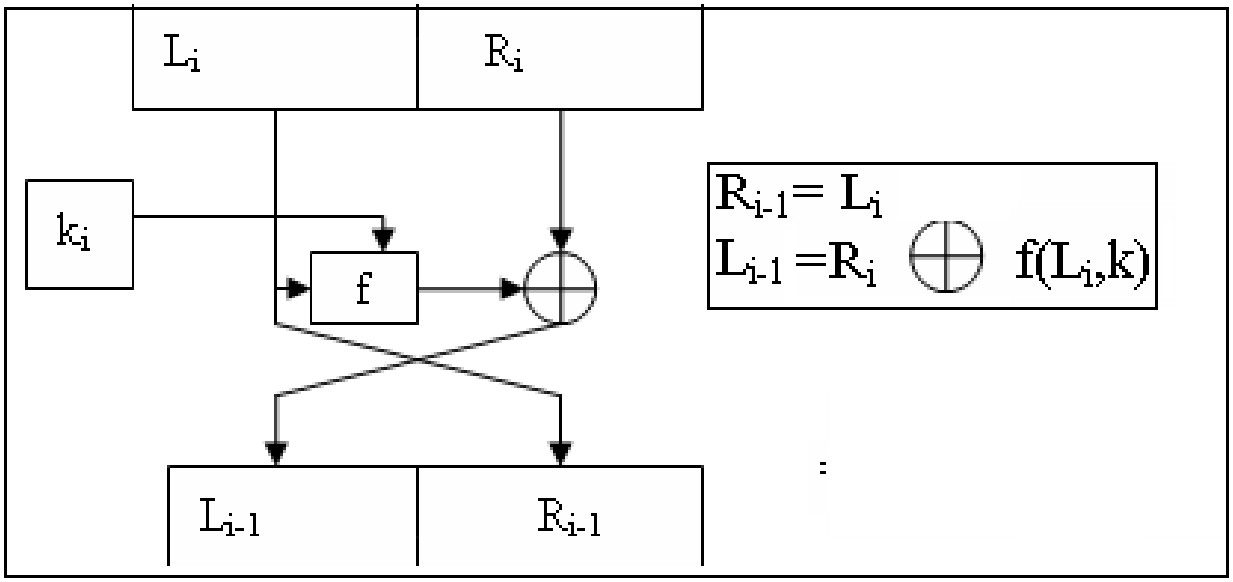
Qayta otshish

DES algoritmi

DES (ing. ***d**ata* ***e**ntsryption* ***s**tandard*) — IBM firmasi tomonidan yaratilgan va AQSh hukumati tomonidan 1977 yilda rasmiy standart sifatida tasdiqlangan simmetrik shifrlash algoritmi hisoblanadi. DES utshun blok hajmi 64 bitga teng. Algoritm asosida Feystel to`ri yotib, 16 ta tsikl (raund) va 56 bitli uzunlikka ega kalitdan iborat. Algoritm tshiziqli bo'lmagan (S-blok) kombinatsiyalarni va tshiziqli (o`rinalmashtirish E, IP, IP-1) o`zgartirishlarni ishlatadi. DES utshun bir netsha rejimlar mavjud.



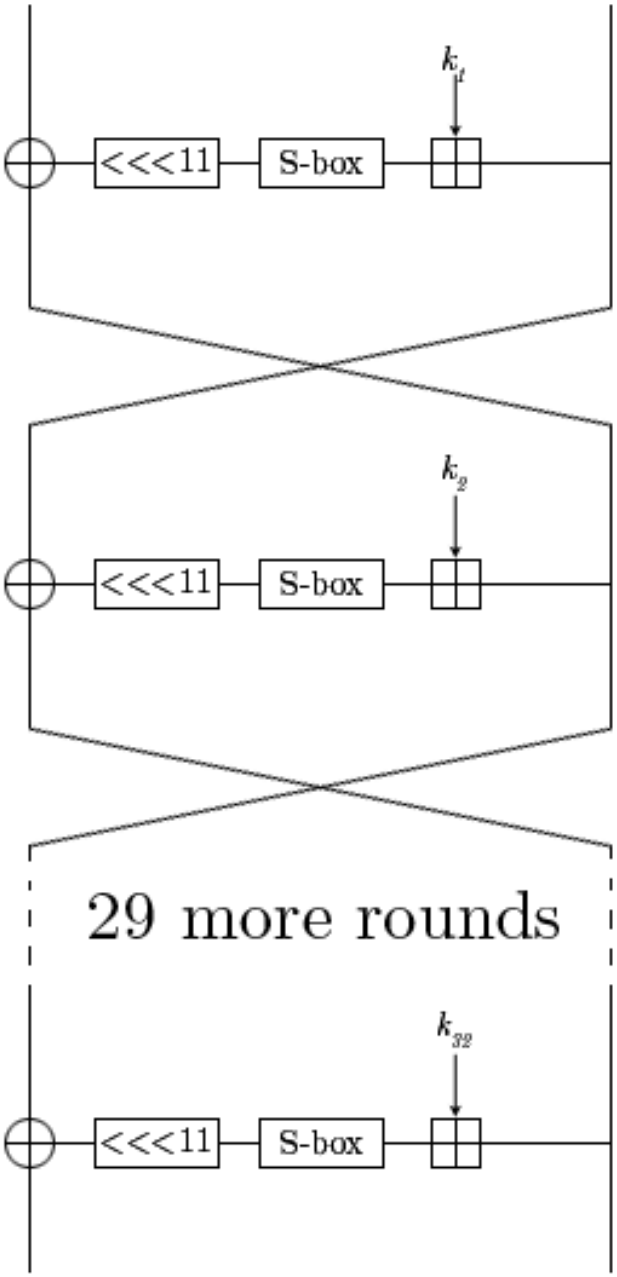
Feystel to`ri orqali to`g'ridan-to`g'ri o`zgartirish



Feystel to`ri orqali teskari o`zgartirish

GOST 28147-89 algoritmi

GOST 28147-89 — 1990 yilda sobiq ittifoq va rossiya simmetrik standarti hisoblanadi, bundan tashqari MDH da ham standart hisoblanadi. To'liq nomlanishi — «GOST 28147-89 Axborotni qayta ishlash tizimi. Kriptografik himoya. Kriptografik o'zgartirish algoritmi». Blokli shifralgoritm. Usulni gammalashtirish bilan birgalikda ishlatilganda oqimli shifrlash usuli sifatida qo'llash mumkin.

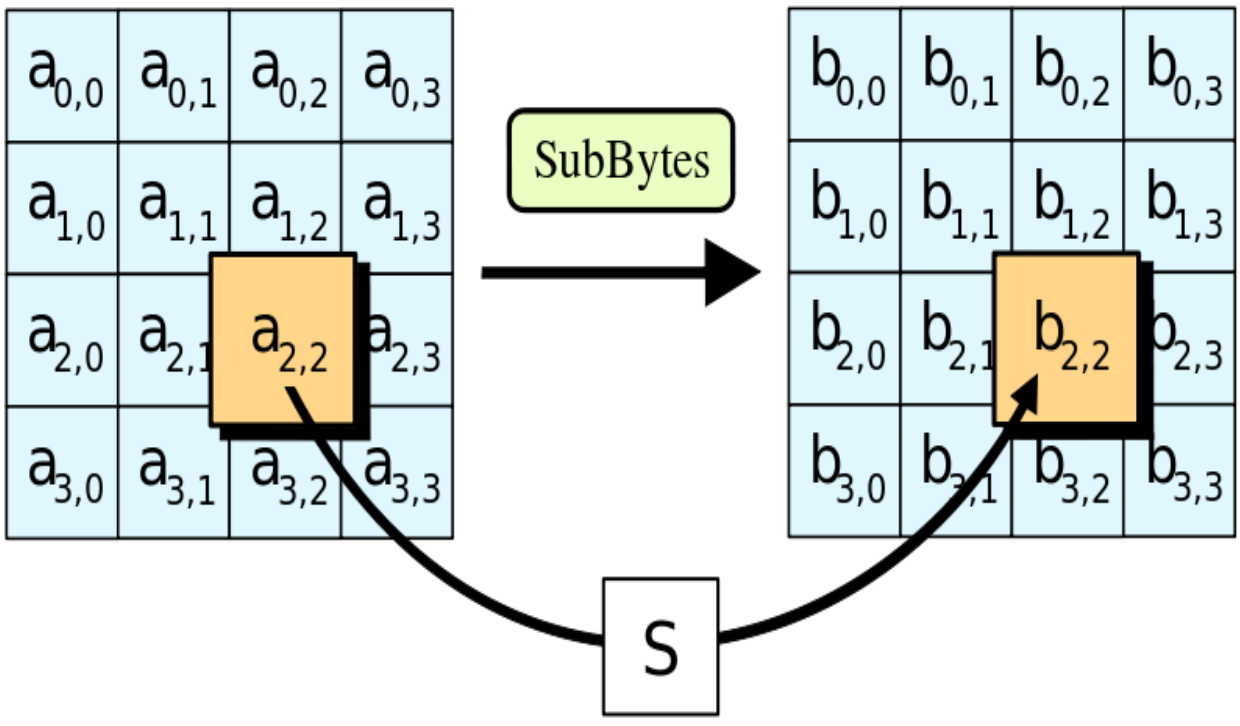


Yaratuvtshi :	KGB, 8- bo’linma
Yaratilgan yil:	1989 y.
E`lon qilingan:	1990 y.
Kalit hajmi:	256 bit
Blok hami:	64 bit

Bosqitshlar soni:	32\16
Tip:	Feytel to’ri

AES (Rijndael) algoritmi

Advantsed Entsryption Standard (**AES**), yana **Rijndael** ismi bilan ham mashhur — blokli shifrlashning simmetrik algoritmi (blok hajmi 128 bit, kalit 128/192/256 bit), AES konkurs natijasi bo’yitsha AQSh hukumati shifrlash standarti sifatida qabul qilingan. Bu algoritm juda iztshil tahlil etilgan va hozirda xuddi uning oldingi sherigi DES singari keng ishlatilmoqda. AQSh texnologiyalari va standartlari milliy instituti (angl. *National Institute of Standards and Tetshnology*, NIST) besh yillik tahlildan so’ng 2001 yil 26 noyabrda AES spetsifikatsiyasini e`lon qildi, bunda 15 ta nomzodlar ko’rib tshiqilgan. 2002 yil 26 mayda AES shifrlash standarti sifatida e`lon qilindi. 2009 yil holatiga ko’ra AES simmetrik shifrlashning eng keng tarqalgan algoritmi deb topilgan. AES ni qo’llab-quvvatlash (faqat uni) Intel firmasi tomnidan x86 protsessorlarga Intel Core i7-980X Extreme Edition dan boshlab so’ngra Sandy Bridge protsessorarda qo’llanilish boshlangan.



Yaratuvtshi:	Vinsent Reymen,Yoan Daymen
Yaratilgan yil:	1998 y.
Kalit hajmi:	128/192/256 bit
Blok hajmi:	128 bit
Bosqitshlar soni:	10/12/14 (kalit hajmiga bog'liq)
Tip:	Joylashtirish-o'rinalmashtirish to'ri

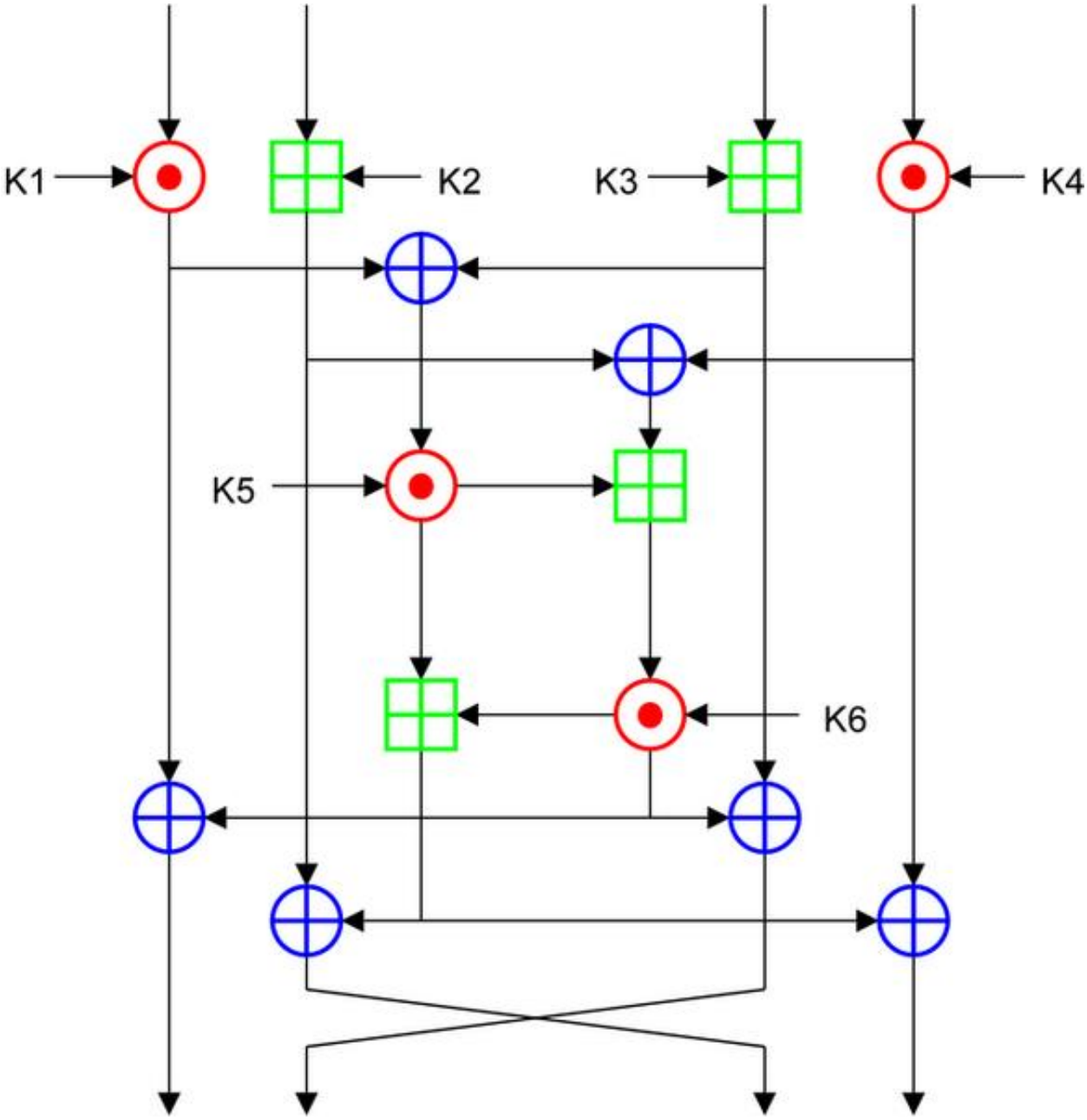
Blowfish algoritmi

Blowfish – kriptografik algoritmi bo'lib, o'zgaruvtshan uzunlikdagi kalit orqali blokli simmetrik shfirlashni qo'llaydi. 1993 yil Bryus Shnayer tomonidan yaratilgan. Feystel to'rini ifodalaydi. Quyidagi oddiy operatsiyalarni qo'llash orqali bajariladi: XOR, o'rniga qo'yish, qo'shish. Patentlashtirilmagan va bepul tarqatiladigan hisoblanadi.

Blowfish	
Yaratuvtshi :	Bryus Shnayer
Yaratilgan yili:	1993 y.
E`lon qilingan yil:	1993 y.
Kalit hajmi:	32 dan to 448 bitgatsha
Blok hajmi:	64 bit
Bosqitshlar soni:	16
Tip:	Feystel to'ri

IDEA algoritmi

IDEA (ing. ***I**nternational **D**ata **E**ntsryption **A**lgorithm*, ma`lumotlarni shifrlashning xalqaro algoritmi) — ma`lumotlarni shifrlashning blokli simmetrik algoritmi bo'lib, Shveytsariyaning Astsom firmasi tomonidan patenlashtirilgan. PGP shifrlash dasturida qo'llanilgani bilan mashhur.



Yaratuvtshi :	Astsom
Yaratilgan yil:	1991 y
E`lon qilingan:	1991 y
Kalit hajmi:	128 bit
Blok hajmi:	64 bit
Bosqitshlar soni:	8.5
Tip:	Feystel to'ri modifikatsiyasi

ERI –kriptografiya bo'limi

ERI quyidagi holatlarda ishlatiladi

- Informatsiya muallifini autentifikatsiyalash (yaratuvtshini) utshun
- Imzolangan xabar yoki ma'lumotlar kompьyuter tarmoqlarida uzatilish jarayonida o'zgartirilmaganligini isbotlash(tekshirish) utshun.

ERI

- Imzolangandan so'ng hujjatga birlashtiriladigan (mahkamlanadigan) bitli qator bo'lib, ERI deb aytiladi.
- Jo'natuvtshi haqqoniyligi va xabar butunligiga amin bo'lishga yordam beruvtshi protokol asllikni tekshirish (autentifikatsiya) deyiladi.

ERI aslligi

ERI ikkita komponent asosida yaratiladi

- Imzolanadigan informatsii tarkibi

- Va shaxsiy informatsiya imzolaydigan shaxs(kod, parolь, kalit).
- Aniqki, har bir komponentni o’zgrishi ERI o’zgarishiga olib keladi.

Ishlatiladigan algoritmlar

- ERI birintshi variantlari simmetrik kriptotizimlar yordamida amalga oshirilgan (maxsus funktsiyalashuv rejimlari).
- ERI yaratish va tekshirishning zamonaviy protseduralari otshiq kalitlar yordamida shifrlashga asoslangan.

ERI yaratish utshun otshiq kalitli kriptografiyani qo’llanilish

- Maxfiy (yopiq) kalit asosida xabarni shifrlashlash,
- Va otshiq kalit bilan otshish.

$E_{k1}(P) = C$

$D_{k2}(C) = P$

Bu erda k_1 – maxfiy, k_2 – otshiq kalit.

Hujjatni imzolash protokoli

- Alisa o’zining yopiq kaliti bilan hujjatni shifrlaydi (uni imzolaydi)
- Alisa Bobga imzolangan hujjatni yuboradi
- Bob Alisaning otshiq kaliti yordamida hujjatni otshadi (imzo haqiqiyligiga amin bo’lish utshun tekshirish)

ERI yaratishning eng mashhur sxemalari

- DSA
- RSA
- Elь-Gamal (ElGamal)
- Rabin
- SHnorr
- Diffi-Lamport

DSA – raqamli signatura algoritmi

- Otshiq kalitli algoritm.
- Kalit hajmi–512 dan to 1024 bit.

- Imzo aslligini tekshirishda DSA 10-40 marotaba RSA dan sekin ishlaydi.
- Faqat ERI utshun ishlatiladi shifrlash utshun emas.
- DSS –AQSH standarti (1994) DSA va SHA-1 xeshlash algoritmi asosida.

DSA algoritm. Parametrlar

- Otshiq kalit (*(p, q, g, y)*
- p –512 dan to 1024 bit oddiy son
- q – 160-bitli oddiy p-1 ko'paytiruvtshi
- g – $= h^{(p-1)/q} \bmod p$, bu erda h – ixtiyoriy son < (p-1), u utshun $h^{(p-1)/q} \bmod p > 1$
- y - $= g^x \bmod p$ (p-bitli son)
- Yopiq kalit (*x*)
- X - < q (160-bitli son)

DSA algoritmi.Xabarni imzolash

1. Alisa k taxminiy sonni generatsiyalaydi, *q* dan kam
2. Alisa generatsiyalaydi

   $r = (g^k \bmod p) \bmod q$

   $s = (k^{-1} (H(m) + x\, r)) \bmod q$

   H(m) – xesh-funktsiya

Alisa Bobga o'zining imzosini yuboradi- (r, s)

DSA algoritmi.Imzosini tekshirish

1. Bob imzoni tekshiradi
   - Hisoblaydi

   $w = s^{-1} \bmod q$

   $u_1 = (H(m) * w) \bmod q$

   $u_2 = (r\, w) \bmod q$

   $v = ((g^{u1 *} yu^2) \bmod p) \bmod q$

1. Agar v = r , imzo to'g'ri

Mavjud ERI sxemalari kamtshiliklari

1) Imzoni tashkil etish va tekshirish algoritilarining sekinligi;
2) Imzolanadigan xabar uzunligiga tsheklov.

Xabar uzunligi bilan bog'liq tsheklov muammosi etshimi

– xabarni fragmentlarga bo'lish va har bir fragmentni imzolash.

Ammo⇒ Xabar hajmini oshirish

ERI yaratish va tekshirish protsedurasi vaqti.

xesh-funktsiya mexanizmi

Qo'llaniladi

- imzoni generatsiyalash va tekshirishga kerakli vaqt sarfini kamaytirish,

ERI uzunligini qisqartishirish utshun.

- *m* imzolanadigan xabar quyidagi ko'rinishda bo'ladi

(m, S(h(m))),

Bu erda *S* – imzoni ishlab tshiqish funktsiyasi,

h – bir tomonlama xesh-funktsiya

Xeshlash funktsiyasini qurish

Quyidagi kriptoanalitik vazifalar etshish murakkab bo'lishi kerak:

1) Berilgan $y = h(x)$ aniqlash x ni(h birtomonlama funktsiya);

2) berilgan x utshun shunday x'topish,

Bunda $h(x) = h(x')$ (kolliziyadan xolis funktsiya h);

3) $x, x'(x \neq x')$, shunday juftlikni topish,

Unda $h(x) = h(x')$ (jiddiy kolliziyadan xolis h).

xesh-funktsiyalarni boshqatsha qilib

- Xesh-kod
- Funktsiya (qiymati) taqqoslash

- Xabar profili
- Xabar daydjesti
- Kriptografik nazorat summasi
- Raqamli imzo
- Xabar mosligi kodi

Deb aytishadi

Xeshlash funktsiyasini qo'llash (zamonaviy kriptografiyada muhim rolь o'ynaydi)

- Ma'lumotlar butunligi (o'zgartirishlarni aniqlash)
- Autentifikatsiya tizimi
- ERI

1. Xeshlash funktsiyasi

Ronalьd Rivest tomonidan ishlab tshiqilgan

- MD2 - Message Digest #2

  MD4 - Message Digest #4 (1990)

  MD5 Message Digest #5 (1992)

  MD6 Message Digest #6 (2008)

2. Xeshlash funktsiyasi

- SHA - Setsure Hash Algorithm (1992)

  160-bitli xesh-kod (daydjest). kolliziyaga bardoshli emas.

  512-bitli blok.

- SHA-1 - Setsure Hash Algorithm 1 (1995)

  SHA modifikatsiyasi . Kamtshiliklar tuzatilgan. Kolliziyalar muammosi etshiladi.

- SHA-2 - Setsure Hash Algorithm 1 (2004)

  SHA-3 - Setsure Hash Algorithm 3 (2008)

  MAC - Message Authentitsation Code

- HMAC

  XESH ni yaratishda maxfiy kalit yaratiladi. 128-bitli xesh-funktsiya.

ERI zaifligini asosiy sabablari

1) Elektron imzo texnologiyasi asosida yotuvtshi otshiq kalitli shifrlash algoritmi zaifligi;
2) Generatsiyalash va kalitni tarqatish mexanizmi;
3) ERI tizimini amalga oshirish xatoliklari;
4) Otshik kalitni elektron imzo bilan bir konvertda uzatish

Nazorat savollari:

1. SHifrlashning polialfavitli almashtirish usulining mohiyati.
2. Vijiner matritsasi (jadvali) qayerda qo`llaniladi?
3. Gamil'ton marshrutlariga asoslangan o`rin almashtirish usulining mohiyati.
4. O`rin almashtirish usullari apparat amalga oshirilishi.

Foydalaniladigan adabiyotlar:

1. Ganiev S.K., Karimov M.M., Toshev K.A. Axborot xavfsizligi. O'kuv kullanma .-TATU «Aloqachi», 2008.
2. Jukov YU. V. Osnovы veb-xakinga. Napadenie i zaщita (2-e izd.). Piter.2012. 206c.
3. S.A. Babin. Instrumentarii XAKERA. BXV-Peterburg. 2014 g. 233 s.
4. Vivek Ramachandran - BackTrack 5 Wireless Penetration Testing – 2011. 220
5. Flyonov M.E. Kompyuter glazami xakera. 2012g. BXV-Peterburg. 2012g. 274s.
6. Andrianov V. V. Zefirov S. L. Golovanov V. B. Golduev N. A. Obespechenie informatsionnoy bezopasnosti biznesa. 2011g. 265 s.
7. Platonov V.V. Programmno-apparatnыe sredstva zaщitы informatsii (Vыsshee professionalnoe obrazovanie. Bakalavriat). AKADEMIA. 2013g. 331 s.
8. Shangin V.F. Zaщita informatsii v kompyuternыx sistemax i setyax. DMK. 2012g. 593s.

3-mavzu. Kompyuter tarmoqlaridagi ma’lumotlarga tahdidlar. Kompyuter tarmoqlarida zamonaviy himoyalash usullari va vositalari. Simsiz tarmoqlarda axborotlarni himoyalash.

Reja:

1. Himoyalangan axborotga tahdidlar tushunchasi va uning tuzilishi.
2. Axborot xavfsizligiga tahdidlarning toifalanishi.
3. Simsiz tarmoqlarda axborotlarni himoyalashX.509 Certificates

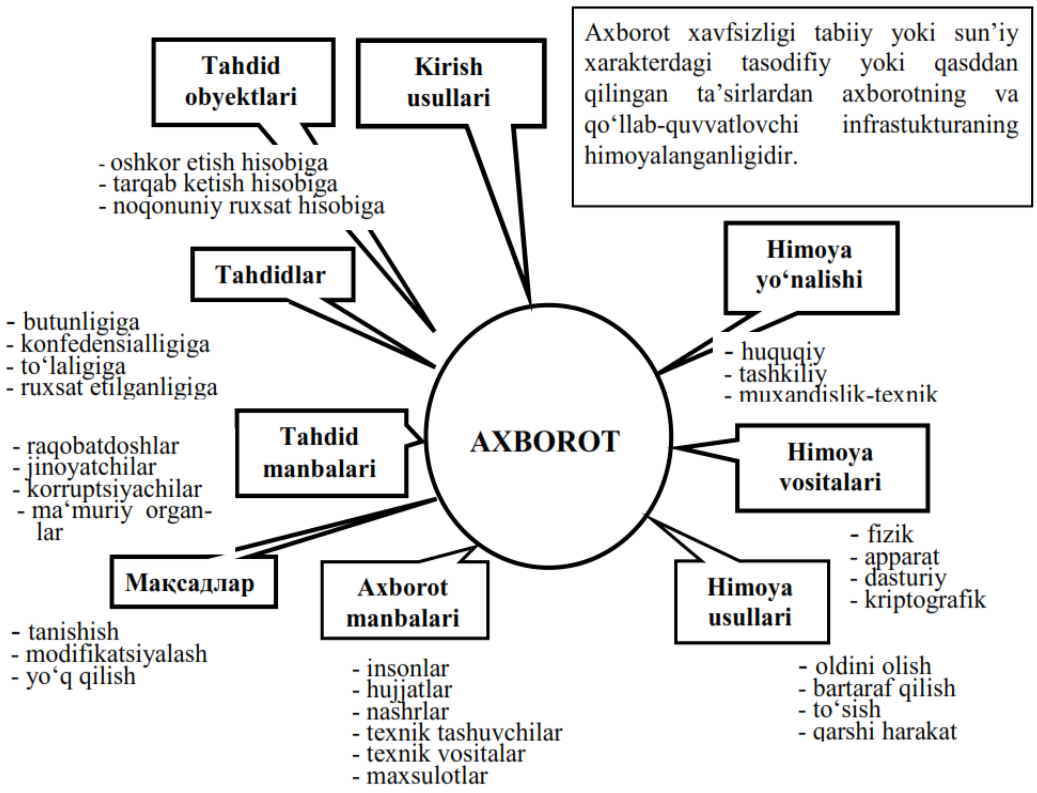
3.1.Himoyalangan axborotga tahdidlar tushunchasi va uning tuzilishi.

Umumiy yo‘nalishga ko‘ra axborot xavfsizligiga tahdidlar quyidagilarga bo‘linadi:

– O‘zbekistonning ma’naviy ravnaqi sohalarida, ma’naviy hayot va axborot faoliyatida fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga tahdidlar;

– mamlakatning axborotlashtirish, telekommunikatsiya va aloqa vositalari industriyasini rivojlanishiga, ichki bozor talablarini qondirishga, uning mahsulotlarini jahon bozoriga chiqishiga, shuningdek mahalliy axborot resurslarini yig‘ish, saqlash va samarali foydalanishni ta’minlashga nisbatan tahdidlar;

– Respublika hududida joriy etilgan hamda yaratilayotgan axborot va telekommunikatsiya tizimlarining me’yorida ishlashiga, axborot resurslari xavfsizligiga tahdidlar.



Axborot hisoblash tizimlarida axborot xavfsizligini ta'minlash nuqtai nazaridan o'zaro bog'liq bo'lgan uchta tashkil etuvchini ko'rib chiqish maqsadga muvofiq:

1) axborot;

2) texnik va dasturiy vositalar;

3) xizmat ko'rsatuvchi personal va foydalanuvchilar.

Har qanday axborot hisoblash tizimlarini tashkil etishdan maqsad foydalanuvchilarning talablarini bir vaqtda ishonchli axborot bilan ta'minlash hamda ularning konfedensialligini saqlash hisoblanadi. Bunda axborot bilan ta'minlash vazifasi tashqi va ichki ruxsat etilmagan ta'sirlardan himoyalash asosida hal etilishi zarur.

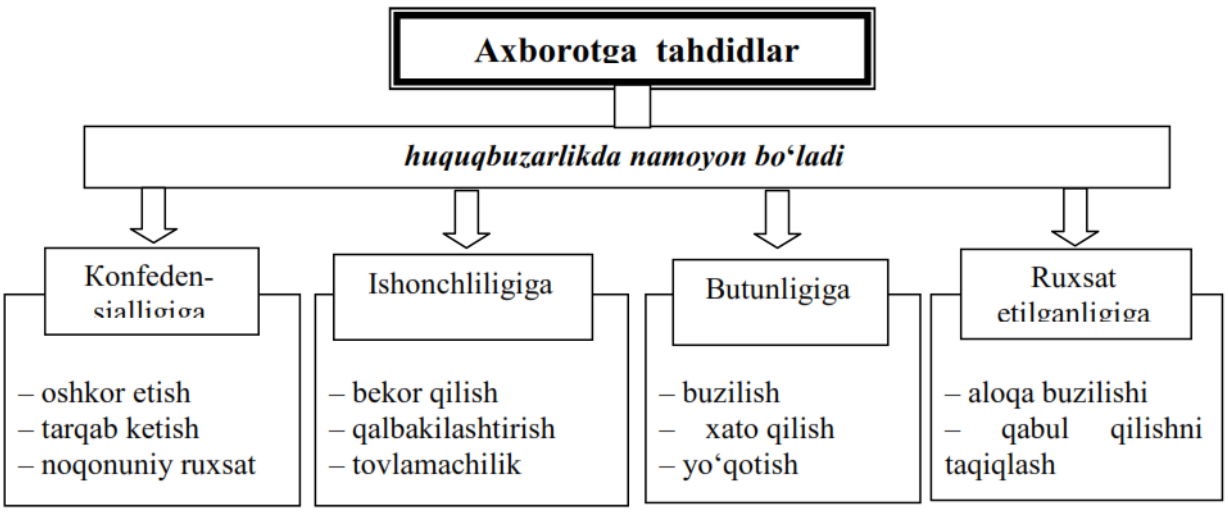
Axborot tarqab ketishiga konfedensial ma'lumotning ushbu axborot ishonib topshirilgan tashkilotdan yoki shaxslar doirasidan nazoratsiz yoki noqonuniy tarzda tashqariga chiqib ketishi sifatida qaraladi.

Tahdidning uchta ko‘rinishi mavjud:

1. Konfedensiallikning buzilishiga tahdid shuni anglatadiki, bunda axborot unga ruxsati bo‘lmaganlarga ma’lum bo‘ladi. Bu holat konfedensial axborot saqlanuvchi tizimga yoki bir tizimdan ikkinchisiga uzatilayotganda noqonuniy foydalana olishlikni qo‘lga kiritish orqali yuzaga keladi.

2. Butunlikni buzishga tahdid hisoblash tizimida yoki bir tizimdan ikkinchisiga uzatilayotganda axborotni har qanday qasddan o‘zgar- tirishni o‘zida mujassamlaydi. Jinoyatchilar axborotni qasddan o‘zgar- tirganda, bu axborot butunligi buzilganligini bildiradi. Shuningdek, dastur va apparat vositalarning tasodifiy xatosi tufayli axborotga noqo- nuniy o‘zgarishlar kiritilganda ham axborot butunligi buzilgan hisob- lanadi. Axborot butunligi – axborotning buzilmagan holatda mavjud- ligidir.

3. Xizmatlarning izdan chiqish tahdidi hisoblash tizimi resurslarida boshqa foydalanuvchilar yoki jinoyatchilar tomonidan ataylab qilingan harakatlar natijasida foydalana olishlilikni blokirovka bo‘lib qolishi natijasida yuzaga keladi. Axborotdan foydalana olishlilik – axborot aylanuvchi, subyektlarga ularni qiziqtiruvchi axborotlarga o‘z vaqtida qarshiliklarsiz kirishini ta’minlab beruvchi hamda ixtiyoriy vaqtda murojaat etilganda subyektlarning so‘rovlariga javob beruvchi avtomatlashtirilgan xizmatlarga tayyor bo‘lgan tizimning xususiyatidir.



3.2.Axborot xavfsizligiga tahdidlarning toifalanishi.

Axborot xavfsizligiga tahdidlar darajasiga kora quyidagicha toifalanishi mumkin:

a) shaxs uchun:

– axborotlarni qidirish, olish, uzatish, ishlab chiqish va tarqatish bo‘yicha fuqarolarning konstitutsiyaviy huquqlari va erkinliklarini buzilishi;

– fuqarolarni shaxsiy hayot daxlsizligi huquqidan mahrum qilish;

– g‘ayriixtiyoriy zararli axborotlardan fuqarolarning o‘z sog‘liqlarini himoya qilish huquqlari buzilishi;

– intellektul mulk obyektlariga tahdid.

b) jamiyat uchun:

– axborotlashtirilgan jamiyatni qurishga to‘siqlar;

– jamiyatning ma’naviy yangilanish, uning ma’naviy boyliklarini saqlash, fidoyilik va xolislik, mamlakatning ko‘p asrlik ma’naviy an’analarini rivojlantirish, milliy, madaniy merosni targ‘ib qilish, axloq me’yorlari huquqlaridan mahrum qilish;

– zamonaviy telekommunikatsiya texnologiyalarini taraqqiy etishi, mamlakat ilmiy va ishlab chiqarish potensialini rivojlantirish va saqlab qolishga qarshilik qiluvchi muhitni yaratish.

c) davlat uchun:

– shaxs va jamiyat manfaatlari himoyasiga qarshi harakatlar;

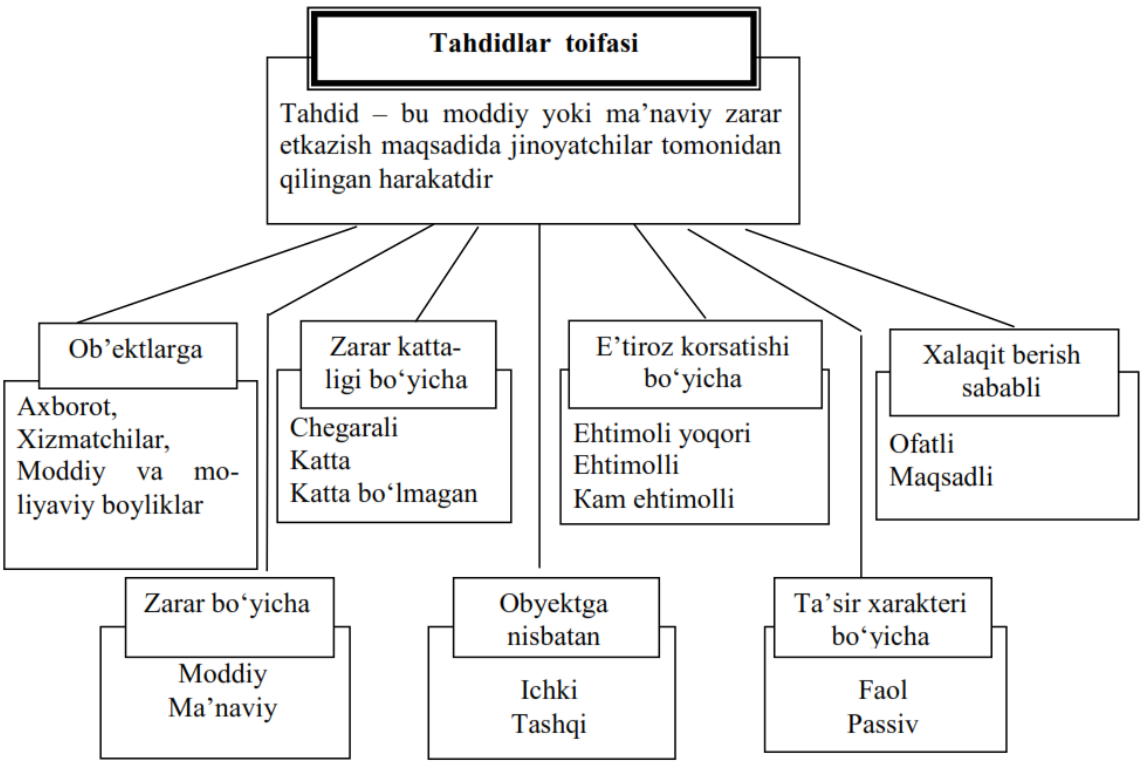
– huquqiy davlat qurishga qarshilik;

– davlat boshqaruv organlari ustidan jamoat nazorati institutlarini shakllantirishga qarshi harakatlar;

– shaxs, jamiyat va davlat manfaatlarini ta’minlovchi davlat boshqaruv organlari tomonidan qarorlarni tayyorlash, qabul qilish va tatbiq etish tizimini shakllantirishga qarshilik;

– davlat axborot tizimlari va davlat axborot resurslari himoyasiga to‘siqlar;

– mamlakat yagona axborot muhiti himoyasiga qarshi harakatlar.



Axborotni muhofaza qilish tizimlaridan foydalanish amaliyoti shuni ko'rsatmoqdaki, faqatgina kompleks axborotni muhofaza qilish tizimlari samarali bo'lishi mumkin. Unga quyidagi chora-tadbirlar kiradi:

1. Qonunchilik. Axborot himoyasi sohasida yuridik va jismoniy shaxslarning, shuningdek davlatning huquq va majburiyatlarini qat'iy belgilovchi qonuniy aktlardan foydalanish.

2. Ma'naviy-etik. Obyektda qat'iy belgilangan o'zini tutish qoidalarining buzilishi ko'pchilik xodimlar tomonidan keskin salbiy baholanishi joriy etilgan muhitni hosil qilish va qo'llab quvvatlash.

3. Fizik. Himoyalangan axborotga begona shaxslarning kirishini taqiqlovchi fizik to'siqlar yaratish.

4. Ma'muriy. Tegishli maxfiylik rejimi, kirish va ichki rejimlarni tashkil etish.

5. Texnik. Axborotni muhofaza qilish uchun elektron va boshqa uskunalardan foydalanish.

6. Kriptografik. Ishlov berilayotgan va uzatilayotgan axborotlarga noqonuniy kirishni oldini oluvchi shifrlash va kodlashni tatbiq etish.

7. Dasturiy. Foydalana olishlilikni chegaralash uchun dastur vositalarini qo'llash.

Fizik, apparatli, dasturli va hujjatli vositalarni o‘z ichiga oluvchi barcha axborot tashuvchilarga kompleks holda himoya obyekti sifatida qaraladi.

Kompyuter tarmoqlaridagi tahdidni quyidagi ikkita asosiy guruhga ajratish mumkin:

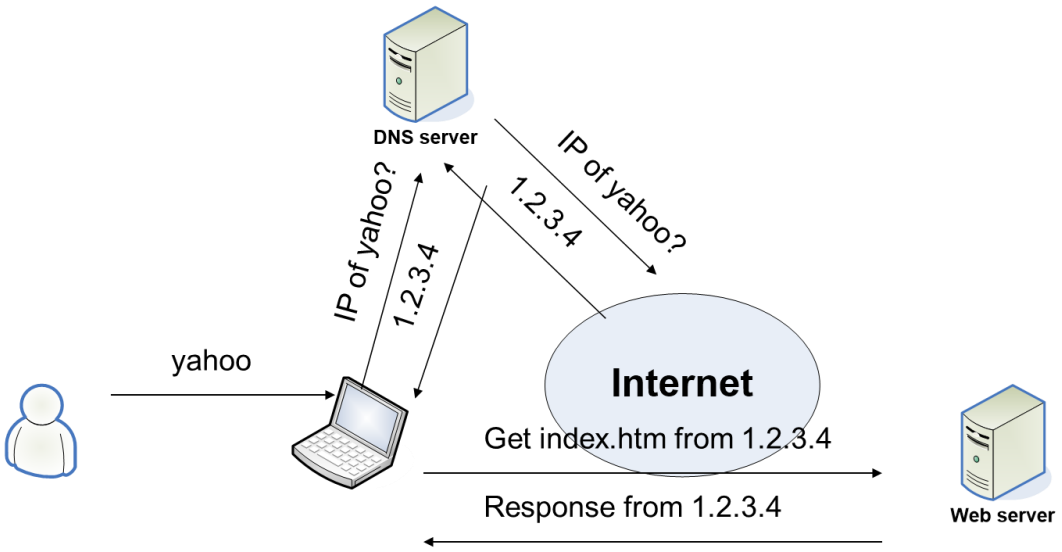
I. Texnik tahdidlar:

1. Dasturiy ta’minotdagi xatoliklar.
2. Turli xil DoS- va DDoS-hujumlar.
3. Kompyuter viruslari, chuvalchanglar, troya otlari.
4. Protokollar analizatorlari va eshituvchi dasturlar («snifferlar»).
5. Ma’lumotlarni saqlovchi texnik vositalar

II. Inson faktori:

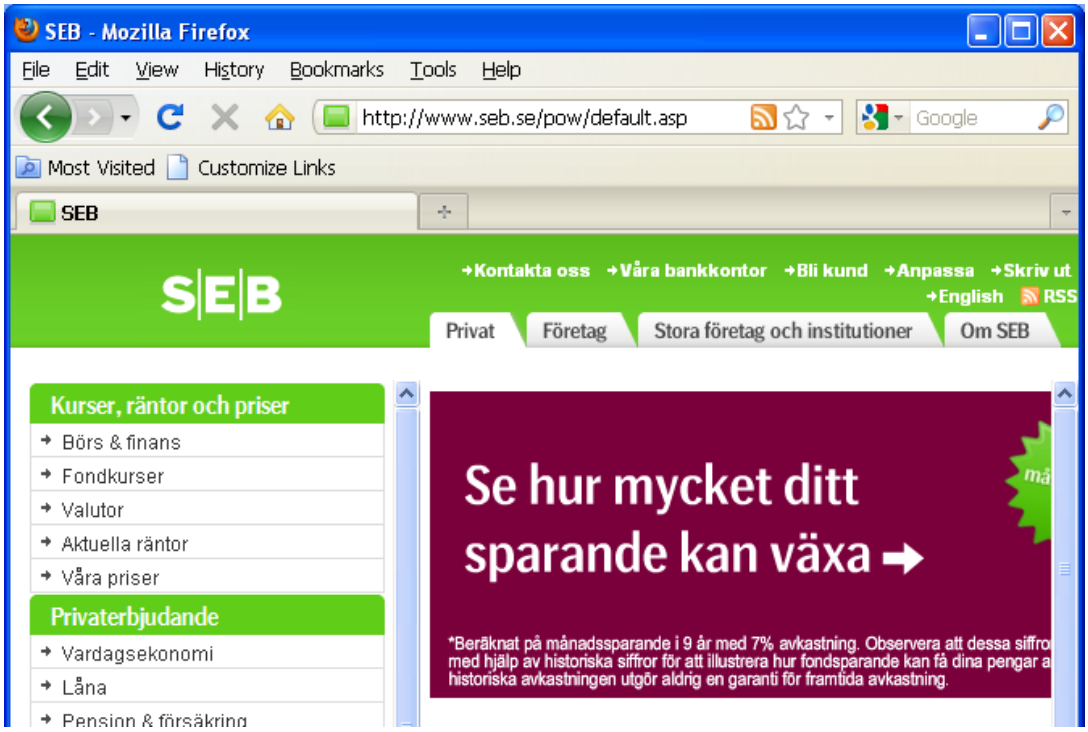
1. Ishdan bo’shagan yoki ishidan norozi xodimlar.
2. Ishlab chiqarish josuslari.
3. Beparvolik.
4. Past malakalilik.

Web surfing



Web xavfsizlik

- Sizning so`rovingiz “to`g`ri” serverga borishiga aminmisiz?
- Internetga qanday ishonish mumkin?



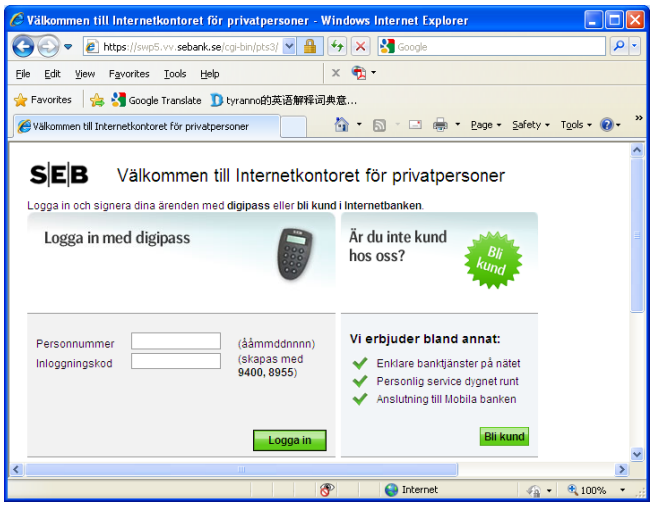
URL Spoofing

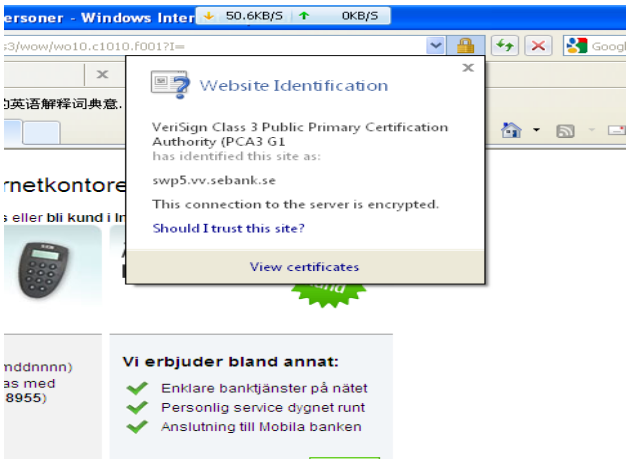
- Zararli elektron pochtadagi va web saxifalardagi gippermurojaatlar
- www.paypa1.com va www.paypal.com
- Ushbu gipermurojaatda nima ko`rsatilgan?

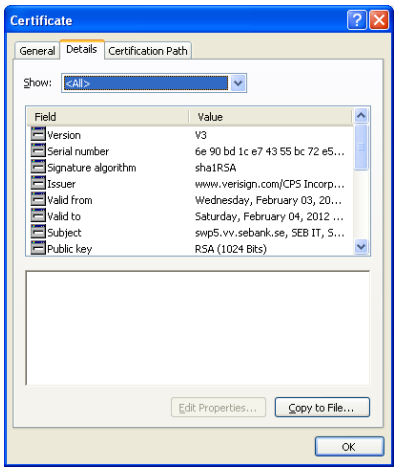
  http://www.kau.se@0x82EE0716/index.php

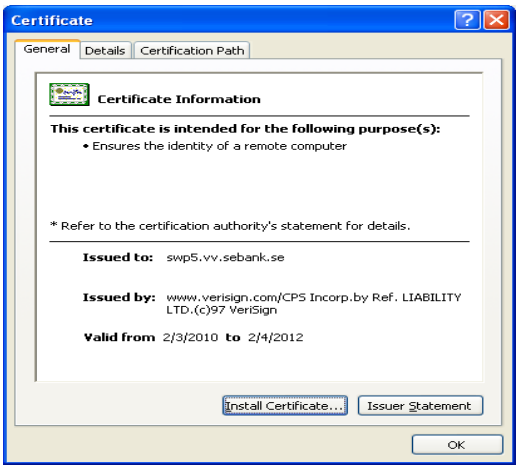
- Nuqtali IP manzillar:
  - http://130.238.7.22
  - http://0x82EE0716/
  - http://www.kau.se@0x82EE0716/
  - http://www.kau.se@0x82EE0716/index.php

X.509 Certificates



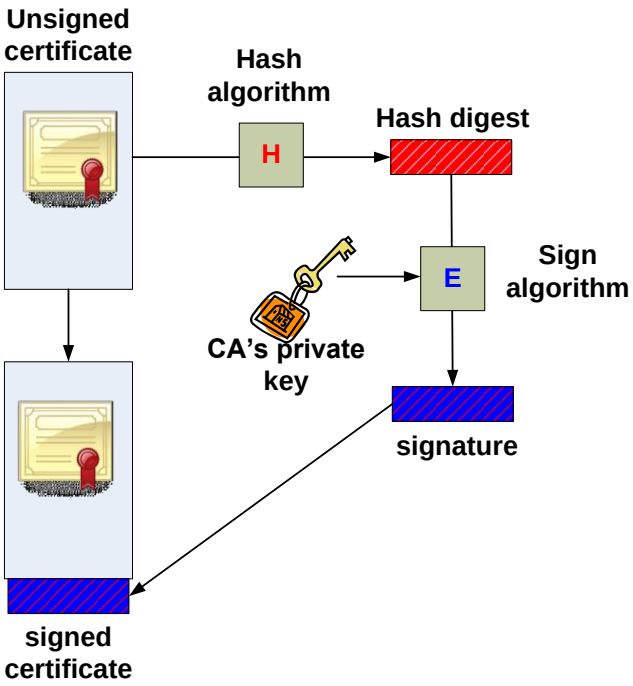






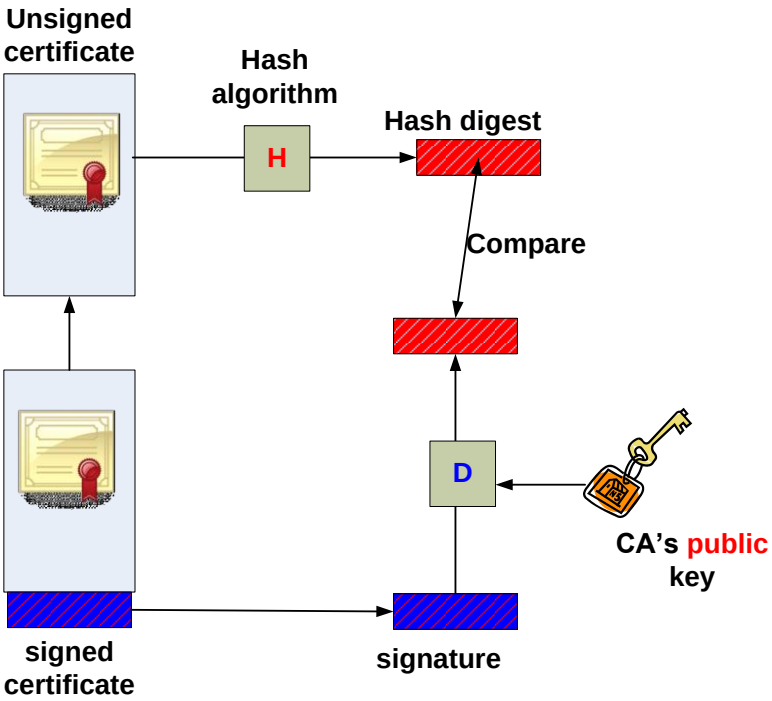
X.509 certificate

- Ochiq kaitli kriptografiya va raqamli imzoga asoslangan
- CA: certification authority(sertifikatli avtorizatsiya)



Tekshirish

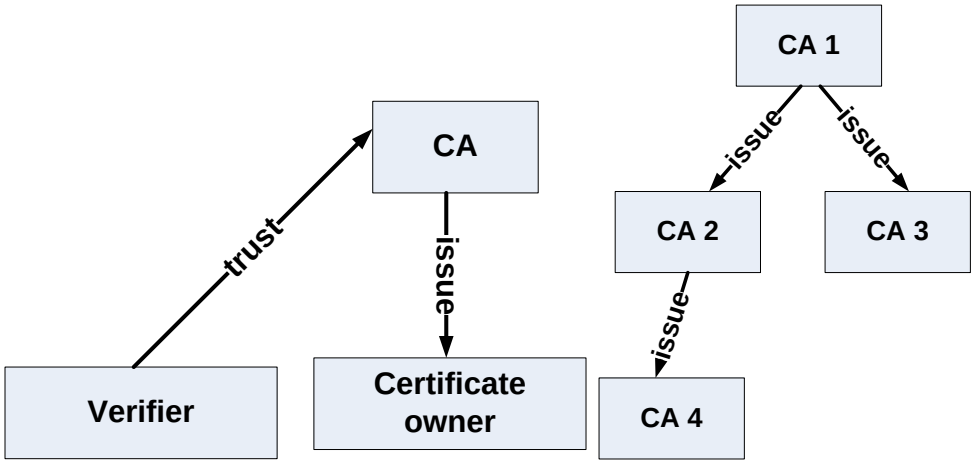
- Imzoni tekshirish uchun qolganlar ochiq kalitdan foydalanishlari mumkin



Sertifikatni tekshirish

- Metafora (1):

  - CA: BMTI (Buxoor muhandislik-texnologiya instituti)
  - Certificate egasi: talaba(kimki magistrlik darajasiga ega)
  - Tekshiruvchi : ish beruvchilar
- Metafora (2):
  - CA1: O`zbekiston ta`lim vazirligi
  - CA2: Buxoro muhandislik-texnologiya instituti



Man-in-the-middle attacks (O`rtadagi inson hujumi)

- HTTP traffikdagi tarkibni o`qishi mumkin
  - Sizning parolingizni (hattoki XESH langan bo`lsa hamki?)
- HTTP trafik tarkibini o`zgartirishi ham mumkin
  - Sizning hisob raqamingizdan hujumchini hisob raqamiga.

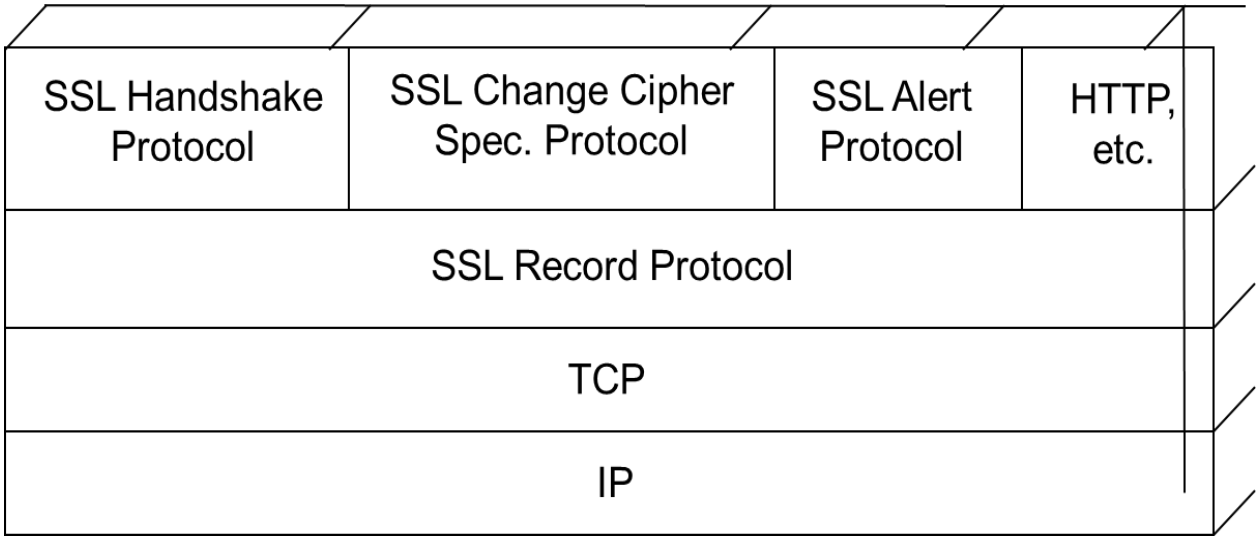
SSL/TLS tarixi

- SSLv2
  - Birinchi marotaba 1995 yil Netscape 1.1 da qo`llanilgan
  - Kalitlarni generatsiyalash algoritmi maxfiy saqlanadi
  - Reverse engineered orqali Wagner va Goldberg tomonidan buzilgan
- SSLv3
  - 1996 yil tuzatilgan va yaxshilangan holatda qo`llanilgan
  - Jarayon ochiq holatda bo`ladi
- TLS: versiyasi joriy standart hisoblanadi

SSL/TLS Umumiy qarash

- Sessiyani o`rnatish (qo`l qisish qatlami)
  - Algoritmlar haqida kelishish
  - Sirlarni almashinish
  - Autentifikatsiyani amalga oshirish
- Dastur ma`lumotlarini uzatish (yozish qatlami)
  - Konfedentsiallik va butunlikni ta`minlash

SSL Architecture



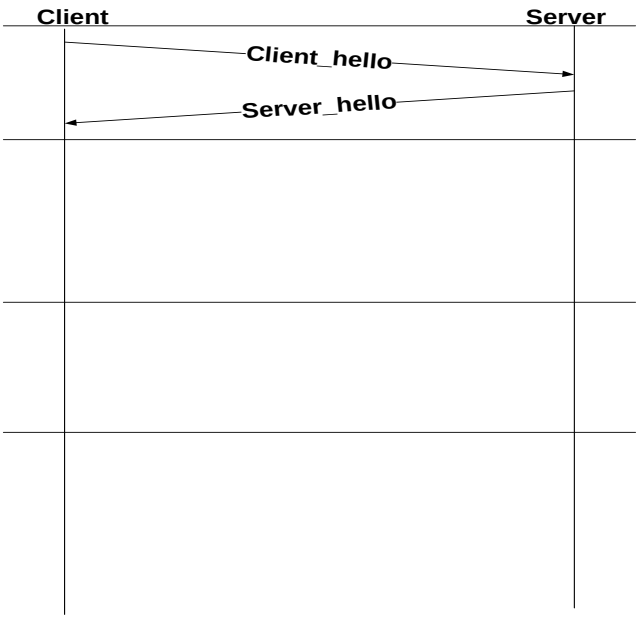
- Record Protocol: Message encryption/authentication
- Handshake P.: Identity authentication & key exchange
- Alert P.: Error notification (cryptographic or otherwise)
- Change Cipher P.: Activate the pending crypto suite

SSL Handshake Protocol

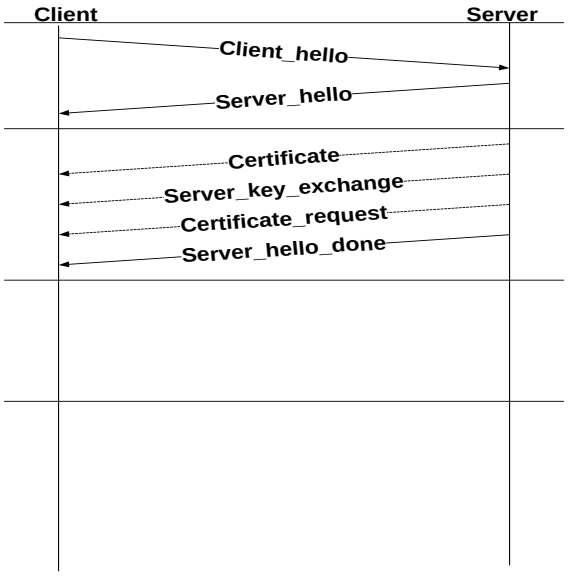
- Ikki tomon: mijoz va server
- Ishlatiladigan kriptografik algoritmlar va protocol versiyalarini kelishish
  - Protokollarni turli amalga oshirilishi o`rtasida moslik
  - Mijoz va serverni qo`shimcha autentifikatsiyasi
  - Raqamli sertifikatlar yordamida ochiq kalitlarni va butunlikni o`rganish
- O`zari maxfiylikni o`rnatish uchun ochiq kalitlarni ishlatish

Handshake Protocol (1)

- Client_hello: version, random, session id, cipher suite, compression method
- Server_hello: version, random, session id, cipher suite, compression method

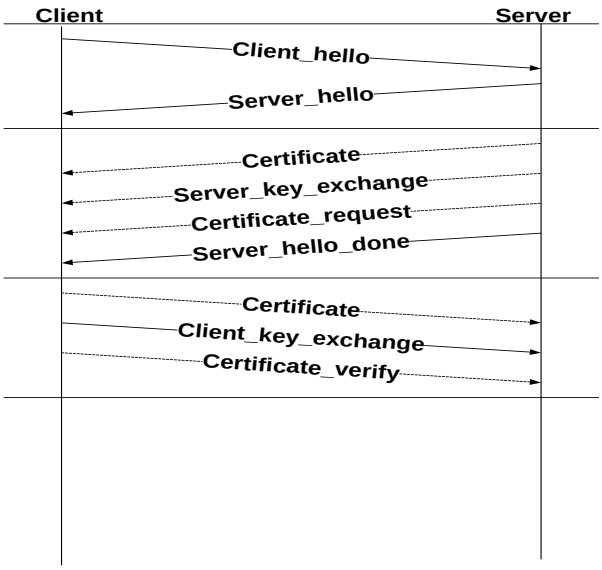


- Certificate: X.509 certificate chain
- Server_key_exchange: parameters, signature
- Certificate_request: type, authorities
- Server_hello_done: null



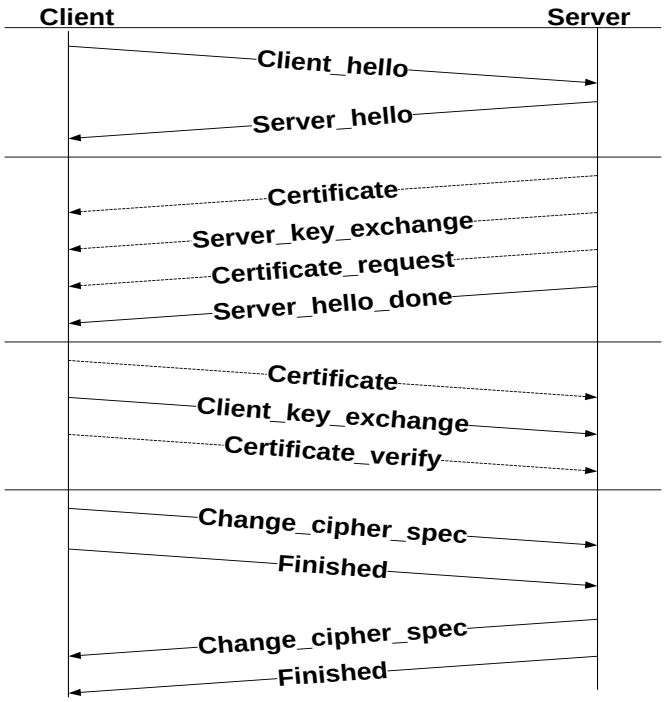
Handshake Protocol (3)

- Certificate: X.509 certificate chain
- Client_key_exchange: parameters, signature
- Certificate_verify: signature



Handshake Protocol (4)

- Change_cipher_spec: a single message, which consists of a single byte with value 1.
- Finished: hash value

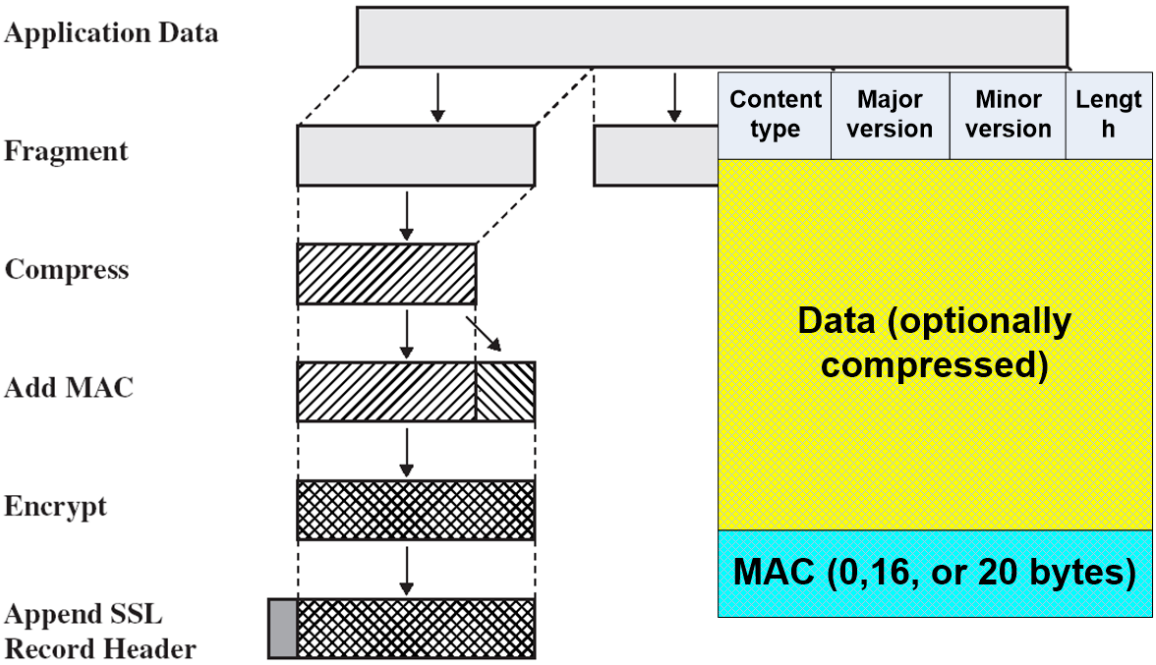


SSL Encryption

- Asosiy sir
  - Ikkala tomon ham maxfiy sir va taxminiy qiymatlarni generatsiyalashi
- Kalitli ma`lumot
  - Asosiy maxfiy ma`lumot va taxminiy qiymatlarni generatsiyalash
- Shifrlash kalitlari

- Kalitli materialdan olingan

SSL Record Protocol



Ogohlantirish va yopish

- Boshqa tomonni istisno holatlar haqida xabardor etish
  - Kutilmagan xabar
  - Yomon mac xabar
  - Qo`l siqish bo`lmadi
  - Mavjud bo`lmagan parametr
  - Yomon sertifikat
  - …
- Ikki qatlam
  - Ogohlantirish
  - Tuzatib bo`lmas

SSL Kutishlar

- TCP seansidan k`ora 2-10 marotaba sekin
- Qaerda biz vaqtdan yutqazamiz
  - Qo`l siqish fazasida
    - kalitli ma`lumotlarni hisbolashda

- Ma`lumotlarni uzatish fazasida
  - Shifrlash jarayonida

TLS/SSL ilovalar

- HTTP -> HTTPS
- Telnet -> SSH
- FTP -> SFTP
- SIP -> SIPS
- Resources: http://www.openssl.org/related/apps.html

DNS zaifliklari

Ko`p blokli ismlarni o`tkazish orqali ma`lumotlar bazasi amalga oshiriladi

- Distributed

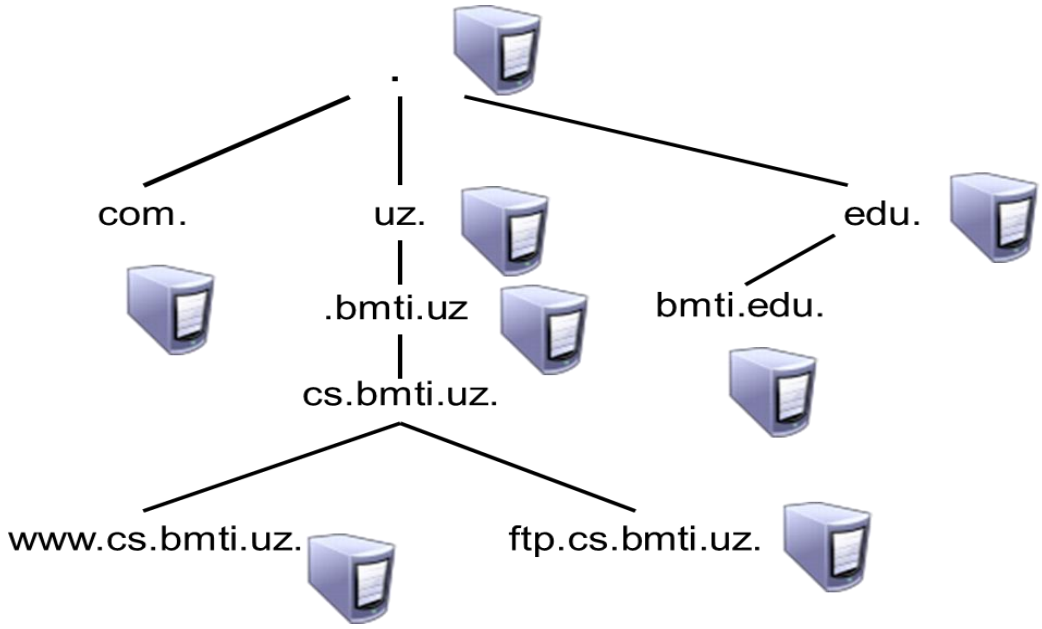
(Taqsimlangan)

- Replicated

(Tirajlangan ko`p nusxali)

- Hierarchical

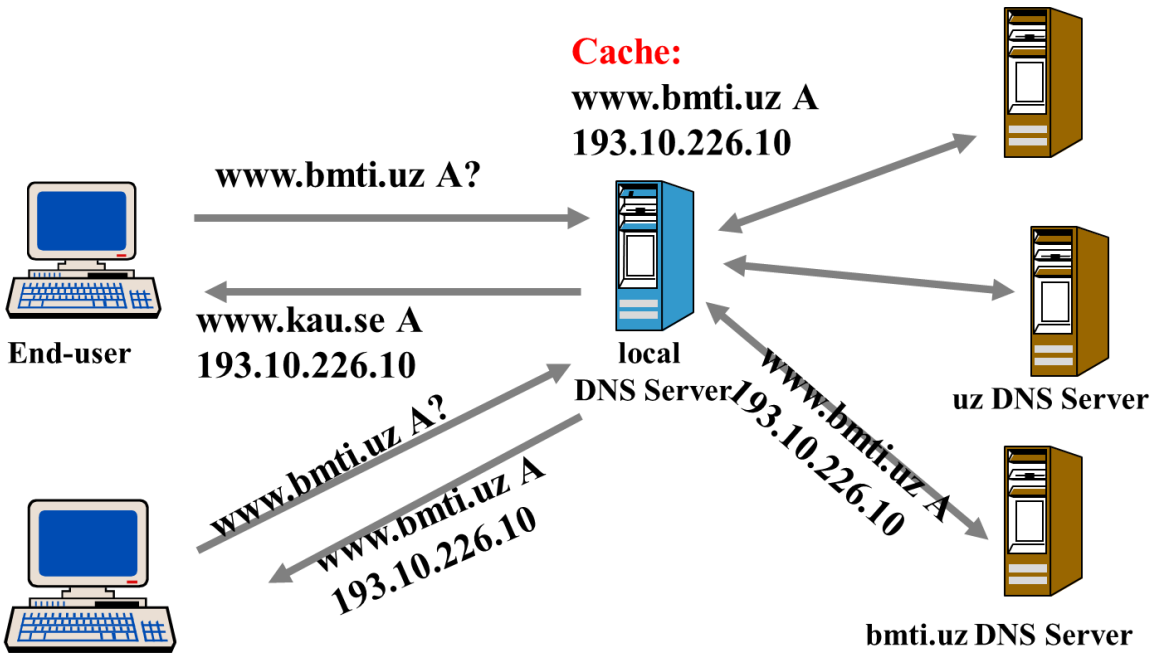
(Ierarxik)



Avtoritet serverlar

- Avtoritet DNS serverlar
  - Tashkilot serverlariga ishonchli ma`lumotlarini yetkazuvchi DNS server

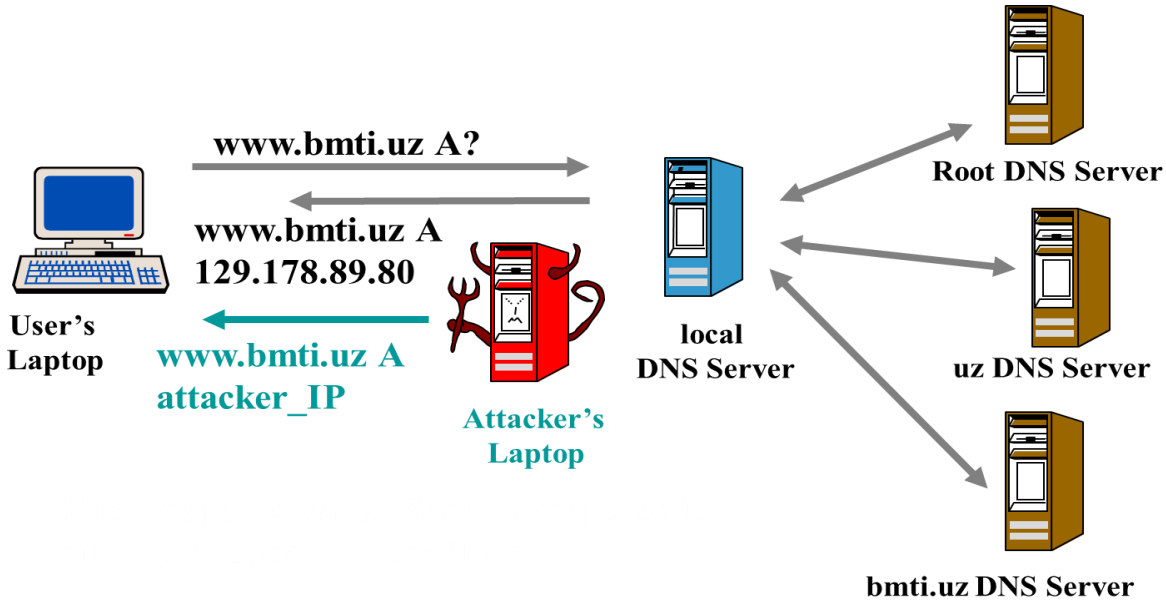
- Servis ko`rsatuvchi provayderlar va asosiy tashkilotlar tomonida saqlanadi



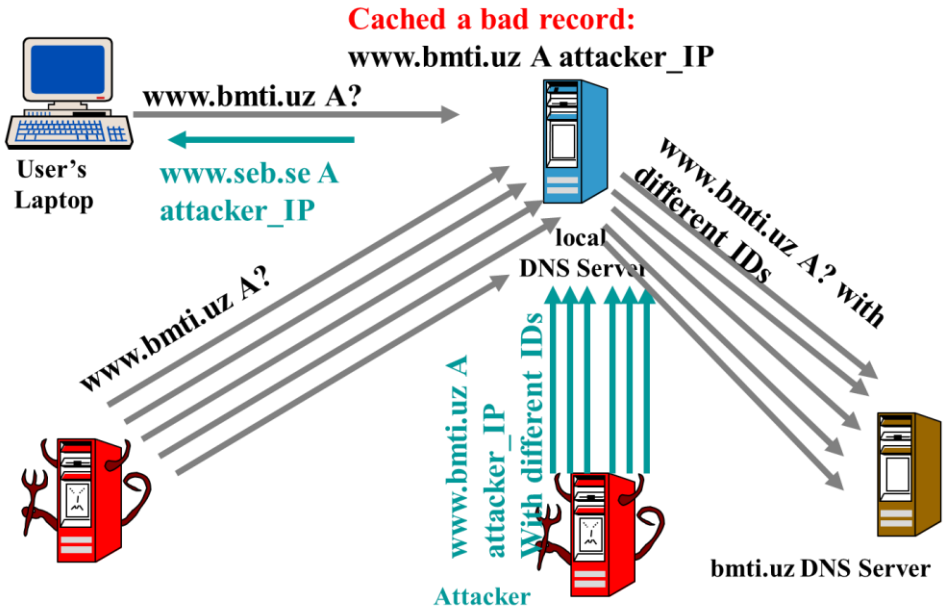
DNS zaifliklar

- No authentication. (Autentifikatsiya mavjud emas)
  - DNS_response.ID == DNS_request.ID ? (16 bit length)
  - DNS_response.dport == DNS_request.dport?
- Significance: DNS is widely used in (Qiymat: DNS juda keng quydagilarda qo`llaniladi)
  - Web
  - VoIP
  - Email

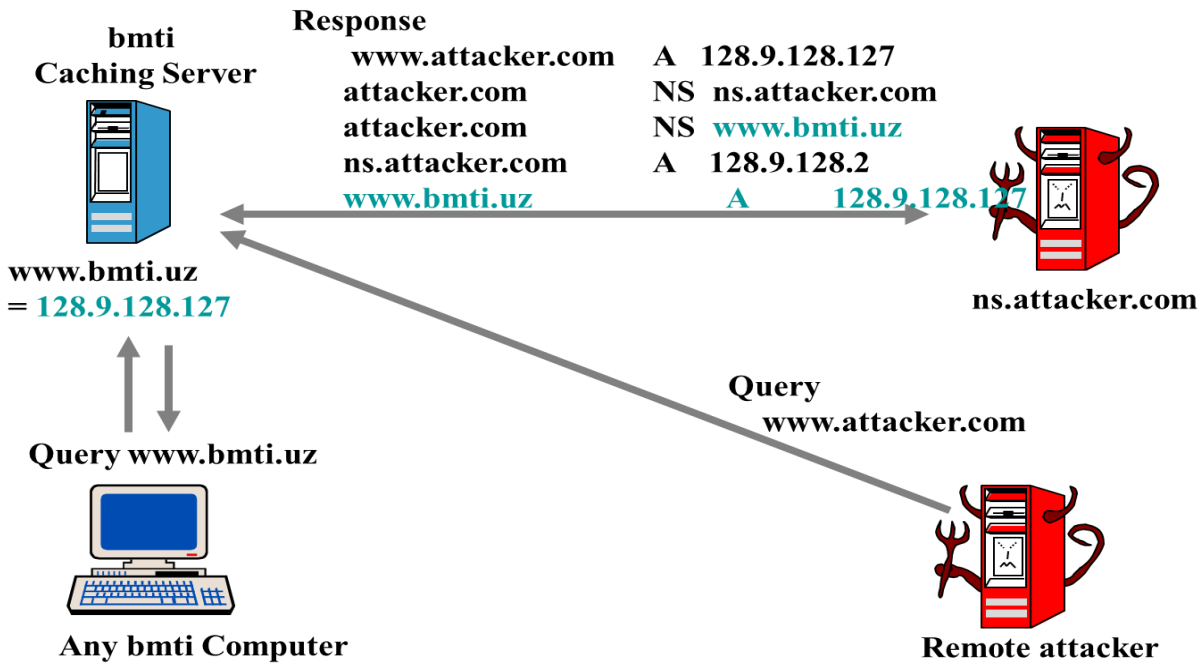
Oddiy DNS hujum



A cache poisoning Attack (Keshni zaharlash hujumi)



Kompleks hujum



3.3.Simsiz tarmoqlarda axborotlarni himoyalash

1. Simsiz tarmoqlarga kirish.
   Tarixi, asosiy standartlari, topologiyasi.
2. Simsiz tarmoq xavfsizligi masalalari.
   Mahfiylikni saqlash, yaxlitlik,ma'lumotlardan erkin foydalanish,ruxsatni nazorat qilish.
3. Simsiz tarmoqlarni aniqlash va axborot yig'ish usullari.
   Wardriving texnologiyasi.
4. WEP protokoli. Ishlash printsipi,fundamental zaifliklari.
   WEP-kalitini sindirish utilitalari.
5. Tarmoqni himoya qilish muqobil usullari va ularni chetlab o’tish
6. Simsiz tarmoqlarda AP (Access Point) va mijozlarga hujumlar. DoS-hujumlar. “man in the middle” hujumlar. Paketlarni amalga oshirish
7. 802.11i xavfsizlik standartlari. WPA / WPA2.
8. Sankt-Peterburgda Simsiz tarmoqlar. Statistika

IEEE 802.11 ma'lumotlarni uzatish standartlari:

802.11legacy – 1997 y., 2,4 ГГц, 2 Мбит/с

802.11b – 1999 y., 2,4 ГГц, 11 Мбит/с

802.11a – 1999 y., 5 ГГц, 54 Мбит/с

802.11g – 2003 y., 2,4 ГГц, 54 Мбит/с

802.11n – 2004 y., 540 Мбит/с

- Dastlab "Wi-Fi" - faqat 802.11b

- Tezlik signal kuchi(quvvati)ga bog'liqligi

- aralashuv (chunki bi qancha kanallar)

- Bundan tashqari, "nostandart" standartlari ham bor (802.11b +, 802.11-turboG, va hokazo)

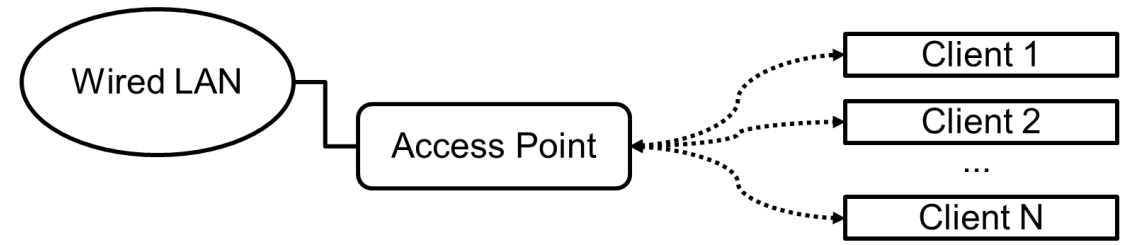
IEEE 802.11g

- 14 ta yopuvchi kanallar. Amerika Qo'shma Shtatlarida 1-11 foydalanadi. 2412 МГц - 2477 МГц.
- 1, 6, 11, 14 – yopilmaydi,agar kanal “kengligi” <5 Гц
- Tezlik: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с, kuch (quvvat) iga qarab
- 802.11b bilan teskari moslik
- Evropada, 1-13 kanallar ishlatiladi, lekin chiqish signali quvvati cheklangan holda

Сравнительная таблица стандартов беспроводной связи

Технология	Стандарт	Использование	Пропускная способность	Радиус действия	Частоты
Wi-Fi	802.11a	WLAN	до 54 Мбит/с	до 100 метров	5,0 ГГц
	802.11b		до 11 Мбит/с		2,4 ГГц
	802.11g		до 54 Мбит/с		
	802.11n		до 300 Мбит/с (в перспективе до 450, а затем до 600 Мбит/с)		2,4—2,5 или 5,0 ГГц
	802.11ac		до 3.39 Гбит/с / клиент; 6.77 Гбит/с / AP		2.4 + 5.0 ГГц
WiMax	802.16d	WMAN	до 75 Мбит/с	6-10 км	1,5—11 ГГц
	802.16e	Mobile WMAN	до 40 Мбит/с	1—5 км	2,3—13,6 ГГц
	802.16m	WMAN, Mobile WMAN	до 1 Гбит/с (WMAN), до 100 Мбит/с (Mobile WMAN)	н/д (стандарт в разработке)	
Bluetooth v. 1.1	802.15.1	WPAN	до 0,7 Мбит/с	до 10 метров	2,4 ГГц
Bluetooth v. 2.0	802.15.3		до 3 Мбит/с	до 100 метров	
Bluetooth v. 3.0	802.11		от 3 Мбит/с до 24 Мбит/с		
UWB	802.15.3a		110—480 Мбит/с	до 10 метров	3,1—10,6 ГГц
ZigBee	802.15.4		от 20 до 250 Кбит/с	1—100 м	2,4 ГГц (16 каналов), 915 МГц (10 каналов), 868 МГц (один канал)
Инфракрасный порт	IrDa		до 16 Мбит/с	от 5 до 50 сантиметров, односторонняя связь — до 10 метров	

WLAN Topologiyasi



Ad-Hoc simsiz o'zi tashkil qilinadigan tarmoq

- Bluetooth (IEEE 802.15.1)
- WiFi (IEEE 802.11)
- ZigBee (IEEE 802.15.4)
- ONE-NET
- Wideband Networking Waveform

WLAN aniqlash

SSID – tarmoqni aniqlash (AP)

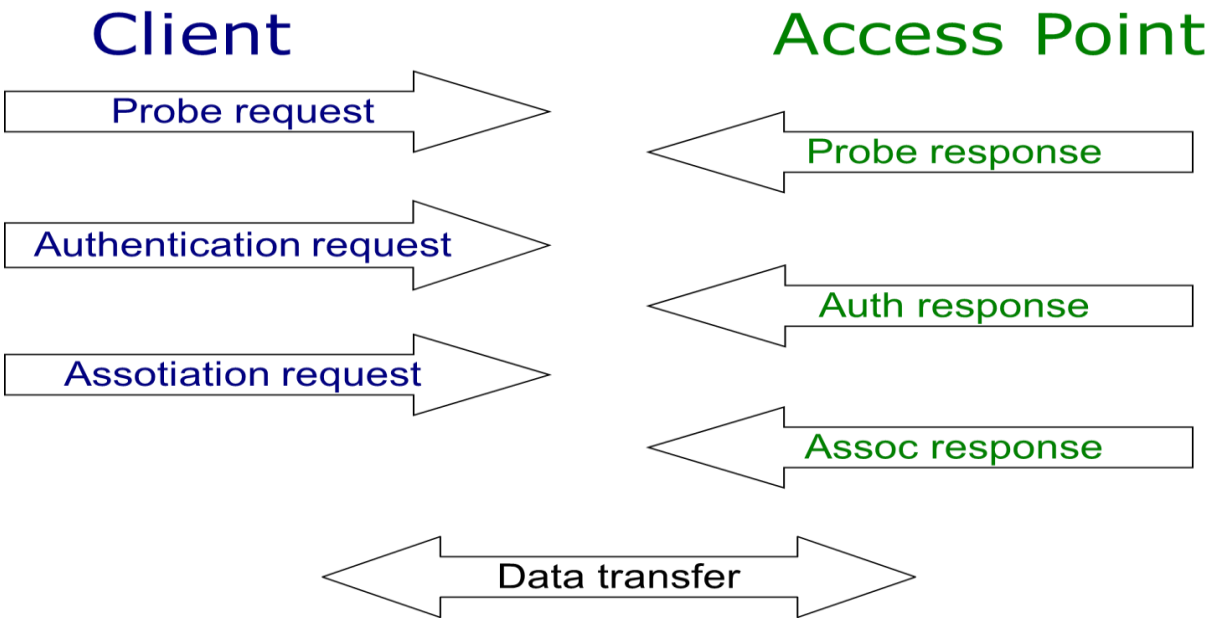
BSSID – AP MAC-manzil

Channel – tarmoq qaysida ishlayotgani

Beacon frame – axborotni keng ommaga tarqatadigan freym. AP minimal tezlik bilan doimiy uzatiladi. Tarmoq haqida ma'lumotni saqlaydi.

Freymlar: axborotli va boshqariladigan (auth, deauth, assoc, deassoc).

WLAN mijozi holatining diagrammasi



WLAN xavfsizligi

Maxfiylik(Конфиденциальность)

Ruxsatni nazorat qilish(Контроль доступа)

Ma’lumotlar yaxlitligi(Целостность данных)

Ma’lumotlardan erkin foydalanish(Доступность данных)

Tarmoqni:

Trafikni eshitish

Trafikni o’zgartirish

avtorlashtirilmagan ruxsat

dan qanday himoyalash mumkin

Dastlab: **WEP** (Wired Equivalent Privacy)

2002 yil: **WPA** (Wireless Protected Access)

802.11i: **WPA2** (RC4 -> AES)

Qo’shimcha metodlar (IPSec, SSL-tunnel)

WLANni topish

(((Wardriving)))

Beacon frames – axborotni keng ommaga tarqatadi va

SSID

BSSID (AP MAC)

Tarmoq tipi

shifrlash mavjudligini

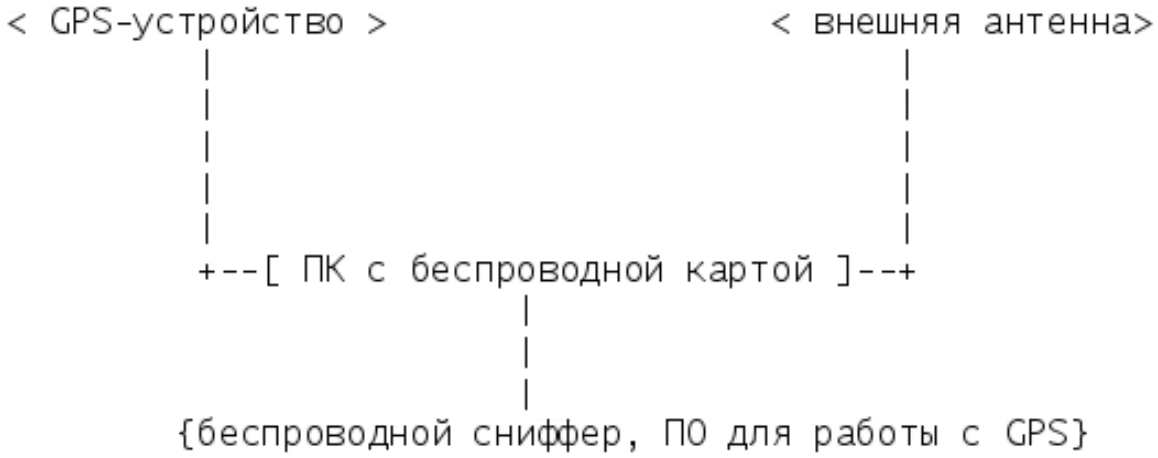
Tarmoq haqida ma’lumotni saqlaydi.

Simsiz sniffer (tarmoq trafigini tahlil qiluvchi dastur yoki dastur-apparat vosita)

GPS-qabul qiluvchi (приемник)

Simsiz tarmoq kartasi

Portativ SHK



Simsiz snifferlar

Passiv: **Kismet**

Faol (skanerlar): **Netstumbler**

<u>Passiv snifferlar ishlash prinsipi:</u>

Kartalarni **RFMON (Monitor mode) + Channel Hopping ga jo’natish**

RFMON: karta barcha freymlarni qabul qiladi va ularni OS ga jo’natadi.

Firmware ni qo’llab quvvatlash lozim!

Channel Hopping – kanallar o’rtasida ketma-ket almashish.

Simsiz snifferlar (2)

Faol skanerlarning ishlash prinsipi :

Probe request-freymlarini SSID dan “” (ANY) barcha ruxsat etilgan kanallarga jo’natish. AP javoblarini kutish va tahlil qilish.

Usul freymlar jo’natishni talab qiladi, shuning uchun :

- Vardrayver o’zini topishni imkoniyatini beradi;
- Qamrash zonasi passivga qaraganda kamroq bo’ladi

WEP Protokoli

Trafikni yovuzniyatlilar o’qishidan himoyalash

Tarmoq resurslariga nazoratsiz ruxsatdan himoyalash Uzatiladigan ma’lumotni o’zgartirishdan himoyalash.

40 bit (104 bit) – maxfiy kalit (**K**)

24 bit – parametrni aniqlash vektori (**IV**)

RC4(K,IV) – traffic key (**T**)

O – shifrlanmagan ma’lumot

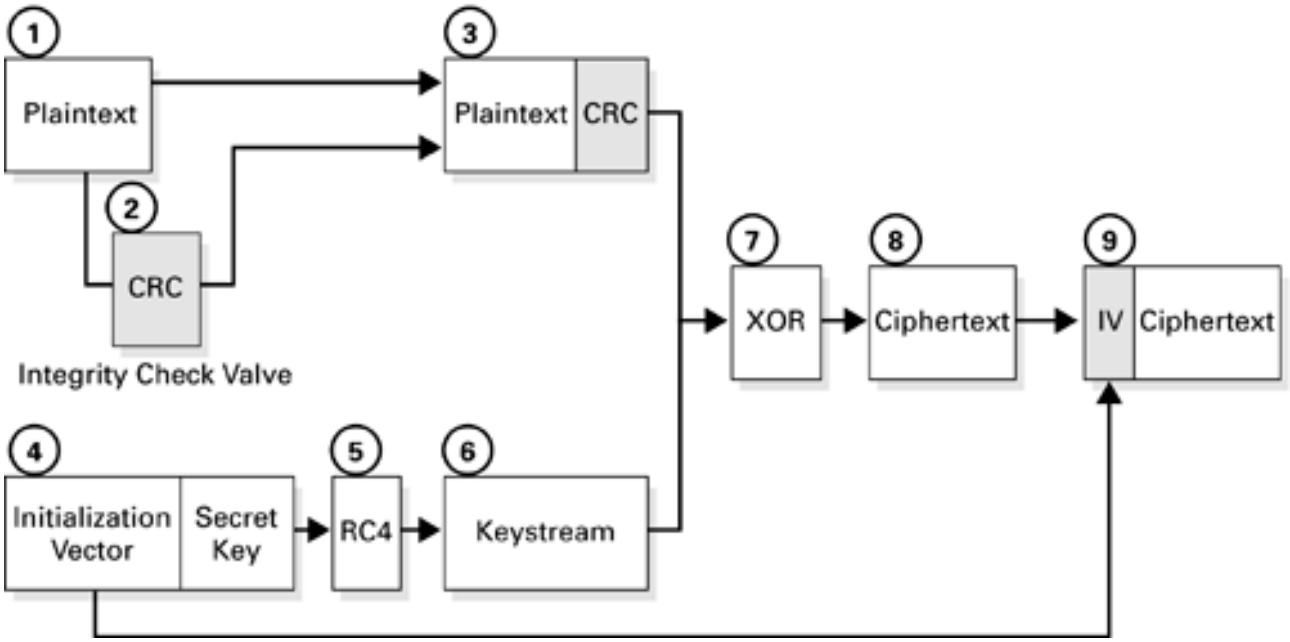
CRC – yaxlitlikni nazorat qilish uchun,

M = <CRC(O),O>

P – shifrlangan ma’lumot, **P = T XOR M**

[IV,P] – tarmoq bo’icha uzatiladi

WEP Protokoli (2)



WEP Protokol: zaif tomonlari

Potok shifrlash(RC4): bitta Ivni ikki marta ishlatish mumkin emas. Lekin 24 bit kam!

CRC chiziqli va IV siz hisoblanadi

2001. Scott Fluhrer, Itzik Mantin, Adi Shamir: FMS-hujum

2002 yil: yaxshilangan FMS-ataka

2004 yil: yangi metod (Korek Attack). Aircrack.

Kalitni sindirish uchun ko’plab utilitalar bor

WEP Protokol: zaif tomonlari (2)

Kalitni ochish uchub paketni ushlash shart emas.Hatto kalitni ham ochish shart emas, chunki...

Paketlarni autentifikatsiyasiz joriy qilish

Xabarlarni kalitsiz ochish

Shifrlangan paketlarni o’zgartirirsh

Soxta autentifikatsiyalash (spufing)

WEP HECH NARSANI HIMOYALAMAYDI.

U to’liq yaroqsiz.

Boshqa “Himoya” usullari

Hidden SSID – qonuniy mijoz ulanayotganda SSID baribir uzatiladi;

MAC filtering – qonuniy mijoz MAC manzili qalbakilashtiriladi, interfeysdan arp ni o'chirib bemalol ishlash mumkin;

Mavjud insrumentlar quyidagi imkoniyatlarga ega:

- WEP-kalitni sindirish
- Tarmoqqa paket joriy qilish
- Soxta boshqaruvchi freymlarni jo'natish

Simsiz tarmoqqa hujumlar

Tarmoqda turgan subyektga

Aloqa kanalida

Ruxsat nuqta(AP) Mijoz DT(ПО)ning ojiz nuqtalari

Trafikni ushlab olish va o'zgartirish ("man-in-the-middle")

avtorlashmagan subyektlarning ulanishi

Yolg'on AP joriy qilinishi ("Evil Twin")

Xizmat ko''rsatishdan bosh tortish hujumi

Mijoz stansiyalarga hujum

Tarmoq ta'sir zonasida joylashgan va kerakli qurilmaga ega bo'lgan ixtiyoriy sub'yekt yovuzniyatli bo'lishi mumkin

Misol

WEP himoyalangan simsiz tarmoq bor

WEP- "passiv" va "faol" metodli kalitni sindirish, aircrack va airodump utilitalari bilan.

Paketlarni joriy etish (ARP injection, Interactive packet reply) bilan

Soxta autentifikatsiyalanish(fake authentication, fake deassotiation attack)

WLAN: 802.11i himoyasi

2002 yil: WEP yaroqsiz bo'lgandan keyin **WPA** tezlik bilan ishlab chiqildi

2004 yil: **802.11i**, tarkibiga **WPA2 ni oluvchi yaratildi**

WPA = {802.1X + EAP + TKIP + MIC + (RADIUS)}

WPA-PSK = {802.1X + EAP + TKIP + MIC}

802.1x – mualliflashtiruvchi protokol

EAP – Extensible Authentication Protocol

TKIP – WEP o'rniga "almashtirish"

WPA2 da TKIP o'rniga –**AES** ishlatiluvchi **CCMP** (Counter-Mode CBC MAC Protocol) kiritildi.

MIC - CRC o'rniga "almashtirish"

802.11i ojizliklari?

EAP – protokollar to'plami. EAP-TTLS ishonchli. **LEAP** (Lightweight EAP) – esa yo'q.

WPA-PSK – parol iborasiga luga't bo'yicha hujum imkoniyati

WPA-PSK va LEAP ga qarshi "**WPA cracking tools**"

RADIUS-сервер ojizliklari?

Amaliy DT ojizliklari? (wpa_supplicant)

WLAN himoyasi: boshqa vositalar

IPSec-tunneli

SSL/TLS (HTTPS, SSH) dan foydalanish

***WIDS** (Wireless Intrusion Detection Systems) dan foydalanish*

Wireless IDS:

mualliflashtirilmagan Aplarni topish

OSI modelining 2-3 darajalaridagi hujumlarni aniqlash

Imkoni yo'q:

- Paketlarni ushlab olish dalilini aniqlash (снифинг)
- Faol ta'sirlarni aniqlash(RFMON) (ba'zi bir drayverlarda buning imkoni bor)

WLAN himoyasi: o'ziga xosliklari

Mijoz va ruxsat nuqtasi(AP) bir-birini mualliflashtirishi lozim

Mijozning xavfsizlik profili mijoz bilan birgalikda aralashtirib yuborilishi lozim

IPSec, SSL/TLS –AP va mijoz autentifikatsiyasini OSI modelining 2 darajasida ta'minlamaydi.

Nazorat savollari:

1. Tahdid turlari.
2. Tahdidlarni amalga oshirish usullari nomini sanab bering.
3. Simsiz snifferlar haqida malumot bering.
4. WLAN xavfsizligi qanday bo’ladi

Foydalaniladigan adabiyotlar:

1. Ganiev S.K., Karimov M.M., Toshev K.A. Axborot xavfsizligi. O’kuv kullanma .-TATU «Aloqachi», 2008.
2. Jukov YU. V. Osnovы veb-xakinga. Napadenie i zaщita (2-e izd.). Piter.2012. 206c.
3. S.A. Babin. Instrumentarii XAKERA. BXV-Peterburg. 2014 g. 233 s.
4. Vivek Ramachandran - BackTrack 5 Wireless Penetration Testing – 2011. 220 p.
5. Flyonov M.E. Kompyuter glazami xakera. 2012g. BXV-Peterburg. 2012g. 274s.
6. Andrianov V. V. Zefirov S. L. Golovanov V. B. Golduev N. A. Obespechenie informatsionnoy bezopasnosti biznesa. 2011g. 265 s.
7. Platonov V.V. Programmno-apparatnыe sredstva zaщitы informatsii (Vыsshee professionalnoe obrazovanie. Bakalavriat). AKADEMIA. 2013g. 331 s.
8. SHangin V.F. Zaщita informatsii v kompyuternыx sistemax i setyax. DMK. 2012g. 593s.
9. Romanets YU.V.,Timofeev P.A., SHangin V.F. Zaщita informatsii v kompyuternыx sistemax i setyax./ M.: Radio i svyaz,2010.-376s.\
10. Barry L. Williams. «Information Security Policy Development for Compliance»: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0. 2013 year.

IV. AMALIY MASHG'ULOT MATERIALLARI

1-amaliy mashg'ulot: Autentifikatsiya va uning turlari.

Kirish. Axborotlarni qayta ishlash jarayonlarini avtomatlashtirish vositalari, usullari va formalari murakkablashuvi va rivojlanishi bo`yicha ularni axborot texnologiyalarida ularni qo`llanilish xavfsizlik darajasidan oshib bormoqda.

1.Ishdan maqsad: Autentifikatsiya va uning turlarini o`rganish va tadqiq etish.

2.Qisqacha nazariy ma`lumot:

Autentifikatsiya nima?

Autentifikatsiya (ingliz tilidan authentication , grek tilidan αὐθεντικός [authentikos] –haqiqiy, αὐθέντης [authentes]-muallif) – haqiqiylikni tekshirish jarayoni.

- Kiritilgan Parolni Foydalanuvchining bazada mavjud paroli bilan solishtirish orqali foydalanuvchining haqiqiyligini tekshirish
- Uzatuvchining xatidagi elektron imzoni ni ochiq kalit orqali tekshirish yo'li bilan electron xatlarning haqiqiyligini tekshirish
- Fayl muallifi tomonidan ko'rsatilgan hajmni nazorat qilinayotgan hajm bilan mos kelishini tekshirish

Elektron imzo yordamidagi Autentifikatsiya

- Oddiy elektron imzo
- Kvalifikatsiyalashmagan elektron imzo
- Kvalifikatsiyalashgan elektron imzo

Parolli Autentifikatsiya

- Kop' martali parolli autentifikatsiya
- Bir martali parolli autentifikatsiya

SMS yordamida Autentifikatsiya

Mobil aloqa vositalari orqali xavfsizlikni ta'minlash

Biometrik Autentifikatsiya

- Barmoq izini olish
- Qo'l geometriyasi
- Ko'z qorachig'i rang baranglari
- Kishining termik
- Yuz bo'yicha tanib olish
- Tovush
- Klaviaturadan kiritish

- Imzo

Geografik joylashuv bo’yicha Autentifikatsiya

- GPS yordamida
- Internetga kirish joyi orqali

Ko’p faktorli Autentifikatsiya

- PIN –kod mobil telefonlardagi SIM-kartalarda
- Notebooklardagi barmoq izini skanerlash

O`rin almashtirishga misol tariqasida dastlabki axborot blokini matritsaga qator bo`yicha yozishni, o`qishni esa ustun bo`yicha amalga oshirishni ko`rsatish mumkin. Matritsa qatorlarini to`ldirish va shifrlangan axborotni ustun bo`yicha o`qish ketma-ketligi kalit yordamida berilishi mumkin. Usulning kriptoturg`unligi blok uzunligiga (matritsa o`lchamiga) bog`liq. Masalan uzunligi 64 simvolga teng bo`lgan blok (matritsa o`lchami 8x8) uchun kalitning $1,6 \circ 10^9$ kombinatsiyasi bo`lishi mumkin. Uzunligi 256 simvolga teng bo`lgan blok (matritsa o`lchami 16x16) kalitning mumkin bo`lgan kombinatsiyasi $1,4 \bullet 10^{26}$ ga etishi mumkin. Bu holda kalitni saralash masalasi zamonaviy EHMlar uchun ham murakkab hisoblanadi.

O`rin almashtirish shifri oddiy shifrlash hisoblanib, bu usulda qator va ustundan foydalaniladi. CHunki shifrlash jadval asosida amalga oshiriladi. Bu yerda kalit (K) sifatida jadvalning ustun va qatori xizmat qiladi. Matn ($T_0$) simvollarining o`lchamiga qarab NxM jadvali tuziladi va ochiq matnni (T_0) ustun bo`yicha joylashtirilib chiqiladi, qator bo`yicha o`qilib shifrlangan matnga ($T_1$) ega bo`linadi va bloklarga bo`linadi.

**Ikki tomonlama o`rin almashtirish usuli.** Bu usulda kalit sifatida ustun va qatordagi harflar tartibidagi sonlardan foydalaniladi. Avvalam bor kalit simvollariga qarab jadval tuziladi, va ochiq $T_0$ matn joylashtirilib chiqiladi, so`ngra esa raqamlar navbatma – navbat tartiblanib, avval ustun, so`ngra esa qatorlar o`rni almashtiriladi va jadvaldagi ma`lumot qator bo`yicha o`qilib $T_1$ga ega bo`linadi. Masalan: «Intilganga tole yor» ochiq matni shifrlash talab etilsin. Bu yerda kalit bo`lib 1342 va 2314 xizmat qiladi. YAxshiroq izohlanishi uchun K_1=1342 va K_2=2314, V=4 deb belgilab olamiz.

4x4 jadval yaratib T_0 qator bo`yicha yozamiz:

	2	3	1	4
1	I	N	T	I
3	L	G	A	N
4	G	A	T	O

K_2

2	L	E	YO	R

Endi qator va ustunla K_1 bo`yicha o`rinlari almashtiriladi.

	2	3	4	1
1	I	N	T	I
2	L	E	YO	R
3	L	G	A	N
4	G	A	T	O

	2	3	4	1
1	I	I	N	T
2	R	L	E	YO
3	N	L	G	A
4	O	G	A	T

Oxirgi jadvalga asosan shifrlangan matnni yozamiz va bloklarga bo`lib chiqamiz.

T_1 =IINT_RLEYO_NLGA_OGAT

Ikki tomonlama almashtirishda jadval kattaligiga qarab variantlar ham ortib boradi. Jadval o`lchamining kattaligi shifr chidamliligini oshiradi: 3x3 jadvalda 36 ta variant, 4x4 jadvalda 576 ta variant, 5x5 jadvalda 14400 variant;

Murakkab almashtirishli shifr. Murakkab almashtirishli shifr ko`p alfavitli bo`lib, shifrlashda keluvchi matnning xar bir harfi o`zining oddiy almashtirish shifri kabi shifrlanadi. Ko`p alfavitli almashtirishda alfavit ketma-ketligi va tsiklidan foydalaniladi.

A-alfavitli almashtirishda kiruvchi axborotning X_0-harfi V_0-alfavitning Y_0-harfi bilan almashtiriladi, X_1-xarfi esa V_1-alfavitning Y_1-harfi bilan almashtiriladi, X_{r-1}-xarfi V_{r-1}-alfavitning Y_{r-1}-xarfi bilan almashtiriladi va hokazo.

Ko`p alfavitli almashtirishning r=4 bo`lgan hol uchun umumiy ko`rinishi quyidagi jadvalda keltirilgan.

Kiruvchi harflar	X0	X1	X2	X3	X4	X5	X6	X7	X8	X9
Alfavit almashtirish	B0	B1	B2	B3	B0	B1	B2	B3	B0	B1

Bu usul bilan shifrlangan matnni ochishda etarli qiyinchiliklar tug`diradi, endi k-kalit bir-necha marotaba o`zgaradi. Bunda dushman har bir matn bo`lagini qanday qilib ochishni bunday shifrlashda ximoyalanganlik darajasi foydalaniyotgan $V_j$-alfavit ketma-ketligiga bog`liqdir. Ko`p alfavitli almashtirish shifrini Leon Batist Al`bert kriptografiyaga kiritdi. 1566-yilda uning “Traktat o shifre” kitobi chiqqan. Butun dunyoda kiriptologiya (kriptotahlil) asosini L. Al`bert nazariyasi tashkil qiladi.

3. Ishni bajarilish tartibi va qo`yilgan vazifa:

Ixtiyoriy autentifikatsiya turini tanlab izohlansin. SHuningdek **Delphi, VBA, C++** va **C#** dasturlash tizimlaridan birida autentifikatsiya turi uchun dasturiy ta`minot yaratilsin.

2- amaliy Mashg’ulot: Shifrlash algoritmlari

1. Ishdan maqsad: Komp’yutyerdagi ma`lumotlar himoyasi va ularni qayta tiklash.

2. Qisqacha nazariy ma`lumot:

Gamil’ton marshrutlariga asoslangan usulda ham o`rin almashtirishlardan foydalaniladi. Ushbu usul quyidagi qadamlarni bajarish orqali amalga oshiriladi.

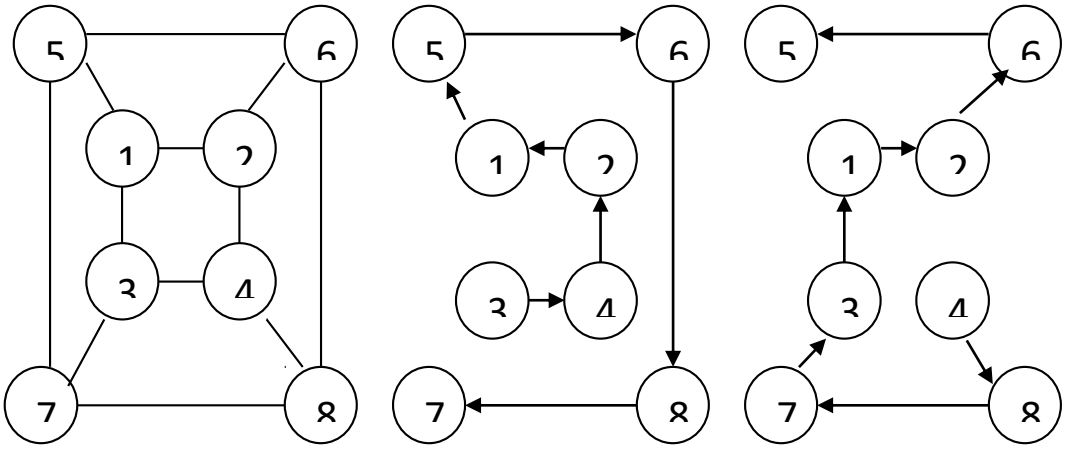
1-qadam. Dastlabki axborot bloklarga ajratiladi. Agar shifrlanuvchi axborot uzunligi blok uzunligiga karrali bo`lmasa, oxirgi blokdagi bo`sh o`rinlarga maxsus xizmatchi simvollar-to`ldiruvchilar joylashtiriladi(masalan, *).

2-qadam. Blok simvollari yordamida jadval to`ldiriladi va bu jadvalda simvolning tartib raqami uchun ma`lum joy ajratiladi. (1 - rasm)

3-qadam. Jadvaldagi simvollarni o`qish marshrutlarning biri bo`yicha amalga oshiriladi. Marshrutlar sonining oshishi shifr kriptoturg`unligini oshiradi. Marshrutlar ketma-ket tanlanadi yoki ularning navbatlanishi kalit yordamida beriladi.

4-qadam. Simvollarning shifrlangan ketma-ketligi belgilangan L uzunlikdagi bloklarga ajratiladi. L kattalik 1-qadamda dastlabki axborot bo`linadigan bloklar uzunligidan farqlanishi mumkin.

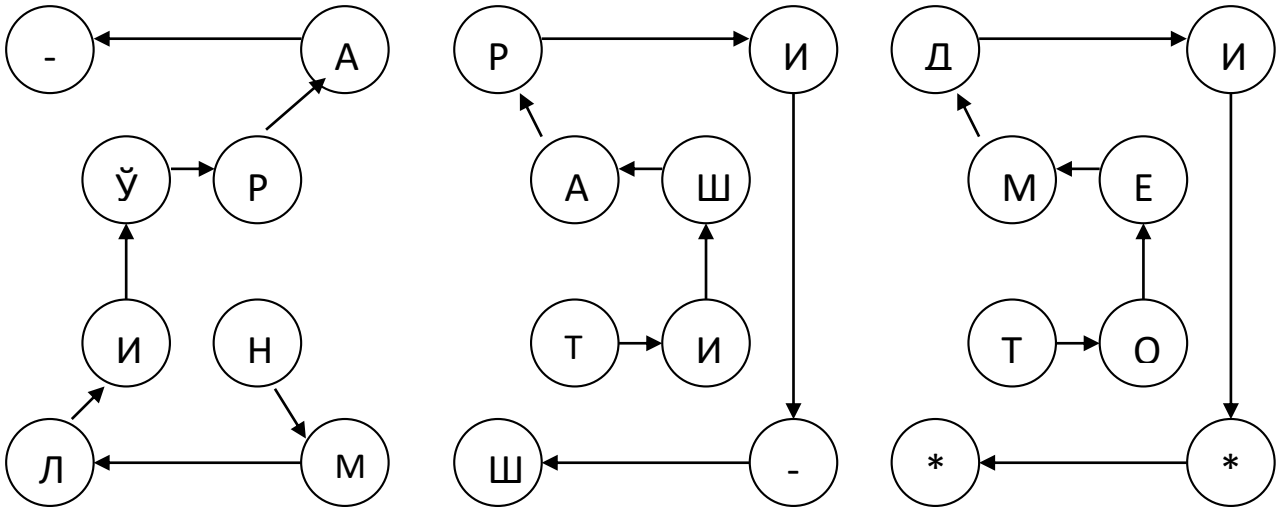
Deshifrlash qilish teskari tartibda amalga oshiriladi. Kalitga mos holda marshrut tanlanadi va bu marshrutga binoan jadval to`ldiriladi.



1-rasm. 8-elementli jadval va Gamil’ton marshrutlari variantlari.

Jadvaldan simvollar element nomerlari kelishi tartibida o`qiladi.

Misol. Dastlabki matn T_0 «O`rin almashtirish usuli»ni shifrlash talab etilsin. Kalit va shifrlangan bloklar uzunligi mos holda quyidagilarga teng: K=<2,1,1>, L=4. SHifrlash uchun 2.5-rasmda keltirilgan jadval va ikkita marshrutdan foydalaniladi. Berilgan shartlar uchun matritsalari to`ldirilgan marshrutlar 2.6-rasmda keltirilgan ko`rinishga ega.



2 - rasm. Gamil’ton marshruti yordamida shifrlash misoli.

1-qadam. Dastlabki matn uchta blokka ajratiladi. B1=<O`rin_alm>, B2=<ashtirish->, B3=<usuli**>;

2-qadam. 2,1,1 marshrutli uchta matritsa to`ldiriladi;

3-qadam. Marshrutlarga binoan simvollarni joy-joyiga qo`yish orqali shifrmatnni hosil qilish.

T_1=<NMLIO`RA_TISHARI_SHTOEMDI**>

4-qadam. SHifrmatnni bloklarga ajratish.

T_1=<NMLI O`RA_ TISHA RI_SH TOEM DI**>

3.Qo`yilgan vazifa:

Keltirilgan usullar uchun dastur ishlab chiqilsin. Dastur **VBA, S++** yoki C# dasturlash tizimidan foydalangan holatda yaratilsin.

Topshiriq variantlari

1. Texnologik jarayonlarni boshqarish
2. Axborot kommunikatsiya tizimlari
3. Dasturiy taminotni loyihalash
4. Malumotlar bazasini himoyalash
5. Kompyuter tarmoqlarida malumotlarni himoyalash
6. Bugun havo yaxshi
7. Ertaga dars bo`lmaydi
8. Axborot xavfsizligi fanini organish
9. Axborot xavfsizligini taminlash vositalari
10. Ertaga men darsda bo`lmayman

3- amaliy mashg'ulot: Kompyuter tarmoqlarida ma'lumotlariga tahdidlar.

Kirish. Hozirgi vaqtda axborotlarni himoyalashni ta`minlashning qandaydir biror texnik usuli yoki vositasi mavjud emas, ammo ko`p xavfsizlik muammolarini echishda kriptografiya va axborotlarni kriptoo`xshash almashtirishlari ishlatiladi.

1. Ishdan maqsad: Kompyuter tarmoqlarida ma'lumotlarga tahdidlar va ularni himoyalash usulaari to'g'risida ma'lumotga ega bo'lish.

2. Qisqacha nazariy ma`lumot:

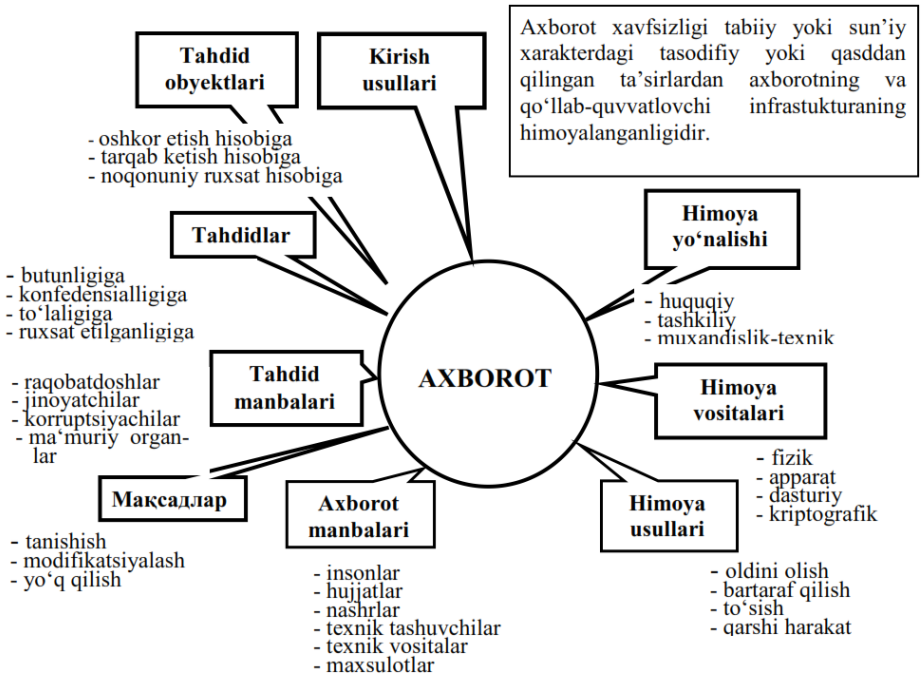
Himoyalangan axborotga tahdidlar tushunchasi va uning tuzilishi.

Umumiy yo'nalishga ko'ra axborot xavfsizligiga tahdidlar quyidagilarga bo'linadi:

– O'zbekistonning ma'naviy ravnaqi sohalarida, ma'naviy hayot va axborot faoliyatida fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga tahdidlar;

– mamlakatning axborotlashtirish, telekommunikatsiya va aloqa vositalari industriyasini rivojlanishiga, ichki bozor talablarini qondirishga, uning mahsulotlarini jahon bozoriga chiqishiga, shuningdek mahalliy axborot resurslarini yig'ish, saqlash va samarali foydalanishni ta'minlashga nisbatan tahdidlar;

– Respublika hududida joriy etilgan hamda yaratilayotgan axborot va telekommunikatsiya tizimlarining me’yorida ishlashiga, axborot resurslari xavfsizligiga tahdidlar.



Axborot hisoblash tizimlarida axborot xavfsizligini ta’minlash nuqtai nazaridan o‘zaro bog‘liq bo‘lgan uchta tashkil etuvchini ko‘rib chiqish maqsadga muvofiq:

1) axborot;

2) texnik va dasturiy vositalar;

3) xizmat ko‘rsatuvchi personal va foydalanuvchilar.

Har qanday axborot hisoblash tizimlarini tashkil etishdan maqsad foydalanuvchilarning talablarini bir vaqtda ishonchli axborot bilan ta’minlash hamda ularning konfedensialligini saqlash hisoblanadi. Bunda axborot bilan ta’minlash vazifasi tashqi va ichki ruxsat etilmagan ta’sirlardan himoyalash asosida hal etilishi zarur.

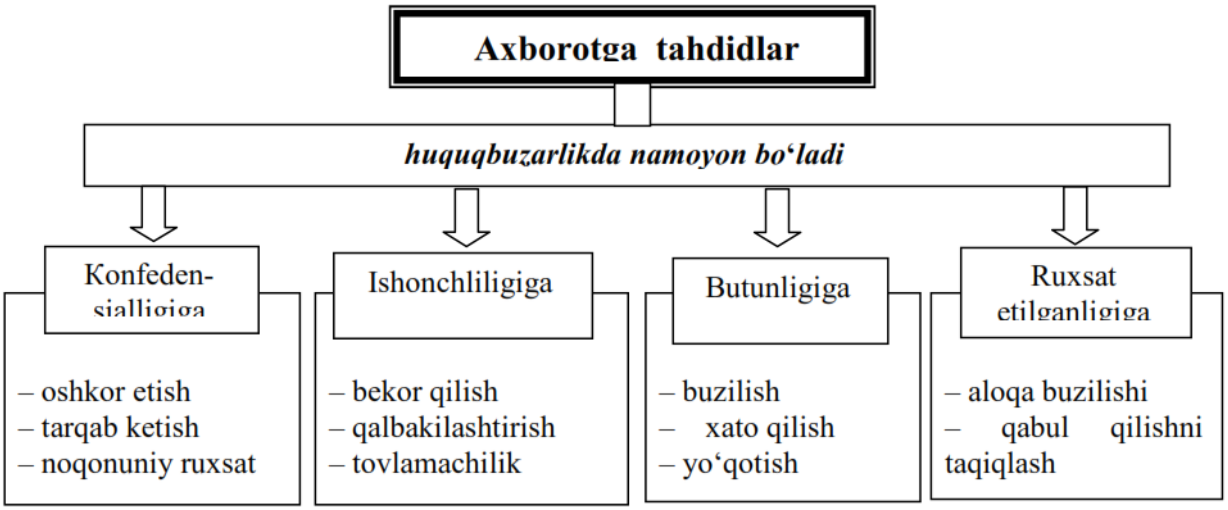
Axborot tarqab ketishiga konfedensial ma’lumotning ushbu axborot ishonib topshirilgan tashkilotdan yoki shaxslar doirasidan nazoratsiz yoki noqonuniy tarzda tashqariga chiqib ketishi sifatida qaraladi.

Tahdidning uchta ko‘rinishi mavjud:

1. Konfedensiallikning buzilishiga tahdid shuni anglatadiki, bunda axborot unga ruxsati bo‘lmaganlarga ma’lum bo‘ladi. Bu holat konfedensial axborot saqlanuvchi tizimga yoki bir tizimdan ikkinchisiga uzatilayotganda noqonuniy foydalana olishlikni qo‘lga kiritish orqali yuzaga keladi.

2. Butunlikni buzishga tahdid hisoblash tizimida yoki bir tizimdan ikkinchisiga uzatilayotganda axborotni har qanday qasddan o‘zgar- tirishni o‘zida mujassamlaydi. Jinoyatchilar axborotni qasddan o‘zgar- tirganda, bu axborot butunligi buzilganligini bildiradi. Shuningdek, dastur va apparat vositalarning tasodifiy xatosi tufayli axborotga noqo- nuniy o‘zgarishlar kiritilganda ham axborot butunligi buzilgan hisob- lanadi. Axborot butunligi – axborotning buzilmagan holatda mavjud- ligidir.

3. Xizmatlarning izdan chiqish tahdidi hisoblash tizimi resurslarida boshqa foydalanuvchilar yoki jinoyatchilar tomonidan ataylab qilingan harakatlar natijasida foydalana olishlilikni blokirovka bo‘lib qolishi natijasida yuzaga keladi. Axborotdan foydalana olishlilik – axborot aylanuvchi, subyektlarga ularni qiziqtiruvchi axborotlarga o‘z vaqtida qarshiliklarsiz kirishini ta’minlab beruvchi hamda ixtiyoriy vaqtda murojaat etilganda subyektlarning so‘rovlariga javob beruvchi avtomatlashtirilgan xizmatlarga tayyor bo‘lgan tizimning xususiyatidir.



Axborot xavfsizligiga tahdidlarning toifalanishi.

Axborot xavfsizligiga tahdidlar darajasiga kora quyidagicha toifalanishi mumkin:

a) shaxs uchun:

– axborotlarni qidirish, olish, uzatish, ishlab chiqish va tarqatish bo‘yicha fuqarolarning konstitutsiyaviy huquqlari va erkinliklarini buzilishi;

– fuqarolarni shaxsiy hayot daxlsizligi huquqidan mahrum qilish;

– g‘ayriixtiyoriy zararli axborotlardan fuqarolarning o‘z sog‘liqlarini himoya qilish huquqlari buzilishi;

– intellektul mulk obyektlariga tahdid.

b) jamiyat uchun:

– axborotlashtirilgan jamiyatni qurishga to‘siqlar;

– jamiyatning ma’naviy yangilanish, uning ma’naviy boyliklarini saqlash, fidoyilik va xolislik, mamlakatning ko‘p asrlik ma’naviy an’analarini rivojlantirish, milliy, madaniy merosni targ‘ib qilish, axloq me’yorlari huquqlaridan mahrum qilish;

– zamonaviy telekommunikatsiya texnologiyalarini taraqqiy etishi, mamlakat ilmiy va ishlab chiqarish potensialini rivojlantirish va saqlab qolishga qarshilik qiluvchi muhitni yaratish.

c) davlat uchun:

– shaxs va jamiyat manfaatlari himoyasiga qarshi harakatlar;

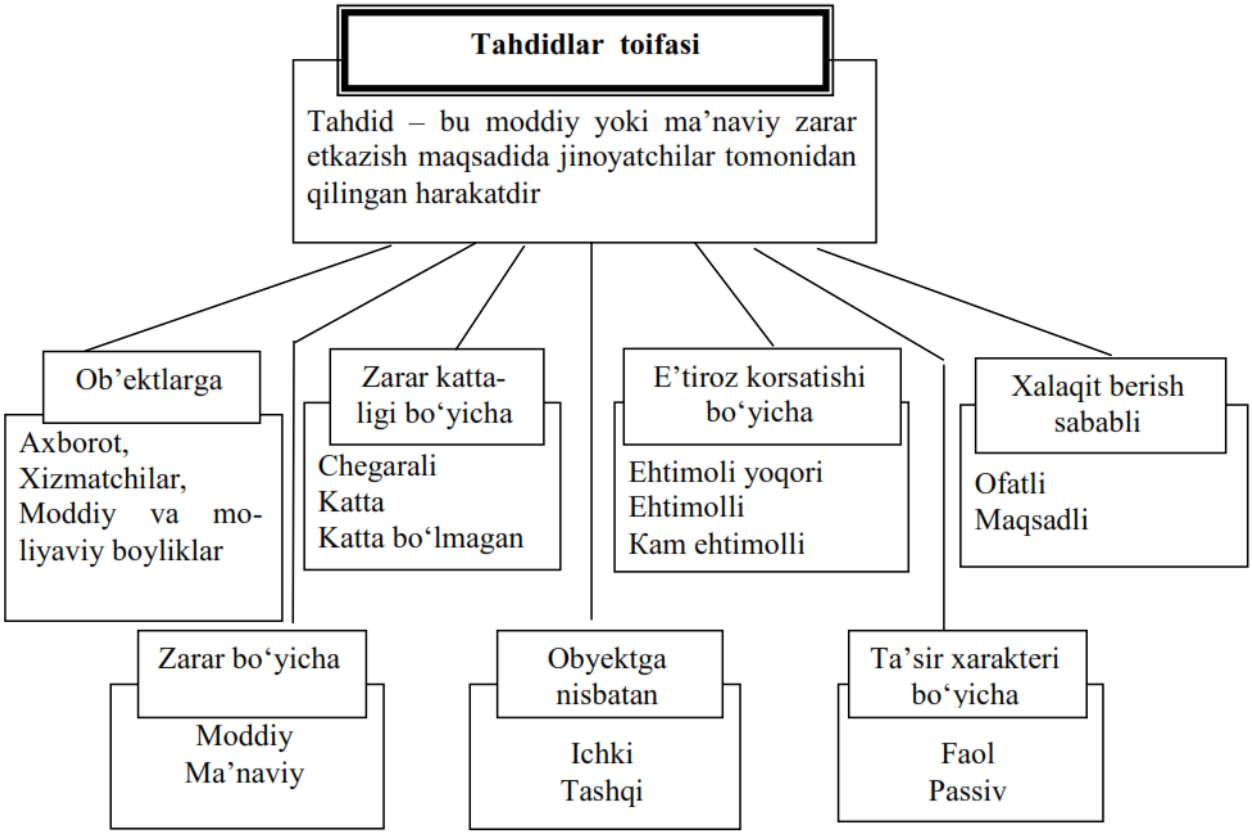
– huquqiy davlat qurishga qarshilik;

– davlat boshqaruv organlari ustidan jamoat nazorati institutlarini shakllantirishga qarshi harakatlar;

– shaxs, jamiyat va davlat manfaatlarini ta’minlovchi davlat boshqaruv organlari tomonidan qarorlarni tayyorlash, qabul qilish va tatbiq etish tizimini shakllantirishga qarshilik;

– davlat axborot tizimlari va davlat axborot resurslari himoyasiga to‘siqlar;

– mamlakat yagona axborot muhiti himoyasiga qarshi harakatlar.



Axborotni muhofaza qilish tizimlaridan foydalanish amaliyoti shuni ko'rsatmoqdaki, faqatgina kompleks axborotni muhofaza qilish tizimlari samarali bo'lishi mumkin. Unga quyidagi chora-tadbirlar kiradi:

1. Qonunchilik. Axborot himoyasi sohasida yuridik va jismoniy shaxslarning, shuningdek davlatning huquq va majburiyatlarini qat'iy belgilovchi qonuniy aktlardan foydalanish.

2. Ma'naviy-etik. Obyektda qat'iy belgilangan o'zini tutish qoidalarining buzilishi ko'pchilik xodimlar tomonidan keskin salbiy baholanishi joriy etilgan muhitni hosil qilish va qo'llab quvvatlash.

3. Fizik. Himoyalangan axborotga begona shaxslarning kirishini taqiqlovchi fizik to'siqlar yaratish.

4. Ma'muriy. Tegishli maxfiylik rejimi, kirish va ichki rejimlarni tashkil etish.

5. Texnik. Axborotni muhofaza qilish uchun elektron va boshqa uskunalardan foydalanish.

6. Kriptografik. Ishlov berilayotgan va uzatilayotgan axborotlarga noqonuniy kirishni oldini oluvchi shifrlash va kodlashni tatbiq etish.

7. Dasturiy. Foydalana olishlilikni chegaralash uchun dastur vositalarini qo'llash.

Fizik, apparatli, dasturli va hujjatli vositalarni o‘z ichiga oluvchi barcha axborot tashuvchilarga kompleks holda himoya obyekti sifatida qaraladi.

Kompyuter tarmoqlaridagi tahdidni quyidagi ikkita asosiy guruhga ajratish mumkin:

I. Texnik tahdidlar:

1. Dasturiy ta’minotdagi xatoliklar.
2. Turli xil DoS- va DDoS-hujumlar.
3. Kompyuter viruslari, chuvalchanglar, troya otlari.
4. Protokollar analizatorlari va eshituvchi dasturlar («snifferlar»).
5. Ma’lumotlarni saqlovchi texnik vositalar

II. Inson faktori:

1. Ishdan bo’shagan yoki ishidan norozi xodimlar.
2. Ishlab chiqarish josuslari.
3. Beparvolik.
4. Past malakalilik.

3. Ishni bajarilish tartibi va qo`yilgan vazifa:

Asosiy tahdid usullaridan birini tanlang va unga himoya vositasi qadamma – qadam izohlansin. SHuningdek **Delphi**, **VBA** yoki **C++** dasturlash tizimida dasturiy ta`minot yaratilsin.

4-amaliy mashg’ulot. Web dasturlaridagi axborot himoyasi

Kirish. Hozirgi vaqtda axborotlarni himoyalashni ta`minlashning qandaydir biror texnik usuli yoki vositasi mavjud emas, ammo ko`p xavfsizlik muammolarini echishda kriptografiya va axborotlarni kriptoo`xshash almashtirishlari ishlatiladi.

1. Ishdan maqsad: Web dasturlash muhitida axborotlarga tahdidlar va ularni himoyalash usulari to’g’risida ma’lumotga ega bo’lish.

2. Qisqacha nazariy ma`lumot:

Korxonalarda joriy etilayotgan avtomatlashtirilgan axborot tizimining xavfsizligini ta’minlash, birinchi navbatda, ushbu tizimni loyixalash bosqichida kuzda tutilgan bulishi lozim. Korxona mikyosida qabul qilingan xavfsizlik siyosatining axborot tizimida qanday darajada aks ettirilishi muxim masalalardan biri xisoblanadi. Lekin, axborot-kommunikatsiyalar texnologiyalarining keskin rivojlanishi, axborot oqimlari xajmining oshishi. Internet va intranet texnologiyalarining keng mikyosda kirib kelishi bevosita avtomatlashtirilgan

axborot tizimlarining axborot zaxiralarini ximoyalashga yunaltirilgan vositalarning mavjudligini ta’minlash xamda tizimda mavjud bo’lgan ximoya vositalarini rivojlantirishini takozo etadi.

Avtomatlashtirilgan axborot tizimlariga nisbatan mavjud bo’lgan xavflarni uchta yunalish buyicha ajratish mumkin:

- amaliy dasturlar;
- tarmoq xizmatlari;
- operatsion tizim xizmatlari.

Amaliy dasturlarni tekshirish buyicha xozirgacha yagona vosita mavjud emas. Tarmoq xizmatlari va operatsion tizim xizmatlarida qo’llaniladigan texnologiyalar umumiy asoslarga ega bo’lganligi uchun ularni tekshirish vositalari ishlab chikilgan.

Zamonaviy operatsion tizimlarda axborot zaxiralarini ximoyalash vositalarining mavjudligi ta’kidlab kelinmokda. Bularga autentifikatsiyalash, identifikatsiyalash, ruxsatsiz kirishni ta’kiklash, monitoring va audit, kriptografiya usullarining mavjudligi misol bula oladi. Albatta, ushbu vositalarning operatsion tizimlarda mavjud bo’lganligi korxonaning xavfsizlik siyosatiga mos keladi. Ammo, operatsion tizimning notugri konfiguratsiyalanishi va uning dasturiy ta’minotidagi mavjud xatolar okibatida axborot tizimlariga xujumlar uyushtirilishi imkoniyati paydo buladi.

Shu bois, operatsion tizimni tanlashda undagi kamchiliklarni taxlil qilish, ishlab chiqaruvchi firma tomonidan yul kuyilgan xatolarning tan olinishi va ularni zudlik bilan tuzatishga kirishilishi talab etiladi.

Operatsion tizimning parametrlarining tugri urnatilganligini yoki ularning uzgarmaganligini tekshirish uchun «tizim xavfsizligini skanerlash» deb nomlanuvchi 10 ga yakin maxsus dasturlar ishlab chikarilgan. Masalan, Solaris operatsion tizimi uchun muljallangan ASET, Netware va NT uchun KSA, Unix uchun SSS dasturlari mavjud.

SSS (System Security Scanner) dasturi haqida.

Ushbu dastur Unix operatsion tizimi urnatilgan kompyuterlarda xavfsizlik xolatini tekshirish va operatsion tizimning tashki xamda ichki zaif qismlarini aniqlashga yunaltirilgan. Bundan tashkari u kirish xukuklarini, fayllarga egalik qilish xukuklarini, tarmoq zaxiralarini konfiguratsiyalashni, autentafikatsiyalash dasturlarini va boshqalarni tekshirishi mumkin.

Dasturning quyidagi imkoniyatlari mavjud:

- Konfiguratsiyani tekshirish, ya’ni ruxsatsiz kirishlarning oldini olish maksadida konfiguratsiyani tekshirish. Bunga quyidagilar kiradi: konfiguratsiya fayllari, operatsion tizim versiyasi, kirish xukuklari, foydalanuvchilarning zaxiralari, parollar;
- Tizimdagi xavfli o’zgarishlarni tekshirish. Ruxsatsiz kirishlar okibatida tizimda sodir bo’lgan o’zgarishlarni kidirishda qo’llaniladi. Bunday o’zgarishlarga quyidagilar kiradi: fayllar egallagan xotira xajmining o’zgarishi, ma’lumotlarga kirish xukuki yoki fayldagi ma’lumotlarning o’zgarishi, foydalanuvchilarning zaxiralarga kirish parametrlarining uzgari-shi, fayllarni ruxsatsiz boshqa bir tashki kompyuterlarga uzatishlar;
- Foydalanuvchi nnterfeysining kulayligi. By interfeys yordamida nafakat dastur bilan kulay ishlash ta’minlanadi, balki bajarilgan ishlar buyicha xisobotlar xam yaratiladi;
- Masofadan skanerlash. Tarmoqdagi kampyuterlarni tekshirish va aloka jarayonida ma’lumotlarni shifrlash imkoniyati ta’minlanadi;
- Xisobotlar tuzish. Bajarilgan ishlar buyicha tulik, xisobotlap yaratiladi. Ushbu xisobotlarda tizimning aniqlangan zaif buginlarining izoxi keltiriladi va ularni tuzatish buyicha kursatmalar beriladi. Xisobot HTML yoki oddiy matn kurinishida bulishi mumkin.

Tarmoq xizmatlarining ximoyalanganligini taxlil qilish buyicha birinchi bulib ishlab chikarilgan dasturlardan biri bu SATAN dasturidir. Bu dastur 20 ga yakin tarmoq xizmatlaridagi zaifliklarni aniqlay oladi.

Internet Scanner SAFEsuite dasturi haqida.

Agar tekshiruvlar doimiy ravishda va tulik amalga oshirilishi talab qilinsa, u xakda internet

Scanner SAFEsuite dasturlar paketi taklif qilinadi. Bu dasturlar paketi yordamida 140 ta ma’lum bo’lgan zaifliklar va tarmoq vositalari, ya’ni tarmoqlararo ekranlar, Web-serverlar, Unix, Windows 9.x, Windows NT tizimli serverlar va ishchi stansiyalar, umuman TCP/IP protokoli qo’llaniladigan barcha vositalar tekshiriladi. Internet Scanner SAFEsuite paketiniig umumiy imkoniyatlari quyidagilardan iborat:

1. Avtomyatlashtirilgan va konfiguratsiyalangan skanerlash:

- avtomatlashgan identifikatsiyalash va zaif qismlar buyicha xisobot tuzish;
- doimiy reja buyicha skanerlash;
- IP manzillarni skanerlash;

- foydalanuvchi urnatgan parametrlarni skanerlash;
- zaif buginlarni avtomatik ravishda tuzatish;
- ishonchlilik va takrorlanuvchanlikni ta’minlash.

2. Xavfsizlikni ta’minlash:

- tarmoq vositalarini inventarizatsiyalash va mavjud asosiy zaif buginlarni identifikatsiyalash;
- asosiy xisobotlarni takkoslash va kelgusida ulardan foydalanish uchun taxlil qilish.

3. Foydalanishning oddiyligi:

- foydalanuvchining grafik interfeysi;
- HTML turidagi tartiblangan xisobotlarni yaratish;
- skanerlashni markazlashtirilgan xolda bajarish, boshqarish va monitoring utkazish. Internet Scanner SAFEsuite paketida quyidagi dasturlar mavjud:
- Web Security Scanner,
- FireWall Scanner va Intranet Scanner.
- Web Security Scanner bevosita Web-serverlarda mavjud zaif qismlarni aniqlashga muljallangan bulib, bu dasturning imkoniyatlari quyidagilardan iborat:
- Web-server urnatilgan operatsion tizimni auditlash;
- Web-serverda mavjud dasturlarni auditlash;
- Web-fayllarda mavjud skriptlarni auditlash;
- Web-server konfiguratsiyasini testdan utkazish;
- Asosiy fayllar tizimining xavfsizlik darajasini aniqlash;
- Skriptlarda mavjud xatolarni aniqlash;
- Bajarilgan ishlar buyicha xisobotlar yaratish va xatolarni tuzatish borasida takliflar berish.
- FireWall Scanner dasturi bevosita tarmoqlararo ekranda mavjud bo’lgan zaif qismlarni aniqlashga muljallangan bulib, u quyidagi amallarni bajaradi:
- Tarmoqlararo ekranga xujumlar uyushtirib, uni testdan utkazish;
- Tarmoqlararo ekran orkali utadigan tarmoq, xizmatlarini skanerlash.

Intranet Scanner dasturi kompyuter tarmogida mavjud kamchiliklarni tarmoqka ruxsatsiz kirishlarini amalga oshirish orkali testdan utkazish yordamida aniqlashga yunaltirilgan. Tarmoqning xir xil qismlari (xost-kompyuterlar,

yullovchilar, Web-serverlar, Windows 9.x/NT tizimida ishlaydigan kompyuterlar) ni tekshirishni xam amalga oshiradi.

Yuqorida keltirilganlardan tashkari kompyuter tizimlariga ruxsatsiz kirishlarni doimiy ravishda nazorat kiluvchi dasturlar, masalan, Internet Security Systems kompaniyasi tomonidan ishlab chikilgan Real Secure dasturi xam mavjud. Bu dastur tarmoqda sodir etilayotgan xodisalar, masalan, xakerlarning xujumlarini kayd qilish bilan birgalikda faol ximoya chora-tadbirlarini tashkillashtirishi mumkin. Real Secure dasturi yirik tashkilotlar uchun muljallangan bulib, xar kuni tinimsiz ishlashga muljallangan.

Real Secure dasturi ikki qismdan iborat: filtrlash va foylalanuvchining grafik nnterfeysi.

Filtrlash qismi tarmoqda sodir etilayotgan xodisalarni faol kuzatish va boshqarish uchun xizmat qiladi. Dasturning ikkinchi qismi yordamida foylalanuvchi ro`y bergan xodisalar xaqidagi ma’lumotlarni qabul qiladi, ularni boshqaradi va tizim konfiguratsiyasini o`zgartira oladi. Natijada, filtrlash va sodir etilayotgan xodisalarga nisbatan himoya tadbirlarini avtomatik ravishda amalga oshirish mumkin buladi, masalan, qayd qilish, displeyga chiqarish, xodisani man etish va boshqalar.

Bulardan tashqari barcha qayd etilgan xodisalar xaqidagi malumotlarni keyinchalik real masshtabda yoki tezkor yoki sekinlashgan rejimlarda ko`rib chiqish mumkin bo`ladi.

Real Secure dasturi bevosita Sun OS, Solaris va Linux operatsion tizimlarida ishlash uchun muljallangan.

3. Ishni bajarilish tartibi va qo`yilgan vazifa:

Yuqorida ko`rsatilgan dasturlardan foydalanib web dasturlariga bo`ladigan turli xildagi hujumlarni aniqlash. Asosiy tahdid usullaridan birini tanlang va unga himoya vositasi qadamma – qadam izohlansin. SHuningdek **Delphi**, **VBA** yoki **C++** dasturlash tizimida dasturiy ta`minot yaratilsin.

V. GLOSSARIY

1.	**Loyihalash metodologiyasi**	muayyan kontseptsiyaning, loyihalash tamoyillarining mavjudligini nazarda tutadi, bu o'z navbatida, ba'zi usullar bilan qo'llab-quvvatlanishi kerak bo'lgan usullarning to'plami tomonidan amalga oshiriladi.
2.	**Loyihalash tashkiloti**	AT-loyihani yaratish jarayonida dizaynerlarning o'zlari va mijozlar bilan o'zaro munosabatlar usullarini aniqlashni nazarda tutadi, bu ham o'ziga xos vositalar to'plami tomonidan qo'llab-quvvatlanishi mumkin.
3.	**Tizimning texnik loyihasi**	bu texnik hujjat bo'lib, u belgilangan tartibda tasdiqlangan, umumloyihaviy qarorlardan tarkib topgan, masalani yechish algoritmiga ega bo'lgan, shuningdek avtomatlashtirilgan boshqarish tizimining iqtisodiy samaradorligi baholangan va ob'ektni joriy etish bo'yicha tadbirlarni o'z ichiga olgan majmuadir.
4.	**Dastvvval CASE termini**	dasturiy ta'minotni ishlab chiqishni avtomatlashtirish masalalarida qo'llanilgan bo'lsa, hozirgi kunda yangi ma'noda, ya'ni murakkab avtomatlashtirilgan axborot tizimlarini ishlab chiqishda qo'llaniladi.
5.	**CASE-vositalar**	tizimli dasturiy ta'minot va texnik vositalar bilan hamkorlikda axborot tizimini ishlab chiqish muhitining to'liq muhitini hosil etadi.
6.	**CASYe-texnologiyasi**	IT dizayn bir metodologiyasi, shuningdek, taqlid foydalanuvchilar axborot ehtiyojlarini muvofiq rivojlantirish va IT qo'llab-quvvatlash va ilovalar ishlab chiqish, barcha bosqichlarida modelini tahlil qilish mavzu sohada shaklini tasavvur qilish imkonini beradi vositalari to'plamidir.
7.	**Texnologiya.**	Mavjud imkoniyatlarning chegaralanganligini anglab yetish va yangi texnologiyani qabul qilish qobiliyatiga ega bo'lish.
8.	**Madaniyat**.	Ishlab chiquvchilar va foydalanuvchilar orasida yangi jarayonlarni va munosabatlarni joriy etishga tayyor bo'lish.
9.	**Boshqaruv.**	Muhim etaplar va joriy etish jarayonlariga nisbatan aniq rahbarlik va tashkilotchilik qilish.

10.	**Samaradorlik.**	Texnik vositalarga qo’yiladigan talablar. Optimal kattaligi va tashqi xotira, protsessor turi va bajarishi, maqbul ish faoliyatini taminlash uchun talablar.
11.	**Mahsuldorlik.**	CASYe vositasi malum vazifalarni bajarish uchun sarflagan vaqt (masalan, so’rov uchun javob vaqti, 100000 satr kodni tahlil qilish vaqti). Bazi hollarda tashqi manbalardan olinishi mumkin.
12.	**Ko’chuvchanlik.**	Operatsion tizim versiyalariga muvofiqligi (bir xil operatsion tizimning turli xil versiyalari muhitida ishlash qobiliyati, operatsion tizimning yangi versiyalari bilan ishlash uchun CASYe-vositasining modifikatsiyasi qulayligi).
13.	**Tizimning yadrosini**	repozitoriy tashkil etadi. U maxsus ma’lumotlar bazasi bo’lib, ixtiyoriy vaqtda tizim holatini akslantirish uchun qo’llaniladi. Repozitoriy loyihaviy axborot tizimining barcha ob’ektlari xususidagi axborotga ega.
14.	**Loyiha dokumentatori**	ob’ekt holati to’ғrisida hisobot ko’rinishida axborot olish imkonini beradi.
15.	**Loyiha administratori**	instrumentlar bo’lib, ular quyidagi funktsiyalarni bajarish uchun zarur.
16.	**CASE-vositalarni baholash va tanlash**	bir nechta maqsadlarni ko’zlashi mumkin va u quyidagi bitta yoki undan ko’p maqsadlarni ko’zlaydi:
17.	**Servis**	repozitoriyaga xizmat ko’rsatish uchun tizimli utilitalar majmuasi.
18.	**Tizimning texnik loyihasi**	bu texnik hujjatlar bo’lib, unda quyidagi hujjatlar o’z aksini topgan: umumtizimli loyiha qarorlari, masalani yechish algoritmi, ABSning iqtisodiy samaradorligi bahosi, ob’ektni joriy etishga tayorlash tadbirlari va h.k.
19.	**Texnik topshiriq**	bu hujjat bo’lib, u ABS ishlab chiqish uchun zarur bo’lgan maqsadlarni, talablarni va asosiy boshlanғich ma’lumotlarni o’z ichiga oladi.
20.	**Xavfsizlik deganda**	tizimning xususiyati asosida begona shaxslar tashkilotning axborot resurslariga ega bo’lmasligi kerak
21.	**Axborot tizimini loyihalash**	loyihaviy konstruktorlik va texnologik hujjatlar bo’lib, unda aniq dasturiy –texnik muhitda axborot

		tizimini yaratish hamda espluatatsiya qilishning loyihaviy qarorlari o’z aksini topadi.
22.	**Axborot tizimini loyihalash deganda**	ob’ekt xususida boshlanғich kirish axborotni o’zgartirish jarayoni, xuddi shunday ob’ektlarni GOST bo’ymcha axborot tizimiga loyihalash tajribasi tushunaladi.
23.	**Tizimni ishlab chiqish**	masshtabi bo’yicha loyihalash jarayonida qvtnashadigan ijrochilarning tarkibi va soni aniqlanadi.
24.	**Axborot tizimini loyihalash texnologiyasi**	axborot tizimini loyihalashning metodologiyasi va vositalari majmuasi hamda uni tashkil etish usul va vositalaridir (ishlab chiqish jarayonini boshqarish va ATning loyihasini modernizatsiyalash).
25.	**Verifikatsiya**	shu bosqichgacha erishilgan ishlab chiqishning joriy holati, ushbu bosqich talablariga javob bera olishini aniqlaydagan jarayondir.
26.	**Axborot tizimining hayotiy tsikli**	bu uzluksiz jarayon bo’lib, axborot tizimini yaratish zaruriyati haqidagi qarorning qabul qilinishadan boshlab, to uni ekspluatatsiyadan to’la chiqarishgacha bo’lgan davrni o’z ichiga oladi.
27.	**Loyihalash metodologiyasi**	ayrim kontseptsiyaning mavjudligi bo’lib, unda metodlar majmuasi asosida loyihalash printsiplari o’z aksini topadi.
28.	**Tizimning texnik loyihasi**	bu texnik hujjatlar bo’lib, unda quyidagi hujjatlar o’z aksini topgan: umumtizimli loyiha qarorlari, masalani yechish algoritmi, ABSning iqtisodiy samaradorligi bahosi, ob’ektni joriy etishga tayorlash tadbirlari va h.k.
29.	**Texnik topshiriq**	bu hujjat bo’lib, u ABS ishlab chiqish uchun zarur bo’lgan maqsadlarni, talablarni va asosiy boshlanғich ma’lumotlarni o’z ichiga oladi.
30.	**Tipovoy loyihalash yechimi**	bu tiraj qilinadigan loyihaviy yechimdir (ko’p foydalanuv-chiga yaraqli loyiha).
31.	**Axborot tizimining buyurtmachisi**	tashkilot bo’lib, uning talablari asosida axborot tizimini yaratish belgilanadi.
32.	**Axborot tizimini ishlab chiquvchi**	axborot tizimini yaratish bilan shuғullanadigan tashkilot bo’lib, uni loyihalashdan to buyurtmachiga

		ekspluatatsiyaga topshirishgacha bo'lgan ishlarni amalga oshiradi.
33.	**Tranzaktsiyalarni qayta ishlash tizimlari**	o'z novbatida ma'lumotlarni qayta ishlash bo'yicha paketli axborot tizimlariga va tezkor axborot tizimlariga bo'linadi. Tashkiliy boshqaruv tizimlarida tranzaktsiyalarni tezkor qayta ishlash rejimi (OnLine Transaction Processing, OLTP) ustuvor bo'lib, istalgan vaqt momentida predmet sohani dolzarb holatini akslantirish uchun xizmat qiladi. Paketli qayta ishlash esa ning kam qismini tashkil etadi.
34.	**Қarorlar qabul qilishni qo'llab-quvvatlal tizimlari**	(Decision Support System, DSS) boshqa tipdaga axborot tizimi bo'lib, unda nisbatan murakkab so'rovlar yordamida turli kesimlarda (vaqt, geografik va boshqa ko'rsatgichlar) ma'lumotlarni tanlash va tahlil qilish ishlari amalga oshiriladi.
35.	**Axborot-ma'lumotnoma tizimlari**	ularning katta sinfi multimedianing gipermatnli hujjatlariga asoslangan. Bunday axborot tizimlari rivoji Internetda keng tarqalgan.
36.	**Ofisli axborot tizimlari**.	Ularning aksariyati qaғozli hujjatlarni elektron ko'rinishga aylantirishga va ish yuritishni avtomatlashtirishga yo'naltirilgan.
37.	**Ma'lumotlarni saqlash tipi bo'yicha**	ATlari faktografik va hujjatli guruhlarga bo'linadi.
38.	**Faktografik tizimlar**	strukturlashtirilgan ma'lumotlarni son va matn ko'rinishida saqlash va qayta ishlash uchun xizmat qiladi. Bunday ma'lumotlar ustida turli amallarni bajarish mumkin.
39.	**Ҳujjatli tizimlarda**	axborot hujjat ko'rinishida taqdim etilgan bo'lib, ular tavsif, rederat, matnlardan tashkil topgan. Strukturlashtirilmagan ma'lumotlar ustida qidiruv semantik belgilar bo'yicha amalga oshiriladi. Bunday tizimlarda tanlangan hujjatlar foydalanuvchiga taqdim etiladi, ma'lumotlarni qayta ishlash esa deyarli bajarilmaydi.
40.	**Avtomatlashtirish darajasi bo'yicha**	axborot jarayonlarini avtomatlashtirish darajasi bo'yicha axborot tizimlari qo'lda bajariladigan,

		avtomatlashgan va avtomatlashtirilgan guruhlarga bo'linadi.
41.	**Egiluvchanlik**	adaptatsiyalash (moslashganlik) va keyinchalik ham rivojlanishi mumkin bo'lgan axborot tizimining qobiliyati bo'lib, axborot tizimini yangi sharoitlarda mosllashishini va tashkilotning yangi ehtiyojlarini qondirish imkoniyatlarining mavjudligini bildiradi.
42.	**Bunday shartlarni bajarish**	faqat axborot tizimini ishlab chiqish jarayonida umumqabul qilingan hajjatlashtirishning usul va vositalari joriy etilgan bo'lishi kerak.
43.	**Samaradorlik**	tizim samarali hisoblanadi, qachonki una ajratilgan resurslar hisobidan u o'ziga biriktirilgan vazifalarni minimal muddatda bajara olganda. Tizimning samaradorlik bahosi buyurtmachi tomonidan belgilanadi. Tizimning samaradorligiga salbiy baho olmaslik uchun uni ishlab chiqishning barcha bosqichlarida buyurtmachining vakilini jalb etish kerak.
44.	**Xavfsizlik deganda**	tizimning xususiyati asosida begona shaxslar tashkilotning axborot resurslariga ega bo'lmasligi kerak.
45.	**Loyihalash metodologiyasi**	muayyan kontseptsiyaning, loyihalash tamoyillarining mavjudligini nazarda tutadi, bu o'z navbatida, ba'zi usullar bilan qo'llab-quvvatlanishi kerak bo'lgan usullarning to'plami tomonidan amalga oshiriladi.
46.	**Loyihalash tashkiloti**	AT-loyihani yaratish jarayonida dizaynerlarning o'zlari va mijozlar bilan o'zaro munosabatlar usullarini aniqlashni nazarda tutadi, bu ham o'ziga xos vositalar to'plami tomonidan qo'llab-quvvatlanishi mumkin.
47.	**Tizimning texnik loyihasi**	bu texnik hujjat bo'lib, u belgilangan tartibda tasdiqlangan, umumloyihaviy qarorlardan tarkib topgan, masalani yechish algoritmiga ega bo'lgan, shuningdek avtomatlashtirilgan boshqarish tizimining iqtisodiy samaradorligi baholangan va ob'ektni joriy etish bo'yicha tadbirlarni o'z ichiga olgan majmuadir.
48.	**Dastvvval CASE termini**	dasturiy ta'minotni ishlab chiqishni avtomatlashtirish masalalarida qo'llanilgan bo'lsa, hozirgi kunda yangi

		ma’noda, ya’ni murakkab avtomatlashtirilgan axborot tizimlarini ishlab chiqishda qo’llaniladi.
49.	**CASE-vositalar**	tizimli dasturiy ta’minot va texnik vositalar bilan hamkorlikda axborot tizimini ishlab chiqish muhitining to’liq muhitini hosil etadi.
50.	**CASYe-texnologiyasi**	IT dizayn bir metodologiyasi, shuningdek, taqlid foydalanuvchilar axborot ehtiyojlarini muvofiq rivojlantirish va IT qo’llab-quvvatlash va ilovalar ishlab chiqish, barcha bosqichlarida modelini tahlil qilish mavzu sohada shaklini tasavvur qilish imkonini beradi vositalari to’plamidir.
51.	**Texnologiya.**	Mavjud imkoniyatlarning chegaralanganligini anglab yetish va yangi texnologiyani qabul qilish qobiliyatiga ega bo’lish.
52.	**Madaniyat**.	Ishlab chiquvchilar va foydalanuvchilar orasida yangi jarayonlarni va munosabatlarni joriy etishga tayyor bo’lish.
53.	**Boshqaruv.**	Muhim etaplar va joriy etish jarayonlariga nisbatan aniq rahbarlik va tashkilotchilik qilish.
54.	**Samaradorlik.**	Texnik vositalarga qo’yiladigan talablar. Optimal kattaligi va tashqi xotira, protsessor turi va bajarishi, maqbul ish faoliyatini taminlash uchun talablar.
55.	**Mahsuldorlik.**	CASYe vositasi malum vazifalarni bajarish uchun sarflagan vaqt (masalan, so’rov uchun javob vaqti, 100000 satr kodni tahlil qilish vaqti). Bazi hollarda tashqi manbalardan olinishi mumkin.
56.	**Ko’chuvchanlik.**	Operatsion tizim versiyalariga muvofiqligi (bir xil operatsion tizimning turli xil versiyalari muhitida ishlash qobiliyati, operatsion tizimning yangi versiyalari bilan ishlash uchun CASYe-vositasining modifikatsiyasi qulayligi).

57.	**Tizimning yadrosini**	repozitoriy tashkil etadi. U maxsus ma’lumotlar bazasi bo’lib, ixtiyoriy vaqtda tizim holatini akslantirish uchun qo’llaniladi. Repozitoriy loyihaviy axborot tizimining barcha ob’ektlari xususidagi axborotga ega.
58.	**Loyiha dokumentatori**	ob’ekt holati to’ғrisida hisobot ko’rinishida axborot olish imkonini beradi.
59.	**Loyiha administratori**	instrumentlar bo’lib, ular quyidagi funktsiyalarni bajarish uchun zarur.
60.	**CASE-vositalarni baholash va tanlash**	bir nechta maqsadlarni ko’zlashi mumkin va u quyidagi bitta yoki undan ko’p maqsadlarni ko’zlaydi:
61.	**Servis**	repozitoriyaga xizmat ko’rsatish uchun tizimli utilitalar majmuasi.

VI. FOYDALANGAN ADABIYOTLAR

I. Maxsus adabiyotlar

1. Ganiev S.K., Karimov M.M., Toshev K.A. Axborot xavfsizligi. O'quv qo'llanma .-TATU «Aloqachi», 2008.
2. Jukov YU. V. Osnovы veb-xakinga. Napadenie i zaщita (2-e izd.). Piter.2012. 206c.
3. S.A. Babin. Instrumentarii XAKERA. BXV-Peterburg. 2014 g. 233 s.
4. Vivek Ramachandran - BackTrack 5 Wireless Penetration Testing – 2011. 220 p.
5. Flyonov M.E. Kompyuter glazami xakera. 2012g. BXV-Peterburg. 2012g. 274s.
6. Andrianov V. V. Zefirov S. L. Golovanov V. B. Golduev N. A. Obespechenie informatsionnoy bezopasnosti biznesa. 2011g. 265 s.
7. Platonov V.V. Programmno-apparatnыe sredstva zaщitы informatsii (Vыsshee professionalnoe obrazovanie. Bakalavriat). AKADEMIA. 2013g. 331 s.
8. Shangin V.F. Zaщita informatsii v kompyuternых sistemax i setyax. DMK. 2012g. 593s.
9. Romanets YU.V.,Timofeev P.A., SHangin V.F. Zaщita informatsii v kompyuternых sistemax i setyax./ M.: Radio i svyaz,2010.-376s.\
10. Barry L. Williams. «Information Security Policy Development for Compliance»: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0. 2013 year.