DAVLAT ORGANLARI XIZMATLARI MA'LUMOT BAZASINI AXBOROT XAVFSIZLIGI RISKLARINI TA`MINLASH TA'MOILLARI

X.X.Iminova
Toshkent shahridagi "MMFI" Milliy tadqiqot yadro universiteti
https://doi.org/10.5281/zenodo.10656418

Hozirgi kunda axborotlarni saqlash va ularni qayta ishlash tushunchasi bu juda keng tushunchadir. Barcha mamlakatlarda maxfiy ma`lumotlarni saqlashning o`ziga xos xususiyatlari mavjud. Bunday ma`lumotlarga misol qilib banklar yoki yuridik sistemalar, axborotlarni xavfsiz almashish va boshqa bir qator tizimlarni keltirishimiz mumkin. Bunday tizimlar uchun axborotlarning xavfsizligi risklari darajasi shu tizimda ishlovchilar ma`lumot almashuvchi foydalanuvchilar uchun juda muhim hisoblanadi.

Yangi axborot texnologiyalarining paydo bo`lishi, kompyuter sistemalarining yanada takomillashuviga va mavjud tizimlarning axborotlarini saqlash va ularni qayta ishlashga ketadigan vaqtlari hisobiga axborotlarni muhofazasini oshirishga olib keldi. Maxfiy ma`lumorlar himoyasi majburiy holatga kelib qoldi. Buzg`unchilar esa axborot muhofazasini buzish uchun shu tizim haqida barcha mavjud hujjatlar tayyorlanmoqdalar, tizim mutaxasislarning takliflari hosil qilinmoqda (axborot tizimlariga asosan yuqori malakaga ega bo`lgan mutaxasislar tahdid soladilar) va albatta tizimda mavjud muammolar o`rganilmoqda. Bu esa o`z o`rnida axborotlarni himoyasiga bo`ladigan tahdidlarni oshiradi. Bularning barchasi kelib chiqib aytadigan bo`lsak, axborot tizimlarida axborot xavfsizligi risklari asosiy xususiyatlardan biriga aylandi.

Avvalambor axborot xavfsizligi tushunchasiga qisqacha ta`rif berib o`tsak axborot xavfsizligi bu ma`lumotlarni yo`qotish yoki o`zgartirish yo`naltirilgan tabiiy yoki sun`iy xossali tasodifiy yoki qasddan bo`ladigan ta`sirlardan har qanday axborotlarni himoyalanganligiga aytiladi.

Axborot himoya tushunchasi haqida fikr yuritishdan oldin axborotlarga nimalar xavf solishi mumkinligi haqida qisqacha to`xtalib o`tsak. Harqanday korxonaning maxfiy axborotiga 2 xil risk (xavf) bo`lishi mumkin, bu risklar (xavflar) biz shartli ***ICHKI*** va ***TASHQI*** risklar (xavflar) deb ataymiz. Tashqi xavflar -bu internet orqali yoki qo`shimcha zararli dasturlar orqali buzg`unchilar tomonidan axborotni buzish yoki o`zgartirishga urunish bo`lsa, ichki xavf bu tashkilot ishchilari ehtiyotsizliklari (qastdan yoki tasodifiy), fizik qurilmalarning nosozligi va shunga o`xshash manbalardan kelib chiqadigan xavflar hisoblanadi.

Tashqi omillar internet orqali axborotlar quyida risk tug`ilishi mumkin: ***BRUTE FORCE, DDOS, PHP-INEKSIYA, XSS, CSRF, SQL-INYEKSIYA***

Yuqorida keltirilgan axborotlarni buzish manbalari haqida to`xtalib o`tamiz:

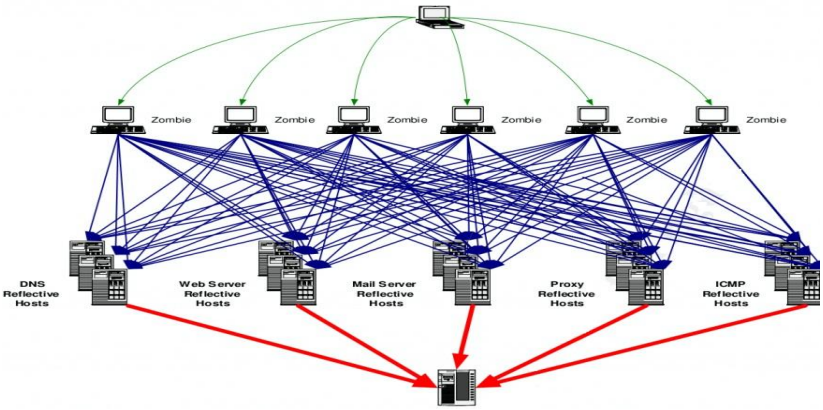
Brute force- matematik usul bo`lib, bu usul yordamida kalitning barcha mavjud variantlari ko`rib chiqiladi. Shuni unutmaslik kerak-ki har qanday axborotni *Brute force* usuli orqali buzish mumkin, faqat buning uchun vaqt talab qilinadi. Vaqt esa albatta kalit uzunligiga bog`liq. Kalit uzunligi yetarli darajada bo`lmagan ma`lumotlarni buzish uchun eng yaxshi holatda bir necha soat talab qilinsa, kalit uzunligi yetarli darajada bo`lgan axborotlarni esa buzish uchun bir necha yillar yoki bir necha yuz yillar kerak bo`ladi. Quyida oddiy kompyuterda himoyalangan axborotlarni buzish uchun *Brute force* usuli orqali talab qilinadigan vaqtlarni ko`rsatib o`tamiz: (taxmin qilamiz 36 xil belgidan foydalangan holda parol qo`yilgan va electron hisoblash mashinasining 1 sekundda kalitlarni ko`rish tezligi 100 000 ta)

Belgilar soni	Variantlar soni	Kalit uzunlig	Kalitni topish vaqit
1	36	5 бит	**Sekunddan kam vaqt**
2	1296	10 бит	**Sekunddan kam vaqt**
3	46 656	15 бит	**Sekunddan kam vaqt**
4	1 679 616	21 бит	**17 sekund**
5	60 466 176	26 бит	**10 minutda**
6	2 176 782 336	31 бит	**6 soatda**
7	78 364 164 096	36 бит	**9 kunda**
8	2,821 109 9x10^{12}	41 бит	**11 oyda**
9	1,015 599 5x10^{14}	46 бит	**32 yilda**
10	3,656 158 4x10^{15}	52 бита	**1 162 yilda**
11	1,316 217 0x10^{17}	58 бит	**41 823 yilda**
12	**4,738 381 3x10^{18}**	**62 бита**	**1 505 615 yilda**

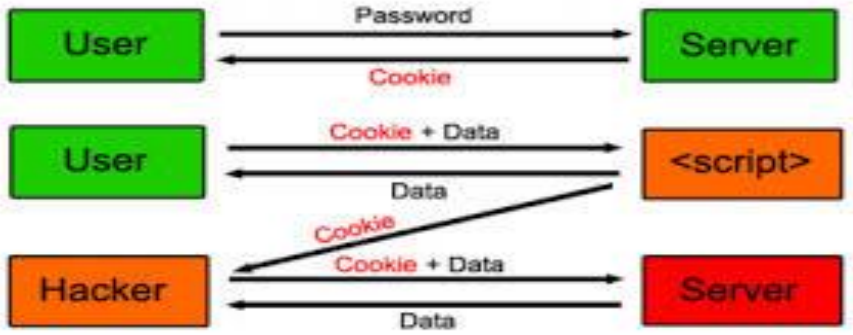
Bu jadvaldan kelib chiqib ma`lumotlarni himoya qilishda foydalanadigan kalit uzunligini tanlash mumkin. Shuni unutmasligimiz kerak hozirgi kunda eng zamonaviy kompyuterlardan biri hisoblangan ROADRUNNER (IBM kompaniyasi mahsuloti) bir sekundda 1 000 000 000 000 tagacha amal bajarishlari mumkin, hamda EHM-lari amal bajarish tezligi vaqt o`tgan sari kamayib bormoqda. Demak 10 yil oldin *Brute force* usuli bilan biror bir axborotni buzish uchun bir necha yil talab qilingan bo`lsa, hozirgi kunga kelib buning uchun bir necha soat yoki undan ham kam vaqt yetarli bo`lishi mumkin.

DOS (Denial of Service) yoki DDOS (Distributed Denial of Service)

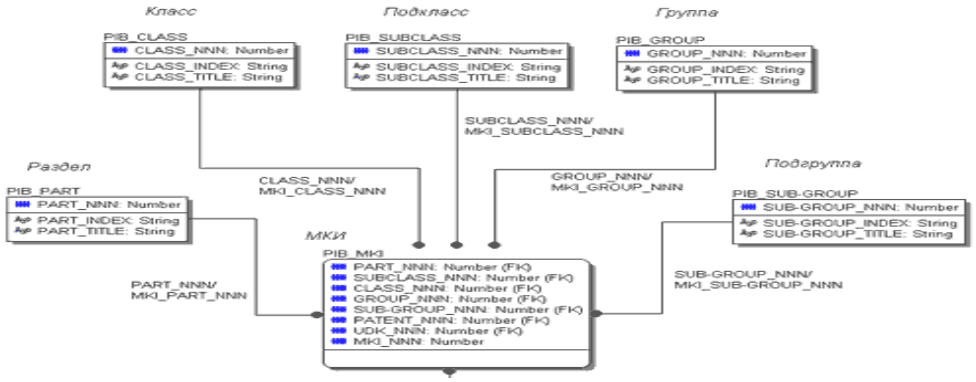
DoS (denial-of-service) –xujum qilinayotgan server (nishon) ni faoliyatini vaqtinchalik to'xtatib qo'yish. Bunda xujum qiluvchi nishondagi (target) mavjud xatoliklardan foydalanib unga maxsus noto'gri so'rovlar orqali murojat qilib buffer to'lishini (buffer overflow) ni yuzaga keltiradi. Yana bir usuli nishonga to'xtovsiz juda ko'p so'rovlar jo'natish (flood – so'rovlar bilan bombardimon qilish) orqali ham amalga oshirilishi mumkin.



XSS (*Cross Site Scripting)*-web sahifalarga tashrif buyuruvchilarga hujum qilish turi. Bunday hujum tirida buzgunchilar ko`proq HTTP protocol kamchiliklaridan foydalanadilar. Bu usuldan birinchi marta 2000 yillarda foydalanilgan.



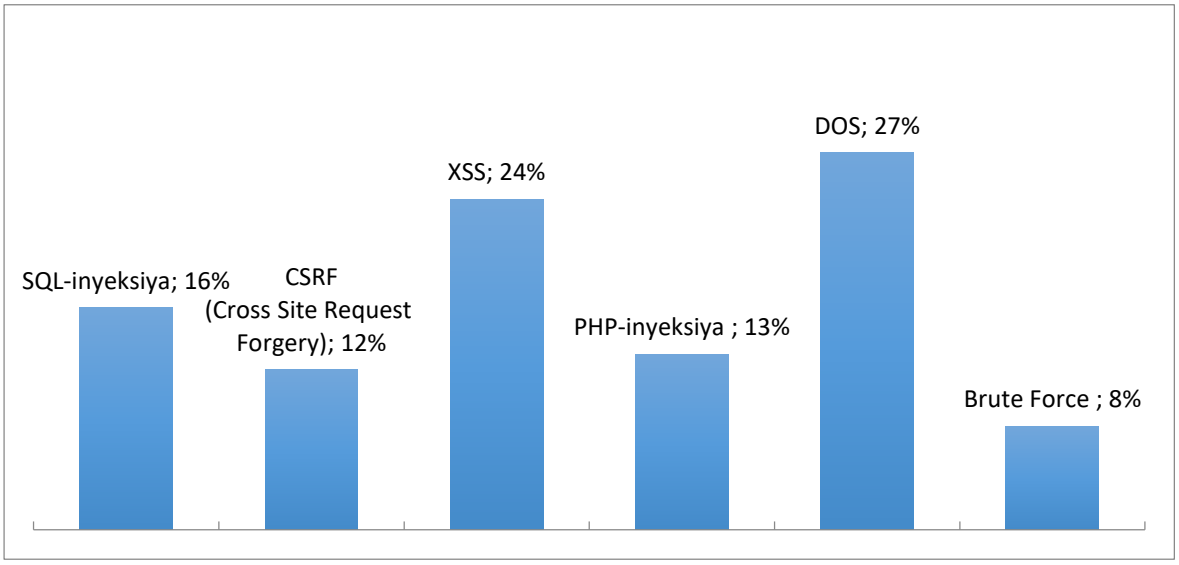
SQL(SQL injection)- keng tarqalgan usullardan biri hisoblanadi. Saytlarni yoki ma`lumotlar ombori bilan ishlaydigan dasturlarni buzish uchun xizmat qiladi.



CSRF (Cross Site Request Forgery) — HTTP protokolning kamchiliklaridan foydalangan holda web saytlarga tashrif buyuruvchilarni zarar yetkazish (hujum qilish) usulidir.

```
<input type="hidden" name="edit_done" value="1"/>
<input type="hidden" name="upload_ids" value="14401638983"/>
<input type="hidden" name="just_photo_ids" value=""/>
<input type="hidden" name="set_id" value=""/>
<input type="hidden" name="magic_cookie" value=""/>
<input type="hidden" name="title_14401638983" value="XSRF bug POC1"/>
<input type="hidden" name="description_14401638983" value="XSRF bug POC1"/>
<input type="hidden" name="tags_14401638983" value="XSRF POC1"/>
<input type="hidden" name="Submit" value="SAVE"/>
<input type="submit" value="click here to see magic">
```

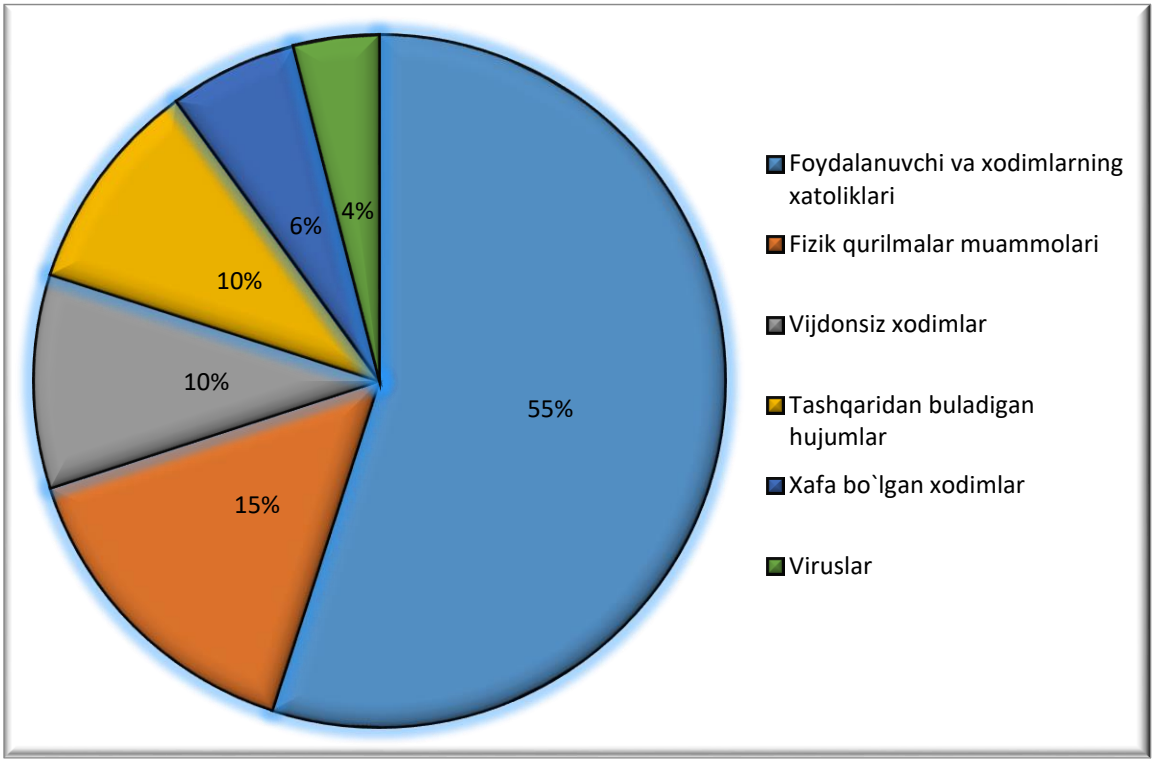
Yuqorida keltirilgan usullar korxonalarda internet manbalarini buzish usullari hisoblanadi va bularning umumiy statistikasi, xavflilik darajasi va shu usullar yordamida buzish ko`rsatkichlari quyidagicha:



Bundan xulosa qilishimiz mumkin hozirda buzgunchilar ko`proq dasturiy vositalardan foydalanib ma`lumotlarni bazalarini buzishga harakat qiladilar EHM kuchi yordamida ma`lumotlarni buzish juda kam ko`rsatkichni tashkil qiladi.

Shu ko`rsatkichlar korxona xavfsizligini buzilish manbalarida ahamiyatga ega va ichki xavflar qanchalik ahamiyatga ega ekanligini ko`rib o`tamiz. Quyida mamlakatimizdagi korxona xavfsizligini buzilish manbalari diagrammasi

keltirilgan (uz-cert ma`lumotlariga tayangan holda).



Diagrammaga qisqacha tuxtalib o`tsak eng ko`p axborot buzilishi bu xodimlarning xatoliklari tufayli kegin fizik qurilmalarning kamchiliklari va kegingi o`rinda qolgan ko`rsatkichlar turadi. Shu ikki kamchilik 70 % axborotlarni buzilishiga olib kelar ekan. Demak korxonalarda xodimlarni aynan axborot texnologiyalari buyicha o`qitish agar maxfiy axborot saqlanishi lozim bo`lgan korxona bo`lsa, albatta axborot xavfsizlik bo`yicha mutaxasis bo`lishi yoki kerak bo`lsa aynan shunday bo`limning bo`lishi va fizik qurilmalardan samarali foydalanish muhim sanalgan ma`lumotlarni nusxasini alohida serverlarda saqlash taklif qilinadi. Xulosa o`rnida INFOWATCH analitik markazning 2013 yildagi aynan axborotlarni himoyalash buyicha statistic tahlil natijalarini keltirib o`taman.

INFOWATCH analitik markazining tadqiqodlari natijasida shu ma`lum bo`lganki tashkilot rahbarlarining (so`rovnomada qatnashgan) 77 % va Axborot xavfsizligi mutaxasislarining 85% dan ko`prog`i axborotlarga ko`proq tashqi xavflar emas balki ichki xavflar xatar keltirarkan. Xuddi shu analitik markazning tadqiqotlari va so`rovlari natijasida shu malum bo`lganki 77 % axborot texnologiya rahbarlari va axborot xavsizlik xizmatchilari korporativ tizimlarni ishonchsiz deb bilishar ekan va 85 % axborot texnologiyalar sohasida xizmat ko`rsatadigan xodimlarning fikricha agarda axborot buzilish holatlari va uning oqibatlari haqida korxona va firmalar rahbarlarini ogoh qilinsa ular axborot xavfsizligini

ta`minlash uchun hozirgi holatda ancha kup miqdorda mablag` ajratishni boshlaydilar.

Bundan ko`rinib turibdiki, biz avvalo davlat organlari ma'lumotlar bazalarini turli risklardan, korxonalarda mavjud maxfiy axborotlarnini ichki manbalardan himoya qilishimiz kerak.

Adabiyotlar ro'yxati:

1. Якубов М.С., Юлдашев Д.Б. Организация контроля по соблюдению информационной безопасности на предприятии. Сборник докладов Республиканского семинара "Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения" Ташкент. 2012 г. с. 30-32.
2. Абдуллаева Л.Х., Очилов Ш.К., Якубов М.С. Правовое обеспечение информационной безопасности личности в информационной среде."Ахборот хуружи даврида ёшлар онгини шакллантириш омиллари" мавзусида ўтказилган Республика илмий-амалий конференция материаллари тўплами. I – қисм. ТУИТ. Тошкент-2013г. 31-1 июнь.263-267с.
3. Securing an open society - one year later: progress report on the implementation of Canada's national security policy / Library and Archives Canada Cataloguing in Publication. - 2005 - 53 p.