Ma’ruza materialini mustaqil o‘zlashtirish.

14-ma’ruza (Axborot xavsizligi. Kriptografiya asoslari, ma’lumotlarni himoya qilish yo‘llari).

Kalit so‘zlar: *kiber tahdidlar, axborot texnologiyalari, ma'lumotlar yaxlitligi, kirish, maxfiylik.*

Kirish: ushbu maqolada ma'lumotlarni himoya qilish tushunchasi ko'rib chiqilgan. Axborot xavfsizligining asosiy printsiplari, axborotni himoya qilish tizimi. Maqolada axborot xavfsizligining asosiy tamoyillari va ularning foydalanuvchilar uchun ahamiyati va axborotni xavfsizligini ta'minlaydigan ma'lumotlarni shifrlash usullari ochib berilgan. Axborotni himoya qilish usullarini bilish va tushunish ma'lumotlarimiz xavfsizligini ta'minlaydi.

Maqsad: talabalarda axborot xavfsizligi asoslari haqida bilim va ko’nikmalarni shakllantirish bo‘yicha ilmiy asoslangan amaliy tavsiyalar berish.

Materiallar va metodlar: metodik tadqiqotlarda o‘quvchilarning o‘quv-biluv faoliyatini rivojlantirish muammosi ancha keng o‘rganilgan. Bu izlanishlarning aksariyatida o‘quvchilarning o‘quv-biluv faoliyatini shakllantirish masalalari таьiimda o‘quvchilarning faolligi va mustakilligini tarbiyalash muammosi bilan aloqadorlikda o‘rganilgan. Innovatsion ta’lim sharoitida boshlang‘ich sinf ona tili darslarining samaradorligini oshirish muammosiga daxldor tadqiqotlar oidagicha guruhlarga ajratib tahlil qilindi. Qator tadqiqotlarda ta’limni loyihalashtirishning psixologik muammolari yoritilgan.

Muhokama va natijalar: o‘quvchilarga zamonaviy ta’lim-tarbiya berish vazifalaridan biri ularda axborot xavsizligi bo’yicha dunyoqarash elementlarini shakllantirishdir. Bu vazifani hal qilishda maqsadga muvofiq ishlashning yetakchi sharti − ma'lumotlar va tarmoqlarni kiber tahdidlardan himoya qilishdir.

Umumjahon axborot globallashuvi jarayonlari axborot-kommunikatsiya texnologiyalarini nafaqat mamlakatlar iqtisodiyoti va boshqa sohalariga joriy etish, balki axborot tizimlari xavfsizligini ta’minlashni ham taqozo etadi. Axborot va kommunikatsiya texnologiyalari sohasidagi xalqaro xavfsizlik tizimiga Markaziy Osiyoda birinchilardan bo`lib qo`shildi. Axborot xavfsizligini ta’minlash bo`yicha aloqa axborotlashtirish va telekommunikatsiya texnologiyalari davlat qo`mitasi

tamonidan quyidagi choratadbirlar amalga oshiriladi: Ma’lumotlar uzatish, telekommunikatsiya tarmoqlari, teleradioefir, hamda axborot tizimlarida axborot xavfsizligini ta’minlashni takomillashtirish va rivojlantirish bo`yicha davlat siyosatini yuritish; Axborot xavfsizligiga oid qonunchilik va me’yoriy-huquqiy hujjatlarining yaratilishini tashkil qilish va bunda ishtirok etish; Axborot tizimlari komplekslari, resurslari va ma’lumotlar bazalarining axborot xavfsizligini ta’minlash; Davlat organlarining axborot tizimlari va resurslari axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirishga ko`maklashish; Davlat axborot tizimlari va resurslarining axborot xavfsizligini ta’minlash yuzasidan monitoring natijalari to`g’risidagi statistik ma’lumotlarni axborotlashtirish va telekommunikattsiya texnologiyalari davlat qo`mitasiga belgilangan tartibda taqdim etish;

Telekommunikatsiyalar tarmoqlarining operatorlari va provayderlari bilan hamkorlik qilish, davlat organlarining kompyuter va axborot texnologiyalaridan foydalanish sohasidagi qonun buzilishlarining oldini olish masalalari bo`yicha birgalikdagi ishlarini tashkil etish va ularning faoliyatini muvofiqlashtirish; Internetning milliy foydalanuvchilarini Internet tarmogi milliy segmentida axborot xavfsizligida paydo bo`layotgan tahdidlar to`g’risida o`z vaqtida xabardor qilish, shuningdek axborotlarni muhofaza qilish bo`yicha konsultattsiya xizmatlari ko`rsatish;

qonun buzuvchilarni tahlil qilish, identifikattsiyalashda, axborotlar makonidagi ruxsatsiz yoxud buzuvchi harakatlarni amalga oshirishda foydalaniladigan metodlar va vositalarni tahlil qilishda huquqni muhofaza qilish organlari bilan hamkorlik qilish;

Internet tarmogi milliy segmentida axborot xavfsizligi hodisalarining oldini olish bo`yicha o`zaro amaliy ishlarni tashkil etish maqsadida axborot xavfsizligi sohasidagi xalqaro hamkorlikni rivojlantirish;

Axborotni tegishli xukuklarga ega blmagan shaxslar yoki jarayonlar orkali tarmokdan ruxsat etilmagan xolda olishga yul kuymaslik;

Egasi tomonidan berilayotgan (sotilayotgan) axborot va resurslar faqat tomonlar o`rtasida kelishilgan shartnomalar asosida qo`llanilishiga ishonish kabilar tushuniladi.

Xavfsizlikning asosiy yo`nalishlari.

Axborot xavfsizligi. Axborot xavfsizligining dolzarblashib borishi, axborotning strategik resursga aylanib borishi bilan izohlash mumkin. Zamonaviy davlat infratuzilmasini telekommunikatsiya va axborot tarmoqlari hamda, turli xildagi axborot tizimlari tashkil etib, axborot texnologiyalari va texnik vositalar jamiyatning turli jabhalarida keng qo`llanilmoqda.

Iqtisodiy xavfsizlik. Milliy iqtisodda axborotlarni yaratish, tarqatish, qayta ishlash va foydalanish jarayoni hamda vositalarini qamrab olgan yangi tarmoq vujudga keldi. «Milliy axborot resursi» tushunchasi yangi iqtisodiy kategoriya bo`lib xizmat qilmoqda. Davlatning axborot resurslariga keltirilayotgan zarar axborot xavfsizligiga xam ta’sir ko`rsatmoqda. Mamlakatimizda axborotlashgan jamiyatni shakllantirish va uning asosida jahon yagona axborot maydoniga kirib borish natijasida milliy iqtisodimizga turli xildagi zararlar keltirish xavfi paydo bo`lmoqda.

Mudofaa xavfsizligi. Mudofaa sohasida xavfsizlikning asosiy ob’ektlaridan bo`lib, mamlakatning mudofaa potentsialining axborot tarkibi va axborot resurslari hisoblanmoqda. Hozirgi kunda barcha zamonaviy qurollar va harbiy texnikalar juda ham kompyuterlashtirilib yuborildi. SHuning uchun xam ularga axborot qurollarini qo`llash ehtimoli katta.

Ijtimoiy xavfsizlik. Zamonaviy axborot – kommunikatsiyalar texnologiyalarining milliy iqtisod barcha tarmoqlarida keng qo`llanishi inson psixologiyasi va jamoa ongiga «yashirin» ta’sir ko`rsatish vositalarining samaradorligini yuksaltirib yubordi.

Ekologik xavfsizlik. ekologik xavfsizlik – global masshtabdagi muammodir. «Ekologik toza», energiya va resurs tejaydigan, chiqindisiz texnologiyalarga o`tish faqat milliy iqtisodni axborotlashtirish hisobiga qayta qurish asosidagina yo`lga qo`yish mumkin.

Axborot xavfsizligi deb, ma’lumotlarni yo`qotish va o`zgartirishga yo`naltirilgan tabiiy yoki sun’iy xossali tasodifiy va qasddan ta’sirlardan xar qanday tashuvchilarda axborotning himoyalanganligiga aytiladi. Ilgarigi xavf faqatgina konfidenttsial (maxfiy) xabarlar va xujjatlarni o`girlash yoki nusxa olishdan iborat bo`lsa, hozirgi paytdagi xavf esa kompyuter ma’lumotlari to`plami, elektron ma’lumotlar, elektron massivlardan ularning egasidan ruxsat so`ramasdan foydalanishdir. Bulardan tashqari, bu xarakatlardan moddiy foyda olishga intilish ham rivojlandi.

Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta’minlovchi va tashkilot axborot zaxiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta’minlovchi qatiy reglamentlangan dinamik texnologik jarayonga aytiladi. Axborotning egasiga, foydalanuvchisiga va boshka shaxsga zarar etkazmokchi bo`lgan nohuquqiy muomaladan xar qanday xujjatlashtirilgan, ya’ni identifikattsiya qilish imkonini beruvchi rekvizitlari qo`yilgan xolda moddiy jismda qayd etilgan axborotximoyalanishi kerak. Axborot xavfsizligi nuqtai nazaridan axborotni quyidagicha turkumlash mumkin:

maxfiylik — aniq bir axborotga fakat tegishli shaxslar doirasigina kirishi mumkinligi, ya’ni foydalanilishi qonuniy xujjatlarga muvofik cheklab qo`yilib, xujjatlashtirilganligi kafolati. Bu bandning buzilishi o`rtasilik yoki axborotni oshkor qilish, deyiladi;

konfidenttsiallik - inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; yaxlitlik— axborot boshlangich ko`rinishda ekanligi, ya’ni uni saqlash va uzatishda ruxsat etilmagan o`zgarishlar qilinmaganligi kafolati; bu bandning buzilishi axborotni soxtalashtirish deyiladi;

autentifikatsiya – axborot zaxirasi egasi deb e’lon qilingan shaxs xaqiqatan xam axborotning egasi ekanligiga beriladigan kafolat; bu bandning buzilishi xabar muallifini soxtalashtirish deyiladi;

apellyattsiya qilishlik – etarlicha murakkab kategoriya, lekin elektron biznesda keng qo`llaniladi. Kerak bo`lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati.

Yukoridagidek, axborot tizimiga nisbatan quyidagicha tasnifni keltirish mumkin: ishonchlilik – tizim meyoriy va ayrim tabiiy xollarda rejalashtirilganidek o`zini tutishlik kafolati;

aniqlilik – xamma buyruqlarni aniq va to`liq bajarish kafolati; tizimga kirishni nazorat qilish – turli shaxs guruxlari axborot manbalariga xar xil kirishga egaligi va bunday kirishga cheklashlar doim bajarilishlik kafolati;

nazorat qilinishi – istalgan paytda dastur majmuasining xoxlagan kismini tulik tekshirish mumkinligi kafolati;

identifikattsiyalashni nazorat qilish – xozir tizimga ulangan mijoz aniq o`zini kim deb atagan bulsa, aniq o`sha ekanligining kafolati;

**qasddan buzilishlarga to`sqinlik** – oldindan kelishilgan me'yorlar chegarasida qasddan xato kiritilgan ma'lumotlarga nisbatan tizimning oldindan kelishilgan xolda o`zinitutishi.

Tarmoq texnologiyalari rivojining boshlangich bosqichida viruslar va kompyuter xujumlarining boshqa turlari ta'siridagi zarar kam edi, chunki u davrda dunyo iqtisodining axborot texnologiyalariga bogliqligi katta emas edi. Hozirda, xujumlar sonining doimo o`sishi hamda biznesning axborotdan foydalanish va almashishning elektron vositalariga bogliqligi sharoitida mashina vaqtining yo`qolishiga olib keluvchi hatto ozgina xujumdan kelgan zarar juda katta raqamlar orqali hisoblanadi.

Misol tariqasida keltirish mumkinki, faqat 2014 yilning birinchi choragida dunyo miqyosidagi yo`qotishlar 2015 yildagi barcha yo`qotishlar yigindisining 50%ini tashkil etgan, yoki bo`lmasa 2006 yilning o`zida Rossiya Federeatsiyasida 14 mingdan ortiq kompyuter jinoyatchiligi holatlari qayd etilgan.

Korporativ tarmoqlarda ishlanadigan axborot, ayniqsa, zaif bo`ladi. Hozirda ruxsatsiz foydalanishga yoki axborotni modifikattsiyalashga, yolgon axborotning muomalaga kirishi imkonining jiddiy oshishiga quyidagilar sabab bo`ladi:

kompyuterda ishlanadigan, uzatiladigan va saqlanadigan axborot hajmining oshishi;

ma’lumotlar bazasida muhimlik va mahfiylik darajasi turli bo`lgan axborotlarning to`planishi;

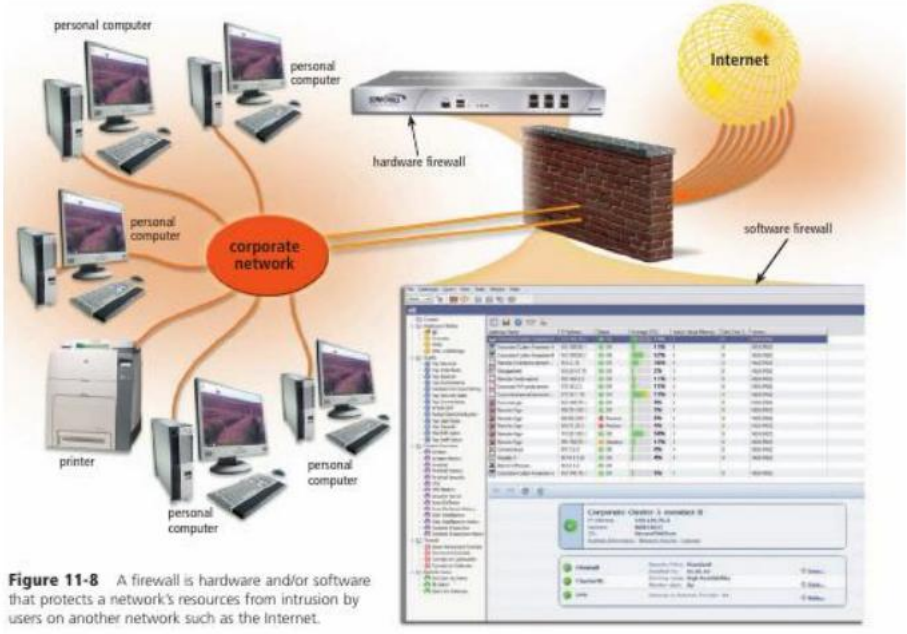

Figure 11-8 A firewall is hardware and/or software that protects a network's resources from intrusion by users on another network such as the Internet.

ma’lumotlar bazasida saqlanayotgan axborotdan va hisoblash tarmoq resurlaridan foydalanuvchilar doirasining kengayishi;

masofadagi ishchi joylar soninig oshishi;

foydalanuvchilarni bog’lash uchun internet global tarmogini va aloqaning turli kanallarini keng ishlatish;

foydaluvchilar kompyuterlari o`rtasida axborot almashinuvining avtomatlashtirilishi.

Axborot xavfsizligiga tahdid deganda axborotning buzilishi yoki yo`qotilishi xavfiga olib keluvchi himoyalanuvchi ob’ektga qarshi qilingan harakatlar tushuniladi. Oldindan shuni aytish mumkinki, so`z barcha axborot xususida emas, balki uning faqat, mulk egasi fikricha, kommerttsiya qiymatiga ega bo`lgan qismi xususida ketyapti.

Zamonaviy korporativ tarmoqlar va tizimlarga duchor bo`ladigan keng tarqalgan tahdidlarni tahlillaymiz. Hisobga olish lozimki, xavfsizlikka tahdid manbalari korporativ axborot tizimining ichida (ichki manba) va uning tashqarisida (tashqi manba) bo`lishi mumkin. Bunday ajratish to`g’ri, chunki bitta tahdid uchun

(masalan, o`g’irlash) tashqi va ichki manbalarga qarshi harakat usullari turlicha bo`ladi. Bo`lishi mumkin bo`lgan tahdidlarni hamda korporativ axborot tizimining zaif joylarini bilish xavfsizlikni ta’minlovchi eng samarali vositalarni tanlash uchun zarur hisoblanadi.

Tez-tez bo`ladigan va xavfli (zarar o`lchami nuqtai nazaridan) tahdidlarga foydalanuvchilarning, operatorlarning, ma’murlarning va korporativ axborot tizimlariga xizmat ko`rsatuvchi boshqa shaxslarning atayin qilmagan xatoliklari kiradi. Ba’zida bunday xatoliklar to`g’ridan to`g’ri zararga olib keladi. Ba’zida ular niyati buzuq odamlar foydalanishi mumkin bo`lgan nozik joylarni paydo bo`lishiga sabab bo`ladi. Global axborot tarmog’ida ishlash ushbu omilning etarlicha dolzarb qiladi. Bunda zarar manbai tashkilotning foydalanuvchisi ham, tarmoq foydalanuvchisi ham bo`lishi mumkin, oxirgisi ayniqsa xavfli.

Zarar o`lchami bo`yicha ikkinchi o`rinni o`g’irlashlar va soxtalashtirishlar egallaydi. Tekshirilgan holatlarning aksariyatida ishlash rejimlari va himoyalash choralari bilan a’lo darajada tanish bo`lgan tashkilot shtatidagi xodimlar aybdor bo`lib chiqdilar. Global tarmoqlar bilan bolangan quvvatli axborot kanalining mavjudligida, uning ishlashi ustidan etarlicha nazorat yo`qligi bunday faoliyatga qo`shimcha imkon yaratadi.

Xafa bo`lgan xodimlar tashkilotdagi tartib bilan tanish va juda samara bilan ziyon etkazishlari mumkin. Xodim ishdan bo`shaganida uning axborot resurslaridan foydalanish xuquqi bekor qilinishi nazoratga olinishi shart.

Hozirda tashqi kommunikatsiya orqali ruxsatsiz foydalanishga atayin qilingan urinishlar bo`lishi mumkin bo`lgan barcha buzilishlarning 10%ini tashkil etadi. Bu kattalik anchagina bo`lib tuyulmasa ham, internetda ishlash tajribasi ko`rsatadiki, qariyb har bir Internet-server kuniga bir necha marta suqilib kirish urinishlariga duchor bo`lar ekan. Xavf-xatarlar tahlil qilinganida tashkilot korporativ yoki lokal tarmog’i kompyuterlarining xujumlarga qarshi turishi yoki bo`lmaganida axborot xavfsizligi buzilishi faktlarini qayd etish uchun etarlicha himoyalanmaganligini hisobga olish zarur. Masalan, axborot tizimlarini himoyalash Agentligining (AQSH) testlari ko`rsatadiki, 88% kompyuterlar axborot xavfsizligi nuqtai nazaridan nozik

joylarga egaki, ular ruxsatsiz foydalanish uchun faol ishlatishlari mumkin. Tashkilot axborot tuzilmasidan masofadan foydalanish xollari alohida ko`rilishi lozim. Himoya siyosatini tuzishdan avval tashkilotda kompyuter muhiti duchor bo`ladigan xavf-xatar baholanishi va zarur choralar ko`rilishi zarur. Ravshanki, himoyaga tahdidni nazoratlash va zarur choralarni ko`rish uchun tashkilotning sarfharajati tashkilotda aktivlar va resurslarni himoyalash bo`yicha hech qanday choralar ko`rilmaganida kutiladigan yo`qotishlardan oshib ketmasligi shart.

Himoyalanishni tahlillash vositalari zaifliklarni topib va o`z vaqtida yo`q qilib xujumni amalga oshirish imkoniyatini bartaraf qiladi. Natijada, himoyalash vositalarini ishlatilishiga bo`ladigan barcha sarf-harajatlar kamayadi.

Himoyalanishni tahlillash vositalari tarmoq sathida, operattsion tizim sathida va ilovalar sathida ishlashi mumkin. Ular tekshirishlar sonini bora-bora ko`paytirish, axborot tizimiga "ichkarilab borish" va uning barcha sathlarini tadqiqlash orqali zaifliklarni qidirishi mumkin.

Himoyalanishni tahlillash vositalari zaifliklarni topib va o`z vaqtida yo`q qilib xujumni amalga oshirish imkoniyatini bartaraf qiladi. Natijada, himoyalash vositalarini ishlatilishiga bo`ladigan barcha sarf-harajatlar kamayadi.

Himoyalanishni tahlillash vositalari tarmoq sathida, operatsion tizimda va ilovalar sathida ishlashi mumkin. Ular tekshirishlar sonini bora-bora ko`paytirish, axborot tizimiga "ichkarilab borish" va uning barcha sathlarini tadqiqlash orqali zaifliklarni qidirishi mumkin.

Tarmoq protokollari va servislari himoyalanishini tahlillash vositalari. Har qanday tarmoqda abonentlarning o`zaro aloqasi ikkita va undan ko`p uzellar orasida axborot almashinish muolajalarini belgilovchi tarmoq protokollari va servislaridan foydalanishga asoslangan. Tarmoq protokollari va servislarini ishlab chiqishda ularga ishlanuvchi axborot xavfsizligini ta’minlash bo`yicha talablar (odatda shubxasiz etarli bo`lmagan) qo`yilgan. SHu sababli, tarmoq protokollarida aniqlangan zaifliklar xususida axborotlar paydo bo`lmoqda. Natijada, korporativ tarmoqda foydalanadigan barcha protokol va servislarni doimo tekshirish zaruriyati tug’iladi. Himoyalanishni tahlillash tizimi zaifliklarni aniqlash bo`yicha testlar

seriyasini bajaradi. Bu testlar niyati buzuq odamlarning korporativ tarmoqlarga xujumlarida qo`llaniladiganiga o`xshash. Zaifliklarni aniqlash maqsadida skanerlash tekshiruvchi tizim xususidagi dastlabki axborotni, xususan, ruxsat etilgan protokollar va ochiq portlar, operatsion tizimning ishlatiluvchi versiyalari va boshkalari xususidagi axborotni olish bilan boshlanadi. Skanerlash keng tarqalgan xujumlar, masalan, to`liq saralash usuli bo`yicha parollarni tanlashdan foydalanib, suqilib kirishni imitatsiyalashga urinish bilan tugaydi.

Himoyalanishni tahlillash vositalari yordamida tarmoq sathida nafaqat Internetning korporativ tarmoqdan ruxsatsiz foydalanishi imkoniyatini testlash, balki tashkilot ichki tarmog'ida tekshirishni amalga oshirish mumkin. Tarmoq sathida himoyalanishni tahlillash tizimi tashkilot xavfsizlik darajasini baholashga hamda tarmoq dasturiy va apparat ta'minotini sozlash samaradorligini nazoratlashga xizmat qiladi.

Xujumlarni aniqlash

Tarmoq axborotini tahlillash usullari. Mohiyati bo`yicha, xujumlarni aniqlash jarayoni korporativ tarmoqda bo`layotgan shubhali harakatlarni baholash jarayonidir. Boshqacha aytganda xujumlarni aniqlash - hisoblash yoki tarmoq resurslariga yo`naltirilgan shubhali harakatlarni identifikattsiyalash va ularga reaktsiya ko`rsatish jarayoni. Hozirda xujumlarni aniqlash tizimida quyidagi usullar ishlatiladi:

- statistik usul;
- ekspert tizimlari;
- neyron tarmoqlari.

Statistik usul. Statistik yondashishning asosiy afzalligi allaqachon ishlab chiqilgan va o`zini tanitgan matematik statistika apparatini ishlatish va sub'ekt xarakteriga moslash. Avval tahlillanuvchi tizimning barcha sub'ektlari uchun profillar aniqlanadi. Ishlatiladigan profillarning etalondan har qanday chetlanishi ruxsat etilmagan foydalanish hisoblanadi. Statistik usullar universal hisoblanadi, chunki mumkin bo`lgan xujumlarni va ular foydalanadigan zaifliklarni bilish talab

etilmaydi. Ammo bu usullardan foydalanishda bir qancha muammolar paydo bo`ladi:

1. Statistik tizimlar xodisalar kelishi tartibiga sezuvchanmaslar; ba’zi xollarda bir xodisaning o`zi, kelishi tartibiga ko`ra anomal yoki normal faoliyatni xarakterlashi mumkin.

2. Anomal faoliyatni adekvat identifikattsiyalash maqsadida xujumlarni aniqlash tizimi tomonidan kuzatiluvchi xarakteristikalar uchun chegaraviy qiymatlarni berish juda qiyin.

3. Statistik usullar vaqt o`tishi bilan buzunchilar tomonidan shunday "o`rnatilishi" mumkinki, xujum harakatlari normal kabi qabul qilinadi.

Ekspert tizimlari. ekspert tizimi odam-ekspert bilimlarini qamrab oluvchi qoidalar to`plamidan tashkil topgan. ekspert tizimidan foydalanish xujumlarni aniqlashning keng tarqalgan usuli bo`lib, xujumlar xususidagi axborot qoidalar ko`rinishida ifodalanadi. Bu qoidalar harakatlar ketma-ketligi yoki signaturalar ko`rinishida yozilishi mumkin. Bu qoidalarning har birining bajarilishida ruxsatsiz faoliyat mavjudligi xususida qaror qabul qilinadi. Bunday yondashishning muhim afzalligi - yolg’on trevoganing umuman bo`lmasligi.

Ekspert tizimining ma’lumotlari bazasida hozirda ma’lum bo`lgan aksariyat xujumlar stsenariyasi bo`lishi lozim. ekspert tizimlari, dol-zarblikni saqlash maqsadida, ma’lumotlar bazasini muttasil yangilashni talab etadi. Garchi ekspert tizimlari qaydlash jurnallaridagi ma’lumotlarni ko`zdan kechirishga yaxshi imkoniyatni tavsiya qilsada, so`ralgan yangilanish e’tiborsiz qoldirilishi yoki ma’mur tomonidan qo`lda amalga oshirilishi mumkin. Bu eng kamida, ekspert tizimi imkoniyatlarining bo`shashiga olib keladi.

Ekspert tizimlarining kamchiliklari ichida eng asosiysi - noma’lum xujumlarni akslantira olmasligi. Bunda oldindan ma’lum xujumning xatto ozgina o`zgarishi xujumlarni aniqlash tizimining ishlashiga jiddiy to`siq bo`lishi mumkin.

Neyron tarmoqlari. Xujumlarni aniqlash usullarining aksariyati qoidalar yoki statistik yondashish asosida nazoratlanuvchi muhitni tahlillash shakllaridan foydalanadi. Nazoratlanuvchi muhit sifatida qaydlash jurnallari yoki tarmoq trafigi

ko`rilishi mumkin. Bunday tahlillash ma’mur yoki xujumlarni yaniqlash tizimi tomonidan yaratilgan, oldindan aniqlangan qoidalar to`plamiga tayanadi. Xujumni vaqt bo`yicha yoki bir necha niyati buzuq odamlar o`rtasida har qanday bo`linishi ekspert tizimlar yordamida aniqlashga qiyinchilik tudiradi. Xujumlar va ular usullarining turli-tumanligi tufayli, ekspert tizimlari qoidalarining ma’lumotlar bazasining hatto doimiy yangilanishi ham xujumlar diapazonini aniq identifikattsiyalashni kafolatlamaydi.

Nazariy savollar

1. Axborot xavfsizligining maqsadi.
2. Axborot xavfsizligining yo`nalishlari.
3. Axborot xavfsizligining turkumlanishi.
4. Axborotlarga nisbatan xavf-xatarlar tasnifi.
5. Axborotni himoyalash tizimi.
6. Axborotni himoyalash tizimining komplekslиligi va elementlari.
7. Himoyaning buzilishlariga sabab bo`luvchi xujumlar qanday klassifikatsiyalanadi?
8. Passiv taxdidga qanday xujumlar taalluqli?
9. Aktiv tahdidga qanday xujumlar taalluqli?
10. Himoya mexanizmlari qanday usullarga asoslanadi?
11. Himoya xizmati. Konfidentsiallik. Autentifikatsiya. YAxlitlik. Yolg’onning mumkin emasligi. Resurslardan foydalanuvchanlik. Foydalanuvchanlikni boshqarish.

Foydalanilgan adabiyotlar ro‘yxati

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley. ISBN: 978-1119642787.
2. Easttom, C. (2019). Computer Security Fundamentals (4th ed.). Pearson IT Certification. ISBN: 978-0789757463.
3. Harris, S. (2019). CISSP All-in-One Exam Guide (8th ed.). McGraw-Hill Education. ISBN: 978-1260142655.

4. Mitnick, K. D., & Vamosi, R. (2017). The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. Little, Brown and Company. ISBN: 978-0316380508

5. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson. ISBN: 978-0134444284.

6. Stallings, W. (2020). Network Security Essentials: Applications and Standards (6th ed.). Pearson. ISBN: 978-0134444284.

7. Ross, R. S., et al. (2018). NIST Special Publication 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-37r2.

8. Ataeva G. I., Xamroeva X. Yu. Analiz vozmojnosti ispolzovaniya oblachnых texnologiy v vыsshem obrazovanii Uzbekistana //Universum: texnicheskie nauki. – 2022. – №. 1-1 (94). – S. 16-18.