AXBOROT-KOMMUNIKATSION TIZIMLAR VA TARMOQLAR XAVFSIZLIGIGA QO‘YILADIGAN TALABLAR

Farmanov M G

O‘zbekiston Respublikasi harbiy xavfsizlik va mudofaa universiteti Janubiy operativ qo‘mondonlik fakulteti Istiqbolli harbiy texnologiyalari kafedrasi boshlig‘i, podpolkovnik

Annotatsiya: *Bugungi kunda mobil qurilmalar xotirasida zararli dasturlarni aniqlash va tahlil qilishning ilmiy asoslangan usuli mavjud emasligi sababli, ushbu maqolada keltirilgan ma'lumotlar Android operatsion tizimida ishlaydigan mobil qurilmalarda axborotni himoya qilish samaradorligini oshirishga yordam beradi.*

Kalit so'zlar: *axborot xavfsizligi, mobil qurilmalar, android, operatsion tizim, avtomatlashtirilgan tizimlar.*

Qo‘yida Rossiya Fedaratsiyasida ishlab chiqilgan kompyuter tarmoqlarida axborotni himoyalash sohasiga taalluqli hujjatlar xususida so‘z yuritiladi. Xujjatlarda qo‘yilgan talablar davlat sektorida yoki tarkibida davlat siri bo‘lgan axborotni ishlovchi tijorat tashkilotlarida bajarilishi shart. Boshqa tijorat tuzilmalar uchun xujjatlar tavsiya xarakteriga ega.

Xujjatlardan biri axborotdan ruxsatsiz foydalanishdan himoyalash bo‘yicha talablarni aks ettiradi va "avtomatlashtirilgan tizimlar. Axborotdan ro‘xsatsiz foydalanishdan himoyalash. Avtomatlashtirilgan tizimlarning turkumlanishi va axborotni himoyalash bo‘yicha talablar" deb nomlanadi.

Bu xujjatda xavfsizlikning istalgan darajasiga erishish bo‘yicha asoslangan choralarni ishlab chiqish va qo‘llash maqsadida avtomatlashtirilgan tizimlarning axborotni himoyalash nuqtai nazaridan ishlashi sharoitlari bo‘yicha turkumlanishi keltirilgan. Har bir himoyalash bo‘yicha ma’lum minimal talablar majmui orqali xarakterlanuvchi himoyalanishning to‘qqizta sinfi belgilanadi (1-jadval).

1-jadval. Kompyuter tarmoqlarining ximoyalanish sinflari.

Talablar	Sinflar								
	3B	ZA	2B	2A	1D	1G	1B	1B	1A
Foydalanishni boshqarish qism tizimiga									
Identifikatsiyalash, xaqiqiyligini tekshirish va subyektlar foydalanishining nazorati									
- tizimga	x	x	x	x	x	x	x	x	x
- terminallarga, EXMga, EXM tarmog‘i uzellariga, aloqa kanallariga, EXMni tashqi qurilmalariga				x		x	x	x	x
- dasturlarga				x		x	x	x	x
- jildlarga, kataloglarga, fayllarga, qaydlarga				x		x	x	x	x
Axborot oqimlarini boshqarish				x			x	x	x
Ro‘yxatga va xisobga olish qism tizimiga									
Ro‘yxatga va hisobga olish									

- subyektlarning tizimga(dan) kirishini (chiqishini)	x	x	x	x	x	x	x	x	x
- bosma (grafik) hujjatlarni berishni		x		x		x	x	x	x
- dasturni va jarayonlarni (topshiriqlar, masalalar)ishga tushirishni (tugallashni)		x		x		x	x	x	x
- subyekt dasturlaridan foydalanishni (ximoyalanuvchi fayllardan foydalanish, ularni yaratish va yuqotish, aloqa liniyalari va kanallari orqali uzatishni)				x		x	x	x	x
- subyekt dasturlaridan foydalanishni (terminallardan, EXMdan, EXM tarmog‘i uzellaridan, aloqa kanallaridan, EXM tashqi qurilmalaridan, dasturli jildlardan, kataloglardan, fayllardan, qaydlar xoshiyalaridan foydalanishni)				x		x	x	x	x
- foydalanuvchi subyektlar vakolatlarini uzgartirishlarni							x	x	x
- ximoyalanuvchi foydalanish obyektning yaratilishini				x			x	x	x
axborot eltuvchilarini xisobga olish	x	x	x	x	x	x	x	x	x
operativ xotira va tashqi tuplagichlarni tozalash		x		x		x	x	x	x
ximoyani buzishga urinishni signalizasiyasi						x	x	x	x
Kriptografik qism tizimiga									
Konfidensial axborotni shifrlash							x	x	x
foydalanishni turli subyektlariga (subyektlar guruxiga) tegishli axborotni turli kalitlarda shifrlash	-				-	-	-	-	x
attestatsiyadan utgan (sertifikatsiyalangan) kriptografik vositalardan foydalanish	-		-		-	-	-	x	x
Yaxlitlikni ta’minlovchi qism tizimiga									
Dasturiy vositalar va ishlanuvchi axborotning yaxlitligini ta’minlash	x	x	x	x	x	x	x	x	x
xisoblash texnikasi vositalari va axborot eltuvchilarini qo‘riqlash	x	x	x	x	x	x	x	x	x
axborot ximoyasi ma’muriyatining (xiz matining) mavjudligi				x			x	x	x
axborot ximoyasi tizimini vaqti-vaqti bilan testlash	x	x	X	x	x	x	x	x	x
axborot ximoyasi tizimini tiklash vo- sitalarining mavjudligi	x	x	x	x	x	x	x	x	x
sertifikatsiyalangan himoya vositalaridan foydalanish		x		x			x	x	x

Sinflar axborot ishlanishi xususiyatlari bilan bir-biridan farqlanuvchi uchta guruxga bo‘linadi. Har bir gurux ichida axborotning qiymatligiga (konfidensialligiga) bog‘liq holda ximoya bo‘yicha talablar iyerarxiyasi va demak, ximoyalanish sinflari saqlanadi. Har bir gurux ko‘rsatkichlarini, oxirgisidan boshlab ko‘rib chiqamiz.

Uchinchi gurux bir xil konfidensiallik darajasiga ega bo‘lgan eltuvchilarda joylashtirilgan barcha axborotdan foydalanuvchi bitta foydalanuvchi ishlaydigan tizimlardan iborat. Guruxda ikkita - 3B va ZA sinflari mavjud.

Ikkinchi gurux har xil konfidensiallik darajasiga ega bo‘lgan ishlanuvchi va yoki eltuvchilarda joylashtirilgan barcha axborotdan foydalanishga bir xil xuquqli foydalanuvchilari bo‘lgan tizimlardan iborat. Guruxda ikkita - 2B va 2A sinflari mavjud.

Birinchi gurux ko‘pchilik foydalanuvchi tizimlardan iborat bo‘lib, ularda bir vaqtning o‘zida konfidensiallik darajasi turli axborot ishlanadi yoki saqlanadi. Guruxda beshta - 1D, 1G, 1V, 1B va 1A sinflari mavjud.

- umumiy xolda ximoyalash tadbirlari 4 ta qism tizimni o‘z ichiga oladi:
- foydalanishni boshqarish;
- ro‘yxatga va xisobga olish;
- kriptografik;
- yaxlitlikni ta’minlash.

Xisoblash texnikasi vositalarini ruxsatsiz foydalanishdan ximoyalanish ko‘rsatkichlari "Xisoblash texnikasi vositalari. Axborotni ruxsatsiz foydalanishdan himoyalash. Ximoyalash ko‘rsatkichlari" deb ataluvchi xujjatda keltirilgan. Unda axborotdan ruxsatsiz foydalanishdan ximoyalanishning 7-sinfi aniqlangan. Eng pastki sinf - yettinchi, eng yuqori sinf - birinchi. Har bir sinf ximoyalanish talablarini oldingisidan meros qilib oladi. Himoyaning amalga oshirilgan modellari va ularni tekshirish ishonchliligiga bog‘liq holda sinflar to‘rtta guruxga ajratiladi.

Birinchi guruxda faqat yettinchi sinf bo‘ladi (minimal ximoyalanish).

Ikkinchi gurux tanlanadigan ximoya bilan xarakterlanib oltinchi va beshinchi sinflarni o‘z ichiga oladi. Tanlanuvchi ximoya nomma-nom aytilgan obyektlarning tizimning nomma-nom aytilgan obyektlardan foydalanishni ko‘zda tutadi. Bunda har bir "subyekt-obyekt" juftligi uchun foydalanishning ruxsat etilgan turlari aniqlanishi shart. Foydalanish nazorati har bir obyektga va har bir subyektga qo‘llaniladi.

Uchinchi gurux muxtor xuquqli himoya bilan xarakterlanib, to‘rtinchi, uchinchi va ikkinchi sinflarni o‘z ichiga oladi. Muxtor xuquqli himoya tizimning har bir subyekt va obyektiga, uning mos iyerarxiyadagi urnini ko‘rsatuvchi turkumlash belgisini berish tizimdan foydalanuvchi yoki maxsus ajratilgan subyekt tomonidan amalga oshiriladi. Ushbu xuquqga kiruvchi sinflardan talab qilinadigan narsa foydalanishning dispetcherini (reference monitor-xavolalar monitori) amalga oshirilishi.

Foydalanish nazorati barcha obyektlarga nisbatan har qanday subyekt tomonidan ochiq va yashirin foydalanishda amalga oshirilishi shart. Foydalanishga ruxsat berish faqat tanlanadigan va muxtor xuquqli qoidalarning birgalikda ruxsati bo‘lgandagina amalga oshirilishi mumkin.

To‘rtinchi gurux tasdiqlangan himoya bilan xarakterlanib faqat birinchi sinfni o‘z ichiga oladi.

Tizim ximoyalanish sinfini olishi uchun qo‘yidagilarga ega bo‘lishi lozim:

- tizim bo‘yicha ma’mur qo‘llanmasi;
- foydalanuvchi qo‘llanmasi;
- testlash va konstruktorlik xujjatlar.

Yuqorida ko‘rib o‘tilganidek, xozirda kompyuter jinoyatchiligi juda ham turli tuman. Bu kompyuterdagi axborotdan ruxsatsiz foydalanish, dasturiy ta’minotga mantiqiy bombalarni kiritish, kompyuter viruslarini ishlab chiqish va tarqatish, kompyuter axborotini o‘g‘irlash, dasturiy hisob komplekslarini ishlab chiqishda, qurishda va ekspluatatsiyasida pala-partishlik.

Axborot xavfsizligining bevosita ta’minlovchi, kompyuter jinoyatchiligining oldini oluvchi barcha choralarni quyidagilarga ajratish mumkin:

- xuquqiy;
- tashkiliy-ma’muriy;
- injener-texnik.

Xuquqiy choralarga kompyuter jinoyatchiligi uchun javobgarlikni belgilovchi meyorlarni ishlab chiqish, dasturchilarning mualliflik xuquqini ximoyalash, jinoiy va fuqarolik qonunchiligini hamda sud jarayonini takomillashtirish kiradi. Ularga yana kompyuter tizimlarini yaratuvchi ustidan jamoatchilik nazorati masalalari hamda, agar kompyuter tizimlarining bitimga kelgan mamlakatlarning harbiy, iqdisodiy va ijtimoiy jixatlariga tasiri bo‘lsa, cheklashlar bo‘yicha mos xalqoro shartnomalarni qabul qilish kiradi. Faqat oxirgi yillarda kompyuter jinoyatchiliklariga xuquqiy kurash muammolari bo‘yicha ishlar paydo bo‘ldi.

Tashkiliy-ma’muriy choralarga kompyuter tizimlarini qo‘riqlash, xodimlarni tanlash, maxsus muxim ishlarni bir kishi tomonidan bajarilishi xollariga yo‘l qo‘ymaslik, markaz ishdan chiqqanida uning ishga layoqatligini tiklash rejasining mavjudligi, barcha foydalanuvchilardan (yuqori raxbarlar ham bunga kiradi) himoyalanish vositalarining universalligi, markaz xavfsizligini taminlashga mutasaddi shaxslarga javobgarlikni yuklash, markaz joylanadigan joyni tanlash va x. kiradi.

Injener-texnik choralarga kompyuter tizimidan ruxsatsiz foydalanishdan ximoyalashni, muxim kompyuter tizimlarni rezervlash va diversiyadan ximoyalanishni taminlash rezerv elektr manbai, xavfsizlikning maxsus dasturiy va apparat vositalarini ishlab chiqish va amalga oshirish va x. kiradi.

FOYDALANILGAN MANBALAR:

1. “Киберхавфсизлик тўғрисида”ги Ўзбекистон Ренспубликаси қонуни 2022 йил 15 март.

2. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006. – взамен ГОСТ Р 50922-96; введ. 01.02.2008 // СПС «Консультант-Плюс». – Режим доступа: http://www.consultant.ru.

3. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. –Введ. 2009-10-01.

4. Доктрина информационной безопасности Российской Федерации : утв.

Президентом Российской Федерации №646 от 06.12.2016 // СПС «Консультант Плюс». Режим доступа: http://www.consultant.ru.

5. Нестеров, С. А. Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров. Москва: Издательство Юрайт, 2017. 321 с. (Университеты России). ISBN 978-5-534-00258-4. Текст: электронный // ЭБС Юрайт [сайт]. URL: https://www.biblio-online.ru/bcode/398687 (дата обращения: 15.06.2019).

6. Бирюков А.А. Информационная безопасность. Защита и нападение. 2-е издание. М.: ДМК-Пресс, 2017.