Kiberxavfsizlik hodisalarini tasniflash va boshqarish bo‘yicha qo‘llanma

UZCERT

MUNDARIJA

1. Kirish

Ushbu qo‘llanma “FIRST” xalqaro tashkilotining kiberxavfsizlik intsidentlarini tasniflash va boshqarish bo‘yicha (kompyuter) kiberxavfsizlik hodisalariga javob berish xizmatlari bo‘yicha tavsiyalariga muvofiq ishlab chiqilgan. Tasniflash hodisalarning sinflari va kichik klasslarini, shuningdek, milliy kibermakondagi kiberxavfsizlik hodisalarini boshqarish va ularga chora ko‘rish jarayonini tavsiflaydi.

Qo‘llanmani yozish uchun asos sifatida axborot xavfsizligi sohasidagi davlat standartlari, shuningdek, “SIM3” kompyuter hodisalariga chora ko‘rish xizmatining yetukligini baholash modeli olingan.

Qo‘llanmani ishlatish doirasi: kiberxavfsizlik hodisalari turlarini tasniflash yo‘li bilan bo‘lish va standartlashtirish, shuningdek, “Monitoring” tizimidan foydalangan holda kiberxavfsizlik hodisalariga chora ko‘rish jarayonini tavsiflash uchun foydalaniladi.

2. Normativ havolalar

1. “SIM3” modeli (https://sim3-check.opencsirt.org/).

2. Hodisalarni tasniflash bo‘yicha Yevropa taksonomiya standarti ENISA «Reference Incident Classification Taxonomy» (https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/@@download/fullReport).

3. “O‘z DSt ISO/IEC 27000:2014” davlat standartlari. Axborot xavfsizligini boshqarish tizimlari – Umumiy ko‘rinish va lug‘at.

4. “O‘z DSt 3386:2019” (ISO/IEC 27035-1:2016, MOD) davlat standarti. Hodisalarni boshqarish tamoyillari.

5. “O‘z DSt 3387:2019” (ISO/IEC 27035-1:2016, MOD) davlat standarti. Hodisalarga chora ko‘rish rejasini ishlab chiqish bo‘yicha ko‘rsatmalar.

3. Ishlatilgan qisqartmalar va ta’riflar

CERT/CSIRT – kiberxavfsizlik hodisalariga chora ko‘rish guruhi (yoki kompyuter hodisalariga chora ko‘rish guruhi) - hodisalar to‘g‘risida ma’lumotlarni to‘plash, ularni tasniflash va bartaraf etish bo‘yicha kiberxavfsizlik mutaxassislaridan iborat guruh.

FIRST – bu axborot va kiberxavfsizlik hodisalarini birgalikda oldini olish dasturlarini amalga oshiradigan ishonchli kiberxavfsizlik hodisalariga chora ko‘rish guruhlari xalqaro tashkiloti.

“Monitoring” tizimi – Internet tarmog‘ining milliy segmenti veb-resurslarida aniqlangan kiberxavfsizlik hodisalari, texnik hodisalar, zaifliklar hamda Markaz tomonidan ko‘rsatiladigan xizmatlar miqyosidagi ma’lumotlarni qayd etish va qayta ishlashga mo‘ljallangan maxsus tizim.

SIM3 (SIMMM, System Incident Management Maturity Model) – tizim hodisalarini boshqarish yetuklik modeli. Ya’ni, kompyuter hodisalariga chora ko‘rish

guruhi o‘z faoliyatini qanchalik to‘g‘ri baholashi va belgilangan vazifalarni o‘z vaqtida bajarishi, hujjatlashi va boshqarishini o‘lchash modeli.

Tiketlash (ro‘yxatga olish) – kiberxavfsizlik hodisasiga chora ko‘rish ishlarini nazorat qilish uchun unikal identifikatsiya raqamini berish orqali ro‘yxatga olish.

Konfidensiallik – axborotning avtorizatsiya qilinmagan shaxslar, mantiqiy obyektlar yoki jarayonlar uchun foydalanib bo‘lmaslik yoki yopiqlik xususiyati;

Yaxlitlik – axborotning to‘g‘riligini va to‘liqligini saqlab qolish xususiyati;

Foydalana olishlik – ma’lumotlar yoki resurslarning, vakolatli mantiqiy obyektning so‘roviga ko‘ra, foydalana olish mumkin bo‘lgan va foydalanishga yaroqlilik xususiyati.

4. Kiberxavfsizlik hodisalarini tasniflash

Hodisalarni tasniflash jarayonida mas’ul mutaxassislar quyidagi jadvalga muvofiq aniqlik kiritishlari lozim. 1-jadvalda 35 ta kichik klasslarga bo‘lingan hodisalarning 12 ta asosiy turi tasvirlangan.

1-jadval.

T/r	Hodisa klassi	Hodisa kichik klassi va tavsifi	Xavf darajasi
1	Bulk spam emails (Spam xabarlarni ommaviy yuborish)	Spam - bu so‘ralmagan keraksiz elektron xabarlarni ommaviy yuborish orqali tizim yoki resursni band qiladigan kutilmagan xabar.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik, — foydalana olishlik. Hodisaga qarab, xavf darajasi past darajadan o‘rta darajagacha baholanishi mumkin.
2	Malicious Code (Zararli kod)	Malicious Code (Zararli kod) – bu ma’lumotlar va shaxsiy ma’lumotlarni o‘g‘irlash, ma’lumotlar va resurslarni yo‘q qilish, DoS/DDoS hujumlarini, spam xabarlarini yuborish kabi potentsial xavfli faoliyatni amalga oshirishga yo‘naltirilgan zararli dastur yoki dasturning bir qismi sifatida ta’riflanadi.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik, — foydalana olishlik. Xavf darajasi yuqori.

		Zararli kodlar besh toifaga bo‘linadi: viruslar, troyan oti, josus dasturlar, mobil kodlar va aralash toifalar.	
		Infected System (Infektsiyalangan tizim) Tizim zararli dasturlar bilan zararlangan. Misol uchun, ShK, smartfon yoki server, “rootkit” orqali zararlanish.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik, — foydalana olishlik. Xavf darajasi yuqori.
		C2 Server (C2 server) Infektsiyalangan tizimlardagi zararli dasturlar bilan aloqa qiladigan buyruq va boshqaruv serveri.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik, — foydalana olishlik. Xavf darajasi o‘rta darajadan yuqori darajagacha baholanishi mumkin.
		Malware Distribution (Zararli dasturlarning tarqalishi) SPAM xabarlarga biriktirilgan zararli dasturlarni yuklab olish URL manzili orqali tarqatish.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik, — foydalana olishlik. Hodisa tafsilotlariga qarab, xavf darajasi past yoki yuqori bo‘lishi mumkin.
		Malware Configuration (Zararli dastur konfiguratsiyasi) zararli dastur konfiguratsiyasini o‘z ichiga olgan URI, misol uchun, bank troyanlari uchun ishlatiladigan veb-injektorlar.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik, — foydalana olishlik. Xavf darajasi hodisaning tafsilotlariga bog‘liq.
3	Information Gathering	Scanning (Skanerlash) – bu resursga yoki tizimga so‘rovlar yuborish orqali	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi:

	(Ma’lumotlarni yig‘ish)	zaif tomonlarini aniqlash hujum turi. Shu bilan birga, skanerlash orqali xostlar, xizmatlar va foydalanuvchilarning qayd yozuvlari to‘g‘risidagi ma’lumotlarni to‘plashda ishlatiladi. Misol uchun: fingerd, DNS-so‘rovlar, ICMP, SMTP (EXPN, RCPT), portlarni skanerlash.	— konfidensiallik, — yaxlitlik, — foydalana olishlik. Skanerlash bilan bog‘liq xavf darajasi bir nechta omillarga qarab farq qilishi mumkin, masalan, skanerlash hajmi va intensivligi, skanerga berilgan ruxsatlar va ruxsatlar darajasi, maqsadli tizim yoki tarmoqning sezgirligi.
		Sniffing (Tutib olish) – bu tarmoq trafigini kuzatish va yozib borish.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik, — foydalana olishlik. Xavf darajasi yuqori.
		Social Engineering (Ijtimoiy muhandislik) Shaxsdan texnik bo‘lmagan usulda ma’lumot yig‘ish (yolg‘on, hiyla, pora, yoki tahdid orqali).	Kiberxavfsizlikning quyidagi asosiy tamoyilini buzilishiga olib keladi: — konfidensiallik.
4	Intrusion Attempts (Bostirib kirishga urinishlar)	Exploitation of known Vulnerabilities (Ma’lum zaifliklardan foydalanish) Taniqli CVE identifikator raqamiga ega zaifliklardan foydalanish orqali tizimni yoki har qanday xizmatni buzishga urinish (masalan: buferni to‘ldirish, bekdor, saytlararo skripting va boshqalar).	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik, — foydalana olishlik. Xavf darajasi yuqori.
		Login Attempts (Tizimga kirishga urinish) Ko‘p marotaba tizimga kirishga urinishlar (Parollarni terish/buzish).	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik.

			Xavf darajasi yuqori. Tizimga kirishga urinishlarning xavf darajasi urinishlarning konteksti va jiddiyligiga qarab farq qilishi mumkin.
		New Attack Signature (Yangi hujum signaturalari) Noma'lum eksploytlarni qo'llagan holda hujum uyishtirish.	Kiberxavfsizlikning asosiy tamoyillarini buzmaydi. Xavf darajasi hujum usulining murakkabligi va muvaffaqiyatiga qarab past darajadan yuqori darajagacha baholanishi mumkin.
5	Intrusions (Bostirib kirish)	Privileged Account Compromise (Imtiyozli hisob yozuvlarni buzish) Jinoyatkor administrator (imtiyozli hisob yozuvi) huquqiga ega bo'lish orqali tizimni buzishi.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — foydalana olishlik. Xavf darajasi yuqori.
		Unprivileged Account Compromise (Imtiyozsiz hisob yozuvlarni buzish) Jinoyatkor imtiyozsiz hisob yozuviga ega bo'lish orqali tizimni buzishi.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik. Xavf darajasi hujumning xarakteriga, jinoyatkor erishgan kirish darajasiga va tizimda saqlangan ma'lumotlarning konfidensiallik darajasiga qarab farq qilishi mumkin.
		Application Compromise (Ilovani buzish) Dasturiy ta'minotning (noma'lum) zaifliklaridan foydalanish orqali ilovani buzish, misol uchun SQL-inyeksiya.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik, — foydalana olishlik. Xavf darajasi ilovaning xarakteriga, u saqlaydigan ma'lumotlarning konfidensialligiga va zarar

			ko‘rgan foydalanuvchilar soniga bog‘liq.
		Burglary (Jismoniy buzish) Misol uchun: korporativ binoga yoki ma’lumotlarni saqlash markaziga jismoniy kuch ishlatgan holda buzib kirish.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlik, — foydalana olishlik. Xavf darajasi hodisaning xarakteri va oqibatiga qarab farq qilishi mumkin.
6	Availability (Foydalana olishlik)	DoS (Denial of Service, Xizmat ko‘rsatishni rad etish) и DDoS (Distributed denial of service, Xizmat ko‘rsatishni taqsimlangan rad etish). Ushbu turdagi hodisalar tizim, xizmat yoki tarmoqning to‘liq potentsialida ishlashini to‘xtatishga olib kelib, ko‘pincha avtorizatsiya qilingan foydalanuvchilarga xizmat ko‘rsatishni rad etishga olib keladi. Texnik vositalardan kelib chiqib, DoS va DDoS hodisalarining ikkita asosiy turi mavjud: nishonni yo‘q qilishga qaratilgan yoki uni ishlashini to‘xtatib qo‘yishga. Ba’zi texnik DoS hodisalari tizimlarning noto‘g‘ri konfiguratsiyasi yoki dasturiy ta’minotning mos kelmasligi kabi hodisalar tufayli yuzaga kelishi mumkin, lekin	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik, — foydalana olishlik. Xavf darajasi (riski) hujumning jiddiyligi va davomiyligiga, maqsadliligiga, tizimning yoki tarmoqning muhimligiga qarab farq qilishi mumkin.

		aksariyat hollarda ular qasddan sodir etiladi.	
		Misconfiguration (Noto‘g‘ri konfiguratsiya) Dasturiy ta’minotning noto‘g‘ri konfiguratsiyasi foydalana olishlik bilan bog‘liq muammolarni keltirib chiqaradi. Unga misol qilib, eski DNSSEC KSK ildiz zonasiga ega DNS server.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik, — foydalana olishlik. Xavf darajasi (riski) tizim yoki dasturiy ta’minotning turidan kelib chiqib aniqlanadi.
		Sabotage (Sabotaj) Jismoniy sabotaj. Masalan, simlarni kesish yuborish yoki yomon niyat bilan tizim yoki tarmoqqa o‘t qo‘yish orqali zarar yetkazish.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik, — foydalana olishlik Xavf darajasi (riski) hujumning harakteridan va ko‘lamidan kelib chiqib aniqlanadi.
		Outage (Uzilishlar) Masalan, konditsionerning ishlamay qolishi yoki tabiiy ofat tufayli yuzaga kelgan uzilish.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik, — foydalana olishlik Уровень риска зависит от критичности затронутых систем или служб, продолжительности сбоя и способности организации восстановиться после него. Xavf darajasi (riski) ta’sir doriasidagi tizimlar yoki xizmatlarning muhimlilik darajasiga, uzilish davomiyligiga va tashkilotning uzilishdan tiklanish qobiliyatiga bog‘liq.

7	Information Content Security (Axborot kontentining xavfsizligi)	Unauthorised access to information (Axborotdan ruxsat etilmagan tarzda foydalana olish) Tizimdan, xizmatlardan yoki tarmoqdan ruxsatsiz foydalanish yoki shunday urunishlar. Masalan, parol fayllarini tiklashga urinish, ob'ektga imtiyozli ruxsat olish yoki kirish uchun buferni to'ldirish hujumlarini amalga oshirish.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik. Xavf darajasi (riski) ruxsat olinayotgan axborotning konfidensiallik darajasi va uni turidan kelib chiqib belgilanadi.
		Unauthorised modification of information (Axborotni ruxsat etilmagan tarzda o'zgartirish) Axborotni ruxsatsiz o'zgartirish. Masalan, tajovuzkorning tizimga yoki ilovaga o'g'irlangan ma'lumotlar yordamida kirishi yoki tovlamachi zararli dastur yordamida axborotni shifrlashi.	Kiberxavfsizlikning "yaxlitlilik" tamoyilini buzilishiga olib keladi. Xavf darajasi (riski) ruxsatsiz o'zgartirilayotgan axborotning xarakteri va kontekstidan kelib chiqib belgilanadi.
		Data Loss (Axborotning yo'qotilishi) Axborotning yo'qotilishi, masalan, qattiq diskning xatosi yoki uning o'g'irlanishi oqibatida.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik, — foydalana olishlik. Xavf darajasi (riski) yo'qotilgan axborotning hajmiga va turiga shuningdek uni tashkilotga ta'siridan kelib chiqib aniqlanadi.
		Leak of Confidential Information (Konfidensial axborotning sizdirilishi)	Kiberxavfsizlikning "konfiensiallik" prinsipi buzilishiga olib keladi.

		Konfidensial axborotning sizdirilishi. Masalan, shaxsiy identifikatsion axborotlar yoki hisob ma’lumotlari.	Xavf darajasi (riski) ko‘lami sizdirilgan axborotning xarakteridan va holat yuz bergan kontekstdan kelib chiqib aniqlanadi.
8	Fraud (Firibgarlik)	Unauthorized Use of Resources (Resurslardan ruxsatsiz foydalanish) Resurslardan rusxat etilmagan maqsadlarda (moliyafiy foyda olishda) foydalanish. Masalan, elektron pochtadan noqonuniy ravishda moliyaviy piramida yoki foyda haqida spam xabarlar yuborishda qatnashish.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik, — foydalana olishlik. Resurslardan ruxsatsiz foydalanish orqali kelib chiqadigan xavf darajasi (riski) ko‘lami ruxsatsiz foydalanilayotgan resurs hajmidan va xarakteridan kelib chiqib belgilanadi.
		Phishing (Fishing) Foydalanuvchilarning shaxsiy identifikatsion ma’lumotlarini ochiqlashlariga aldov yoki ijtimoiy muhandislik usuli orqali (maskirovka) undash.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik, — foydalana olishlik. Fishing hujumlarning xavf darajasi (riski) zarar ko‘rgan axborot hajmi va hujumning xususiyatidan kelib chiqib belgilanadi.
9	Vulnerable (Zaiflik)	Weak Crypto (Zaif kriptografiya) POODLE/FREAK hujum turlariga moyil bo‘lgan zaif kriptografiyani taqdim qiluvchi veb-serverlar va boshqa xizmatlar.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik. Kelib chiqadigan risk darajasi ushbu hujumni ishlatish kontekstidan kelib chiqib belgilanadi.
		DDoS Amplifier (DDoS Amplifikatsiya) DDoS hujumlarini aks ettirish/kuchaytirish uchun	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik,

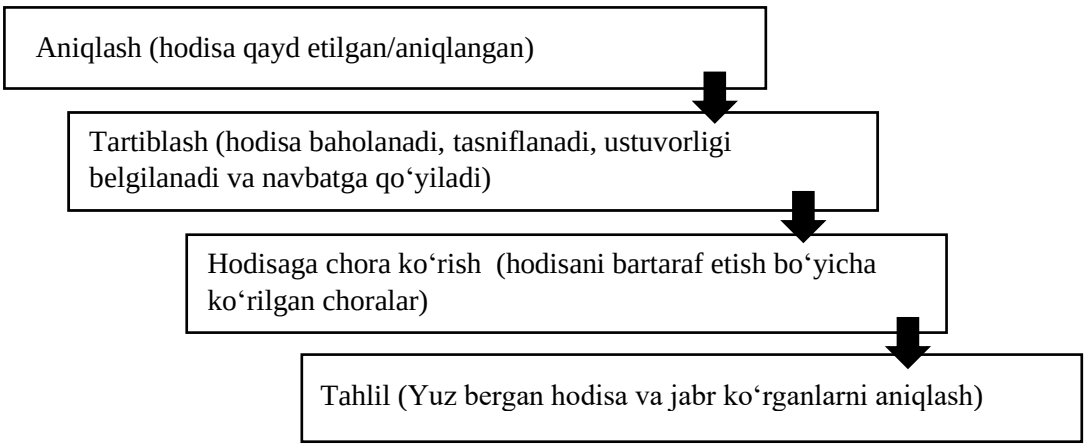
		suiiste’mol qilinishi mumkin bo‘lgan ochiq xizmatlar (servislar). Misol tariqasida, ochiq DNS (resolver) serverlar, monlist funksiyasi bor bo‘lgan ochiq NTP-serverlar.	— yaxlitlilik, — foydalana olishlik. DDoS Amplifikatsiya hujumlarining xavf (risk) darajasi ularning ko‘lami va davomiyligiga qarab belgilanadi.
		Potentially Unwanted Accessible Services (Maqsadsiz ishlatishga ochiq qoldirilgan servis/xizmatlar) Maqsadsiz umumiy foydalanish uchun ochiq qoldirilgan xizmat/servislar. Masalan, Telnet, RDP yoki VNC.	Kiberxavfsizlikning asosiy tamoyillarini buzmaydi. Xavf (risk) darajasi ko‘lami ma’lum dasturiy ta’minot yoki xizmatga va tajovuzkorlar tomonidan qanday suiiste’mol qilinishi mumkinligiga qarab aniqlanadi.
		Information disclosure (Axborotning oshkor bo‘lishi) Maxfiy ma’lumotlarni oshkor qilishi mumkin bo‘lgan xizmatlar (servislar). Masalan, SNMP yoki Redis serverlari.	Kiberxavfsizlikning “konfidensiallik” prinsipi buzilishiga olib keladi. Keltirib chiqaruvchi xavfi (riski) oshkor bo‘lgan axborotning turi va konfidensialligiga qarab belgilanadi.
		Vulnerable system (Zaiflik tizim) Muayyan hujumlarga qarshi himoyasiz tizim. Misol tariqasida: noto‘g‘ri konfiguratsiya qilingan proksi-server sozlamalari (masalan: WPAD), operatsion tizimning eskirgan versiyasi va boshqalar.	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik, — foydalana olishlik. Zaif tizim bilan bog‘liq xavf darajasi zaiflikning jiddiyligiga va zararli dasturiy kod (eksploit) keltirib chiqaradigan oqibatiga qarab belgilanadi.
10	Misuse (Suiiste’mol)	Misuse (Suiiste’mol) Bunday hodisa foydalanuvchi tomonidan tashkilot axborot tizimining xavfsizlik	Kiberxavfsizlikning quyidagi asosiy tamoyillarini buzilishiga olib keladi: — konfidensiallik, — yaxlitlilik,

		siyosati buzilganida sodir bo‘ladi. Quyidagilar holatlarda suiiste’mol qilinganlik holati yuzaga kelishi mumkin: buzuvchi/xakerlik vositalarini yuklab olish va o’rnatish; korporativ elektron pochtani shaxsiy maanfatlar uchun ishlatish yoki SPAM xabarlar yuborishda qo‘llash; korporativ resurslardan buzg‘unchi veb-saytlar yaratishda foydalanish; internet qaroqchilik bilan shug‘ullanish va markazlashmagan peer-to-peer tarmoqlar orqali noqonuniy ravishda video, dasturiy ta’minot va musiqa tarqatish.	— foydalana olishlik. Foydalanish suiiste’mol qilish keltirib chiqaradigan risk darajasi amalga oshirilgan harakatlarning jiddiyligiga qarab belgilanadi.
11	Other (Boshqalar)	Uncategorised (Kategoriyalanmagan) Belgilangan toifalardan biriga to‘g‘ri kelmaydigan barcha hodisalar ushbu turga kiritilishi kerak, aks holda hodisa tasniflanmaydi.	
		Undetermined (Noma’lum/Identifikatsiyalanmagan) Hodisaning klassifikatsiyasi noma’lum	
12	Test (Test)	Test (Test) Tekshiruv/Testlar uchun mo‘ljallangan.	

5. Kiberxavfsizlik hodisalarini boshqarish

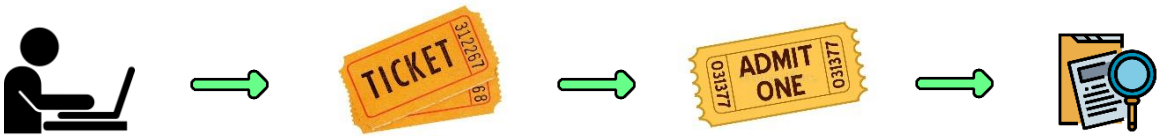
Tiketlash jarayoni “Monitoring” tizimi yordamida amalga oshiriladi.

Tiketlash jarayonining asosiy maqsadi kompyuter hodisalariga javob berish guruhlari (CERT/CSIRT) a’zolarining hodisalarni hal qilish bo‘yicha majburiyatlarini izchil va samarali bajarishlarini ta’minlashdir. Shuningdek, tiketlash tizimi uchun kelishilgan yagona ish jarayoni shabloniga rioya amal qilishga chaqirish. Quyida hodisalarni ko‘rib chiqish/chora ko‘rish jarayonining tavsifi keltirilgan:



Tiketlash jarayoni quyida keltirilgan sxema asosida faoliyat yuritadi:

2-jadval.

Ochiq manbalar /tashkilotlar	**24/7 navbatchi (Monitoring bo‘limi)**	**Chora ko‘rish bo‘yicha mutaxassis (Chora ko‘rish bo‘limi)**	**Tekshirish bo‘yicha mutaxassis (Tekshirish bo‘limi)**
Hodisa haqida xabar	Hodisa tiketi	Hodisa tiketi	Tekshirish tiketi
	Ushbu tiket elektron pochta/portal xabarlari orqali tizimga kelib tushadi, yoki telefon/faks orqali yuborilgan bo‘lsa, 24/7 navbatchi tomonidan tizimda yaratiladi.	Ushbu tiket chora ko‘ruvchi tomonidan faktlar tekshirilgandan so‘ng va hodisa haqida hisobotning barcha tafsilotlari olindandan so‘ng tuziladi.	Ushbu tiket hodisani tekshirish bo‘yicha mutaxassis tomonidan tekshirish davomida tuziladi va hodisa tiketi bilan bog‘lanadi.
	Hodisa hisoboti tiketi	Hodisa tiketi	Tekshirish tiketi
			

6. Tiketlash jarayonida foydalanuvchilarning roli va mas’uliyati

CERT/CSIRT jamoalarida 3 ta asosiy rol mavjud bo‘lib, har bir rol o‘ziga tegishli mas’uliyatlariga ega va bir-biri bilan o‘zaro bog’liq:

– **24/7 navbatchi**. Kiberxavfsizlik hodisalari yuzaga kelganligini aniqlab ularni “Monitoring” tizimida qayd etadi va monitoring jarayoni bilan shug’ullanadi. Tizimda hodisa tiketlarini yaratish uchun javobgar.

– **Chora ko‘rish bo‘yicha mutaxassis**. 24/7 navbatchi tomonidan xabar berilgan barcha kiberxavfsizlik hodisalari hisobotlari bilan ishlaydi. Xabar berilgan hodisa kiberxavfsizlik hodisasiligini, uni jamoada kim ko‘rib chiqishini, qachon ko‘rib chiqilishini tegishli ish jarayoniga asosan hal qiladi. Hodisa holatini kuzatib boradi va nazorat qiladi.

– **Tekshirish bo‘yicha mutaxassis**. Hodisa haqida ma’lumot to‘playdi va tahlil qiladi. Shuningdek, mavjud ma‘lumotlarga asoslanib voqealar xronologiyasini tiklaydi. Kiberxavfsizlik hodisasini yuzaga kelish sabablari va texnik tafsilotlarini aniqlaydi, tavsiyalar ishlab chiqadi.

Tiketlashda kiberxavfsizlik hodisalarini ko‘rib chiqish jarayoni quyidagilardan iborat:

– Hodisa haqida xabar olish;

– Hodisa hisobotini tekshirish;

– Tiketni rad etish (bir qator hodisalar haqida kiruvchi xabarlar faqat ma’lumot uchun mo‘ljallangan bo‘lib ular qabul qilingan va o‘rganilgandan so‘ng, qo‘shimcha etiborni talab etmaydi);

– Ayni hodisa haqida avval xabar berilgan/berilmaganligi tekshiriladi;

– Tiket chora ko‘rish bo‘yicha mutaxassisga yuboriladi;

– Hodisaning prioriteti (ustuvorligi) va klassifikatsiyasi aniqlanadi;

– Mavjud hodisalar bilan bog‘liqliligi tekshiriladi;

– Zaiflik haqidagi hisobotga javob beriladi (amalga oshirilgan ishlar yuzasidan izoh qoldiriladi hamda arizachiga avtomatik tarzda javob yuboriladi);

– Saralash jarayoni;

– Tekshiruv so‘rovini yaratish;

– Tekshiruv so‘rovini yopish;

– Hisobotni tayyorlash.

7. Kiberxavfsizlik hodisalariga chora ko‘rish jarayoni

Yuqorida qayd etilgan kiberxavfsizlik hodisalariga chora ko‘rish jarayoni (1-jadval) ro‘yxatga olish bosqichidan boshlab va keyinchalik uni vakolatli organga yuborish uchun hisobot tayyorlashgacha qadar 3-bosqichdan iborat.

Birinchi bosqich. Hodisani aniqlash va ro‘yxatga olish.

Dastlabki bosqich hodisani ro‘yxatga olish va hodisa haqida quyidagi asosiy ma’lumot manbalaridan axborot to‘plashni o‘z ichiga oladi

– ichki monitoring tizimlari va tashqi manbalar;

– kiberxavfsizlik sohasida faoliyat olib boruvchi tashkilotlar;

– Milliy internet segmenti foydalanuvchilari;

– kiberxavfsizlik masalalarida vakolatga ega bo‘lgan xalqaro tashkilotlar;

– Internetning ochiq manbalaridan olinadigan axborotlar;

Ikkinchi bosqich. Chora ko‘rish va xabar berish.

Ushbu bosqich hodisaga chora ko‘rish jarayonini tavsiflaydi:

– kiberxavfsizlik hodisasi ta’sir doirasidagi axborot tizimlari/axborot resurslarini aniqlash;

– Kiberxavfsizlik hodisasi sodir bo‘lgan axborot tizimlarini/axborot resurslarini vaqtincha izolyatsiya qilish;

– hodisa oqibatida keltirilgan zararni baholash;

– raqamli dalillarni saqlash;

– vakolatli organga kiberxavfsizlik hodisasi to‘g‘risida xabar berish;

– hodisa ta’sir doirasidagi Internet-provayderlarni hodisaga birlamchi choralarni ko‘rish zarurligi to‘g‘risida xabardor qilish.

Uchinchi va to‘rtinchi bosqich. Hodisani tekshirish, qayta tiklash va xulosalar.

Hodisani tekshirish jarayonida quyidagi amallarni o‘z ichiga oladi:

– kiberxavfsizlik hodisasi haqida axborot va ma’lumotlarni jamlash;

– mavjud ma’lumotlarga asoslanib voqealar xronologiyasini tiklash;

– kiberxavfsizlik hodisasi yuzaga kelish sabablari va texnik tafsilotlarini aniqlash;

– hodisaning yakuniy hisobotini tayyorlash va kelajakda yuzaga kelishi mumkin bo‘lgan hodisalarni oldini olish to‘g‘risida tavsiyalar berish;

– vakolatli organga bajarilgan ishlar yuzasidan hisobot yuborish.