|  |
| --- |
| Level 4 | Cyber Security |
| Abdulloh Xalilov |

**Unit 3:** Level 4 | Cyber Security

**O‘qituvchi:** Azizbek Xoshimov

**Guruh identifikatori:** 23-412 Software (C#)

**Talaba ID:** 231397

**Taqdim etilgan sana:** 31.05.2025 yil

**BTEC o'quvchilar topshiriqlarini baholash va deklaratsiya**

Baholash uchun ishlarni taqdim etganda, har bir o'quvchi ish o'ziniki ekanligini tasdiqlovchi deklaratsiyani imzolashi kerak.

|  |  |
| --- | --- |
| **O‘quvchi (talaba) identifikatori:** | 231397 |
| **Baholovchi nomi:** | Azizbek Xoshimov |
| **BTEC dasturi nomi:** | Pearson BTEC Higher Nationals in Information Technologies |
| **Birlik yoki komponent raqami va nomi:** | Level 4 | Cyber Security |
| **Topshiriq nomi:** | Level 4 | Cyber Security |
| **Topshiriq topshirilgan sana:** | 31.05.2025yil |

Iltimos, har bir topshiriq uchun berilgan ishlarni sanab o'ting. Ishlarni topish mumkin bo'lgan sahifa raqamlarini ko'rsating yoki ishlarning mohiyatini tavsiflang (masalan, grafik, rasm).

|  |  |  |
| --- | --- | --- |
| **Topshiriq vazifasi ma'lumoti** | **Ishlar taqdim etildi** | **Sahifa** |
|  |  |  |
|  |  |  |
|  |  |  |

|  |
| --- |
| **O'quvchi deklaratsiyasi**  Men ushbu topshiriq uchun taqdim etilgan ish meniki ekanligini tasdiqlayman. Ishda foydalanilgan manbalarga aniq havola qildim. Men noto'g'ri deklaratsiya noto'g'ri ishlashning bir shakli ekanligini tushunaman.  **O‘quvchi imzosi:**  **Sana:** 31.05.2025 yil |

Mundarija

[KIRISH 3](#_Toc199602561)

[Kiberjinoyat va kiber tahdid aktorlarining tabiati 4](#_Toc199602562)

[Kiberxavfsizlik tahdidlari va xavflarini tadqiq etish 6](#_Toc199602563)

[Axborot xavfsizligi ta’minoti konsepsiyalarining AKT infratuzilmasiga qo‘llanilishining samaradorligini o‘rganish 10](#_Toc199602564)

[Kiberxavfsizlik tahdidlariga javob berish usullarini tadqiq etish 11](#_Toc199602565)

[Xulosa 13](#_Toc199602566)

[ADABIYOTLAR RO'YXATI 14](#_Toc199602567)

KIRISH

Zamonaviy dunyoda raqamli texnologiyalarning misli ko‘rilmagan sur’atlar bilan jadal rivojlanishi va jamiyat hayotining barcha jabhalariga chuqur kirib borishi bilan bir qatorda, kiberxavfsizlik masalalari global miqyosda faoliyat yurituvchi yirik korporatsiyalar uchun nafaqat dolzarb, balki strategik ustuvorlik kasb etayotgan fundamental muammoga aylandi. Ayniqsa, moliya (yuqori likvidli aktivlar va maxfiy moliyaviy ma’lumotlar), sog‘liqni saqlash (bemorlarning o‘ta nozik shaxsiy va tibbiy qaydlari) va texnologiya (qimmatbaho intellektual mulk va innovatsion ishlanmalar) kabi strategik ahamiyatga ega sohalarda faoliyat ko‘rsatuvchi, keng ko‘lamli, murakkab va geografik jihatdan tarqoq raqamli infratuzilmaga hamda ulkan hajmdagi nozik axborotlar massivlariga ega bo‘lgan xalqaro korporatsiyalar, o‘z navbatida, tobora kuchayib borayotgan va takomillashayotgan kiberjinoyatchilar guruhlari uchun asosiy va jozibador nishonga aylanib, ko‘plab murakkab, ko‘p qatlamli va oldindan aytib bo‘lmaydigan kiberxavf-xatarlarga duch kelmoqdalar. Ushbu tahliliy hisobot yetakchi kiberxavfsizlik konsalting kompaniyasining Cyber Security Analysti sifatida, mazkur xalqaro korporatsiyaning bebaho raqamli aktivlarini himoya qilish, uning faoliyatiga xos bo‘lgan noyob zaifliklarni va potentsial tahdidlarni har tomonlama aniqlash hamda ularga qarshi samarali, proaktiv va barqaror kurashish strategiyalarini ishlab chiqish maqsadida sinchkovlik bilan tayyorlangan.

Mazkur tadqiqotning asosiy va keng qamrovli maqsadi – korporatsiyaning hozirgi kundagi kiberxavfsizlik holatini chuqur va ob’ektiv tahlil qilish, uning operatsion faoliyatiga, biznes jarayonlariga va strategik maqsadlariga xos bo‘lgan o‘ziga xos zaiflik nuqtalarini (vulnerabilities) va tashqi hamda ichki tahdid vektorlarini (threat vectors) batafsil o‘rganishdan iboratdir. Shu bilan birga, ushbu tadqiqot axborot xavfsizligini ta’minlashning ilg‘or konsepsiyalarini amaliyotga tatbiq etish, kiberhujumlarga nisbatan tashkiliy va texnologik chidamlilikni (cyber resilience) oshirish hamda yuzaga kelishi mumkin bo‘lgan kiber insidentlarga tezkor, samarali va minimal yo‘qotishlar bilan javob qaytarish bo‘yicha aniq, o‘lchanadigan, erishiladigan, tegishli va vaqt bilan cheklangan (SMART) amaliy tavsiyalar taqdim etishni o‘z oldiga qo‘yadi. Hisobotda kiberjinoyatlar evolyutsiyasi va ularning zamonaviy ko‘rinishlari, turli motivlarga ega bo‘lgan tahdid aktorlarining (threat actors) faoliyati, axborotni himoyalashning ko‘p qatlamli (defense-in-depth) konsepsiyalari, risklarni boshqarish (risk management) metodologiyalari hamda insidentlarga javob berish (incident response) va faoliyatni tiklash (disaster recovery and business continuity) usullari kabi muhim jihatlar xalqaro standartlar va eng yaxshi amaliyotlar (best practices) asosida atroflicha yoritiladi. Ushbu tahlillar va takliflar korporatsiyaning kiberxavfsizlik bo‘yicha umumiy strategik yondashuvini tubdan mustahkamlashga, uning raqamli landshaftdagi obro‘sini himoya qilishga va pirovardida uning uzoq muddatli barqaror o‘sishi hamda innovatsion rivojlanishini ta’minlashga xizmat qilishi ko‘zda tutilgan.

Kiberjinoyat va kiber tahdid aktorlarining tabiati

Kiberjinoyatchilikning zamonaviy ko‘rinishlari va ularning tashkilotlarga ta’siri tobora ortib bormoqda. Tashkilot uchun kiberjinoyatlarning asosiy turlari va ularning potentsial tahdidlarini chuqur anglash, ularning rivojlanish tendensiyalarini kuzatib borish muhimdir (P1). Ilgari sanab o‘tilgan **phishing**, **ransomware**, **DDoS hujumlari**, **malware** va **Advanced Persistent Threats (APTs)** kabi xavflarga qo‘shimcha ravishda, **Business Email Compromise (BEC)** – ya’ni, biznes elektron pochta manzillarini komprometatsiya qilish orqali moliyaviy firibgarliklar, **ma’lumotlar sizib chiqishi (data breaches)** – nafaqat ransomware orqali, balki boshqa usullar bilan ham maxfiy ma’lumotlarning ruxsatsiz shaxslar qo‘liga tushishi, hamda **ichki tahdidlar (insider threats)** – ya’ni, tashkilot xodimlarining qasddan yoki beparvolik oqibatida kiberxavfsizlikka zarar yetkazishi kabi holatlar ham keng tarqalgan. APT hujumlari, o‘z navbatida, oddiy zararli dasturlardan farqli o‘laroq, yuksak darajada yashirinlik, uzoq muddatli maqsadlar (ko‘pincha josuslik yoki yirik miqyosdagi sabotaj) va maxsus mo‘ljallangan vositalar bilan ajralib turadi. Ushbu hujumlarning barchasi nafaqat to‘g‘ridan-to‘g‘ri moliyaviy yo‘qotishlarga (masalan, to‘lov talablari, jarimalar, tiklash xarajatlari), balki tashkilot obro‘sining (reputatsiyasining) jiddiy zarar ko‘rishiga, mijozlar va hamkorlar ishonchining yo‘qolishiga, operatsion faoliyatning uzoq muddatga izdan chiqishiga va hatto tartibga soluvchi organlar tomonidan jiddiy sanktsiyalarga olib kelishi mumkin. Ayniqsa, sizning korporatsiyangiz kabi moliya (moliyaviy aktivlar va tranzaksiyalar), sog‘liqni saqlash (bemorlarning shaxsiy va tibbiy ma’lumotlari) va texnologiya (intellektual mulk, ilmiy-tadqiqot natijalari) kabi yuqori darajadagi maxfiy va qimmatli axborotlar bilan ishlaydigan sohalarda bu kabi tahdidlar o‘ta jiddiy va ko‘p qirrali oqibatlarga ega bo‘lishi mumkin.

Potensial hujum nishonlari sifatida sizning korporatsiyangizda bir nechta muhim aktivlar mavjud bo‘lib, ularning zaiflik sabablarini tushunish va bartaraf etish strategik ahamiyatga ega (P2). **Mijozlar ma’lumotlari** (shaxsiy identifikatsiya ma’lumotlari (PII), moliyaviy hisob raqamlari, kredit karta detallari, sog‘liqqa oid qaydlar (PHI)) kiberjinoyatchilar uchun eng qimmatli nishonlardan biri hisoblanadi, chunki bu ma’lumotlar qora bozorda sotilishi, shaxsiyatni o‘g‘irlash yoki moliyaviy firibgarlik uchun ishlatilishi mumkin. **Moliyaviy tizimlar** (onlayn banking platformalari, to‘lov shlyuzlari, tranzaksiya ma’lumotlari bazalari, investitsiya portfellari) to‘g‘ridan-to‘g‘ri pul o‘g‘irlash yoki bozor manipulyatsiyasi uchun hujumga uchrashi mumkin. **IT infratuzilmasi** (serverlar, tarmoq uskunalari, ma’lumotlar bazalari, bulutli xizmatlar, operatsion texnologiyalar (OT) va sanoat boshqaruv tizimlari (ICS) – ayniqsa texnologiya va ishlab chiqarish bilan bog‘liq bo‘limlarda) hamda **intellektual mulk** (patentlar, tijorat sirlari, dasturiy ta’minot kodlari, ilmiy-tadqiqot natijalari) raqobatbardoshlikni yo‘qotish, sanoat josusligi yoki sabotaj maqsadida nishonga olinishi mumkin. Ushbu nishonlarning zaifligi bir necha omillarga bog‘liq: **eskirgan dasturiy ta’minot va apparat vositalari** (ular ma’lum bo‘lgan, ammo yamanmagan zaifliklarni o‘z ichiga olishi mumkin), **noto‘g‘ri konfiguratsiya qilingan xavfsizlik sozlamalari** (masalan, standart parollardan foydalanish, keraksiz ochiq portlar, ruxsatlarni noto‘g‘ri boshqarish), **xodimlarning kiberxavfsizlik bo‘yicha xabardorlik darajasining pastligi** (bu ijtimoiy muhandislik hujumlarining muvaffaqiyatli bo‘lishiga olib keladi), **murakkab va o‘zaro bog‘langan tizimlardagi yashirin zaifliklar** (bu yerda bitta komponentning komprometatsiyasi butun tizimga ta’sir qilishi mumkin) hamda **ijtimoiy muhandislikning turli taktikalariga moyillik** (phishingdan tashqari, pretexting – ya’ni, yolg‘on bahona bilan ma’lumot olish, baiting – ya’ni, qiziqtiruvchi o‘lja orqali zararli dastur o‘rnatishga undash kabi usullar). Masalan, sog‘liqni saqlash sohasida bemor ma’lumotlarining maxfiyligi buzilishi nafaqat bemorlarning shaxsiy hayotiga jiddiy zarar yetkazishi, balki HIPAA (AQShda) yoki GDPR (Yevropa Ittifoqida) kabi qonunlar asosida katta miqdordagi moliyaviy jarimalarga va huquqiy ta’qiblarga olib kelishi mumkin.

Raqamli tizimlarning o‘zi ham murakkab va ko‘p qirrali tabiatga ega bo‘lib, ular bir vaqtning o‘zida ham hujum “nishoni”, ham hujum “vositasi” bo‘lib xizmat qilishi mumkinligini tahlil qilish muhimdir (M1). Korporativ serverlar nafaqat qimmatli ma’lumotlarni (mijozlar bazalari, moliyaviy hisobotlar, intellektual mulk) saqlash uchun jozibador nishon bo‘lishi, balki kiberjinoyatchilar tomonidan komprometatsiya qilinganidan so‘ng, **botnetning bir qismi sifatida** boshqa tashkilotlarga yoki hatto davlat infratuzilmalariga qarshi keng ko‘lamli DDoS hujumlarini amalga oshirish uchun kuchli vosita sifatida ham ishlatilishi mumkin. Shuningdek, xodimlarning ish stansiyalari, noutbuklari yoki mobil qurilmalari orqali amalga oshirilgan phishing yoki malware hujumi natijasida olingan kirish huquqlari (credentials) yordamida tajovuzkorlar ichki tarmoqqa kirib, u yerdan yanada muhimroq tizimlarga **lateral harakat (lateral movement)** qilishlari va o‘zlarining imtiyozlarini oshirishlari (privilege escalation) mumkin. Hozirgi kunda keng tarqalayotgan **Internet of Things (IoT)** qurilmalari (aqlli sensorlar, kameralar, tibbiy asboblar) ham ko‘pincha yetarli darajada himoyalanmaganligi sababli, ham hujum uchun oson nishon, ham tarmoqqa kirish uchun zaif nuqta, hamda yirik botnetlarning bir qismi bo‘lib xizmat qilishi mumkin. Hatto korporatsiya foydalanadigan **bulutli infratuzilma** ham noto‘g‘ri konfiguratsiya qilingan taqdirda yoki zaif kirish nazorati tufayli ham nishonga aylanishi, hamda komprometatsiya qilinganidan so‘ng boshqa hujumlarni amalga oshirish uchun platforma bo‘lishi mumkin. Bu esa raqamli tizimlarning himoyasini ko‘p qatlamli (defense-in-depth) va kompleks yondashuv asosida, har bir komponentning potentsial ikki tomonlama rolini hisobga olgan holda qurish zarurligini yaqqol ko‘rsatadi.

Tahdid aktorlariga qarshi kurashish uchun keng qamrovli va adaptiv strategiyalar ishlab chiqish lozim bo‘lib, ular nafaqat texnologik yechimlarni, balki huquqiy-me’yoriy asoslarni va inson omilini ham qamrab olishi kerak (D1). **Texnologik choralar** doimiy ravishda yangilanib turishi va zamonaviy tahdidlarga moslashishi kerak. Bularga ilgari aytib o‘tilgan xavfsizlik devorlari (firewalls), intruziv aniqlash va oldini olish tizimlari (IDS/IPS), anti-malware dasturlari, ma’lumotlarni shifrlash va ko‘p faktorli autentifikatsiya (MFA) kabi fundamental vositalarga qo‘shimcha ravishda, **Endpoint Detection and Response (EDR)** – ya’ni, oxirgi nuqtalarda (kompyuterlar, serverlar) tahdidlarni aniqlash va ularga javob qaytarish tizimlari, **Extended Detection and Response (XDR)** – ya’ni, turli xavfsizlik qatlamlaridan (oxirgi nuqtalar, tarmoq, bulut, elektron pochta) ma’lumotlarni yig‘ib, kompleks tahlil qiluvchi tizimlar, **Data Loss Prevention (DLP)** – ya’ni, ma’lumotlar sizib chiqishining oldini olish vositalari va **Zero Trust Architecture (Nol Ishonch Arxitekturasi)** prinsiplarini joriy etish (bu yerda hech bir foydalanuvchi yoki qurilmaga sukut bo‘yicha ishonilmaydi va har bir kirish so‘rovi tekshiriladi) kabi ilg‘or yechimlar kiradi. Muntazam ravishda **xavfsizlik auditlari** va **penetratsion testlar (penetration testing)** o‘tkazish ham tizimdagi zaifliklarni aniqlash va ularni bartaraf etish uchun muhimdir. **Huquqiy choralar** nafaqat kiberjinoyatlarga qarshi kurash bo‘yicha milliy va xalqaro qonunchilikka (masalan, GDPR, CCPA, Budapesht konvensiyasi) rioya qilishni, balki huquqni muhofaza qilish organlari bilan samarali hamkorlik qilishni, kiberhujum sodir bo‘lgan taqdirda tegishli yuridik choralarni o‘z vaqtida ko‘rishni, shuningdek, aniq **ichki siyosatlar va tartiblar** (ma’lumotlarga ishlov berish, insidentlarga javob qaytarish, parollar siyosati) ishlab chiqish va ularga qat’iy amal qilishni nazarda tutadi. **Xodimlarni o‘qitish** va kiberxavfsizlik madaniyatini shakllantirish esa inson omili bilan bog‘liq xavflarni kamaytirishning eng muhim yo‘nalishlaridan biridir. Bu nafaqat bir martalik treninglar bilan cheklanib qolmasdan, balki muntazam **phishing simulyatsiyalari**, interaktiv o‘quv modullari, xabardorlikni oshirish kampaniyalari va aniq rollarga moslashtirilgan maxsus treninglar orqali amalga oshirilishi kerak. Xodimlar nafaqat kibergigiyena qoidalariga rioya qilishni (masalan, kuchli va unikal parollardan foydalanish, shubhali havolalarni ochmaslik), balki phishing xabarlarini va boshqa shubhali harakatlarni aniqlashni hamda ular haqida o‘z vaqtida mas’ul bo‘limga (masalan, xavfsizlik operatsiyalari markazi - SOC) xabar berishni o‘rganishlari lozim. Ushbu uch yo‘nalish – texnologiya, huquq va inson omili – birgalikda va uyg‘unlikda qo‘llanilgandagina tahdid aktorlariga qarshi chindan ham samarali va ko‘p qatlamli mudofaa tizimini yaratish mumkin. Bundan tashqari, **MITRE ATT&CK Framework** kabi bilimlarga asoslangan bazalardan foydalanish, tahdid aktorlarining taktikasi, texnikasi va protseduralarini (TTPs) tushunish va ularga qarshi himoya strategiyalarini moslashtirish imkonini beradi.

Kiberxavfsizlik tahdidlari va xavflarini tadqiq etish

Tashkilotingiz duch kelishi mumkin bo‘lgan potentsial risklarni aniqlash va ularning ehtimoliy oqibatlarini baholash uchun risklarni tahlil qilish jadvalini tuzish muhim ahamiyatga ega. Quyida sizning korporatsiyangiz faoliyat yuritayotgan sohalar (moliya, sog‘liqni saqlash, texnologiya) uchun moslashtirilgan namunaviy risk tahlili jadvali keltirilgan:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk Tavsifi | Ehtimollik (Likelihood) | Mumkin Bo‘lgan Zarar (Risk Impact/Cost) | Sektorga Xos Ta’siri |
| Mijoz/bemor ma’lumotlar bazasiga ransomware hujumi | O‘rta | Yuqori (moliyaviy yo‘qotish, obro‘ga putur yetishi, jarimalar, operatsion to‘xtashlar) | Moliya: hisob ma’lumotlari; Sog‘liqni saqlash: bemor qaydlari; Texnologiya: foydalanuvchi ma’lumotlari. |
| Onlayn moliyaviy tranzaksiya platformasiga DDoS hujumi | O‘rta-Yuqori | O‘rta (xizmat ko‘rsatishda uzilishlar, mijozlar noroziligi, qisqa muddatli moliyaviy yo‘qotishlar) | Moliya: bank operatsiyalari, to‘lov tizimlari. |
| Phishing orqali xodimlar hisob ma’lumotlarining komprometatsiyasi va ichki tizimlarga ruxsatsiz kirish | Yuqori | O‘rta-Yuqori (ma’lumotlar sizib chiqishi, ichki tizimlarga zarar, moliyaviy o‘g‘irliklar) | Barcha sektorlar uchun umumiy, ammo texnologiya sohasida intellektual mulk o‘g‘irlanishi xavfi yuqori. |
| Ichki tahdid (malicious insider yoki beparvo xodim) tomonidan maxfiy ilmiy-tadqiqot ma’lumotlarining (R&D) sizdirilishi | Past-O‘rta | Juda Yuqori (raqobatbardoshlikni yo‘qotish, bozor ulushining kamayishi, uzoq muddatli moliyaviy zarar) | Texnologiya: yangi mahsulotlar, patentlar; Moliya: savdo strategiyalari; Sog‘liqni saqlash: tadqiqot natijalari. |
| Ta’minot zanjiri hujumi (supply chain attack) orqali korporatsiya tomonidan ishlatiladigan dasturiy ta’minotning komprometatsiyasi | O‘rta | Yuqori (keng ko‘lamli tizim komprometatsiyasi, ma’lumotlar o‘g‘irlanishi, tizimni tiklash xarajatlari) | Barcha sektorlar uchun xavfli, ayniqsa, ko‘plab uchinchi tomon dasturlariga tayanadigan tashkilotlar uchun. |

Ushbu jadval asosida, tashkilotga tahdid soluvchi asosiy xavflar va ularning mumkin bo‘lgan oqibatlarini chuqurroq tahlil qilish mumkin (P3). Masalan, **ransomware** hujumi nafaqat moliyaviy to‘lov talabi bilan cheklanib qolmay, balki sog‘liqni saqlash sohasida bemorlarning hayotiga xavf soluvchi darajada xizmatlarning to‘xtab qolishiga olib kelishi mumkin. Texnologiya sohasida esa, intellektual mulkning o‘g‘irlanishi kompaniyaning yillar davomida erishgan yutuqlarini yo‘qqa chiqarishi mumkin. Bunday xavflarning oldini olish va ularning ta’sirini kamaytirish uchun texnik himoya vositalarini qo‘llash zarur (P4). Bularga kuchli **shifrlash (encryption)** algoritmlaridan foydalanish (ham saqlanayotgan, ham uzatilayotgan ma’lumotlar uchun), \*\*ko‘p faktorli autentifikatsiya (Multi-Factor Authentication - MFA)\*\*ni barcha muhim tizimlar va foydalanuvchilar uchun majburiy qilish, tarmoq segmentatsiyasi, muntazam ravishda zaifliklarni skanerlash va patch management (yamalarni o‘rnatish) kabi choralar kiradi.

Kiber tahdidlar doimiy ravishda o‘zgarib va rivojlanib borayotgan bir sharoitda, **Threat Intelligence (tahdidlar haqida razvedka ma’lumotlari)** tushunchasining ahamiyati beqiyosdir (M2). Threat intelligence – bu potentsial va mavjud kiber tahdidlar, ularning motivlari, usullari va nishonlari haqida ma’lumot to‘plash, qayta ishlash va tahlil qilish jarayonidir. Ushbu ma’lumotlar tashkilotga proaktiv himoya choralarini ko‘rish, xavflarni oldindan bashorat qilish va hujumlarga samaraliroq javob qaytarish imkonini beradi. **SIEM (Security Information and Event Management)** tizimlari threat intelligence’ni amalda qo‘llashning yorqin misollaridan biridir. SIEM tizimlari tashkilotning butun IT infratuzilmasidan (serverlar, tarmoq qurilmalari, xavfsizlik vositalari, ilovalar) loglar va hodisalar haqidagi ma’lumotlarni bir joyga to‘playdi, ularni real vaqt rejimida tahlil qiladi, shubhali faoliyatlarni va potentsial hujumlarni aniqlaydi hamda xavfsizlik xodimlariga ogohlantirishlar yuboradi. Zamonaviy SIEM tizimlari threat intelligence manbalari bilan integratsiya qilinib, ma’lum bo‘lgan zararli IP-adreslar, domenlar va hujum signaturalari asosida tahdidlarni aniqlash samaradorligini oshiradi.

Ushbu integratsiya korporatsiyaga nafaqat ma'lum bo‘lgan tahdidlarga qarshi kurashish, balki yangi va rivojlanayotgan hujum vektorlarini ham oldindan aniqlash imkonini beradi. **Threat Intelligence platformalari (TIPs)** SIEM tizimlariga tahdid ma’lumotlarini samarali yetkazib berish va ularni boshqarish uchun muhim vosita bo‘lib xizmat qiladi. Ushbu platformalar turli manbalardan (ochiq manbalar, tijorat manbalari, hukumat axborotnomalari, sanoat ISAC'lari – Information Sharing and Analysis Centers) olingan indikatorlarni (Indicators of Compromise - IoCs, masalan, zararli IP-adreslar, fayl heshlari, domen nomlari) to‘playdi, ularni normallashtiradi, boyitadi va SIEM tizimiga uzatadi. SIEM tizimi esa ushbu indikatorlarni real vaqt rejimida ichki tarmoq trafikidagi va tizim loglaridagi hodisalar bilan taqqoslab, potentsial mos kelishlarni aniqlaydi va zudlik bilan xavfsizlik guruhiga ogohlantirish yuboradi. Bu esa, o‘z navbatida, hujumning dastlabki bosqichlaridayoq uni aniqlash va zararni minimallashtirish uchun qimmatli vaqtni tejashga yordam beradi (M2).

Bundan tashqari, SIEM tizimlarining zamonaviy avlodlari nafaqat loglarni yig‘ish va oddiy korrelyatsiya qilish bilan cheklanib qolmaydi. Ular **User and Entity Behavior Analytics (UEBA)** kabi ilg‘or tahliliy imkoniyatlarni o‘z ichiga oladi. UEBA texnologiyasi foydalanuvchilar (xodimlar, pudratchilar) va tizim obyektlarining (serverlar, ish stansiyalari, ilovalar) odatiy faoliyat modellarini (baselines) o‘rganadi va ushbu modellardan chetga chiqadigan anomal xatti-harakatlarni aniqlaydi. Masalan, agar biror xodim odatda ish vaqtidan tashqari tizimga kirmasa yoki ma’lum bir turdagi fayllarga murojaat qilmasa, ammo birdaniga shunday harakatlarni amalga oshira boshlasa, UEBA buni shubhali deb topib, tekshirish uchun signal berishi mumkin. Bu, ayniqsa, yuqoridagi jadvalda keltirilgan "Ichki tahdid (malicious insider yoki beparvo xodim)" kabi xavflarni yoki komprometatsiya qilingan hisob qaydnomalari orqali amalga oshirilayotgan hujumlarni aniqlashda juda samarali (P3, P4).

SIEM va Threat Intelligence birgalikda tashkilotning kiberxavfsizlik holati haqida yaxlit va kontekstual tasavvur hosil qilishga yordam beradi. Bu nafaqat reaktiv himoyani kuchaytiradi, balki proaktiv choralarni rejalashtirish uchun ham asos bo‘ladi. Masalan, muayyan sanoat tarmog‘iga yoki geografik mintaqaga qaratilgan yangi kiberhujum kampaniyasi haqida Threat Intelligence orqali olingan ma’lumotlar asosida, tashkilot o‘zining himoya tizimlarini (masalan, xavfsizlik devorlari qoidalari, intruziv aniqlash tizimi signaturalari) oldindan moslashtirishi, xodimlarni ushbu yangi tahdid haqida ogohlantirishi va potentsial zaifliklarni bartaraf etish bo‘yicha qo‘shimcha choralar ko‘rishi mumkin. Shunday qilib, tashkilot hujumchilar harakatidan bir qadam oldinda bo‘lishga intiladi. Bu jarayonda malakali kiberxavfsizlik tahlilchilarining roli beqiyosdir, chunki ular SIEM tizimidan kelayotgan ogohlantirishlarni va Threat Intelligence ma’lumotlarini to‘g‘ri talqin qila olishlari, yolg‘on pozitivlarni (false positives) ajrata bilishlari va haqiqiy tahdidlarga o‘z vaqtida va adekvat javob qaytara olishlari kerak. Ushbu texnologiyalar va inson ekspertizasining uyg‘unligi korporatsiyaning kiberxavfsizlik tahdidlari va xavflariga qarshi samarali kurashish qobiliyatini sezilarli darajada oshiradi.

Axborot xavfsizligi ta’minoti konsepsiyalarining AKT infratuzilmasiga qo‘llanilishining samaradorligini o‘rganish

**Information Assurance (Axborot Xavfsizligini Ta’minlash - IA)** konsepsiyasi tashkilotning axborot aktivlarini himoya qilish, ularning maxfiyligi, yaxlitligi va foydalanishga yaroqliligini ta’minlashga qaratilgan keng qamrovli yondashuvdir (P5). IA shunchaki texnologik yechimlarni joriy etishdan iborat bo‘lmay, balki risklarni boshqarish (risk management), siyosatlar va protseduralarni ishlab chiqish, xodimlarni o‘qitish va doimiy monitoringni o‘z ichiga oladi. **Risk management** IA ning asosiy tarkibiy qismlaridan biri bo‘lib, u potentsial xavflarni aniqlash, ularning ehtimolligi va ta’sirini baholash hamda ularni kamaytirish yoki bartaraf etish bo‘yicha choralar ko‘rishni nazarda tutadi. Yuqorida keltirilgan risk tahlili jadvali aynan shu jarayonning bir qismidir. **Encryption (shifrlash)** esa ma’lumotlarni ruxsatsiz shaxslar tomonidan o‘qilishidan himoya qilishning muhim texnik vositasidir. Masalan, mijozlarning moliyaviy ma’lumotlari yoki bemorlarning sog‘lig‘iga oid qaydlar kabi nozik axborotlar ham ma’lumotlar bazasida saqlanayotganda (data at rest), ham tarmoq orqali uzatilayotganda (data in transit) kuchli shifrlash algoritmlari yordamida himoyalanishi kerak. Amaliy misol sifatida, shifrlangan noutbuk o‘g‘irlangan taqdirda ham, undagi ma’lumotlarga kirish imkoniyati deyarli yo‘qqa chiqadi, bu esa ma’lumotlar sizib chiqishi xavfini keskin kamaytiradi.

Tashkilotning IT infratuzilmasining kiber hujumlarga chidamliligini oshirish uchun xalqaro standartlar va framework’lardan foydalanish muhim ahamiyatga ega (M3). **ISO 27001** standarti axborot xavfsizligi boshqaruvi tizimini (Information Security Management System - ISMS) yaratish, joriy etish, qo‘llab-quvvatlash va doimiy takomillashtirish uchun talablarni belgilaydi. Ushbu standart risklarni baholash va boshqarishga asoslangan bo‘lib, tashkilotga o‘zining axborot xavfsizligi bo‘yicha majburiyatlarini tizimli ravishda bajarishga yordam beradi. ISO 27001 sertifikatini olish tashkilotning axborot xavfsizligiga jiddiy yondashishini va mijozlar hamda hamkorlar oldidagi ishonchliligini oshiradi. **NIST Cybersecurity Framework** esa AQSh Milliy Standartlar va Texnologiyalar Instituti tomonidan ishlab chiqilgan bo‘lib, u tashkilotlarga kiberxavfsizlik risklarini boshqarish bo‘yicha ko‘ngilli yo‘riqnoma taklif etadi. Ushbu framework beshta asosiy funksiyadan iborat: Identify (Aniqlash), Protect (Himoya qilish), Detect (Aniqlash), Respond (Javob qaytarish) va Recover (Tiklash). NIST framework’ini qo‘llash orqali tashkilot o‘zining mavjud kiberxavfsizlik holatini baholashi, maqsadli holatni belgilashi va ushbu maqsadga erishish uchun yo‘l xaritasini ishlab chiqishi mumkin. Sizning korporatsiyangiz kabi turli sohalarda faoliyat yurituvchi yirik tashkilot uchun ushbu framework’lardan birini yoki ularning kombinatsiyasini joriy etish IT infratuzilmaning umumiy chidamliligini sezilarli darajada oshiradi.

Turli tashkilotlar tomonidan kiber hujumlarga javob berish uchun joriy etilgan strategiyalarni tahlil qilish orqali qimmatli saboqlar olish mumkin (D2). Masalan, 2017-yilda **Equifax** kompaniyasi duch kelgan yirik ma’lumotlar sizib chiqishi hodisasi shuni ko‘rsatdiki, zaifliklarni o‘z vaqtida bartaraf etmaslik va sekin javob qaytarish juda katta moliyaviy va obro‘ga oid zararlarga olib kelishi mumkin. Aksincha, ba’zi tashkilotlar proaktiv yondashuvni qo‘llab, insidentlarga tez va samarali javob qaytarish rejasini (Incident Response Plan) oldindan ishlab chiqadilar. Bunday rejalar odatda quyidagi bosqichlarni o‘z ichiga oladi: tayyorgarlik, aniqlash va tahlil qilish, cheklash, bartaraf etish, tiklash va hodisadan keyingi tahlil (post-incident activity). Muvaffaqiyatli javob strategiyalariga ega bo‘lgan tashkilotlar, odatda, maxsus insidentlarga javob qaytarish guruhiga (Incident Response Team - IRT) ega bo‘ladilar, muntazam ravishda mashg‘ulotlar o‘tkazadilar va kommunikatsiya rejalarini aniq belgilab qo‘yadilar. Masalan, **Maersk** kompaniyasi 2017-yilda NotPetya ransomware hujumidan katta zarar ko‘rgan bo‘lsa-da, ularning tiklanish jarayoni va undan keyingi xavfsizlik choralarini kuchaytirishi boshqa tashkilotlar uchun muhim o‘rnak bo‘ldi. Ushbu tajribalarni o‘rganish sizning korporatsiyangizga yanada mustahkam va samarali javob strategiyalarini ishlab chiqishga yordam beradi.

Kiberxavfsizlik tahdidlariga javob berish usullarini tadqiq etish

Har bir sektor o‘ziga xos xavfsizlik standartlari va qonuniy talablarga ega bo‘lib, ularga rioya qilmaslik jiddiy oqibatlarga olib kelishi mumkin (P6). **Moliya sektori** uchun PCI DSS (Payment Card Industry Data Security Standard) kabi standartlar to‘lov kartalari ma’lumotlarini himoya qilish bo‘yicha qat’iy talablarni qo‘yadi. Shuningdek, ko‘plab mamlakatlarda moliyaviy institutlar uchun maxsus kiberxavfsizlik qoidalari va nazorat organlari mavjud (masalan, AQShda SEC, Yevropa Ittifoqida EBA). Ushbu qoidalarga rioya qilmaslik katta miqdordagi jarimalar, litsenziyadan mahrum bo‘lish va jinoiy javobgarlikka tortilishga olib kelishi mumkin. **Sog‘liqni saqlash sektori** uchun esa HIPAA (Health Insurance Portability and Accountability Act) AQShda bemorlarning shaxsiy sog‘liq ma’lumotlari (Protected Health Information - PHI) maxfiyligini ta’minlash bo‘yicha asosiy qonun hisoblanadi. Yevropa Ittifoqida esa GDPR (General Data Protection Regulation) barcha shaxsiy ma’lumotlar, shu jumladan sog‘liqqa oid ma’lumotlar uchun ham qat’iy himoya talablarini belgilaydi. Ushbu qonunlarning buzilishi nafaqat moliyaviy jarimalarga, balki jiddiy reputatsion zararga ham olib keladi. **Texnologiya sektori** esa intellektual mulkni himoya qilish, dasturiy ta’minot xavfsizligi va foydalanuvchi ma’lumotlarining maxfiyligi bilan bog‘liq turli xil standartlar va qoidalarga duch keladi. Sizning korporatsiyangiz ushbu uchala sektorda ham faoliyat yuritishi sababli, har bir sektor uchun tegishli bo‘lgan barcha xavfsizlik standartlari va qonuniy talablarga qat’iy rioya qilishi shart.

Kiberxavfsizlik insidentlari sodir bo‘lgan taqdirda, ularga samarali javob qaytarish uchun turli usullar va mexanizmlar mavjud (P7). **Data recovery (ma’lumotlarni tiklash)** ransomware hujumi yoki tizim ishdan chiqishi kabi holatlarda yo‘qotilgan yoki shikastlangan ma’lumotlarni qayta tiklash jarayonidir. Buning uchun muntazam ravishda zaxira nusxalarini (backups) yaratish va ularni xavfsiz joyda saqlash, shuningdek, zaxira nusxalarini tiklash protseduralarini sinovdan o‘tkazib turish muhim. **Incident management (insidentlarni boshqarish)** esa kiberhujum yoki xavfsizlik buzilishi sodir bo‘lganda amalga oshiriladigan kompleks chora-tadbirlar majmuasidir. U insidentni aniqlash, uning ko‘lamini baholash, tarqalishini cheklash, bartaraf etish, tizimlarni tiklash va kelajakda shunga o‘xshash hodisalarning oldini olish uchun saboqlar chiqarish kabi bosqichlarni o‘z ichiga oladi. Samarali insidentlarni boshqarish rejasi (Incident Response Plan - IRP) oldindan ishlab chiqilgan bo‘lishi, unda mas’ul shaxslar, kommunikatsiya kanallari va har bir bosqichda bajariladigan aniq harakatlar belgilangan bo‘lishi kerak. Shuningdek, forensik tahlil (digital forensics) o‘tkazish orqali hujumning manbasini, usulini va ko‘lamini aniqlash ham insidentga javob berishning muhim qismidir.

Kiberjinoyatlarning oldini olish va ularga qarshi kurashishda milliy va xalqaro qonunchilikning, xususan, **Jinoyat kodeksi** va boshqa tegishli qonunlarning roli katta (M4). Ko‘pgina davlatlar o‘z jinoyat kodekslariga kiberjinoyatlar uchun alohida moddalar kiritgan bo‘lib, ular kompyuter tizimlariga ruxsatsiz kirish, ma’lumotlarni o‘g‘irlash, zararli dasturlarni tarqatish, firibgarlik va boshqa noqonuniy harakatlar uchun jazo choralarini belgilaydi. Masalan, O‘zbekiston Respublikasining Jinoyat kodeksida ham axborot texnologiyalari sohasidagi jinoyatlar uchun tegishli moddalar mavjud. Xalqaro miqyosda esa, Budapesht konvensiyasi (Council of Europe Convention on Cybercrime) kiberjinoyatlarga qarshi kurashish bo‘yicha asosiy xalqaro shartnoma hisoblanadi va u a’zo davlatlar o‘rtasida hamkorlikni rivojlantirishga yordam beradi. Ushbu qonunlar va xalqaro kelishuvlar kiberjinoyatchilarni javobgarlikka tortish uchun huquqiy asos yaratadi, ammo ularning samaradorligi huquqni muhofaza qilish organlarining texnik salohiyati, xalqaro hamkorlik darajasi va qonunlarning doimiy ravishda yangilanib turishiga bog‘liq. Tashkilotlar esa o‘z navbatida, kiberjinoyat sodir bo‘lgan taqdirda huquqni muhofaza qilish organlari bilan faol hamkorlik qilishi va qonuniy choralarni qo‘llashga yordam berishi lozim.

Xulosa

Ushbu tahliliy hisobot mazkur xalqaro korporatsiya duch kelayotgan kiberxavfsizlik muammolarining keng qamrovli tahlilini taqdim etishga qaratildi. Kiberjinoyatlar turlari, potentsial nishonlar, tahdid aktorlari, risklarni baholash, axborot xavfsizligini ta’minlash konsepsiyalari va insidentlarga javob berish usullari kabi muhim jihatlar ko‘rib chiqildi. Korporatsiyaning moliya, sog‘liqni saqlash va texnologiya kabi o‘ta nozik ma’lumotlar bilan ishlaydigan sohalarda faoliyat yuritishi, uning kiberxavfsizlikka nisbatan kompleks va proaktiv yondashuvni qo‘llashini hayotiy zaruratga aylantiradi. Bu nafaqat aktivlarni himoya qilish, balki korporativ obro‘ni saqlash va uzoq muddatli biznes barqarorligini ta’minlashning muhim garovidir.

Taqdim etilgan tahlillardan kelib chiqqan holda, korporatsiyaning kiberxavfsizlik holatini yanada mustahkamlash uchun quyidagi asosiy tavsiyalar ilgari suriladi:

Birinchidan, xavfsizlik choralarini doimiy ravishda qayta ko‘rib chiqish va takomillashtirish lozim. Bu muntazam zaifliklarni skanerlash, penetratsion testlar o‘tkazish va xavfsizlik konfiguratsiyalarini audit qilishni o‘z ichiga oladi.

Ikkinchidan, ISO 27001 yoki NIST Cybersecurity Framework kabi xalqaro standartlarni joriy etishni ko‘rib chiqish tavsiya etiladi. Bu tizimli yondashuvni ta’minlaydi va me’yoriy-huquqiy talablarga muvofiqlikni oshiradi.

Uchinchidan, xodimlarning kiberxavfsizlik bo‘yicha xabardorligini oshirish uchun uzluksiz trening dasturlarini amalga oshirish muhim. Bu muntazam phishing simulyatsiyalari va rolga asoslangan o‘quv modullarini qamrab olishi kerak.

To‘rtinchidan, har tomonlama Insidentlarga Javob Qaytarish Rejasini (IRP) ishlab chiqib, uni muntazam sinovdan o‘tkazib turish shart. Ushbu reja texnik, yuridik va kommunikatsion jihatlarni o‘z ichiga olishi lozim.

Beshinchidan, Threat Intelligence manbalaridan faol foydalanish hamda SIEM va SOAR kabi zamonaviy texnologiyalarni samarali qo‘llash orqali kiber tahdidlarni o‘z vaqtida aniqlash va ularga qarshi kurashish samaradorligini oshirish mumkin.

Ushbu tavsiyalarning izchil amalga oshirilishi korporatsiyaning kiberxavfsizlik himoyasini sezilarli darajada kuchaytirishga va raqamli muhitda barqaror rivojlanishini ta’minlashga xizmat qiladi. Kiberxavfsizlik – bu doimiy e’tibor va takomillashtirishni talab qiladigan uzluksiz jarayondir.

ADABIYOTLAR RO'YXATI

1. Choriyev, A. (2023) *Kiberxavfsizlik Asoslari va Zamonaviy Tahdidlar*. Toshkent: Fan va Texnologiya nashriyoti.
2. International Organization for Standardization (ISO) (2022) *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Geneva: ISO.
3. Kshetri, N. (2013) 'Cybercrime and Cybersecurity in the Global South: A Comparative Analysis', *Journal of Global Information Technology Management*, 16(4), pp. 1-5.
4. National Institute of Standards and Technology (NIST) (2018) *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1. Gaithersburg, MD: NIST.
5. Schneier, B. (2015) *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company.
6. Verizon (2023) *Data Breach Investigations Report (DBIR)*. Basking Ridge, NJ: Verizon Enterprise Solutions.
7. World Economic Forum (2024) *The Global Risks Report 2024*. Geneva: World Economic Forum.
8. O‘zbekiston Respublikasining Jinoyat Kodeksi (2024 yil tahririda). Toshkent: Adolat.
9. SANS Institute (2023) CIS Critical Security Controls. Version 8. Bethesda, MD: SANS Institute.
10. Cybersecurity & Infrastructure Security Agency (CISA) (2024) Known Exploited Vulnerabilities Catalog. Washington, D.C.: CISA.
11. European Union Agency for Cybersecurity (ENISA) (2023) ENISA Threat Landscape 2023. Heraklion: ENISA.
12. Kim, D. and Solomon, M.G. (2021) Fundamentals of Information Systems Security. 4th edn. Burlington, MA: Jones & Bartlett Learning.
13. McMillan, T. (2019) Hacking Exposed 7: Network Security Secrets & Solutions. 7th edn. New York: McGraw-Hill Education.
14. Ponemon Institute (2023) Cost of a Data Breach Report 2023. Traverse City, MI: Ponemon Institute LLC.
15. Council of Europe (2001) Convention on Cybercrime (Budapest Convention). CETS No.185. Strasbourg: Council of Europe.
16. The MITRE Corporation (2024) MITRE ATT&CK® Framework. Bedford, MA: The MITRE Corporation. [Online]. Available at: https://attack.mitre.org (Accessed: 31 May 2025).