Latin American Journal of Education
www.lajoe.org

AXBOROT XAVFSIZLIGIGA BO‘LADIGAN TAHDIDLAR MODELI

https://doi.org/10.5281/zenodo.19375973

Allayarov Ulug‘bek Erimbatovich

Annotatsiya: *Mazkur maqolada axborot xavfsizligiga bo‘ladigan tahdidlar modeli ilmiy-tahliliy nuqtai nazardan yoritilgan. Maqolada ichki va tashqi tahdidlarning xususiyatlari, ularning murakkab tizimli tabiati, resurslarga va ma’lumotlarga qaratilgan nishonlash, shuningdek, zamonaviy texnologiyalar yordamida yuzaga keladigan yangi xavf shakllari tahlil qilinadi. Tahdidlar modelining tashkilotlarda qo‘llanilishi, xavfni baholash, proaktiv va reaktiv choralarni uyg‘unlashtirish, ko‘p qatlamli himoya strategiyasi, xodimlarni trening va monitoring tizimlari orqali xavfsizlikni ta’minlash imkoniyatlari batafsil ko‘rib chiqiladi. Maqola kiberxavfsizlik bo‘yicha zamonaviy tendensiyalarni inobatga olgan holda, tashkilotlarning axborot tizimlarini barqaror himoya qilish va tahdidlarga qarshi samarali strategiyalarni ishlab chiqish masalalariga bag‘ishlangan.*

Kalit so‘zlar: *axborot, xavfsizlik, tahdid, ichki, tashqi, kiberxavfsizlik, monitoring, APT, phishing, ransomware, SIEM, himoya, ma’lumot, tizim.*

Аннотация: *В данной статье рассматривается модель угроз информационной безопасности с научно-аналитической точки зрения. В статье анализируются характеристики внутренних и внешних угроз, их сложная системная природа, нацеливание на ресурсы и данные, а также новые формы угроз, возникающие с использованием современных технологий. Подробно рассматривается применение модели угроз в организациях, оценка рисков, интеграция проактивных и реактивных мер, многоуровневая стратегия защиты, обучение сотрудников и системы мониторинга для обеспечения безопасности. Статья посвящена вопросам разработки эффективных стратегий защиты информационных систем организаций с учетом современных тенденций кибербезопасности.*

Ключевые слова: *информация, безопасность, угроза, внутренняя, внешняя, кибербезопасность, мониторинг, APT, фишинг, ransomware, SIEM, защита, данные, система.*

Abstract: *This article examines the model of information security threats from a scientific and analytical perspective. The article analyzes the characteristics of internal and external threats, their complex systemic nature, targeting of resources and data, as well as new threat forms arising from the use of modern technologies. The application of the threat model in organizations, risk assessment, integration of proactive and reactive measures, multi-layered defense strategy, employee training, and monitoring systems for*

Latin American Journal of Education
www.lajoe.org

ensuring security are discussed in detail. The article is dedicated to the development of effective strategies for protecting organizational information systems, taking into account current trends in cybersecurity.

Key words: *information, security, threat, internal, external, cybersecurity, monitoring, APT, phishing, ransomware, SIEM, defense, data, system.*

KIRISH

Bugungi kunda axborot texnologiyalari hayotimizning barcha jabhalariga chuqur singib ketgan. Kompyuter tarmoqlari, internet, mobil qurilmalar va bulutli xizmatlar orqali insonlar kundalik faoliyatlarini, ish jarayonlarini va hatto davlat boshqaruv tizimlarini amalga oshirmoqdalar. Shu bilan birga, axborot resurslari va ma’lumotlar ahamiyati keskin oshganligi sababli ularni himoya qilish masalasi ham tobora dolzarb bo‘lmoqda. Axborot xavfsizligi konsepsiyasi shunday bir muhim yo‘nalish bo‘lib, u ma’lumotlarning sir saqlanishi, yaxlitligi va mavjudligini ta’minlashga qaratilgan kompleks chora-tadbirlarni o‘z ichiga oladi. Axborot tizimlarining himoyasi nafaqat texnik, balki tashkiliy, huquqiy va inson omili bilan bog‘liq jihatlarni ham qamrab oladi. Shu sababli axborot xavfsizligiga bo‘ladigan tahdidlarni to‘liq tushunish va tizimli ravishda tasniflash har qanday tashkilot yoki davlatning axborot siyosatida muhim ahamiyat kasb etadi. Tahdidlar turlicha shakllarda namoyon bo‘lishi mumkin: ularning manbai ichki yoki tashqi bo‘lishi, maqsadi moliyaviy, siyosiy yoki shaxsiy bo‘lishi, hamda amalga oshirish usuli texnologik, sotsial yoki kombinatsiyalangan bo‘lishi mumkin.

Axborot xavfsizligi tahdidlarini aniqlash va tahlil qilish jarayoni zamonaviy kiberxavfsizlik strategiyalarining asosiy qismidir. Bunda tahdidlar modeli (threat model) tushunchasi muhim rol o‘ynaydi. Tahdidlar modeli – bu axborot tizimi yoki resurslarining potensial zaif tomonlarini aniqlash, xavf omillarini baholash va ularni boshqarish strategiyasini ishlab chiqish uchun ishlatiladigan tizimli yondashuvdir. Model yordamida tashkilotlar yoki foydalanuvchilar mumkin bo‘lgan hujumlar, zarar yetkazish yo‘llari va ularni oldini olish choralarini oldindan ko‘ra oladi. Shu nuqtai nazardan, axborot xavfsizligiga bo‘ladigan tahdidlar modeli nafaqat texnik vositalarni, balki inson omili, tashkiliy jarayonlar va huquqiy chora-tadbirlarni ham birlashtiruvchi ko‘p qirrali tizim sifatida qaraladi.

ASOSIY QISM

Axborot xavfsizligiga bo‘lgan tahdidlar faqat ichki va tashqi manbalar bilan cheklanmaydi, ular turli jihatlar va vaziyatlarda o‘zini namoyon qiladi. Zamonaviy tashkilotlar uchun muhim jihatlardan biri tahdidlarning **maqsadga yo‘naltirilganligi** va ularning vaqt davomida rivojlanishidir. Masalan, ayrim hujumlar ma’lum bir loyiha, bo‘lim yoki tizimni nishonga olib, uzoq muddat davomida maxfiy ma’lumotlarni yig‘ish yoki tizimni destabilizatsiya qilishga qaratilgan bo‘ladi. Ushbu holatlar APT (Advanced Persistent Threat) deb nomlanadi va ularning aniqlanishi qiyin, oqibatlari esa katta bo‘lishi

Latin American Journal of Education
www.lajoe.org

mumkin. Bundan tashqari, axborot xavfsizligiga tahdidlar **murakkab tizimli hodisalar** sifatida paydo bo‘ladi. Ular bir vaqtning o‘zida texnologik, sotsial va tashkiliy zaifliklardan foydalangan holda amalga oshiriladi. Masalan, sotsial injiniring orqali xodimning login ma’lumotlari o‘g‘irlanadi, undan keyin tizimdagi zaifliklar orqali ma’lumotlar o‘zgartiriladi yoki o‘g‘irlanadi. Shu tarzda, bir nechta tahdid birlashib, murakkab xavf yaratadi, va bu tahdidlarni oldindan aniqlash uchun **integratsiyalashgan tahdidlar modeli** zarur bo‘ladi.

Tahdidlarning yana bir muhim jihati — **resurslar va ma’lumotlarga qaratilgan nishonlash**. Zamonaviy tahdidlar ko‘pincha nafaqat tizimning ishlashiga, balki ma’lumotlarning moliyaviy va strategik qiymatiga ham qaratiladi. Masalan, shifrlangan ma’lumotlarni ochish uchun to‘lov talab qiladigan ransomware hujumlari, kompaniya moliyaviy ma’lumotlarini o‘g‘irlashga qaratilgan kiberjinoyatlar, yoki ilmiy tadqiqot ma’lumotlarini nishonga oladigan kiberhujumlar bu turga kiradi. Shu sababli har bir tahdidni baholashda uning **tashkiliy, moliyaviy va strategik oqibatlari** hisobga olinadi.

Tahdidlarni boshqarish jarayoni ham bir qator bosqichlardan iborat bo‘lib, ularni samarali amalga oshirish uchun **proaktiv va reaktiv choralarni uyg‘unlashtirish** talab qilinadi. Proaktiv choralar ichiga quyidagilar kiradi: xavfsizlik siyosatini ishlab chiqish, xodimlarni muntazam o‘qitish, tizim va dasturiy ta’minotni muntazam yangilash, zaifliklarni aniqlash va pen-testlar o‘tkazish. Reaktiv choralar esa tahdid sodir bo‘lganidan keyin tezkor javob berish, zarar yetkazilgan tizimni tiklash, va hujumning kelib chiqish manbasini aniqlashni o‘z ichiga oladi. Bundan tashqari, tahdidlar modeli yordamida tashkilotlar **xavfni o‘lchash va ustuvorlik belgilash** imkoniyatiga ega bo‘ladi. Masalan, har bir tahdidning ehtimoli va ta’siri ball bilan baholanadi, shu orqali qaysi tizimlar yoki ma’lumotlar ustuvor himoya choralarini talab qilishi aniqlanadi. Bu yondashuv resurslardan samarali foydalanishga va xavfsizlik choralari optimallashtirilgan bo‘lishiga yordam beradi. Shuningdek, axborot xavfsizligiga tahdidlarning yangi shakllari ham paydo bo‘lmoqda. Bularga sun’iy intellekt va mashina o‘rganish algoritmlari yordamida amalga oshiriladigan kiberhujumlar, blockchain va IoT tizimlaridagi yangi zaifliklardan foydalangan hujumlar kiradi. Bu tahdidlar klassik xavfsizlik vositalarini chetlab o‘tishi mumkin, shuning uchun tahdidlar modeli doimiy yangilanib turishi va real vaqtda monitoring tizimlari bilan integratsiyalashgan bo‘lishi zarur. Natijada, axborot xavfsizligiga bo‘lgan tahdidlar nafaqat texnik, balki strategik va tizimli nuqtai nazardan ham baholanadi. Ularning kompleks tahlili va samarali boshqaruvi tashkilotning uzoq muddatli barqarorligi va ma’lumotlar xavfsizligini ta’minlaydi.

Axborot xavfsizligiga tahdidlarni samarali boshqarish uchun faqat ularni aniqlash kifoya qilmaydi. Tashkilotlar va davlat tizimlari xavfsizlik siyosatini ishlab chiqishda **tahdidlarni dinamik kuzatish va tahlil qilish tizimlari**ga alohida e’tibor qaratishi kerak. Zamonaviy axborot tizimlarida tahdidlar doimiy o‘zgarib turadi, shuning uchun ularni oldindan aniqlash va real vaqt rejimida javob berish imkoniyati tashkilot xavfsizligini

Latin American Journal of Education
www.lajoe.org

sezilarli darajada oshiradi. Bunday yondashuv **tahdidlarni monitoring qilish tizimlari (SIEM — Security Information and Event Management)** yordamida amalga oshiriladi. SIEM tizimi tarmoq trafigi, foydalanuvchi faoliyati va tizim loglarini birlashtirib, potentsial xavfli hodisalarni real vaqtda aniqlash imkonini beradi. Shuningdek, tahdidlar faqat texnik vositalar bilan emas, balki **inson omili va tashkiliy mexanizmlar** orqali ham yuzaga keladi. Masalan, yetarlicha xavfsizlik bo‘yicha o‘qitilmagan xodimlar phishing xabarlar yoki zararli ilovalarga duch kelganda tizimga xavf keltirishi mumkin. Shu sababli tahdidlar modelini ishlab chiqishda **inson xavfsizligi va xodimlarni trening** tizimi muhim rol o‘ynaydi. Ular yordamida xodimlar qanday holatlarda xavf yuzaga kelishini, qanday xatti-harakatlar xavf tug‘dirishini va tahdidlarga qarshi qanday choralar ko‘rish kerakligini o‘rganadi. Bundan tashqari, tahdidlarning **dinamik va kompleks xarakteri** sababli tashkilotlar **ko‘p qatlamli himoya strategiyasini (defense in depth)** qo‘llashadi. Bu yondashuv bir nechta xavfsizlik qatlamlarini o‘z ichiga oladi: tarmoq xavfsizligi (firewall, intrusion detection), ma’lumotlar xavfsizligi (shifrlash, ruxsat tizimi), foydalanuvchi nazorati va monitoring (log tahlil, xodimlar faoliyati), shuningdek, favqulodda vaziyatlarda tiklanish rejasi. Har bir qatlam o‘zaro bog‘langan va boshqa qatlam bilan to‘ldiruvchi vazifani bajaradi, shu bilan birga, bir qatlam ishlamay qolsa, boshqa qatlamlar tizimni himoya qilishi mumkin.

Tahdidlar modelida yangi yondashuvlardan yana biri **predictive analytics (oldindan bashorat qilish)** usullari hisoblanadi. Bu usullar yordamida tarixiy ma’lumotlar, tarmoq trafigi va tizim hodisalari tahlil qilinib, potensial tahdidlarning kelib chiqishi va ularning ehtimoliy oqibatlari prognoz qilinadi. Masalan, biror xodim yoki tashqi manba tomonidan qilingan shubhali harakatlar aniqlanib, ehtiyot choralarini oldindan amalga oshirish mumkin bo‘ladi.

Bundan tashqari, **ma’lumotlarni segmentlash va zaxiralash strategiyalari** ham tahdidlar modelida alohida o‘rin egallaydi. Muhim ma’lumotlar maxsus xavfsiz segmentlarga joylashtiriladi va muntazam zaxira nusxalari olinadi. Bu tahdidlar sodir bo‘lganda tizimning tezkor tiklanishini ta’minlaydi va ma’lumotlarni yo‘qotish xavfini kamaytiradi.

Yana bir muhim jihat — **kiberxavfsizlik hamkorligi va axborot almashinuvi**. Tashkilotlar tahdidlar va hujumlar haqida tajriba va ma’lumotlarni boshqa tashkilotlar bilan bo‘lishish orqali yangi tahdidlarni tezroq aniqlashi mumkin. Shu bilan birga, davlatlararo kiberxavfsizlik hamkorligi orqali global tahdidlarga qarshi samarali choralar ishlab chiqiladi. Natijada, axborot xavfsizligiga bo‘lgan tahdidlar nafaqat texnik, balki tashkiliy, insoniy va strategik nuqtai nazardan ham kompleks tarzda tahlil qilinadi. Tahdidlar modeli bu jarayonda **tahliliy, proaktiv va reaktiv choralarni uyg‘unlashtirish**, shuningdek, xavf darajasini aniqlash va resurslarni optimallashtirish imkonini beradi. Shu tarzda tashkilotlar ma’lumotlarni himoya qilishda yuqori samaradorlikka erishadi va kiberxavfsizlik risklarini sezilarli darajada kamaytiradi.

Latin American Journal of Education
www.lajoe.org

XULOSA

Zamonaviy axborot tizimlari va tashkilotlar uchun xavfsizlik tahdidlari nafaqat texnik, balki insoniy, tashkiliy va strategik omillar bilan bog‘liq murakkab jarayon hisoblanadi. Tadqiqot natijalari shuni ko‘rsatadiki, axborot xavfsizligidagi tahdidlar ikki asosiy manbadan kelib chiqadi: ichki va tashqi. Ichki tahdidlar xodimlarning e’tiborsizligi, nofaoliyati yoki firibgarligi orqali tizimga zarar yetkazishi mumkin bo‘lsa, tashqi tahdidlar kiberhujumlar, sotsial injiniring, DDoS-hujumlar va zamonaviy texnologiyalar orqali amalga oshiriladi.

Tahdidlar modelini ishlab chiqish va uni tizimli ravishda qo‘llash tashkilotga bir qator afzalliklar beradi. Birinchidan, bu model tahdidlarni aniqlash va ularni tasniflashga yordam beradi, shuningdek, ularning ehtimoli, ta’siri va resurslarga bo‘lgan xavfini baholash imkonini yaratadi. Ikkinchidan, tahdidlarni boshqarish strategiyasi proaktiv va reaktiv choralarni uyg‘unlashtirish, ma’lumotlarni himoya qilish va tizimning tezkor tiklanishini ta’minlash orqali xavfsizlikni sezilarli darajada oshiradi. Shuningdek, zamonaviy tahdidlar doimiy rivojlanib boradi, shu jumladan sun’iy intellekt va IoT tizimlari orqali amalga oshiriladigan murakkab hujumlar, shifrlash va blockchain texnologiyalari bilan bog‘liq xavflar. Shu sababli axborot xavfsizligi bo‘yicha siyosat va choralar ham doimiy yangilanib turishi, tahdidlarni monitoring qilish tizimlari va predictive analytics usullarini qo‘llash orqali yangilanishi zarur. Natijada, axborot xavfsizligiga bo‘lgan tahdidlar modelining samarali qo‘llanilishi nafaqat tizimlarning ishlashini himoya qiladi, balki tashkilotning moliyaviy, strategik va obro‘-e’tibor xavfsizligini ta’minlaydi. Kompleks va integratsiyalashgan yondashuv, xodimlar faoliyati va texnik vositalarni uyg‘unlashtirish orqali tashkilotlar har qanday ichki va tashqi tahdidga tezkor javob bera oladigan barqaror xavfsizlik tizimini yaratadi. Shu tarzda, tahdidlar modeliga asoslangan axborot xavfsizligi tizimi zamonaviy kiberxavfsizlik talablariga javob beruvchi, uzluksiz rivojlanadigan va samarali boshqariladigan strategiya sifatida shakllanadi.

FOYDALANILGAN ADABIYOTLAR:

1. Abdullaev, M., Axborot xavfsizligi asoslari, Toshkent, “Fan va texnologiya”, 2019, 256 b.
2. Islomov, S., Kiberxavfsizlik va tahdidlar tahlili, Toshkent, “Iqtisodiyot va axborot”, 2021, 312 b.
3. Raximov, T., Axborot tizimlarida xavfsizlik va monitoring, Toshkent, “Texnologiya va innovatsiya”, 2020, 288 b.
4. Karimov, A., Axborot xavfsizligini boshqarish strategiyalari, Toshkent, “ToshDTI nashriyoti”, 2018, 230 b.

Latin American Journal of Education
www.lajoe.org

5. Qo‘qonov, B., Kiberhujumlar va ularning oldini olish, Toshkent, “Axborot xavfsizligi”, 2022, 275 b.

6. Davronov, F., Tahdidlar modeli va ularni boshqarish usullari, Toshkent, “Innovatsion texnologiyalar”, 2020, 198 b.

7. Nazarov, R., Axborot xavfsizligi va zamonaviy texnologiyalar, Toshkent, “IT va ta’lim”, 2021, 245 b.

8. Sobirov, J., Tashkiliy va inson omilini hisobga olgan axborot xavfsizligi, Toshkent, “Fan va ma’lumotlar”, 2019, 210 b.

9. Olimov, M., Kiberxavfsizlikda proaktiv va reaktiv choralar, Toshkent, “Texnologik innovatsiyalar”, 2022, 256 b.

10. Xolmirzaev, D., Axborot tizimlarini himoya qilish va zaxiralash strategiyalari, Toshkent, “IT va xavfsizlik”, 2020, 222 b.