IDS VA IPS TIZIMLARI BILAN ISHLASH

WORKING WITH IDS AND IPS SYSTEMS

РАБОТА С СИСТЕМАМИ IDS И IPS

Babakulov Bekzod Mamatkulovich

Jizzakh Branch of the National University of

Uzbekistan Jizzakh, Uzbekistan b_babakulov@jbnuu.uz

Saidnazarov Shohruh Dilshod o'g'li

Mirzo Ulug'bek nomidagi O'zbekiston Milliy universiteti

Jizzax filiali Axborot xavfsizligi (sohalar bo'yicha) 3-kurs talabasi

sidnazarovshohruh45@gmail.com

tel: +998996684163

Annotatsiya:

Ushbu maqola IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlarining asosiy xususiyatlari, ularning farqlari, afzalliklari va cheklovlarini muhokama qiladi. IDS hujumlarni aniqlashga ixtisoslashgan bo'lsa, IPS ushbu tahdidlarni bloklash va oldini olish imkoniyatiga ega. Maqolada IDS/IPS texnologiyalarining rivojlanishi, mashinani o'rganish va sun'iy intellektdan foydalanish, shuningdek, bulutga asoslangan yechimlarning ahamiyati haqida batafsil ma'lumot beriladi. IDS va IPS vositalarining IT xavfsizligini ta'minlashdagi roli, me'yoriy talablar bilan muvofiqlik, hamda eng yaxshi amaliyotlar haqida fikr yuritiladi.

Kalit so'zlar: IDS (Intrusion Detection System), IPS (Intrusion Prevention System), kibertahdidlar, tarmoq xavfsizligi, mashinani o'rganish, sun'iy intellekt,

tahdidlarni aniqlash, real vaqt rejimida himoya, bulutga asoslangan yechimlar, normativ muvofiqlik.

Annotation:

This article discusses the main features, differences, advantages, and limitations of IDS (Intrusion Detection System) and IPS (Intrusion Prevention System). While IDS specializes in detecting attacks, IPS actively blocks and prevents these threats. The article provides detailed insights into the advancements in IDS/IPS technologies, including the use of machine learning and artificial intelligence, as well as the importance of cloud-based solutions. It also highlights the role of IDS and IPS tools in ensuring IT security, regulatory compliance, and best practices.

Keywords: IDS (Intrusion Detection System), IPS (Intrusion Prevention System), cyber threats, network security, machine learning, artificial intelligence, threat detection, real-time protection, cloud-based solutions, regulatory compliance.

Аннотация:

В данной статье рассматриваются основные характеристики, различия, преимущества и ограничения IDS (Intrusion Detection System) и IPS (Intrusion Prevention System). IDS специализируется на обнаружении атак, тогда как IPS активно блокирует и предотвращает эти угрозы. В статье представлены подробные сведения о развитии технологий IDS/IPS, включая использование машинного обучения и искусственного интеллекта, а также значение облачных решений. Также подчеркивается роль инструментов IDS и IPS в обеспечении ИТ-безопасности, соответствия нормативным требованиям и лучших практик.

Ключевые слова: IDS (Intrusion Detection System), IPS (Intrusion Prevention System), киберугрозы, сетевой безопасность, машинное обучение, искусственный

интеллект, обнаружение угроз, защита в реальном времени, облачные решения, нормативное соответствие.

Kirish

Hozirgi kunda raqamli infratuzilmalar va IT tizimlari har qachongidan ham ko‘proq murakkablashib, ularga bo‘lgan hujumlar soni ortib bormoqda. Kiberxavfsizlik texnologiyalari orasida IDS (Intrusion Detection System) va IPS (Intrusion Prevention System) tizimlari asosiy o‘rin tutadi. IDS tizimlari tarmoq trafigi va foydalanuvchi xatti-harakatlarini kuzatib, tahdidlarni aniqlashga qaratilgan bo‘lsa, IPS bu tahdidlarni aniqlash bilan bir qatorda ularning oldini olish imkonini ham taqdim etadi.

Mazkur maqola IDS va IPS tizimlarining xususiyatlarini chuqurroq o‘rganish, ularning afzalliklari, cheklovlari hamda IT xavfsizligidagi ahamiyatini tahlil qilishga bag‘ishlangan. Shuningdek, ushbu texnologiyalarning zamonaviy imkoniyatlari, jumladan, mashinani o‘rganish va sun’iy intellektni qo‘llash bilan bog‘liq istiqbollar, bulutga asoslangan yechimlar va amaliyotlar ko‘rib chiqiladi. Maqola tashkilotlar uchun IDS va IPS tizimlarini tanlash va joriy etish jarayonida foydali qo‘llanma sifatida xizmat qiladi.

IDS (Intrusion Detection System)

Buzilishlarni aniqlash tizimi (IDS) tarmoq trafigini va shubhali xatti-harakatlarni kuzatuvchi kiberxavfsizlik yechimidir. IDS xavfsizlik tizimlari tajovuzlar va xavfsizlik buzilishlarini aniqlashga qaratilgan bo‘lib, tashkilotlar potentsial tahdidlarga tezda javob bera oladilar.

IDS turlariga quyidagilar kiradi:

- ***Tarmoqqa asoslangan*:** tarmoqqa asoslangan IDS (NIDS) kompyuter tarmog'ining strategik nuqtalarida kiruvchi va chiquvchi trafikni tekshirib o‘rnatiladi. U tarmoq protokollarini, trafik naqshlarini va paket sarlavhalarini kuzatishga qaratilgan.

➢ ***Xostga asoslangan*:** Xostga asoslangan IDS (HIDS) IT muhitidagi alohida mashinalar yoki serverlarga o‘rnatiladi. U ruxsatsiz kirish urinishlari va tizimdagi g'ayritabiiy o‘zgarishlar kabi hodisalarni aniqlash uchun tizim jurnallari va fayllarini kuzatishga qaratilgan.

➢ ***Gibrid:*** Gibrid IDS ham tarmoqqa, ham xostga asoslangan yondashuvlarni birlashtiradi. Ushbu turdagi IDS IT ekotizimidagi voqealarning to‘liqroq ko‘rinishini ta'minlaydi.

IDS vositalari tarmoq paketlarini tahlil qilish va ularni ma'lum hujum imzolari yoki xatti-harakatlar naqshlari bilan solishtirish orqali ishlaydi. Agar IDS buzg'unchini aniqlagan deb hisoblasa, u tizim ma'murlari yoki xavfsizlik guruhlariga ogohlantirish yuboradi. Ushbu ogohlantirishlar aniqlangan faoliyat haqida batafsil ma'lumotni o‘z ichiga oladi, bu esa xodimlarga tezda tekshirish va javob berish imkonini beradi. IDS kompyuter tarmoqlari va tizimlarining xavfsizligi va yaxlitligini ta'minlashda muhim rol o‘ynaydi.

IDS ning afzalliklari quyidagilardan iborat:

➢ ***Tahdidlarni erta aniqlash*:** IDS vositalari hujumning dastlabki bosqichida potentsial tahdidlarni aniqlash orqali kiberhujumlardan faol himoyalanishi mumkin.

➢ ***Ko‘proq ko‘rinish*:** IDS yechimlari tashkilotlarning IT muhitida ko‘rinishini kuchaytirib, xavfsizlik guruhlariga hujumlarga tezroq va samaraliroq javob berishga yordam beradi.

IDS cheklovlari quyidagilarni o‘z ichiga oladi:

➢ ***Noto‘g'ri ijobiy va noto‘g'ri salbiy*:** IDS vositalari mukammal emas; ular noto‘g'ri pozitivlarni (xavfsiz hodisalarni tahdid sifatida belgilash) va noto‘g'ri salbiylarni (haqiqiy tahdidlarni aniqlay olmaslik) yaratishi mumkin.

➢ ***Hujumlarning oldini olishning imkoni yo‘q*:** IDS yechimlari hujumlarni sodir bo‘lgandan keyin aniqlay oladi, lekin ular birinchi navbatda ularni oldini olishga qodir emas.

IPS (Intrusion oldini olish tizimi)

Tarmoqlarda IPS nima va u IDS dan qanday farq qiladi? Bosqinning oldini olish tizimi (IPS) IDS imkoniyatlariga asoslangan kiberxavfsizlik yechimidir. IPS kiberxavfsizlik vositalari nafaqat mumkin bo‘lgan hujumlarni aniqlabgina qolmay, balki ularni faol ravishda oldini oladi va yumshatadi.

IDSda bo‘lgani kabi, IPS turlariga quyidagilar kiradi:

- ***Tarmoqqa asoslangan*:** Tarmoqqa asoslangan IPS (NIPS) kompyuter tarmog'idagi strategik nuqtalarda, ko‘pincha tarmoq shlyuzlarida o‘rnatiladi. U tashkilotning butun tarmog'ini, shu jumladan bir nechta ulangan xostlar va qurilmalarni himoya qilishi mumkin.
- ***Xostga asoslangan*:** Xostga asoslangan IPS (HIPS) ma'lum bir mashina yoki serverda o‘rnatiladi va bitta xostni himoya qiladi. U tizim faoliyatini nazorat qiladi va tizim resurslariga kirishni bloklash yoki cheklash bo‘yicha choralar ko‘rishi mumkin.
- ***Gibrid*:** Gibrid IPS ham tarmoqqa, ham xostga asoslangan yondashuvlarni birlashtiradi. Misol uchun, gibrid IPS birinchi navbatda tarmoqqa asoslangan bo‘lishi mumkin, lekin shaxsiy xostlarni himoya qilish uchun xususiyatlarni ham o‘z ichiga oladi.

IPS ning afzalliklari quyidagilardan iborat:

- ***Haqiqiy vaqtda tahdidlarning oldini olish*:** IPS real vaqt rejimida aniqlangan tahdidlarni bloklashi yoki kamaytirishi mumkin, bu esa AT muhitlari uchun 24/7 avtomatlashtirilgan himoyani ta'minlaydi.
- ***Kengaytirilgan tarmoq himoyasi*:** IDS vositalaridan farqli o‘laroq, IPS tizimlari nafaqat tahdidlarni aniqlay oladi, balki zararli va shubhali trafikni blokirovka qilish orqali ularga qarshi himoya choralarini ko‘radi.

IPS cheklovlari quyidagilarni o‘z ichiga oladi:

- ***Ishlash effekti:*** IPS vositalari barcha kiruvchi va chiquvchi trafikni tekshirishi kerak, bu esa kechikishni keltirib chiqarishi va tarmoq ish faoliyatini sekinlashtirishi mumkin.

- ***Tez-tez yangilanishlar*:** Maksimal samaradorlik uchun IPS yechimlari jiddiy vaqt sarmoyasi va tajriba talab qilishi mumkin bo‘lgan tahdid imzolari haqidagi so‘nggi ma'lumotlar bilan muntazam yangilanib turishi kerak.

IDS va IPS o‘rtasidagi farqlar

IDS va IPS o‘rtasidagi asosiy farq shundaki, IDS vositalari faqat hujumlarni aniqlashga qodir bo‘lsa-da, IPS vositalari ham ularni faol ravishda oldini oladi. Bu asosiy farq IDS va IPS o‘rtasidagi savolga bir qancha muhim ta’sir ko‘rsatadi:

- ***Funktsionallik*:** IDS vositalari tahdidlarni aniqlash bilan cheklangan, IPS vositalari esa ularni aniqlashi va oldini olishi mumkin.
- ***Javob*:** IDS vositalari tahdid aniqlanganda ogohlantirishlar yuboradi, IPS vositalari esa oldindan belgilangan xavfsizlik siyosati yoki qoidalari asosida tahdidlarni avtomatik ravishda bloklashi mumkin.
- ***Ish jarayoni*:** IDS vositalari ma'lumotlar oqimini passiv ravishda kuzatib boradi, IPS vositalari esa tarmoq paketlarini faol ravishda tekshiradi va tahdidlarni oldini olish yoki yumshatish uchun choralar ko‘radi.

IDS/IPS texnologiyasidagi yutuqlar

IDS/IPS texnologiyasi joriy etilganidan beri sezilarli darajada rivojlandi. IDS/IPS yechimlaridagi ba'zi ishlanmalar quyidagilarni o‘z ichiga oladi:

- **Mashinani o‘rganish va sun'iy intellekt:** IDS/IPS asboblari kibertahdidlar haqidagi tarixiy ma'lumotlardan o‘rganish, aniqlash imkoniyatlarini oshirish uchun mashinani o‘rganish va sun'iy intellektdan foydalanishi mumkin.
- **Xulq-atvorni tahlil qilish:** IDS/IPS vositalari xulq-atvor tahlili deb nomlanuvchi usuldan foydalanishi mumkin: tarmoq trafigini yoki foydalanuvchi xatti-harakatlarini anomaliyalar yoki og'ishlarni aniqlashga yordam beradigan asosiy chiziqqa solishtirish.
- **Bulutga asoslangan joylashtirish:** Bulutli hisoblashning tobora kengayib borishi bilan ko‘plab IDS/IPS vositalari endi bulutga asoslangan AT muhitlarida ularni yanada moslashuvchan va kengaytiriladigan qilish uchun joylashtirilishi mumkin.

IDS/IPS va me'yoriy hujjatlarga muvofiqlik

IDS va IPS vositalarini o‘rnatish tashkilotlarning tartibga solish talablariga javob berishi uchun zarur bo‘lishi mumkin. Normativ muvofiqlik uchun IDS va IPS dan foydalanish holatlariga quyidagilar kiradi:

- ***Tahdidlarni aniqlash va hodisalarga javob berish*:** IDS va IPS yechimlari xavfsizlik tahdidlarini aniqlash va himoya qilish uchun tarmoq trafigini, tizim jurnallarini va hodisalarni faol ravishda kuzatib boradi.
- ***Maxfiy ma'lumotlarni himoya qilish*:** Maxfiy ma'lumotlarga ruxsatsiz kirishni bloklash orqali IDS va IPS ma'lumotlar maxfiyligi standartlariga rioya qilish uchun bebaho vositadir.
- ***Ro‘yxatga olish va hisobot berish*:** IDS va IPS yechimlari tizim jurnallarini yaratadi va tashqi audit paytida kompaniyalar foydalanishi mumkin bo‘lgan hisobot berish imkoniyatlarini taqdim etadi.

Ko‘pgina ma'lumotlar maxfiyligi va xavfsizligi qoidalari tashkilotlardan IDS va IPS vositalarini joriy etishni aniq yoki bilvosita talab qiladi. Masalan, PCI DSS to‘lov kartasi ma'lumotlarini qayta ishlaydigan korxonalar uchun xavfsizlik standartidir. PCI DSS 11.4 talabiga ko‘ra, kompaniyalar "tarmoqqa kirishni aniqlash va/yoki oldini olish uchun tarmoqqa kirishni aniqlash yoki oldini olish usullaridan foydalanishlari" kerak.

GDPR (Ma'lumotlarni himoya qilish bo‘yicha umumiy reglament) IDS/IPS yechimlarini talab qilishi mumkin bo‘lgan yana bir qoidadir. GDPR - bu Evropa Ittifoqidagi qonun bo‘lib, u fuqarolarning shaxsiy ma'lumotlarining maxfiyligini himoya qiladi. GDPRga ko‘ra, korxonalar ushbu ma'lumotlarni buzilishlar va ruxsatsiz kirishdan himoya qilish uchun "tegishli texnik va tashkiliy choralar" ni ko‘rishlari kerak, jumladan IDS/IPSni o‘rnatish.

IDS/IPS haqida noto‘g'ri tushunchalar

IDS va IPS yechimlarining keng qo‘llanilishiga qaramay, ba'zi keng tarqalgan noto‘g'ri tushunchalar mavjud, masalan:

- ***Umumiy oldini olish*:** IDS va IPS vositalari kiberhujumlardan 100 foiz himoya qila olmaydi. Ular faqat oldindan belgilangan qoidalar va imzolar asosida shubhali faoliyatni aniqlashlari mumkin, bu ularni ma'lum hujum naqshlari bilan cheklaydi.
- ***Boshqa himoya vositalari talab qilinmaydi*:** IDS va IPS yechimlari yuqori samarali bo‘lishi mumkin, ammo ular xavfsizlik devori va antimalware dasturlari kabi vositalar bilan bir qatorda kiberxavfsizlik jumboqlarining faqat bir qismidir.
- ***Faqat yirik korxonalar uchun foydalidir*:** IDS/IPS texnologiyasi mayda startaplardan tortib yirik transmilliy firmalargacha bo‘lgan barcha o‘lchamdagi va sohalardagi biznes uchun samarali.

Xulosa

IDS va IPS tizimlari zamonaviy kiberxavfsizlikning ajralmas qismi bo‘lib, tarmoqlarni tahdidlardan himoya qilishda muhim rol o‘ynaydi. IDS tizimlari hujumlarni aniqlashga qaratilgan bo‘lsa, IPS bu tahdidlarni aniqlash bilan bir qatorda ularni bloklash va oldini olish imkonini beradi. Ushbu tizimlarning kombinatsiyasi tashkilotlarga tahdidlarni aniqlash va ularga tezkorlik bilan javob berish imkonini beradi.

Maqolada ko‘rib chiqilgan mashinani o‘rganish, sun’iy intellekt va bulutga asoslangan texnologiyalar IDS/IPS tizimlarining samaradorligini yanada oshiradi. Biroq, IDS va IPS tizimlari boshqa kiberxavfsizlik vositalari bilan birgalikda ishlatilishi kerak, chunki ularning mustaqil ishlashi kiberhujumlardan to‘liq himoya qilishni ta'minlay olmaydi.

Tashkilotlar o‘z IT muhitiga mos keladigan va mavjud xavfsizlik infratuzilmasiga integratsiya qilinadigan IDS/IPS tizimlarini tanlash orqali o‘zlarining xavfsizlik darajasini sezilarli darajada oshirishi mumkin. IDS va IPS vositalarini to‘g‘ri sozlash va

muntazam yangilab turish kiberxavfsizlik tahdidlariga qarshi samarali choralar ko‘rishga imkon beradi. Shu bilan birga, ushbu texnologiyalar me’yoriy hujjatlarga muvofiqlikni ta’minlashda ham katta ahamiyatga ega.

Foydalanilgan adabiyotlar ro'yhati:

1. Bekzod, B., & Daeik, K. (2021). Face recognition based automated student attendance system. Turkish Journal of Computer and Mathematics Education, 12(11), 3531-3534.

2. Mamatkulovich, B. B. (2023). A Design Of Small Scale Deep Cnn Model For Facial Expression Recognition Using The Low-Resolution Image Datasets. Models And Methods For Increasing The Efficiency Of Innovative Research, 2(19), 284-288.

3. Babakulov, B. (2023). UNİVERSİTET TALABALARİ UCHUN CHUQUR O'RGANİSHGA ASOSLANGAN YUZNİ ANİQLASHDAN FOYDALANGAN HOLDA AVTOMATİK DAVOMAT TİZİMİ. Инновационные исследования в современном мире: теория и практика, 2(3), 74-76.

4. Turapova, S. K., & Babakulov, B. M. (2023). IMPROVING TECHNOLOGIES FOR TRAINING 12-14-YEAR-OLD VOLLEYBALL PLAYERS IN SPORTS SCHOOLS FOR CHILDREN AND TEENAGERS. Mental Enlightenment Scientific-Methodological Journal, 4(03), 198-206.

5. Mamatkulovich, B. B. (2023). Alijon o’g’li HA Facial Image-Based Gender and Age Estimation. Eurasian Scientific Herald, 18, 47-50.

6. Mamatkulovich, B. B., Qizi, T. S. X., Qizi, T. O. M., & O’G’Li, X. D. S. (2023). Simplified machine learning for image-based fruit quality assessment. Eurasian Journal of Research, Development and Innovation, 19, 8-12.

7. Mamatkulovich, B. B., Shuhrat o'g'li, M. S., & Jasurjonovich, B. J. (2023). SPECIAL DEEP CNN DESIGN FOR FACIAL EXPRESSION CLASSIFICATION WITH A SMALL AMOUNT OF DATA. Open Access Repository, 4(3), 472-478.

8. Mamatkulovich, B. B., Dilshod o'gli, Y. A., & Akmal o'g'li, A. A. (2023). Predicting daily energy production in a blockchain-based P2P energy trading system. Texas Journal of Engineering and Technology, 18, 7-11.

9. Mamatkulovich, B. B. (2022, May). Automatic Student Attendance System Using Face Recogniton. In Next Scientists Conferences (pp. 6-22).

10. Mamatkulovich, B. B. (2022). Lightweight residual layers based convolutional neural networks for traffic sign recognition. European International Journal of Multidisciplinary Research and Management Studies, 2(05), 88-94.

11. Ikromovich, H. O., & Mamatkulovich, B. B. (2023). Facial recognition using transfer learning in the deep cnn. Open Access Repository, 4(3), 502-507.