INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

YANGI RENESSANS

ILMIY JURNALI

2026/5

+998335668868
www.innoworld.net

YANGI RENESSANS

ILMIY JURNALI
TO'PLAMI

3 - JILD, 5 - SON
2026

www.innoworld.net

O'ZBEKISTON-2026

HONEYPOTLARDAN FOYDALANISH VA HUJUMCHILARNI ANIQLASH

Sobirjonov Behzod Qahramonovich
FarDU Axborot texnologiyalari kafedrasi o‘qituvchisi
Email: behzodbekqahramonovich@gmail.com
Tel.: +998 90 526 87 38
Rahmonaliyeva Durdonaxon Muhammadjon qizi
FarDU Axborot tizimlari va texnologiyalari yo‘nalishi 2-bosqich talabasi
Email: durdona1125.raxmonaliyeva@gmail.com
Tel.: +998 88 292 25 11

Annotatsiya. Ushbu maqolada Honeypot texnologiyasining zamonaviy kiberxavfsizlikdagi o‘rni va ahamiyati tahlil qilinadi. Honeypotlar – bu maxsus tashkil etilgan yolg‘on axborot tizimlari bo‘lib, ular yordamida hujumchilarning xatti-harakatlarini kuzatish, tahlil qilish va yangi tahdidlarni aniqlash imkoniyati yaratiladi. Maqolada honeypotlarning turlari, jumladan past darajali va yuqori darajali honeypotlar, ularning ishlash mexanizmlari hamda real tarmoqlarda qo‘llanilishi ko‘rib chiqiladi.

Shuningdek, Intrusion Detection System bilan integratsiya qilish orqali hujumlarni erta bosqichda aniqlash samaradorligi oshishi yoritiladi. Tadqiqot natijalari shuni ko‘rsatadiki, honeypotlardan foydalanish Kiberxavfsizlikda proaktiv himoya choralarini kuchaytiradi va noma’lum tahdidlarni aniqlashda muhim vosita hisoblanadi.

Kalit so‘zlar: honeypot, kiberxavfsizlik, hujumlarni aniqlash, IDS, tarmoq xavfsizligi, zararli faoliyat, monitoring, tahdid tahlili, axborot xavfsizligi, honeynet

Abstract. This article analyzes the role and significance of Honeypot technology in modern cybersecurity. Honeypots are specially designed decoy information systems that enable the observation and analysis of attacker behavior, as well as the identification of new threats. The article examines the types of honeypots, including low-interaction and high-interaction honeypots, their operational mechanisms, and their application in real networks. Furthermore, it highlights how integration with Intrusion Detection Systems (IDS) enhances the efficiency of early-stage attack detection. The research results indicate that the use of honeypots strengthens proactive defense measures in cybersecurity and serves as a vital tool for detecting unknown threats.

Keywords: Honeypot, cybersecurity, attack detection, IDS, network security, malicious activity, monitoring, threat analysis, information security, honeynet.

Аннотация. В данной статье анализируются роль и значение технологии Honeypot в современной кибербезопасности. Honeypot (ханипоты) — это специально созданные ложные информационные системы, которые позволяют отслеживать и анализировать действия злоумышленников, а также выявлять новые угрозы. В статье рассматриваются виды ханипотов, включая системы с низким и высоким

уровнем взаимодействия, механизмы их работы и применение в реальных сетях. Также освещается вопрос повышения эффективности раннего обнаружения атак путем интеграции с системами обнаружения вторжений (IDS). Результаты исследования показывают, что использование ханипотов усиливает меры проактивной защиты в кибербезопасности и является важным инструментом для выявления неизвестных угроз.

Ключевые слова: Honeypot, кибербезопасность, обнаружение атак, IDS, сетевая безопасность, вредоносная деятельность, мониторинг, анализ угроз, информационная безопасность, honeynet.

Adabiyotlar tahlili va metodologiya. Honeypot texnologiyasi Kiberxavfsizlik doirasida keng o‘rganilgan bo‘lib, Lance Spitzner uni hujumchilar faoliyatini kuzatish va yangi tahdidlarni aniqlash uchun samarali vosita sifatida ta’riflaydi. Niels Provos va Thorsten Holz tadqiqotlarida esa honeypotlarning past va yuqori darajali turlari hamda ularning amaliy qo‘llanilishi yoritilgan. Shuningdek, Honeyd kabi vositalar yordamida virtual muhitda hujumlarni aniqlash va tahlil qilish mumkinligi ko‘rsatib berilgan. Zamonaviy yondashuvlarda honeypotlar Intrusion Detection System bilan birgalikda qo‘llanilib, hujumlarni erta aniqlash samaradorligini oshiradi.

Mazkur tadqiqotda metodologiya sifatida tizimli tahlil va taqqoslash usullaridan foydalanildi. Honeypotlarning turli turlari o‘rganilib, ularning imkoniyatlari solishtirildi hamda virtual muhitda eksperimental sinovlar o‘tkazildi. Natijada honeypot texnologiyasining hujumlarni aniqlash va tahlil qilishdagi samaradorligi asoslab berildi.

Natijalar va muhokama. Tadqiqot natijalari shuni ko‘rsatdiki, honeypot texnologiyasi Kiberxavfsizlikda hujumlarni aniqlash va ularni tahlil qilishda samarali vosita hisoblanadi. Eksperimental sinovlar davomida virtual muhitda tashkil etilgan honeypot tizimi orqali turli xil zararli faoliyatlar, jumladan skanerlash, ruxsatsiz kirish va eksploit urinishlari aniqlanib, ularning xatti-harakatlari qayd etildi. Olingan natijalar Lance Spitzner va Niels Provos tadqiqotlarida keltirilgan xulosalar bilan mos kelishini ko‘rsatdi.

Muhokama jarayonida aniqlanishicha, honeypotlar Intrusion Detection System bilan birgalikda qo‘llanilganda yanada yuqori samaradorlikka erishiladi, chunki ular nafaqat ma’lum tahdidlarni, balki yangi va noma’lum hujumlarni ham aniqlash imkonini beradi. Shu bilan birga, yuqori darajali honeypotlar chuqur tahlil uchun ko‘proq ma’lumot bersa-da, ularni boshqarish murakkabroq ekani ham kuzatildi. Umuman olganda, tadqiqot natijalari honeypotlardan foydalanish zamonaviy axborot tizimlarida proaktiv himoya mexanizmini kuchaytirishini tasdiqlaydi.

Xulosa. Xulosa qilib aytganda, honeypot texnologiyasi Kiberxavfsizlikda hujumlarni aniqlash va ularni chuqur tahlil qilishda muhim vosita hisoblanadi. Tadqiqot natijalari honeypotlar yordamida nafaqat mavjud, balki yangi va

noma’lum tahdidlarni aniqlash mumkinligini ko‘rsatdi. Ayniqsa, ularni Intrusion Detection System bilan birgalikda qo‘llash tizim xavfsizligini sezilarli darajada oshiradi.

Shu bilan birga, honeypotlarning turli turlari turli vazifalar uchun mos kelishi aniqlanib, ularni to‘g‘ri tanlash va joriy etish muhim ahamiyatga ega ekanligi asoslandi. Umuman olganda, honeypot texnologiyasidan foydalanish zamonaviy axborot tizimlarida samarali va istiqbolli himoya yechimi sifatida tavsiya etiladi.

Foydalanilgan adabiyotlar

1. Lance Spitzner (2003). *Honeypots: Tracking Hackers*. Addison-Wesley Professional.
2. Niels Provos, & Thorsten Holz (2007). *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Addison-Wesley Professional.
3. The Honeynet Project (2005). *Know Your Enemy: Learning about Security Threats*.
4. NIST (2012). *Guide to Intrusion Detection and Prevention Systems (IDS/IPS)*. Special Publication 800-94.
5. Clifford Stoll (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Doubleday.
6. Honeyd rasmiy hujjatlari va texnik tavsiflari (https://www.honeyd.org).