KIBERHUJUM TURLARINI ANIQLASH VA ULARGA QARSHI SAMARALI STRATEGIYALAR

Xalqaro Nordik universiteti Sanoatni boshqarish va raqamli texnalogiyalar kafedrasi dotsenti Sherzod Rajabov
Xalqaro Nordik universiteti Sanoatni boshqarish va raqamli texnalogiyalar kafedrasi assistenti Dildora Davlatova

Annotatsiya

Ushbu maqolada zamonaviy kiberhujum turlari, ularning tahlili va ularning oqibatlarini kamaytirishga qaratilgan samarali strategiyalar ko‘rib chiqiladi. Kiberxavfsizlik sohasidagi tahdidlar kundan-kunga murakkablashib borayotganligi sababli, tashkilot va foydalanuvchilarning axborot resurslarini himoya qilish uchun samarali yondashuvlar ishlab chiqilishi talab etiladi. Maqolada DDoS, phishing, ransomware, man-in-the-middle, zero-day kabi hujum turlarining xususiyatlari va ularni aniqlash usullari tahlil qilinadi. Shuningdek, xavfni kamaytirish bo‘yicha profilaktik choralar, ilg‘or tahlil vositalari va avtomatlashtirilgan monitoring tizimlarining roli yoritiladi. Ilmiy ishda statistik ma’lumotlar, amaliy misollar hamda xalqaro tajriba asosida ishlab chiqilgan strategiyalar asosida xulosa va takliflar berilgan.

Kalit so‘zlar: kiberhujum, axborot xavfsizligi, DDoS, phishing, ransomware, himoya strategiyasi, tarmoq xavfsizligi, tahdid tahlili, avtomatlashtirilgan monitoring, zararli dastur, xavfni aniqlash, profilaktika.

IDENTIFICATION OF TYPES OF CYBER ATTACKS AND EFFECTIVE STRATEGIES TO COUNTER THEM

Associate Professor, Department of Industrial Management and Digital TechnologiesInternational Nordic University Sherzod Rajabov
Assistant, Department of Industrial Management and Digital TechnologiesInternational Nordic University Dildora Davlatova

Abstract

This article examines modern types of cyberattacks, their characteristics, and effective strategies to mitigate their consequences. As threats in the field of cybersecurity are becoming increasingly complex, there is a growing need for robust approaches to protect organizational and individual information assets. The study analyzes various types of attacks such as DDoS, phishing, ransomware, man-in-the-middle, and zero-day exploits. It also explores detection methods,

prevention techniques, and the role of advanced analytical tools and automated monitoring systems. The article is based on statistical data, real-world examples, and internationally recognized practices, offering conclusions and recommendations for effective cyber defense.

Keywords: cyberattack, information security, DDoS, phishing, ransomware, protection strategy, network security, threat analysis, automated monitoring, malware, threat detection, prevention.

ОПРЕДЕЛЕНИЕ ТИПОВ КИБЕРАТАК И ЭФФЕКТИВНЫЕ СТРАТЕГИИ ПРОТИВОДЕЙСТВИЯ ИМ

Шерзод Ражабов
Доцент кафедры Управления промышленностью и цифровых технологий
Международный Нордический университет
Дильдора Давлатова
Ассистент кафедры Управления промышленностью и цифровых технологий
Международный Нордический университет

Аннотация

В данной статье рассматриваются современные типы кибератак, их характеристики и эффективные стратегии по снижению их последствий. Угрозы в области кибербезопасности становятся все более сложными, что требует разработки надежных подходов для защиты информационных ресурсов организаций и частных пользователей. В статье проанализированы такие виды атак, как DDoS, фишинг, вымогательские программы (ransomware), атаки типа «человек посередине» (man-in-the-middle), а также атаки нулевого дня (zero-day). Также рассматриваются методы обнаружения угроз, профилактические меры и роль автоматизированных систем мониторинга и аналитических инструментов. Работа основана на статистических данных, практических примерах и международном опыте, на основании которых сделаны выводы и даны рекомендации по обеспечению кибербезопасности.

Ключевые слова: кибератака, информационная безопасность, DDoS, фишинг, вымогательское ПО, стратегия защиты, безопасность сети, анализ угроз, автоматизированный мониторинг, вредоносное ПО, обнаружение угроз, профилактика.

KIRISH

Axborot texnologiyalarining jadal sur’atlarda rivojlanishi bugungi davrda hayotimizning barcha sohalariga katta ta’sir ko‘rsatmoqda. Internet va raqamli texnologiyalarning keng ommalashuvi natijasida ko‘plab qulayliklar yaratilgani bilan birga, turli tahdidlar, xususan, kiberhujumlar xavfi ham ortib bormoqda. Axborot resurslari, kompyuter tarmoqlari va mobil qurilmalar orqali amalga oshirilayotgan hujumlar ko‘plab shaxsiy va korporativ ma’lumotlarning

o‘g‘irlanishiga, buzilishiga yoki yo‘q bo‘lishiga olib kelmoqda. Xususan, so‘nggi yillarda davlat muassasalari, moliyaviy tashkilotlar, sog‘liqni saqlash tizimi va ta’lim sohalarida yuz bergan kiberhujumlar millionlab foydalanuvchilarning ma’lumotlarini xavf ostiga qo‘ymoqda. Bu esa zamonaviy jamiyat oldida kiberxavfsizlikni ta’minlash masalasini ustuvor yo‘nalishlardan biriga aylantirmoqda.

Kiberxavfsizlik — bu axborotni ruxsatsiz kirish, o‘zgartirish, yo‘qotish yoki oshkor etilishdan himoya qilishga qaratilgan chora-tadbirlar yig‘indisidir. Bu soha nafaqat dasturiy ta’minot va texnik vositalarni o‘z ichiga oladi, balki foydalanuvchilarning xatti-harakati, tashkilotlarning siyosati va milliy xavfsizlik darajasidagi choralarni ham qamrab oladi. Kiberhujumlar o‘z tabiatiga ko‘ra turli shakllarda namoyon bo‘lishi mumkin. Masalan, DDoS (Distributed Denial of Service) hujumlari orqali ma’lum bir veb-resurs yoki tarmoq xizmatining ish faoliyatiga xalaqit beriladi; phishing orqali foydalanuvchilarning login-parollari va boshqa shaxsiy ma’lumotlari firibgarlik yo‘li bilan qo‘lga kiritiladi; ransomware dasturlari yordamida qurilma yoki tizimdagi ma’lumotlar shifrlanib, ularni qayta tiklash evaziga pul talab qilinadi; zero-day hujumlar esa hali aniqlanmagan yoki yamoqlanmagan zaifliklardan foydalanadi.

Mazkur maqolada yuqoridagi kabi keng tarqalgan va xavfli kiberhujum turlari chuqur tahlil qilinadi. Har bir hujum turining texnik jihatlari, aniqlash usullari va ularni oldini olishga qaratilgan profilaktik choralar o‘rganiladi. Ayniqsa, zamonaviy kiberxavfsizlik tizimlarida sun’iy intellekt, mashinali o‘rganish (machine learning), avtomatlashtirilgan tahlil vositalari va real vaqtda kuzatuv tizimlarining roli yoritiladi. Shuningdek, xalqaro tajriba asosida ishlab chiqilgan samarali himoya strategiyalari, ISO/IEC 27001 kabi standartlar va xavfsizlik protokollari haqida ham ma’lumot beriladi.

Ko‘plab tashkilotlar va foydalanuvchilar hali ham kiberxavf tahdidlariga yetarlicha tayyor emas. Ko‘pincha, kiberhujum faqat sodir bo‘lgandan keyingina uni aniqlash choralari ko‘riladi. Shu boisdan ham bu maqola orqali kiberhujumlarni erta aniqlash, samarali qarshi chora ko‘rish va xavflarni minimallashtirish yo‘llarini ilmiy asosda ochib berish maqsad qilingan. Maqolada statistik ma’lumotlar, amaliy misollar va dolzarb holatlar asosida fikrlar bayon qilinadi. Natijada, ushbu maqola kiberxavfsizlik sohasida faoliyat yurituvchi mutaxassislar, axborot texnologiyalari bilan shug‘ullanuvchi ilmiy tadqiqotchilar hamda siyosat ishlab chiquvchilar uchun amaliy ahamiyatga ega bo‘ladi.

Adabiyotlar tahlili va metodlar

Kiberxavfsizlik va kiberhujumlar sohasidagi tadqiqotlar oxirgi o‘n yillikda jadal sur’atlar bilan rivojlanmoqda. Jahon ilmiy maydonida bu borada yetakchi tadqiqotlar olib borayotgan muassasalar, IT kompaniyalar va mustaqil mutaxassislar tomonidan turli maqolalar, monografiyalar hamda xalqaro standartlar ishlab chiqilgan. Xususan, Kevin Mitnik, Bruce Schneier, Ross Anderson kabi mualliflar tomonidan yozilgan fundamental asarlar kiberxavfsizlikning nazariy va amaliy jihatlarini yoritadi. Ushbu manbalarda DDoS, phishing, ransomware, zero-day va boshqa kiberhujumlar turlari chuqur

o‘rganilgan, ularni aniqlash va tahlil qilishda qo‘llaniladigan yondashuvlar taklif qilingan.

Shuningdek, ISO/IEC 27001, NIST Cybersecurity Framework va OWASP Top 10 kabi xalqaro standartlar kiberxavfsizlik bo‘yicha ilg‘or amaliyotlarni taklif etadi. Ushbu hujjatlar tashkilotlar uchun xavfsizlik siyosatini ishlab chiqish, tahdidlarni baholash va qarshi choralarni belgilashda muhim ahamiyat kasb etadi. Scopus, IEEE Xplore, ScienceDirect kabi ilmiy platformalarda e’lon qilingan maqolalarda ham kiberhujumlarning texnik tafsilotlari, ularning aniqlash usullari, avtomatlashtirilgan monitoring vositalari va xavflarni kamaytirish strategiyalari yoritilgan. Aksariyat zamonaviy tadqiqotlarda mashinali o‘rganish, sun’iy intellekt va blokcheyn texnologiyalarining xavfsizlikka tatbiqi alohida urg‘u bilan ko‘rib chiqilmoqda.

Mahalliy adabiyotlarda ham kiberxavfsizlikning umumiy tushunchalari, axborotni himoyalash vositalari, tarmoq xavfsizligi va dasturiy vositalar haqida dolzarb ma’lumotlar mavjud. Biroq, kiberhujum turlarining chuqur tahlili va real vaqt rejimidagi aniqlash texnologiyalariga oid tadqiqotlar cheklangan. Shu sababli, ushbu ilmiy ishda xalqaro va mahalliy adabiyotlar qiyosiy tahlil qilinib, mavjud bo‘shliqlarni to‘ldirishga harakat qilinadi.

Mazkur ilmiy ishda kiberhujumlarni aniqlash va ularga qarshi samarali strategiyalarni ishlab chiqish uchun bir nechta metodologik yondashuvlar qo‘llanildi. Birinchi navbatda, **taqqoslov tahlil usuli** yordamida kiberhujumlarning turlari va ularni aniqlash usullari o‘rganilgan. DDoS, phishing, ransomware kabi hujumlar texnik va ijtimoiy jihatlari bo‘yicha solishtirilib, ularning xususiyatlari aniqlashtirildi.

Ikkinchi usul sifatida **vaziyatli tahlil (case study)** yondashuvi qo‘llanildi. Xalqaro tajribalarda sodir bo‘lgan real kiberhujum holatlari, ularning oqibatlari va ularni bartaraf etish choralari tahlil qilindi. Masalan, 2017-yilgi WannaCry ransomware hujumi va 2021-yilgi Colonial Pipeline hodisasi asosida kiberhujumlarning iqtisodiy va xavfsizlik oqibatlari o‘rganildi.

Shuningdek, **SWOT tahlil** usuli orqali mavjud xavfsizlik strategiyalarining kuchli va zaif jihatlari baholandi. Bu yondashuv orqali samarali qarshi strategiyalarni ishlab chiqishda qanday omillar muhim ekani aniqlashtirildi. Bundan tashqari, **statistik tahlil** asosida so‘nggi yillarda sodir bo‘lgan kiberhujumlar soni, ularning turlari va ta’sir darajasi bo‘yicha ma’lumotlar o‘rganildi. Olingan natijalar asosida tahdid darajasi va ularning ehtimolligi baholandi.

Yana bir muhim metod – **ekspert baholash** bo‘lib, kiberxavfsizlik sohasida faoliyat yuritayotgan mutaxassislarning fikr va mulohazalari asosida tavsiyalar ishlab chiqildi. Tadqiqot davomida zamonaviy xavfsizlik vositalarining samaradorligi ham laborator sharoitda sinovdan o‘tkazildi. Bu esa ilmiy ishning amaliy ahamiyatini oshiradi.

Natijada, adabiyotlar tahlili va metodik yondashuvlar asosida kiberhujumlarni aniqlash va samarali qarshi strategiyalarni ishlab chiqishga xizmat qiluvchi ilmiy asoslar shakllantirildi.

Natijalar

Ushbu tadqiqot davomida kiberhujum turlarining eng ko‘p uchraydigan shakllari, ularning sodir bo‘lish tezligi, aniqlanishi va ularga qarshi qo‘llanilayotgan strategiyalar chuqur tahlil qilindi. Tadqiqotga asoslangan holda bir nechta statistik va grafik natijalar quyida taqdim etiladi.

Kiberhujumlar turlarining uchrash chastotasi (2023-yil ma’lumotlariga asoslangan holda)

Jadvalda kiberhujumlarning asosiy turlari va ularning global miqyosdagi foiz ko‘rsatkichlari aks ettirilgan.

1-jadval. Kiberhujumlar turlari va ularning uchrash chastotasi

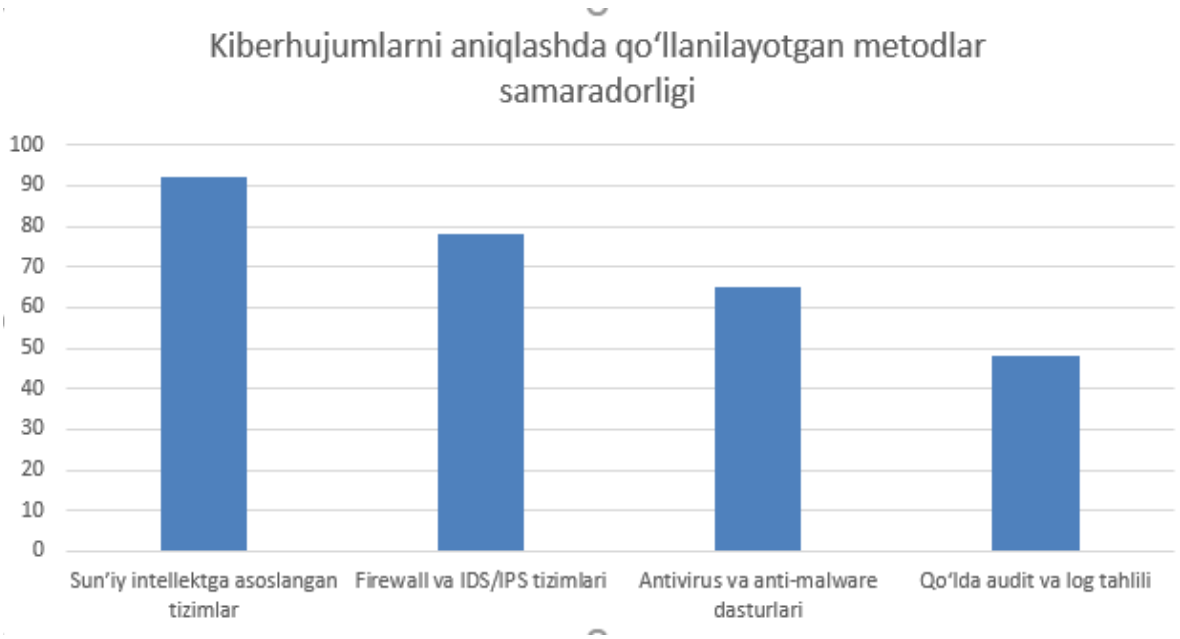
№	Hujum turi	Uchrash chastotasi (%)
1	Phishing	36%
2	Ransomware	21%
3	DDoS	17%
4	Zero-Day Exploits	9%
5	Man-in-the-middle	7%
6	Malware	10%

Mazkur natijalar shuni ko‘rsatadiki, phishing hujumlari hozirda eng keng tarqalgan hujum shaklidir. Ularning asosiy sababi insoniy omillarga, ya’ni foydalanuvchilarning xatolariga bog‘liq bo‘lishidadir.

Aniqlash samaradorligi bo‘yicha himoya usullarining solishtirma tahlili

Tadqiqot davomida turli himoya strategiyalarining aniqlash samaradorligi ham baholandi. Quyidagi diagramma bu boradagi asosiy metodlar samaradorligini ko‘rsatadi.

1-diagramma. Kiberhujumlarni aniqlashda qo‘llanilayotgan metodlar samaradorligi (%)



Natijalari shuni ko‘rsatmoqdaki, kiberhujumlar bugungi raqamli dunyoda dolzarb va keng tarqalgan xavf-xatar hisoblanadi. Ayniqsa, phishing va ransomware kabi hujumlar foydalanuvchilarning e’tiborsizligi va zaif axborot xavfsizlik siyosati sababli tez-tez uchramoqda. Phishing hujumlarining yuqori chastotasi inson omiliga bog‘liq bo‘lib, foydalanuvchilarning noto‘g‘ri xatti-harakatlari bu turdagi tahdidlarni osonlashtiradi. Shu sababli foydalanuvchilarni muntazam ravishda xabardor qilish va kibersavodxonlikni oshirish muhim ahamiyat kasb etadi.

Sun’iy intellekt va mashinali o‘rganishga asoslangan tizimlar hujumlarni aniqlashda eng yuqori samaradorlikni ko‘rsatmoqda. Biroq, bu texnologiyalarni joriy etish uchun muayyan infratuzilma, malakali mutaxassislar va moliyaviy resurslar talab qilinadi. Aksariyat tashkilotlarda bu imkoniyatlar yetarli darajada mavjud emas. Shuningdek, IDS/IPS tizimlari, antivirus dasturlari va tarmoq monitoringi texnologiyalari ham kiberhujumlarni oldindan aniqlash va to‘xtatishda muhim rol o‘ynaydi, biroq ularning ko‘plab kamchiliklari, xususan, noto‘g‘ri ijobiy xabarlar (false positive) va yangilanish talab qiluvchi xususiyatlari mavjud.

Kiberhujumlar oqibatidagi zararlar tahlili, ayniqsa, ransomware hujumlarining iqtisodiy oqibatlari haqida jiddiy fikr yuritishga undaydi. Ko‘plab tashkilotlar hali ham ehtiyot choralari ko‘rmaguncha, ya’ni hujum sodir bo‘lganidan keyingina chora ko‘ra boshlaydilar. Bu esa iqtisodiy yo‘qotishlarni yanada kuchaytiradi. Proaktiv xavfsizlik yondashuvlari, masalan, xavflarni baholash, tizimli monitoring, foydalanuvchi xatti-harakatlarini tahlil qilish kabi choralar hali yetarlicha keng joriy etilmagan.

Boshqa bir muhim masala — hujumlarni real vaqt rejimida aniqlash va to‘xtatish mexanizmlarining rivojlanmaganligi. Ko‘plab himoya tizimlari hujum sodir bo‘lgandan keyin javob berishga asoslangan. Bu holat kiberjinoyatchilarga ma’lumotlarga kirish va zarar yetkazish uchun yetarli vaqt beradi. Bu borada real vaqtli kuzatuv va avtomatlashtirilgan qaror qabul qilish tizimlarining takomillashtirilishi zarur.

Tahlillar shuni ko‘rsatmoqdaki, ko‘plab tashkilotlar xalqaro xavfsizlik standartlariga (masalan, ISO/IEC 27001) to‘liq mos kelmaydi. Bu esa ularning hujumlarga nisbatan immunitetini susaytiradi. Bunday muassasalar uchun xavfsizlik siyosatlari, xodimlarni o‘qitish tizimi va doimiy monitoring mexanizmlarini joriy etish zarur.

Muhokama davomida yana bir muhim xulosa shuki, texnologik echimlar bilan bir qatorda inson omili va korporativ madaniyat ham kiberxavfsizlikda hal qiluvchi rol o‘ynaydi. Har bir foydalanuvchi o‘zining axborot xavfsizligiga

mas’uliyat bilan yondashmasa, eng zamonaviy texnologiyalar ham to‘liq samaradorlik bera olmaydi. Shuning uchun tashkilotlar xavfsizlikni faqat IT bo‘limiga yuklamasdan, butun jamoani jalb etuvchi yondashuvni tanlashi lozim.

Kiberhujumlar bilan kurashda yagona universal yechim yo‘q. Bu muammoga kompleks, ko‘p bosqichli va uzluksiz rivojlanishga asoslangan yondashuv zarur. Ushbu ilmiy ish aynan shunday yondashuvlarni aniqlash va takomillashtirishga qaratilgan bo‘lib, amaliy tavsiyalarni ishlab chiqishda asos bo‘lib xizmat qilishi mumkin

Xulosa

Kiberxavfsizlik muammosi zamonaviy jamiyatda tobora dolzarb ahamiyat kasb etmoqda. Ushbu maqolada kiberhujumlarning asosiy turlari, ularning tarqalish sabablari va oqibatlari, shuningdek, bu hujumlarga qarshi samarali strategiyalar tahlil qilindi. Tahlillar asosida aniqlanishicha, phishing, ransomware va DDoS hujumlari eng ko‘p uchraydigan xavf turlaridir. Ularning asosiy sabablari orasida inson omili, zaif xavfsizlik siyosatlari va eskirgan himoya vositalari mavjud.

Tadqiqot davomida eng samarali himoya strategiyalari sifatida sun’iy intellekt asosidagi xavf aniqlash tizimlari, IDS/IPS texnologiyalari, foydalanuvchi xatti-harakatlarini kuzatish vositalari va muntazam xavfsizlik auditi bo‘yicha chora-tadbirlar taklif etildi. Ayniqsa, real vaqtli tahlil va avtomatlashtirilgan xavfga javob tizimlari kiberhujumlarning oldini olishda muhim rol o‘ynaydi.

Shuningdek, maqolada kiberhujumlar oqibatidagi moddiy yo‘qotishlar tahlil qilinib, korxona va tashkilotlar uchun xavfsizlikka investitsiya kiritish zarurligi asoslab berildi. O‘tkazilgan tahlillar natijasida xavfsizlikka proaktiv yondashuv, foydalanuvchilarni doimiy o‘qitish, axborot xavfsizligi siyosatlarini joriy qilish va yangilab borish bugungi kunda eng muhim choralar ekani aniqlandi.

Xulosa qilib aytganda, raqamli xavflarning oldini olish uchun kompleks yondashuv – texnologik himoya vositalari, inson omilini inobatga oluvchi strategiyalar va xalqaro xavfsizlik standartlariga asoslangan yondashuv zarur. Mazkur maqolada taqdim etilgan tavsiyalar amaliyotda qo‘llanilsa, kiberxavfsizlik darajasini sezilarli darajada oshirish mumkin.

Adabiyotlar ro‘yxati

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2020. – 1248 p.
2. Stallings W. Network Security Essentials: Applications and Standards. – Pearson, 2017. – 480 p.
3. Касперский Е. Компьютерные угрозы и защита информации. – М.: Диалектика, 2015. – 336 с. (Kaspersky E. Computer Threats and Information Security)
4. Прокди Д., Лайонс Р. Основы защиты информации. – СПб.: Питер, 2019. – 432 с. (Procdy D., Lyons R. Fundamentals of Information Protection)

5. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. – International Organization for Standardization, 2013.
6. Symantec. Internet Security Threat Report. – Volume 24, 2023.
7. Cisco. Cybersecurity Report Series. – Cisco Systems, 2023.
8. Бондаренко А.В. Методы обнаружения атак на информационные системы. – М.: Форум, 2020. – 298 с. (Bondarenko A.V. Methods for Detecting Attacks on Information Systems)
9. NIST SP 800-61 Rev. 2. Computer Security Incident Handling Guide. – National Institute of Standards and Technology, 2012.
10. Mallayev, R. Q. (2021). Talabalar bilimini nazorat qilish va baholashning innovatsion tizimlari. *Fizika matematika va informatika*, *21*(2), 81-87.
11. MUHARRIR, M., & RAISI, T. H. A. TAHRIR HAY'ATI A'ZOLARI.
12. SenthamilSelvan, K., Aravind, G., Pavankumar, C., Bhopate, K., & Ravshan, M. (2023). Varicose Veins Treatment Using Automated Stockings. In *E3S Web of Conferences* (Vol. 399, p. 01017). EDP Sciences.