AXBOROT TIZIMLARIDA KIBERXAVFSIZLIK: TAHDIDLAR VA HIMOYA CHORALARI

КИБЕРБЕЗОПАСНОСТЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ: УГРОЗЫ И МЕРЫ ЗАЩИТЫ

CYBERSECURITY IN INFORMATION SYSTEMS: THREATS AND PROTECTIVE MEASURES

Shermatova Xilola Mirzayevna
Farg‘ona davlat universiteti Axborot texnologiyalari kafedrasi dotsenti
shermatovahilola1978@gmail.com
Yunusova Dilrabo Akmaljon qizi
Farg‘ona davlat universiteti
Axborot- tizimlari va texnologiyalari yo‘nalishi II-kurs talabasi
yunusovadilrabo0613@gmail.com

Annotatsiya

Ushbu maqolada kompyuter tizimlari va tarmoqlarida axborotni himoyalash hamda kiberxavfsizlik sohasiga oid asosiy tushunchalar keng yoritilgan. Dastlab kiberxavfsizlikka turli manbalarda berilgan ta ‘riflar, xususan CSEC2017 Joint Task Force hamda Cisco kompaniyasi izohlarining mazmuni tahlil qilingan. Kiberxavfsizlikning shakllanish tarixi, uning texnik, tashkiliy va inson omillari bilan bog‘liq jihatlari hamda zamonaviy sharoitda raqamli hujumlarning ko‘payib borishi natijasida muhofaza choralarini qo‘llashning murakkablashuvi ochib berilgan. Maqolada konfidensiallik, yaxlitlik, foydalanuvchanlik kabi axborot xavfsizligining asosiy tamoyillari mazmunan tushuntirilgan, ularning amaliy ssenariylarda namoyon bo‘lishi misollar orqali ko‘rsatib berilgan. Shuningdek, risk, tahdid, zaiflik, boshqarish vositasi kabi xavfsizlikning fundamental atamalari o‘zaro bog‘liqlikda tahlil qilinib, axborot resurslarini himoyalashda ular muhim o‘rin tutishi asoslab berilgan. Maqola kiberxavfsizlikning nazariy asoslarini, amaliy jihatlarini hamda axborot tizimlari barqarorligini ta ‘minlashda zarur bo‘lgan tushunchalar majmuasini chuqur yoritishga qaratilgan.

Kalit so‘zlar: *kiberxavfsizlik, axborot xavfsizligi, konfidensiallik, yaxlitlik, foydalanuvchanlik, tahdid, zaiflik, risk, boshqarish vositasi, axborotni himoyalash, raqamli hujumlar, kompyuter tizimlari, tarmoq xavfsizligi, aktiv, axborot resurslari, xavfsizlik choralar, CSEC2017, kiberhujum, axborot tizimlari.*

Аннотация

В *данной статье представлен широкий обзор основных понятий защиты информации и кибербезопасности в компьютерных системах и сетях. В первую очередь анализируются определения кибербезопасности, приведенные в различных источниках, в частности, в материалах Совместной рабочей группы CSEC2017 и комментариях Cisco. Раскрываются история становления кибербезопасности, ее технические, организационные и человеческие аспекты, а также сложность применения защитных мер в связи с ростом цифровых атак в современных условиях. В статье объясняются основные принципы информационной безопасности, такие как конфиденциальность, целостность, удобство использования, и на примерах показывается их проявление в практических сценариях. Также анализируются в их взаимосвязи такие основополагающие термины безопасности, как риск, угроза, уязвимость и средства контроля, и обосновывается их важная роль в защите информационных ресурсов. Цель статьи – углубленно осветить теоретические основы кибербезопасности, практические аспекты и набор понятий, необходимых для обеспечения устойчивости информационных систем.*

Ключевые слова: *кибербезопасность, информационная безопасность, конфиденциальность, целостность, удобство использования, угроза, уязвимость, риск, инструмент управления, защита информации, цифровые атаки, компьютерные системы, сетевая безопасность, актив, информационные ресурсы, меры безопасности, CSEC2017, кибератака, информационные системы.*

Abstrakt

This article provides a broad overview of the basic concepts of information protection and cybersecurity in computer systems and networks. First, the definitions of cybersecurity given in various sources, in particular, the content of the CSEC2017 Joint Task Force and Ciscos comments, are analyzed. The history of the formation of cybersecurity, its technical, organizational and human factors aspects, and the complexity of applying protective measures due to the increase in digital attacks in modern conditions are revealed. The article explains the basic principles of information security such as confidentiality, integrity, usability, and their manifestation in practical scenarios is shown through examples. Also, the fundamental terms of security such as risk, threat, vulnerability, and control tools are analyzed in their interrelationships, and their important role in protecting information resources is substantiated. The article aims to provide in-depth coverage of the theoretical foundations of cybersecurity, practical aspects, and a set of concepts necessary to ensure the stability of information systems.

Keywords: *cybersecurity, information security, confidentiality, integrity, usability, threat, vulnerability, risk, management tool, information protection, digital attacks, computer systems, network security, asset, information resources, security measures, CSEC2017, cyberattack, information systems.*

Kompyuter tizimlari va tarmoqlarida axborotni himoyalash va axborot xavfsizligiga tegishli bo‘lgan ayrim tushunchalar bilan tanishib chiqaylik. Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo‘lib, unga berilgan turlicha ta’riflar mavjud. Xususan, CSEC2017 Joint Task Force manbasida kiberxavfsizlikka quyidagicha ta’rif berilgan. kiberxavfsizlik – hisoblashlarga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni to‘g‘ri bajarilishini kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonlarni mujassamlashtiradi. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o‘z ichiga oladi. Kiberxavfsizlik ta’limning mujassamlashgan bilim sohasi bo‘lib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o‘z ichiga oladi. Tarmoqlar sohasida faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta’rif bergan . Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarish, almashtirish yoki yo‘q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi. Hozirgi kunda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar soni va turlarining kattaligi va buzg‘unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda.

Kiberxavfsizlik bilim sohasining zaruriyati birinchi meynfreym kompyuterlar ishlab chiqarilgandan boshlab paydo bo‘la boshlagan. Bunda mazkur qurilmalarni va ularning vazifalari himoyasi uchun ko‘p qatlamli xavfsizlik choralari amalga oshirilgan. Milliy xavfsizlikni ta’minlash zaruriyatini oshib borishi kompleks va texnologik murakkab ishonchli xavfsizlik choralarini paydo bo‘lishiga olib keldi.Kiberxavfsizlikni fundamental atamalarini aniqlashga turli yondashuvlar mavjud. Xususan, CSEC2017 JTF manbasida mualliflar kiberxavfsizlikni quyidagi 6 atamasi keltirishgan

Konfidensiallik – axborot yoki uni eltuvchining shunday holati bo‘lib, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi. Konfidensiallik axborotni ruxsatsiz “o‘qish”dan himoyalash bilan shug‘ullanadi. AOB ssenariysida Bob uchun konfidensiallik juda muhim. Ya’ni, Bob o‘z balansida qancha pul borligini Tridi bilishini istamaydi. Shu sababli Bob uchun balans xususidagi ma ‘lumotlarning konfidensialligini ta ‘minlash muhim hisoblanadi.

Yaxlitlik - axborotning buzilmagan ko‘rinishida (axborotning qandaydir qayd etilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati. Yaxlitlik

axborotni ruxsatsiz “yozish”dan (ya’ni, axborotni 9 o‘zgartirishdan) himoyalash yoki kamida o‘zgartirilganligini aniqlash bilan shug‘ullanadi. AOB ssenariysida Alisaning banki qayd yozuvi butunligini Tididan himoyalashi shart. Masalan, Bob akkauntida balansning o‘zgarishi yoki Alisa akkauntida balansning oshishidan himoyalashi shart.Shu o‘rinda konfidensiallik va yaxlitlik bir narsa emasligiga e ‘tibor berish kerak. Masalan, Tridi biror ma ‘lumotni o‘qiy olmagan taqdirda ham uni sezilmaydigan darajada o‘zgartirishi mumkin. Foydaluvchanlik - avtorizasiyalangan mantiqiy obyekt so‘rovi bo‘yicha uning tayyorlik va foydalanuvchanlik holatida bo‘lishi xususiyati. Foydalanuvchanlik axborotni (yoki tizimni) ruxsatsiz “bajarmaslik”dan himoyalash bilan shug‘ullanadi. AOB ssenariysida AOB veb saytidan Bobning foydalana olmasligi Alisaning banki va Bob uchun foydalanuvchanlik muammosi hisoblanadi. Sababi, mazkur holda Alisa pul o‘tkazmalaridan daromad ola olmaydi va Bob esa o‘z biznesini amalga oshira olmaydi. Foydalanuvchanlikni buzishga qaratilgan hujumlardan eng keng tarqalgani – xizmat ko‘rsatishdan voz kechishga undovchi hujum (Denial of service, DOS)

Risk – potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi. ISO “risk – bu noaniqlikning maqsadlarga ta’siri” sifatida ta’rif bergan

Masalan, universitetga o‘qishga kirish jarayonini ko‘raylik. Umumiy holda bu jarayonni o‘zi risk hisoblanmaydi. Faqatgina abituriyent hujjatlarini va kirish imtihonlarini topshirganda, u o‘qishga kirishi yoki kira olmasligi mumkin. Bu o‘z navbatida qabul qilinish yoki qabul qilinmaslik riskini yuzaga kelishiga olib keladi. Kiberxavfsizlik yoki axborot xavfsizligida risklar salbiy ko‘rinishda qaraladi.Hujumchi kabi fikrlash - bo‘lishi mumkin bo‘lgan xavfni oldini olish uchun qonuniy foydalanuvchini hujumchi kabi fikrlash jarayoni.

Tizimli fikrlash - kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarning o‘zaro ta ‘sirini hisobga oladigan fikrlash jarayoni. Bundan tashqari quyidagi tushunchalar ham kiberxavfsizlik sohasini chuqur o‘rganishda muhim hisoblanadi.

Axborot xavfsizligi - axborotning holati bo‘lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta’sir etishga yoki ruxsatsiz undan foydalanishga yo‘l qo‘yilmaydi. Yoki, axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanish sathi holati. Axborotni himoyalash – axborot xavfsizligini ta’minlashga yo‘naltirilgan choralar kompleksi. Amalda axborotni himoyalash deganda ma’lumotlarni kiritish, saqlash, ishlash va uzatishda uning yaxlitligini, foydalanuv chanligini va agar, kerak bo‘lsa, axborot va resurslarning konfidensialligini madadlash tushuniladi.

Aktiv - himoyalanuvchi axborot yoki resurslar. Yoki, tashkilot uchun qimmatli barcha narsalar. Tahdid – tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan

hodisa. Yoki, tahdid - axborot xavfsizligini buzuvchi potensial yoki real mavjud xavfni tug‘diruvchi sharoit va omillar majmui. Tahdid tashkilotning aktivlariga qaratilgan bo‘ladi. Masalan, aktiv sifatida korxonaga tegishli biror bir saqlanuvchi hujjat bo‘lsa, u holda ushbu hujjat saqlanadigan xonaga nisbatan tahdid amalga oshirilish mumkin.

Zaiflik – bir yoki bir nechta tahdidlarni amalga oshirishga imkon beruvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik hisoblanadi. Masalan, xonada saqlanayotgan tashkilot hujjati qo‘g‘oz ko‘rinishda bo‘lganligi sababli, yonib ketishi mumkin.

Boshqarish vositasi – riskni o‘zgartiradigan harakatlar bo‘lib, boshqarish natijasi zaiflik yoki tahdidlarni o‘zgarishiga ta’sir qiladi. Bundan tashqari boshqarish vositasining o‘zi turli tahdidlar foydalanishi mumkin bo‘lgan zaiflikka ega bo‘lishi mumkin. Masalan, tashkilotda saqlanayotgan qog‘oz ko‘rinishidagi axborotni yong‘indan himoyalash uchun o‘chirish vositalari boshqarish vositasi sifatida ko‘rilishi mumkin. Bundan tashqari, yong‘in bo‘lganda xodimlarning xattixarakatlari va yong‘inni oldini olish bo‘yicha ko‘rilgan chora-tadbirlar ham boshqarish vositasi hisoblanishi mumkin. Yong‘inga qarshi kurashish tizimining ishlamay qolish holatiga esa boshqarish vositasidagi kamchilik sifatida qarash mumkin.

Xulosa

Keltirilgan ma’lumotlar shuni ko‘rsatadiki, kiberxavfsizlik bugungi raqamli davrda tashkilotlar, tarmoqlar va foydalanuvchilar faoliyati barqarorligini ta ‘minlashda eng muhim omillardan biriga aylanmoqda. Kompyuter tizimlari murakkablashib borayotgani, qurilmalar sonining ortishi va buzg‘unchilar imkoniyatlarining kengayishi xavfsizlik choralarini yanada puxta va ko‘p darajali bo‘lishini talab etadi. Kiberxavfsizlikning asosiy tamoyillari – konfidensiallik, yaxlitlik va foydalanuvchanlik – axborotning holatini to‘liq himoya qilishda markaziy o‘rinni egallaydi. Shuningdek, risklarni boshqarish, hujumchi kabi fikrlash va tizimli yondashuv xavfsizlikni samarali tashkil etishning muhim elementlaridir. Axborot xavfsizligi tushunchasi esa tahdidlar, zaifliklar va boshqaruv vositalari o‘zaro bog‘liqligini chuqur anglashni taqozo etadi. Umuman olganda, kiberxavfsizlik nafaqat texnik choralar, balki inson omili, siyosat, etik me‘yorlar va boshqaruv mexanizmlarini o‘zida mujassamlashtirgan keng qamrovli bilim sohasi bo‘lib, tashkilotlarning barqaror rivojlanishida strategik ahamiyat kasb etadi.

FOYDALANILGAN ADABIYOTLAR

1. CSEC2017 Joint Task Force. Curriculum Guidelines for Undergraduate Degree Programs in Cybersecurity. ACM, IEEE, 2017.
2. Cisco Systems. Cisco Cybersecurity Fundamentals. Cisco Press, 2020.
3. Stallings, W. Computer Security: Principles and Practice. Pearson, 2021.

4. Pfleeger, C., & Pfleeger, S. Security in Computing. Prentice Hall, 2015.
5. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection — Requirements. ISO, 2022.
6. Shon Harris. CISSP All-in-One Exam Guide. McGraw-Hill, 2019.
7. Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
8. Bishop, M. Introduction to Computer Security. Addison-Wesley, 2018.
9. NIST SP 800-30. Guide for Conducting Risk Assessments. National Institute of Standards and Technology, 2012.
10. NIST SP 800-53. Security and Privacy Controls for Information Systems and Organizations. NIST, 2020.