AXBOROTGA BO‘LADIGA XAVFLAR VA ULARNING TAHLILI

Мирзаахмедов Дилмурод Мирадилович –
“Рақамли иқтисодиёт ва ахборот технологиялари”
кафедраси катта ўқитувчи

Annotatsiya: Ushbu maqolada ma’lumotlar maxfiyligini xavf ostiga qo‘yishi mumkin bo‘lgan tahdidlar o‘rganiladi. Ushbu mavzu hozirgi vaqtda dolzarbdir, sababi biz noto‘g‘ri qo‘llarga tushib, egasiga zarar etkazishi mumkin bo‘lgan turli xil ma’lumotlarga to‘la zamonaviy raqamli dunyoda yashayapmiz. Maqolada tajovuzkorlar tomonidan ma’lumotlarni o‘g‘irlash usullari, bunday hujumlarga duchor bo‘lgan qurilmalar toifalari tahlil qilingan. Darhaqiqat, shaxsning, alohida kompaniyaning yoki butun jamiyatning axborot ma’lumotlari xavfsizligini shakllantirish uchun axborot xavfsizligiga mumkin bo‘lgan tahdidlar haqida tasavvurga ega bo‘lish talab etiladi.

Kalit so‘zlar: axborot xavfsizligi, zaifliklar, kiberhujumlar, korporativ ma’lumotlar, axborot xavfsizligi tahdidlari.

Kirish

Jamiyat taraqqiyoti haqida gapirganda, axborotni himoya qilish kabi muhim masala haqida unutmaslik kerak, bu esa iqtisodiyot va siyosatning ko‘plab tarmoqlari uchun yanada zaif va ahamiyatli bo‘lib qoldi. asosiy omillar: jamiyatni axborotlashtirish va texnologik taraqqiyotni jadallashtirish. Jamiyatni axborotlashtirish sharoitida biz eng yangi axborot texnologiyalari va axborot va kompyuter texnologiyalari, aloqa va telekommunikatsiya vositalarini tarqatish va joriy etish jarayonini tushunamiz, buning natijasida ma’lumot inson ongining mavhum, boshqarib bo‘lmaydigan sub’ekti bo‘lib qoladi. Zamonaviy sharoitda ma’lumot asosiy bo‘lgan tovarlar va mulkning barcha xususiyatlariga xosdir [1,2].

Iqtisodiyotning tarkibiy qismlari, bu uni juda boshqacha xarakterdagi (tijorat, ijtimoiy, jinoiy va boshqalar) manfaatlar ob’ektiga aylantiradi.

Hozirgi vaqtda eng qimmatli manba sifatida barcha turdagi ma’lumotlarga barqaror munosabat shakllangan. Bu zamonaviy jamiyatda axborot oqimlari hajmining misli ko‘rilmagan o‘sishi bilan izohlanadi. Bu, birinchi navbatda, jamiyat hayotini ta’minlashda muhim ahamiyatga ega bo‘lgan davlat faoliyatining sohalariga taalluqlidir: iqtisodiyot, fan, ta’lim, ijtimoiy soha va boshqalar. Bu sohalarning barchasi chambarchas kesishadi va har birining rivojlanishi foydalanilayotgan axborotning sifati, uning ishonchliligi va to‘liqligi, samaradorligi va taqdim etish shakli bilan bevosita bog‘liqdir. Shu bois axborot-kommunikatsiya texnologiyalaridan foydalanish asosida axborot resurslarini shakllantirish, ulardan foydalanish va muhofaza qilish muammolariga alohida e’tibor qaratish lozim.

Tizim sifatida u axborot xavfsizligi ob’ektlari, axborot xavfsizligini ta’minlovchi organlar (sub’ektlar) va axborotni himoya qilish vositalari kabi elementlardan iborat.

Axborot xavfsizligi ob’ektlari deganda, birinchi navbatda, axborotning o‘zi va uni uzatish kanallari tushuniladi. Shaxslar, ob’ektlar, tashkilotlar (korporativ ma’lumotlar) va boshqalar to‘g‘risidagi ma’lumotlarni o‘z ichiga oladi. Kengroq ma’noda ob’yektlar deganda shaxs (uning huquq va erkinliklari), jamiyat (uning moddiy va ma’naviy qadriyatlari) va davlat (uning suvereniteti, konstitutsiyaviy tuzumi va hududiy yaxlitligi) tushuniladi. Bu ob’ektlarning barchasiga jamiyat hayoti jarayonida doimo yuzaga keladigan axborot tahdidlari ta’sir qiladi.

Metodologiya

Ma’lumotlar yaxlitligining har qanday buzilishi axborot xavfsizligiga tahdid manbai deb ataladigan o‘z sababiga ega. Bu axborot xavfsizligiga tahdidning bevosita sababi bo‘lgan individual, moddiy ob’ekt yoki jismoniy hodisa hisoblanadi. Manba turiga ko‘ra, ular inson harakatlari bilan bog‘liq yoki aloqasiz bo‘lishi mumkin. Masalan, muhim fayl ma’lumotlarining yo‘qolishi foydalanuvchi tomonidan ma’lumotlarning noto‘g‘ri o‘chirilishi (inson faoliyati bilan bog‘liq) yoki dasturning ishdan chiqishi, yong‘in (inson faoliyatiga bog‘liq bo‘lmagan) va boshqalar natijasi bo‘lishi mumkin. O‘z navbatida, inson faoliyati bilan bog‘liq tahdidlar tasodifiy va ataylab sodir bo‘lgan tahdidlarga bo‘linadi. Bunda qasddan tahdid manbai bo‘lgan shaxs buzg‘unchi yoki hujumchi, bu tahdidni amalga oshirishga urinish esa hujum deb ataladi. Axborot xavfsizligiga tahdid – bu axborot xavfsizligi

buzilishining potentsial yoki haqiqiy xavfini yaratadigan shartlar va omillarning kombinatsiyasiga tushuniladi [3]. Rivojlangan axborot muhitiga ega davlatlar iqtisodiy va harbiy-siyosiy maqsadlarga erishish uchun axborot makonidagi o‘zlarining ustunliklaridan foydalanadilar. An’anaviy urush vositalari ancha qimmat, ta’sir qilishning axborot usullari esa ajoyib alternativ hisoblanadi. Ta’sir doirasi juda keng: davlat organlari ishini obro‘sizlantirishdan tortib, muhim infratuzilmaga zarba berishgacha. Bunday harakatlar majmuasini amalga oshirish mamlakatda nazoratni yo‘qotishga, iqtisodiy tanazzulga olib keladi va fuqarolik nizolarining paydo bo‘lishi uchun sharoit yaratadi.

Raqamli dunyo haqida gapirganda, uning o‘ziga xos belgisi axborotlashtirish bo‘lsa, raqamli ma’lumotlarning kiberxavfsizligi (kompyuter xavfsizligi) muhimligini ta’kidlab o‘tish zarur. Kiberxavfsizlik – bu kompyuterlar, serverlar, mobil qurilmalar, elektron tizimlar, tarmoqlar va ma’lumotlarni zararli hujumlardan himoya qilish usullari va amaliyotlari to‘plami [4].

Aytish joizki, axborot urushlari nafaqat davlatlar, balki korporatsiyalar, siyosatchilar, diniy tashkilotlar tomonidan ham olib borilmoqda [6]. Bu holatda asosiy qurol ommaviy axborot vositalaridir.

Hozirgi vaqtda, avionika, missiyani hisoblash va avtomobilni boshqarish kabi xavfsizlik uchun muhim tizimlarda ishlaydigan o‘rnatilgan dasturiy ta’minot asosan tashqi ogohlantirishlardan ma’lumot to‘plash va turli shovqinlarga o‘z vaqtida javob berish uchun ishlatiladi. Misol uchun, IEC61508 [7] xavfni baholash usullari to‘plamini taklif qiladi. Ko‘p sonli namunalar bilan simulyatsiya tajribasiga bog‘liq bo‘lgan vaqtinchalik nosozliklar bilan kurashish uchun Monte-Karlo simulyatsiyasi [8] kabi statistik asoslangan usul ishlatilgan. Tizimning real vaqt rejimida dasturiy ta’minot xatosiga bardosh berish doirasi [9] va nazorat punkti usuli va vaqtinchalik zaxiralash [10] dasturiy ta’minot ishonchliligini bashorat qilishning asosiy modellarini taqdim etadi. A. Berns va boshqalar [11] barcha vazifalar har doim belgilangan muddatlarda bajarilishi kerakligi haqidagi ehtimollik kafolatining bir qismi sifatida jadvalni tahlil qilishda ehtimollik modelini kiritdilar. I. Broster va boshqalar [12] javob vaqtining ehtimollik taqsimotidan muvaffaqiyatsizlik ehtimolining aniq bashoratlarini hisoblash uchun ushbu usulni CAN tarmog‘iga kengaytirdi. Biroq, bu yondashuvlar [11,12] ma’lum cheklovlarga ega va o‘ta pessimistik natijalarga olib keladi.

Tahlil

Kiberhujum – bu shaxs yoki tashkilot tomonidan boshqa odamlar yoki tashkilotlarning axborot tizimiga kirib borishga qaratilgan qasddan, zararli urinishdir. Kiberhujumni amalga oshiruvchi hujumchi xaker deb ataladi. Kiberhujum ta’siriga ko‘ra [5]:

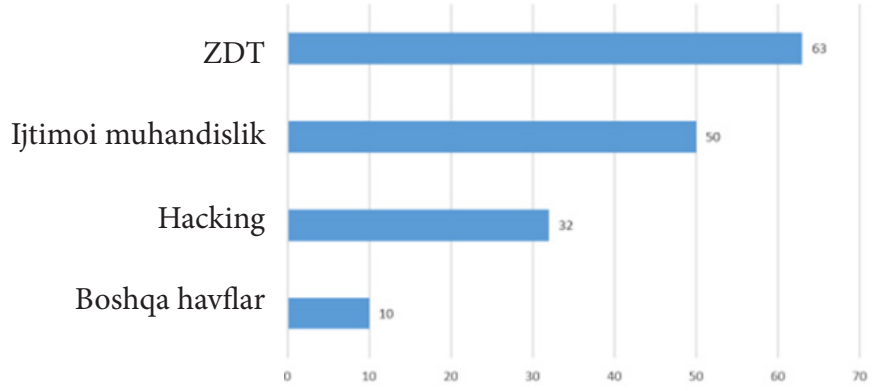
1. Zararli dasturiy ta’minot (ZDT): kompyuter qurilmalariga zarar etkazadigan virus dasturlari hisoblanadi. Zararli dastur alohida xizmatlar va qurilmalarning ishlashini sekinlashtiradi, ularning ishlashini nazorat qiladi, ma’lumotlarni to‘playdi, nusxalaydi yoki oxir oqibat yo‘q qilishgachon borishi mumkin.

2. Ijtimoiy muhandislik: tajovuzkorning maqsadlariga erishish uchun muayyan harakatlarni amalga oshirish uchun odamlar psixologiyasini manipulyatsiya qilish. “Fishing”, ya’ni elektron pochta va xabarlarni zararli kod bilan jo‘natish, axborot xavfsizligi nuqtai nazaridan unga tegishli bo‘lishi mumkin. “Jabrlanuvchi” ni infektsiyalangan havola orqali o‘tishga majbur qilish – bu sizning shaxsiy va to‘lov ma’lumotlaringizga kirish huquqiga ega bo‘lgan firibgarlarning asosiy vazifasi hisoblanadi.

3. “Hacking”: Xakerning axborot xavfsizligi ob’ektlarini buzishga qaratilgan qasddan harakatlari sifatida ta’riflangan. Dasturiy ta’minotdagi zaifliklarni qidirish va ulardan foydalanish bilan bog‘liq, ularni ishlab chiquvchilar o‘zlari hali aniqlamagan va ularni yo‘q qilishga ulgurmagan.

4. Hisob ma’lumotlarini tanlash (parollarni tanlash).

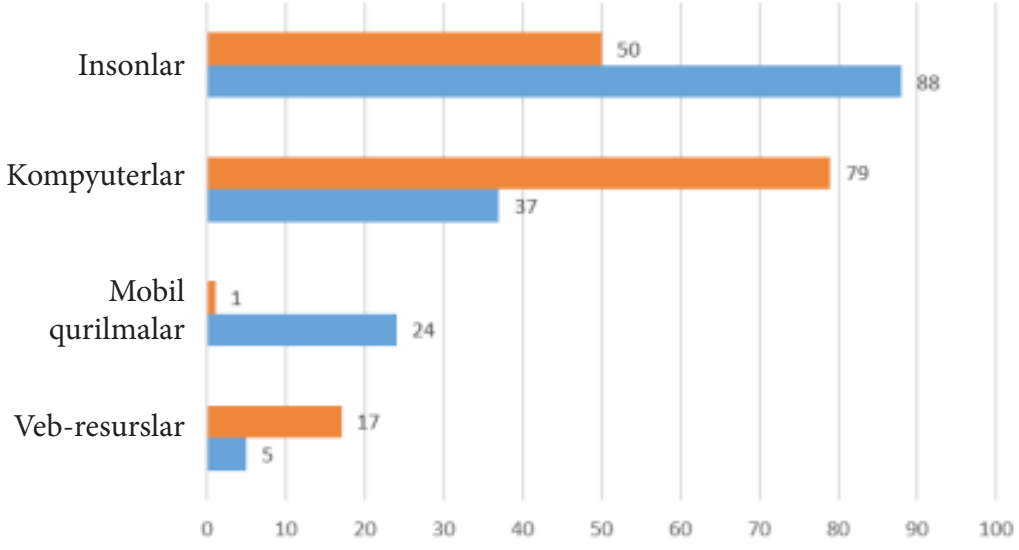
Tahdid ko‘pincha axborot tizimlarini himoya qilishda zaifliklar ya’ni (bo‘shliqlar) mavjudligi natijasidir. Zaiflik deganda, unda qayta ishlangan ma’lumotlarning xavfsizligiga tahdidlarni amalga oshirish imkoniyatini belgilovchi axborot tizimining mulki tushuniladi [3]. Misol sifatida – elektr uzilishlari tufayli ma’lumotlarning yo‘qolishi tahdidi. Ushbu tizim zaifligi qurilmalarni zaxira va uzluksiz quvvat manbalariga ulash orqali yo‘q qilinadi. Agar masalaning texnik bo‘lmagan tomoni haqida gapiradigan bo‘lsak, unda, masalan, ofisda, o‘z eshigini ochiq qoldirib, xodim korporativ sirni tashkil etuvchi muhim hujjatlarni o‘g‘irlash xavfini yaratadi. Albatta, bu xavfning manbai insondir.



1-rasm. Jahonda 2021 yil uchun hujumlar usullari [4]

1-rasmda tasvirlanganidek eng keng tarqalgan va ayni paytda eng xavfli tahdidlar zararli dasturlar va ijtimoiy muhandislik ekanligini ko‘rsatadi barcha zararli hujumlarning yarmidan ko‘pini tashkil qilmoqda.

Kompyuterlar, mobil qurilmalar va axborotni saqlash va ulardan foydalanishning boshqa vositalaridan foydalanuvchilarning barchasi kiberjinoyatchilar qurbonlariga aylanmoqda. Mobil qurilmalar va kompyuterdan tashqari, veb-resursga ham hujum qilish mumkin. Veb-resursga kelsak, xakerlarning maqsadi saytdagi ma’lumotlardan foydalanish yoki o‘zgartirishdir, bu veb-resurs egasi yoki sahifa foydalanuvchisining biznesiga zarar etkazishni mumkin. Shaxsiy va korporativ ma’lumotlar kompyuterdan o‘g‘irlanishi mumkin. Mobil qurilma uchun bu birinchi navbatda jismoniy shaxslarning shaxsiy ma’lumotlari hisoblanadi. Tajovuzkorning (ijtimoiy muhandislik) harakatlari odamlarni manipulyatsiya qilishga ham qaratilgan bo‘lishi mumkin.

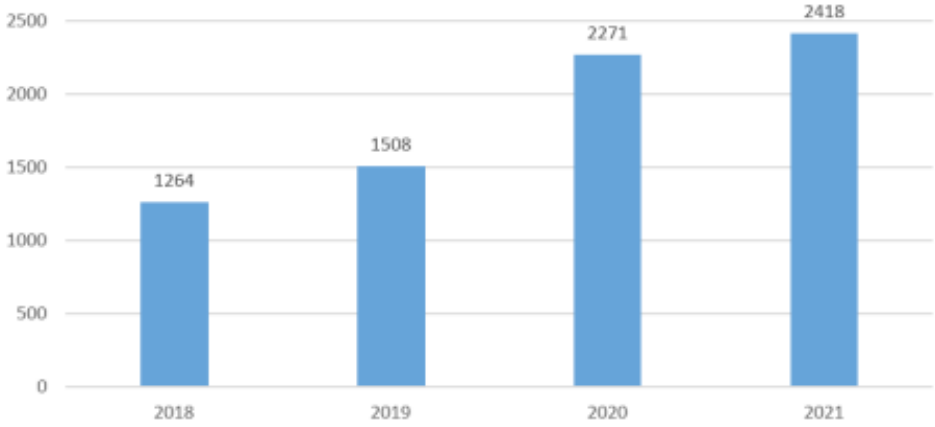


2-rasm. Hujum qilingan ob’yektlar foizi [4]

2-rasmda shaxslar yoki shaxslarga tegishli hujum qilingan ob’ektlarning bo‘linishini ko‘rish mumkin. Barcha hujumlarning qariyb 90% odamlarni manipulyatsiya qilish uchun shaxslarga qaratilgan. Virus hujumlarining 37% kompyuter tizimida amalga oshiriladi. 24% mobil qurilmalardagi ma’lumotlarga duch keldi va faqat 5% veb-resurslarga (foydalanuvchi sahifalariga) tegishliligi kursatilgan.

Yuridik shaxslar uchun biroz boshqacha. Korporativ ma'lumotlar kompyuterning qattiq disklari va serverlarida saqlanadi (mobil qurilmalar uchun 1% va kompyuterlar uchun 79%). Yuridik shaxslar uchun veb-resurslar moliyaviy nuqtai nazardan, tajovuzkorlar shaxsiy foydalanuvchilarning veb-sahifalariga qaraganda ko'proq (17%) qaraydigan biznesdir.

Aytish kerakki, hozirda axborot xavfsizligining dolzarbligi kiberhujumlar sonining ko'payishi bilan bog'liq. Bu 2020 yilda koronavirus tarqalishini to'xtatish bo'yicha ko'rilgan choralar natijasidir.



3-rasm. 2018-2021yillardagi hujumlar soni [4]

3-rasmga ko'ra, o'z-o'zini izolyatsiya qilish, masofadan ishlash, buyurtmalar uchun to'lov va boshqalar kabi choralarda yangi ilovalarning paydo bo'lishiga va shu bilan birgalikda hujumlar uchun yangi nishonlarning paydo bo'lishiga olib keldi. 2020-yilda kiberhujumlar soni 2019-yilga nisbatan 50 foizga oshganini tasdiqlaydi. Bu ko'rsatkich ijobiy tendentsiyaga ega, shunga qaramay, 2021-yilda hujumlar sonining o'sishi sekinlashdi (o'sish pandemiyagacha (2018-yil) 6 foiz edi,. -2019 yil) 19% ni tashkil etdi. Umuman olganda, 4 yil davomida kiberhujumlar soni 91 foizga oshganligini kurish mumkin.

5.Xulosa

Natijada, tizim sifatida axborot xavfsizligi axborot xavfsizligiga xavf soladigan tahdidlarsiz mavjud bo'lmaydi. Tez-tez sodir bo'ladigan tahdidlar odamlarning o'zlarining qasddan yoki tasodifiy harakatlaridan kelib chiqadi. Ushbu ro'yxatda ikkinchi o'rinda zararli dasturlar ko'rinishidagi xakerlik hujumlari. Mobil qurilma va veb-resurslar bilan taqqoslaganda aynan kompyuterlar xavf ostida ko'proq bo'ladi. Bu, ehtimol, tajovuzkor uchun ko'proq foyda bilan bog'liq, chunki korporativ ma'lumotlar kompyuterlarda saqlanishi mumkin. Bu esa aynan yuridik shaxslar axborot xavfsizligi tahdidlariga eng ko'p duchor bo'ladi, degan fikrga olib keladi.

Foydalanilgan adabiyotlar ro'yxati

1. Vasiliy Demin "Axborotni himoya qilish – muammo raqami 1". URL:http://www.it.ru/
2. Gerasimova V.G., Sorokina M.Yu. Bo'limni o'qitish masalasiga
"Intizom bilan axborot xavfsizligi vositalari" Axborot
marketingdagi texnologiyalar" Erkin iqtisodiy jamiyatning ma'ruzalari
Rossiya hukumati, 143-jild, Moskva, 2010 yil – 288–294-betlar
1. Suvorova, G.M. Axborot xavfsizligi: universitetlar uchun darslik. – M.:
Yurait nashriyoti, 2022. – 253 b.
3. GOST R 50922-2006. Rossiya Federatsiyasining milliy standarti. Ma'lumotlarni himoya qilish. Asosiy talablar va tushunchalar: tasdiqlangan. va Rostekhregulirovaniya tomonidan 2006 yil 27 dekabrdagi N 373-st qarori bilan kuchga kirgan // "Consultant Plus" huquqiy tizimi.
4. Kambulatov T.G. Tarmoqda kiberxavfsizlik / T.G. Kambulatov, S.I. Sodiqov // Aholining hayot sifati va ekologiya: Butunrossiya ilmiy-amaliy maqolalar to'plami. Konferentsiya, Penza, 2021 yil 30 okty-

abr. – Penza: Penza davlat agrar universiteti, 2021. – S. 44-47.
5. Haqiqiy kibertahdidlar: 2021 yil natijalari. // Ijobiy texnologiyalar. – [Elektron manba]. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecuritythreatscape-2021/ (Kirish: 05/03/2022).
6. Rossiya Federatsiyasining axborot xavfsizligi sohasidagi ilmiy tadqiqotlarning asosiy yo'nalishlaridan ko'chirma. – elektron. Dan. – Kirish rejimi: http://www.scrf.gov.ru/security/information/document155/ (kirish sanasi: 04/10/2018). – Sarlavha. ma'lumot ekranidan.
7. International Electrotechnical Commission (2010) Functional safety of electrical/electronic/ programmable electronic safety–related systems.
8. M. Sebastian, R. Ernst (2008) Modelling and Designing Reliable On-Chip-Communication Devices in MPSoCs with Real-Time Requirements. In: 13th IEEE International Conference on Emerging Technologies and Factory Automation, pp.1465-1472.
9. T. Anderson, J.C. Knight (1983) A Framework for Software Fault Tolerance in Real-Time Systems. IEEE Transactions on Software Engineering, SE-9(3): 355-364.
10. C. M. Krishna, A. D. Singh (1993) Reliability of Checkpointed real-time systems using time redundancy. IEEE Transactions on Reliability, 42(3): 427-435
11. A. Bums, S. Punnekkat, L. Strigini, D.R. Wright (1999) Probabilistic scheduling guarantees for fault-tolerant real-time systems. In: Dependable Computing for Critical Applications, pp.361-378
12. I. Broster, A. Burns, G. Rodriguez–Navas (2002) Probabilistic analysis of CAN with faults. In: 23rd IEEE Real-Time Systems Symposium, pp 269-278.

ANALYSIS OF MULTIMEDIA DISTANCE EDUCATION PLATFORMS IMPLEMENTED IN THE REPUBLIC OF UZBEKISTAN

Мирзакаримова Мухаббатхон Махмуд қизи –
Тошкент давлат иқтисодиёт университети Рақамли иқтисодиёт ва ахборот технологиялари кафедраси таянч докторанти, Ўзбекистон

Мадиева Зухра Искандарбековна –
Тошкент давлат иқтисодиёт университети Рақамли иқтисодиёт ва ахборот технологиялари кафедраси таянч докторанти, Ўзбекистон

Abstract: The age of information technology and advanced students sets new goals and objectives for education. On the one hand, digital tools help to solve them; on the other hand, they create new challenges. This study is aimed at studying the existing educational platforms in the Republic of Uzbekistan, identifying the pros and cons of each of the systems. The paper also presents electronic resources that used in the enrichment of the educational base of the platforms.

Keywords: e-learning, education, platform, distance learning, distance learning platform, electron resources, information technologies.

INTRODUCTION

Progress does not stand still, every day new methods and technologies appear in the world to make life easier for a person, including in the educational field. Education using modern information technologies is becoming more and more popular. With the development of educational systems, the demand for the use of digital technologies is increasing, elements of electronic and distance learning are being actively introduced. That is why the study of the possibilities of distance learning has recently attracted the active interest of many researchers and practitioners [1; 2; 3]. In addition to general issues, close attention is also paid to the use of distance learning technologies in the education system [4; 5].

According to UNESCO terminology, E-learning means learning using the Internet and multimedia, and distance learning means interaction in which the teacher and student are at a distance,