ELEKTRON BIZNESNING XAVFSIZLIGI MUAMMOLARI VA ULARNI YECHISH USULLARI

Ubaydullayev Oybek Ulug‘bekovich, Guliston davlat universiteti “Ta’limda axborot texnologiyalar” mutaxassisligi magistranti
e-mail: magistr2021yil@gmail.com

Annotatsiya. Elektron biznes xaridor va sotuvchi orasidagi aloqani tashkil etish, buyurtmani ifodalash, muhokama qilish, o‘zgartirish, tovarlarni va xizmatlarni sotish usullarini hamda to‘lovni amalga oshirish jarayonlarini o‘zgartirish uchun yangi texnologiyalardan foydalanadi. Hozirda elektron tijorat va biznesning aksariyat muammolari axborot xavfsizligi bilan bog’liq, ya’ni xavfsizlik muammolari elektron tijorat va biznes rivojidagi jiddiy to‘siq hisoblanadi. Har qanday tijorat kompaniyasining boshqa kompaniyalar bilan yoki ushbu kompaniyaning bo‘limlari orasida aloqa o‘rnatilishi zarur. Hozirda global Internet tarmog’i o‘zining uzellari o‘rtasida ishonchli va arzon axborot almashinuvini ta’minlaydi. Ochiq global Internet tarmog’i kanallaridan faol foydalanuvchi elektron biznesning ishlashi jarayonida ko‘pgina xavf-xatarlar paydo bo‘ladi

Kalit so‘zlar: elektron biznes, axborot xavfsizligi, kiberjinoyat, internet o‘g‘rilari, raqiblar.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО БИЗНЕСА И СПОСОБЫ ИХ РЕШЕНИЯ

Аннотация. Электронный бизнес использует новые технологии для организации связи между покупателем и продавцом, для выражения заказа, для резервирования, для изменения, для изменения способов продажи товаров и услуг, для изменения процессов оплаты. В настоящее время большинство проблем электронной коммерции и бизнеса связаны с информационной безопасностью, то есть проблемы безопасности являются серьезным препятствием в развитии электронной коммерции и бизнеса. Связь любой коммерческой компании с другими компаниями или между отделами этой компании необходима. В настоящее время глобальная сеть Интернет обеспечивает надежный и доступный обмен информацией между ее узлами. В процессе функционирования электронного бизнеса, активно использующего открытые каналы глобальной сети Интернет, возникает множество рисков.

Ключевые слова: электронный бизнес, информационная безопасность, киберпреступность, интернет-воры, оппоненты.

E-BUSINESS SECURITY PROBLEMS AND WAYS TO SOLVE THEM

Annotation. The electronicbusiness uses new technologies to organize communication between the buyer and the seller, to express the order, to make a reservation, to change, to change the methods of selling goods and services, and to change the processes of payment. Currently, most of the problems of e-commerce and business are related to information security, that is, security problems are a serious obstacle in the development of electroniccommerce and business.Communication between any commercial company with other companies or among the Departments of this company is necessary. Currently, the global Internet network provides reliable and affordable information exchange between its nodes. In the process of operation of an electronicbusiness that actively uses open global internet network channels, many risks arise.

Keywords: Electronic business, information security, cybercrime, internet thieves, opponents.

Kirish. Internetdan foydalanish kanallari kompaniyaning axborot resurslaridan chetdan foydalanishga imkon berishi mumkin. Kommunikatsion, xususan HTTP - protokol asosidagi dasturlardan ehtiyotsizlik bilan foydalanish axborot tizimining ishga layoqatligini buzuvchi va yoki axborot tizimi ma’lumotlarini buzuvchi maxsus dastur - "Troyan otlarining" kirishiga olib kelishi mumkin. Bu xil dasturlarning ichida viruslar eng ko‘p tarqalgan. O‘ziga xos malakali mutaxassislar korporativ axborot tarmoqlariga bilinmasdan kirish uchun ko‘pincha umummaqsad tarmoqlardan foydalanadilar.

Elektron qutisining tez-tez ishlatilishi niyati buzuq odamlarga elektron biznes bilan shug‘ullanuvchi tashkilot foydalananuvchilari nomlarini obro‘sizlantirishga yordam berishi mumkin. Foydalanuvchilar ma’lumotlarini (ismlar, parollar, PIN-kodlar va h.) saqlovchi tizimining zaif joylarini qidirishdan tarmoqda keng ishlatiluvchi maxsus dasturlardan foydalanish mumkin [1, 32-b.].

Internet konfidentsial axborotni dunyoning istalgan nuqtasiga yuborishi mumkin, ammo agar u yetarlicha himoyalanmagan bo‘lsa, ushlab qolinishi, nusxalashtirilishi, o‘zgartirilishi hamda har qanday chetdagi foydalanuvchilar -niyati buzuq odamlar, raqiblar va oddiy qiziquvchilar tomonidan o‘qilishi mumkin. Masalan, yetarlicha himoyalanmagan to‘lov topshirig‘i yoki kredit kartochka nomerini jo‘natayotganda esda tutish lozimki, jo‘natish xususiy/shaxsiy tarmoq orqali amalga oshirilmayapti va chetdagi foydalanuvchilar xabaringizni manipulyatsiya qilish imkoniyatiga ega. Undan tashqari xabaringiz almashtirilib qo‘yilishi mumkin: xabarlarni xuddi V foydalanuvchidan yuborilganidek A foydalanuvchidan yuborish usullari mavjud. Internet tarmog’i mahsus paket, tamomila qonuniy paketlar, sonining haddan tashqari ko‘pligi uzatishdagi buzilishlar, tarmoq komponentlarining nosozligi tufayli ishga layoqat bo‘lmasligi mumkin. Bunday hollar “xizmat qilishdan voz kechish” deb ataladi va elektron tijorat uchun eng jiddiy tahdid hisoblanadi.

Tadqiqot materiallari va metodologiyasi. Axborot xavfsizligi elektron biznes tizimining eng muhim elementlaridan biri hisoblanadi va usullar va vositalarning butun bir to‘plami yordamida ta’minlanishi shart. Elektron tijorat sohasidagi savdo ko‘lami Internet xavfsizligi masalalaridan tashvishlangan xaridorlar, sotuvchilar va moliya institutlarining boshidan kechiruvchi qo‘rquvlari bilan chegaralanadi. Bu qo‘rquvlar, hususan, quyidagilarga asoslanadi:

- konfidensiallikka kafolatning yo‘qligi-kimdir ma’lumotlaringizni uzatilayotganida ushlab qolishi va qiymatli axborotni (masalan, kredit kartochkangizning nomerini, tovar yetqazib berish sanasi va adres) topishga urinishi mumkin;

- amalda ishtirok etuvchilarni tekshirish darajasining yetarli emasligi - tranzaktsiya qatnashchilari tekshirilmaganida tomonlarning biri “maskarad” uyushtirishi mumkinki, uning oqibati ikkinchi tomonga ancha qimmatga tushadi. Masalan, xaridor saytga kirib undagi kompaniyaning haqiqiyligiga shubha qiladi, shunday hol ham ro‘y berishi mumkinki, xaridor kredit kartochkasining nomerini yetarlicha vakolatga ega bo‘lmagan shaxsga beradi;

- sotuvchida buyurtma bergan xaridor kredit kartochkasining qonuniy egasi ekanliginining tekshirish imkoni yo‘q;

- kredit kartochkasining bank - emitenti to‘lovni bajarishga talab qo‘ygan sotuvchini tekshirishni istab qolishi mumkin;

- ma’lumotlar yaxlitligiga kafolat yo‘q - xatto ma’lumotlarni jo‘natuvchi indentifikatsiyalangan bo‘lsada, uchinchi tomon ma’lumotlarni, ular uzatilishi vaqtida, o‘zgartirish imkoniyatiga ega. [2, 12-b.]

Tadqiqot natijalari. Axborot xavfsizligini ta’minlash nuqtayi nazaridan elektron tijoratning namunaviy qo‘llanilishini - Internet orqali mahsulotga va xizmatlarga ega bo‘lishni ko‘raylik. Ushbu jarayon quyidagi bosqichlar orqali ifodalanishi mumkin.

Buyurtmachi Web-server orqali mahsulot yoki xizmatni tanlaydi va mos buyurtmani rasmiylashtiradi.

Buyurtma magazinning buyurtmalar ma’lumotlari bankiga kiritiladi.

Buyurtma berilgan mahsulot yoki xizmatni olish mumkinligini ma’lumotlarning markaziy bazasi orqali tekshiriladi.

Agar mahsulotning olinishi mumkin bo‘lmasa, buyurtmachi u to‘g‘rida ogohlantiriladi va mahsulot yoki xizmatga ega bo‘lish jarayoni to‘xtatiladi. Mahsulotga so‘rov boshqa skladga (buyurtmachi roziligida) yo‘naltirilishi mumkin.

Agar maxsulot yoki xizmat mavjud bo‘lsa buyurtmachi to‘lovni tasdiqlaydi va buyurtma mos ma’lumotlar bazasiga kiritiladi. Elektron magazin mijozga buyurtma tasdig’ini yuboradi. Ko‘pgina xollarda (ayniqsa endigina ish boshlagan kompaniyalarda) buyurtmalar, tavarlarning borligini tekshirish va h. uchun yagona ma’lumotlar bazasi mavjud.

Mijoz onlayn rejimida buyurtma xaqini to‘laydi.

Tovar buyurtmachiga yetkaziladi.

Elektron tijorat bilan shug‘ullanadigan kompaniyalar yuqorida keltirilgan bosqichlarda duch keladigan tahdidlar quyidagilar:

elektron magazin Web-saytining sahifasini almashtirib qo‘yish. Bu tahdidni amalga oshirishning asosiy usuli - foydalanuvchi so‘rovini boshqa serverga yo‘llash. Bu tahdid oltinchi bosqichda buyurtmachi kredit kartochkasining nomerini kiritganda kuchayadi;

yolg’on buyurtmalar berish va elektron magazin xodimlari tomonidan firibgarlik qilish. Hozirda ichki/tashqi tahdidlar munosabati 60/40ni tashkil etadi;

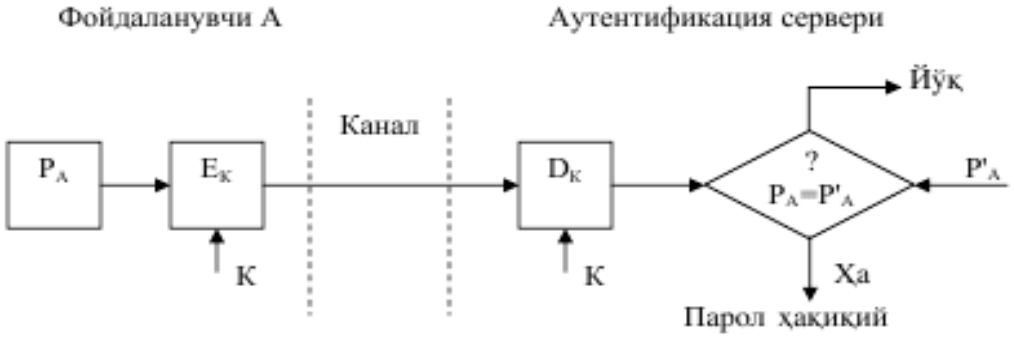
elektron tijorat tizimida uzatiladigan ma’lumotlarni ushlab qolish. Buyurtmachining kredit kartasi xususidagi axborotni ushlab qolish o‘zgacha xavf-xatarni tug‘diradi;

kompaniyaning ichki tarmog‘iga kirish va elektron magazin komponentlarini obro‘sizlantirish;

“xizmat qilishdan voz kechish” (denial of service) hujumini amalga oshirish va elektron tijorat ishlashini yoki uning uzelini buzish [3].

Ushbu tahdidlar natijasida kompaniya - elektron bitim provayderi - mijozlar ishonchini yo‘qotadi, moddiy zarar ko‘radi. Ba’zi hollarda bu kompaniyalarga kredit kartochka nomeri fosh qilingani uchun da’vo qo‘zg‘atilishi mumkin. “Xizmat qilishdan voz kechish” hujumi natijasida elektron magazinning ishlashi buzilishi mumkin, uning ishga layoqatligini tiklashga inson, vaqt va material resurslari talab etiladi.

Eng keng tarqalgan usul - foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Bunda fayllarga o‘qish va yozishdan himoyalash atributlari o‘rnatiladi (masalan, operatsion tizimdan foydalanishni nazoratlash ruyxatidagi mos imtiyozlarni tavsiflash yordamida). Tizim foydalanuvchi kiritgan parolni parollar faylida saqlanayotgan yozuv bilan solishtiradi. Bu usulda shifrlash yoki bir tomonlama funksiyalar kabi kriptografik mexanizmlar ishlatilmaydi. Ushbu usulning kamchiligi - niyati buzuq odamning tizimda ma’mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir.



1-rasm. Autentifikatsiya qilish sxemasi

Oddiy autentifikatsiyani tashkil etish sxemalari(1-rasm) nafaqat parollarni uzatish, balki ularni saqlash va tekshirish turlari bilan ajralib turadi. Eng keng tarqalgan usul – foydalanuvchilar parolini tizimli fayllarda, ochiq holda saqlash usulidir. Ushbu usulning kamchiligi - niyati buzuq odamning tizimda ma’mur imtiyozlaridan, shu bilan birga tizim fayllaridan, jumladan parol fayllaridan foydalanish imkoniyatidir.

Xavfsizlik nuqtai nazaridan parollarni bir tomonlama funktsiyalardan foydalanib uzatish va saqlash qulay hisoblanadi. Bu holda foydalanuvchi parolning ochiq shakli urniga uning bir tomonlama funktsiya h(.) dan foydalanib olingan tasvirini yuborishi shart. Bu o‘zgartirish g’anim tomonidan parolni uning tasviri orqali oshkor qila olmaganligini kafolatlaydi, chunki g’anim yechilmaydigan sonli masalaga duch keladi.

Ko‘p martali parollarga asoslangan oddiy autentifikatsiyalash tizi-mining bardoshligi past, chunki ularda autentifikatsiyalovchi axborot ma’noli so‘zlarning nisbatan katta bo‘lmagan to‘plamidan jamlanadi. Ko‘p martali parollarning ta’sir muddati tashkilotning xavfsizligi siyosatida belgilanishi va bunday parollarni muntazam ravishda almashtirib turish lozim. Parollarni shunday tanlash lozimki, ular lug‘atda bo‘lmasin va ularni topish qiyin bo‘lsin.

Bir martali parollarni generatsiyalash apparat yoki dasturiy usul oqali amalga oshirilishi mumkin. Bir martali parollar asosidagi foydalanishning apparat vositalari tashqaridan to‘lov plastik kartochkalariga o‘xshash mikroprotsessor o‘rnatilgan miniatyur qurilmalar ko‘rinishda amalga oshiradi. Odatda kalitlar deb ataluvchi bunday kartalar klaviaturaga va katta bo‘lmagan displey darchasiga ega.

Muhokama. Foydalanuvchilarni autentifikatsiyalash uchun bir martali parollarni qo‘llashning quyidagi usullari ma’lum:

1. Yagona vaqt tizimiga asoslangan vaqt belgilari mexanizmidan foydalanish.
2. Legal foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan tasodifiy parollar ruyxatidan va ularning ishonchli sinxronlash mexanizmidan foydalanish.
3. Foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan foydalanish.

Birinchi usulni amalga oshirish misoli sifatida SecurID autentikatsiyalash texnologiyasini ko‘rsatish mumkin. Bu texnologiya Security Dynamics kompaniyasi tomonidan ishlab chiqilgan bo‘lib, qator kompaniyalarning, xususan Cisco Systems kompaniyasining serverlarida amalga oshirilgan [4].

Vaqt sinxronizatsiyasidan foydalanib autentifikatsiyalash sxemasi tasodifiy sonlarni vaqtning ma’lum oralig‘idan so‘ng generatsiyalash algoritmiga asoslangan. Autentifikatsiya sxemasi quyidagi ikkita parametrdan foydalanadi:

• har bir foydalanuvchiga atalgan va autentifikatsiya serverida hamda foydalanuvchining apparat kalitida saqlanuvchi noyob 64-bitli sondan iborat maxfiy kalit; • joriy vaqt qiymati.

Autentifikatsiyaning bu sxemasi bilan yana bir muammo bog‘liq. Apparat kalit generatsiyalagan tasodifiy son katta bo‘lmagan vaqt oralig‘i mobaynida haqiqiy parol hisoblanadi. SHu sababli, umuman, qisqa muddatli vaziyat sodir bo‘lishi mumkinki, xaker PIN-kodni ushlab qolishi va uni tarmoqdan foydalanishga ishlatishi mumkin. Bu vaqt sinxronizatsiyasiga asoslangan autentifikatsiya sxemasining eng zaif joyi hisoblanadi [5].

Foydalanuvchini autentifikatsiyalash uchun bir martali paroldan foydalanishning uchinchi usuli foydalanuvchi va tekshiruvchi uchun umumiy bo‘lgan bir xil dastlabki qiymatli psevdotasodifiy sonlar generatoridan

foydalanishga asoslangan. Bu usulni amalga oshirishning quyidagi variantlari mavjud:

• o‘zgartiriluvchi bir martali parollar ketma-ketligi. Navbatdagi autentifikatsiyalash sessiyasida foydalanuvchi aynan shu sessiya uchun oldingi sessiya parolidan olingan maxfiy kalitda shifrlangan parolni yaratadi va uzatadi;

• bir tomonlama funktsiyaga asoslangan parollar ketma-ketligi. Ushbu usulning mohiyatini bir tomonlama funktsiyaning ketma-ket ishlatilishi (Lampartning mashhur sxemasi) tashkil etadi. Xavfsizlik nuqtai nazaridan bu usul ketma-ket o‘zgartiriluvchi parollar usuliga nisbatan afzal hisoblanadi.

XULOSA

Xulosa qilib shuni aytishimiz mumkinki, axborot texnologiyalaridan foydalanishning muhim xususiyati axborot resursini himoya qilish muammosini samarali hal etish zarurati bo‘lib, bu foydalanuvchilar o‘rtasida ma’lumotlarni himoya qilish choralarini tarqatishni nazarda tutadi. Axborot xavfsizligi tizimi-davlatning axborot sohasidagi siyosatini mamlakatda milliy xavfsizlikni ta’minlash davlat siyosati bilan chambarchas bog‘laydi. Bunda axborot xavfsizligi tizimi davlat siyosatining asosiy tashkil etuvchilarini yaxlit bir butunlikka biriktiradi. Bu esa axborot xavfsizligining roli va uning mamlakat milliy xavfsizligi tizimidagi mavqeini belgilaydi.

Axborot xavfsizligi sohasida davlat siyosatini amalga oshirishga imkon beruvchi sharoitlarni yaratish, mamlakatni iqtisodiy va ilmiy-texnikaviy taraqqiyotiga ko‘maklashish, axborotni muhofaza qilishning usul va vositalarini yaratish dolzarb masalalardan biridir.

Amaliyot shuni ko‘rsatadiki, axborotni muhofaza qilishda yetarli darajadagiyutuqlarga erishish uchun huquqiy, tashkiliy va texnik choralani birgalikda amalga oshirish zarur. Bu himoyalanadigan axborotning konfedensialligi, tahdidning tasnifi va himoya vositalarining mavjudligi bilan belgilanadi. Umumiy holda xavfsizlikni ta’minlashning kompleks choralariga:

- ruhsatsiz foydalanishdan kompleks himoya qilish vositalari;
- apparat-dasturiy vositalar;
- kriptografik muhofaza qilishning kompleks vositalari;
- injener-texnik tadbirlar;
- texnik kanallarni blokirovkalash kompleks vositalari;
- obyektlarni jismoniy qo‘riqlashni kiritish mumkin.

Bu choralarning har biri boshqasini to‘ldiradi, bironta usulning yo‘qligi yoki yetishmasligi yetarli darajadagi himayaning buzilishiga sabab bo‘lishi mumkin.

Foydalanilgan adabiyotlar

1. Девянин П.Н. Модели безопасности компьютерных систем. – М.: Академия, 2005.

2. KarimovI.M. Axborot xavfsizligi asoslari. – T.: IIV Akademiyasi, 2013.

3. S.K. G’aniev, Karimov M.M., Toshev K.A. «Axborot xavfsizligi. Axborot - kommunikatsion tizimlari xavfsizligi». – T.: Aloqachi, 2008.

4. Yuldashev U.A. Use of video lesson creative technologies in the process of electronic education/ / Scientific-Methodical Journal. – T., 2021.