AXBOROT TEXNOLOGIYALARI SOHASIDA SODIR ETILAYOTGAN HUQUQBUZARLIKLARNING TURLARI VA TAVSIFI

Esonov Elbek Sayfulla o‘g‘li
Toshkent shahar IIBB Shayxontohur tumani IIO FMB
1-sonli IIB HPB profilaktika inspektori leytenant

Annotatsiya. Ushbu maqolada axborot texnologiyalari (IT) sohasidagi turli xil qonunbuzarliklar ko'rib chiqiladi. Bu kiberhujumlar, ma'lumotlar buzilishi, zararli dasturlar, fishing va xakerlik kabi keng tarqalgan buzilishlarni chuqur tahlil qiladi. Maqolada, shuningdek, ushbu qoidabuzarliklarni sodir etish usullari va ularning oqibatlari muhokama qilinadi. Bundan tashqari, u it buzilishining oqibatlari haqida tushuncha beradi va xavflarni kamaytirish uchun profilaktika choralarini taklif qiladi.

Kalit So'zlar : Axborot texnologiyalari, qoidabuzarliklar, kiberxavfsizlik, ma'lumotlar buzilishi, zararli dastur, fishing, xakerlik.

Аннотация. В этой статье рассматриваются различные нарушения в области информационных технологий (ИТ). Он глубоко анализирует распространенные нарушения, такие как кибератаки, утечки данных, вредоносное ПО, фишинг и взлом. В статье также будут рассмотрены способы совершения этих нарушений и их последствия. Кроме того, он дает представление о последствиях расстройства собаки и предлагает профилактические меры для снижения рисков.

Ключевые слова: информационные технологии, нарушения, кибербезопасность, утечка данных, вредоносное ПО, фишинг, взлом.

Annotation. This article will consider various violations in the field of information technology (it). It provides an in-depth analysis of common disruptions such as cyberattacks, data corruption, malware, phishing, and hacking. The article will also discuss the methods of committing these violations and their consequences. In addition, it provides insight into the consequences of dog breakdowns and offers preventive measures to reduce risks.

Keywords: Information Technology, violations, cybersecurity, data corruption, malware, phishing, hacking.

Axborot texnologiyalari zamonaviy jamiyatning ajralmas qismiga aylandi, biz muloqot qilish, ishlash va biznes yuritish uslubimizni inqilob qildi. Biroq, ko'plab afzalliklari bilan bir qatorda, u turli xil muammolarni, shu jumladan xavfsizlikka tahdid va qoidabuzarliklarni keltirib chiqaradi. Ushbu qoidabuzarliklar raqamli ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini buzishga qaratilgan zararli harakatlarning keng doirasini qamrab oladi. Undagi turli xil buzilishlarni tushunish

raqamli aktivlarni himoya qilish va xavflarni kamaytirish bo'yicha samarali strategiyalarni ishlab chiqish uchun juda muhimdir.

Ko'plab tadqiqotlar va hisobotlar axborot texnologiyalarida buzilishlarning tarqalishi va ta'sirini ta'kidladi. Kiberxavfsizlikni buzish, ma'lumotlarni o'g'irlash va boshqa zararli harakatlar tobora keng tarqalgan bo'lib, butun dunyo bo'ylab shaxslar, korxonalar va hukumatlarga ta'sir ko'rsatmoqda. Tadqiqotchilar zararli dasturlarning infektsiyalari, fishing hujumlari, xakerlik hodisalari va ichki tahdidlar kabi turli xil buzilishlarni aniqladilar. Ushbu qoidabuzarliklar it tizimlari va tarmoqlaridagi zaifliklardan foydalanadi, bu moliyaviy yo'qotishlarga, obro'ga zarar etkazishga va huquqiy oqibatlarga olib keladi.

Axborot texnologiyalari sohasidagi buzilishlar juda xilma-xil bo'lishi mumkin va xavfsizlik, maxfiylik, intellektual mulk huquqlari va tartibga rioya qilishning buzilishini o'z ichiga olishi mumkin. Bu erda tavsiflar bilan birga buzilishlarning ba'zi keng tarqalgan turlari mavjud:

- Kiberxavfsizlik buzilishi: bular kompyuter tizimlari, tarmoqlari yoki ma'lumotlariga ruxsatsiz kirish imkoni paydo bo'lganda, ko'pincha ma'lumotlar o'g'irlanishi, xizmatlarning uzilishi yoki tizimlarning shikastlanishiga olib keladi. Masalan, xakerlik, zararli dastur infektsiyalari va xizmatni rad etish hujumlari.
- Ma'lumotlar buzilishi: bu shaxsiy ma'lumotlar, moliyaviy yozuvlar yoki intellektual mulk kabi maxfiy yoki maxfiy ma'lumotlarga ruxsatsiz kirish, oshkor qilish yoki sotib olishni o'z ichiga oladi. Buzilishlar xakerlik, ijtimoiy muhandislik yoki insayder tahdidlari tufayli yuzaga kelishi mumkin.
- Maxfiylikni buzish: bu shaxslarning shaxsiy ma'lumotlari ularning roziligisiz yoki maxfiylik qonunlari yoki siyosatini buzgan holda to'planganda, foydalanilganda yoki oshkor qilinganda yuzaga keladi. Masalan, onlayn faoliyatni roziligisiz kuzatish, shaxsiy ma'lumotlarni uchinchi shaxslarga sotish yoki ma'lumotlarni etarli darajada himoya qilmaslik.
- Intellektual mulk bilan bog`liq o'g'irlik: bu mualliflik huquqi bilan himoyalangan materiallar, savdo belgilari, patentlar yoki savdo sirlarini ruxsatsiz ishlatish, ko'paytirish yoki tarqatishni o'z ichiga oladi. U dasturiy ta'minotni qaroqchilik, plagiat, qalbakilashtirish yoki teskari muhandislik xususiy texnologiyasini o'z ichiga olishi mumkin.
- Muvofiqlikni buzish: bu tashkilotlar ma'lumotlardan foydalanish, saqlash yoki uzatishni tartibga soluvchi huquqiy, me'yoriy yoki sanoat standartlariga rioya qilmasa sodir bo'ladi. Masalan, ma'lumotlarni himoya qilish qonunlariga rioya qilmaslik sanoat qoidalari yoki shartnoma shartnomalari.
- Ichki tahdidlar: bular tashkilot ichidagi shaxslar, masalan, xodimlar, pudratchilar yoki biznes sheriklar tomonidan zararli yoki beparvo harakatlarni o'z ichiga oladi.

Insider tahdidlari ma'lumotlarni o'g'irlash, sabotaj yoki tizimlar va ma'lumotlarga ruxsatsiz kirishni o'z ichiga olishi mumkin.

- Ijtimoiy muhandislik hujumlari: bular maxfiy ma'lumotlarni oshkor qilish yoki xavfsizlikni buzadigan harakatlarni amalga oshirish uchun odamlarni manipulyatsiya qilishni o'z ichiga oladi. Misollar fishing elektron pochta o'z ichiga oladi, pretexting qo'ng'iroqlar, yoki impersonation scams.
- Zararli dastur: bunga viruslar, qurtlar, troyanlar, to'lov dasturlari va kompyuter tizimlari yoki ma'lumotlarini buzish, buzish yoki ruxsatsiz kirish uchun mo'ljallangan boshqa zararli dasturlar kiradi.
- Firibgarlik: bu boshqa birovning shaxsiy ma'lumotlaridan moliyaviy foyda yoki boshqa zararli maqsadlarda ruxsatsiz foydalanishni o'z ichiga oladi. Bu kredit karta firibgarligi, shaxsni o'g'irlash yoki onlayn operatsiyalarda o'zini taqlid qilishni o'z ichiga olishi mumkin.
- Tasodifiy xatolar va noto'g'ri konfiguratsiya: bular inson xatosi, nazorat yoki xavfsizlik amaliyotining etarli emasligi tufayli yuzaga keladi, bu ma'lumotlarning tasodifiy oqishi, tizimning zaifliklari yoki xizmatlarning buzilishiga olib keladi.

Ushbu qoidabuzarliklar jiddiy oqibatlarga olib kelishi mumkin, jumladan moliyaviy yo'qotishlar, obro'ga etkazilgan zarar, qonuniy majburiyatlar va mijozlarning ishonchini buzish. Shu sababli, tashkilotlar xavflarni kamaytirish va maxfiy ma'lumotlarni samarali himoya qilish uchun kiberxavfsizlik choralarini, xodimlarni o'qitishni va tegishli qoidalarga rioya qilishni birinchi o'ringa qo'yishlari kerak.

Topilmalar shuni ko'rsatadiki, it buzilishi tashkilotlar va shaxslar uchun katta xavf tug'diradi. Ushbu qoidabuzarliklar moliyaviy yo'qotishlarga, obro'ga zarar etkazishga, qonuniy majburiyatlarga va tartibga soluvchi jarimalarga olib kelishi mumkin. Bundan tashqari, ular raqamli texnologiyalarga bo'lgan ishonchni susaytiradi va innovatsion echimlarni qabul qilishga to'sqinlik qiladi. It buzilishlarini bartaraf etish texnik kafolatlar, xodimlarni o'qitish, tartibga rioya qilish va manfaatdor tomonlar o'rtasidagi hamkorlikni o'z ichiga olgan ko'p qirrali yondashuvni talab qiladi. Tashkilotlar rivojlanayotgan tahdidlardan himoya qilish uchun xavfsizlik devorlari, shifrlash, kirishni aniqlash tizimlari va xavfsizlikni anglash dasturlari kabi kiberxavfsizlik choralariga sarmoya kiritishlari kerak. Bundan tashqari, hukumatlar va nazorat qiluvchi organlar muhim infratuzilma va nozik ma'lumotlarni himoya qilish uchun kiberxavfsizlik standartlarini o'rnatish va amalga oshirishda hal qiluvchi rol o'ynaydi.

Xulosa va takliflar:

Axborot texnologiyalaridagi buzilishlar raqamli tizimlar va tarmoqlarning xavfsizligi va yaxlitligiga jiddiy qiyinchiliklar tug'diradi. Tashkilotlar va shaxslar kiberxavfsizlik xavfini aniqlash va kamaytirishda hushyor va faol bo'lishlari shart. Keng qamrovli xavfsizlik choralarini amalga oshirish, xabardorlikni oshirish va

kiberxavfsizlik madaniyatini rivojlantirish orqali biz raqamli asrda o'sib borayotgan tahdidlardan o'zimizni yaxshiroq himoya qila olamiz. Davlat va xususiy sektor o'rtasidagi hamkorlik kiberxavfsizlik muammolarini samarali hal qilish va hamma uchun xavfsizroq raqamli muhitni targ'ib qilish uchun juda muhimdir.

Kelajakdagi tadqiqotlar axborot texnologiyalarida paydo bo'layotgan tahdid va zaifliklarni o'rganishga, shuningdek, turli kiberxavfsizlik choralari va strategiyalarining samaradorligini baholashga qaratilishi kerak. Bundan tashqari, it buzilishlarining tashkilotlarga va umuman jamiyatga uzoq muddatli ta'sirini baholash uchun bo'ylama tadqiqotlar o'tkazish zarur. Bundan tashqari, tadqiqot ishlari kiberxavfsizlikning barqarorligini oshirish va rivojlanayotgan kiber tahdidlar bilan bog'liq xavflarni kamaytirish uchun innovatsion echimlar va texnologiyalarni ishlab chiqishga yo'naltirilishi kerak.

Adabiyotlar.

1. Antonyan Yu.M., Yenikeev M.I., Eminov V.E. Psychology of the criminal and investigation of crimes, Moscow: Yurist, 2006, 190 p (in Russian).

2. Law of the Republic of Uzbekistan «On Informatization» from 11 December 2003 the year number 560-II (in Russian).

3. Kardava N.V. Cyberspace as a new political reality: challenges and answers // History and modernity. 2018. no. 1-2-P. 27-28 (in Russian).

4. Report of the United Nations Office on drugs and crime «Cybercrime and COVID19 coronavirus: risks, threats and responses» (source available at: https://www.unodc.org/documents/Advocacy-Section/Russian_-_UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS1COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf)

5. Baxtiyor ogli, R. I. (2023). Methods for searching and using maps using internet resources in geography lessons. *Journal of Universal Science Research*, *1*(11), 545-548.

6. Baxtiyor o'g'li, R. I. (2023). UMUMTA'LIM MAKTABLARIDA GEOGRAFIYANI O'QITISHNING ZAMONAVIY TA'LIM VOSITALARIDAN FOYDALANISH.

7. http://www.psyfactor.org/

8. https://runet.rbc.ru/materials/pravda-o-feyk-nyus/