



Sadakat ABDIRAZZAKOVA,
Toshkent axborot texnologiyalari universiteti katta o'qituvchisi
E-mail: aasadokat@gmail.com

O'zDSMI dotsenti, f.f.d G.Isakova taqrizi asosida

KIBERXAVFSIZLIK TERMINLARINING PRAGMATIK XUSUSIYATLARI

Аннотация

Ushbu maqolada kiberxavfsizlik terminlari va ularning pragmatik xususiyatlari borasida so'z yuritiladi. Hozirgi kunda kiberxavfsizlik muhim ahamiyatga ega bo'lib, uning ijtimoiy, iqtisodiy va siyosiy jihatlarini jamiyatga katta ta'sir ko'rsatadi. Bu sohadagi terminlarni to'g'ri tushunish va ularni lingvistik nuqtai nazardan tahlil qilish muhim ahamiyatga ega.

Kalit so'zlar: termin, terminologiya, axborot texnologiyalari, kiberxavfsizlik, internet, kompyuter, lingvistika, pragmatika, tahlil.

ПРАГМАТИЧЕСКИЕ ОСОБЕННОСТИ ТЕРМИНОВ КИБЕРБЕЗОПАСНОСТИ

Аннотация

В этой статье рассматриваются термины кибербезопасности и их прагматические особенности. В настоящее время кибербезопасность очень важна, а также ее социальные, экономические и политические аспекты оказывают большое влияние на общество. Важно правильно понимать термины в этой области и анализировать их с лингвистической точки зрения.

Ключевые слова: термин, терминология, информационные технологии, кибербезопасность, интернет, компьютер, лингвистика, прагматика, анализ.

PRAGMATIC CHARACTERISTICS OF CYBER SECURITY TERMS

Annotation

This article discusses cyber security terms and their pragmatic features. Nowadays, cyber security is important, and its social, economic and political aspects have a great impact on society. It is important to correctly understand the terms in this sphere and analyze them from a linguistic point of view.

Key words: term, terminology, information technology, cyber security, internet, computer, linguistics, pragmatics, analysis.

Kirish. Ma'lumki, ilmiy adabiyotlarda terminga nisbatan ko'plab ta'riflar keltirilgan. Termin ma'lum bir tilning so'z, so'z birikmasi, qisqartma, belgi shaklida taqdim etilgan, maxsus terminologik ma'noga ega bo'lgan, ilmiy tushunchaga mos keladigan leksik birligi, ya'ni ifoda jihatidan mantiqiy-konseptual tizimning birligi hisoblanadi.

Tilshunos A.A.Reformatskiy terminga quyidagicha ta'rif bergan: "Terminlar maqsadiga ko'ra, chegaralangan maxsus so'zlardir; tushunchalarning aniq ifodasi va narsalarning nomi sifatida bir ma'noli bo'lishga intiladigan so'zlardir". Muallifning ta'kidlashiga ko'ra, termin fan, texnologiya, siyosat va diplomatiyada zarur. Terminlar nafaqat tilda, balki ma'lum bir terminologiyaning bir qismi sifatida mavjud. Agar umumiy tilda (ma'lum terminologiyadan tashqarida) so'z polisemantik bo'lishi mumkin bo'lsa, u ma'lum bir terminologiyada bir ma'noga ega bo'ladi [10].

Terminlar yoki terminologik so'zlar ma'lum bir bilim sohasida qo'llaniladi. Birgina termin ba'zan ma'lum bir tilning turli terminologiyalarida uchraydi, bu bizga fanlararo terminologik omonimiya haqida gapirish imkonini beradi, ya'ni terminlar turli xil terminologiyada foydalanish kontekstiga qarab o'z ma'nosini o'zgartirishi mumkin.

Ko'plab zamonaviy terminlar bir nechta tarkibiy qismlardan iborat. Ular predlogsiz yoki predlog yordamida bog'langan semantik so'z birikmalari sifatida qabul qilinadi. Terminshunos A.B.Borkovskiyning fikriga ko'ra, ko'p komponentli termin so'z birikmasi bo'lishi mumkin, ulardagi komponentlar o'rtasidagi bog'liqlik bitishuv yoki predlog qo'shimchalarni o'zgartirish yordamida ifodalanadi [3].

Umuman olganda, terminlarga berilgan mavjud tasniflar terminologik tizimlarni tartibga solish, terminologik birliklarni boshqa leksik birliklardan ajratish va asosiy terminologik so'zlarni ajratib ko'rsatish uchun mo'ljallangan.

Mavzuga oid adabiyotlar tahlili. Rus tilshunosligida virtual nutqning lingvistik xususiyatlariga doir masalalar (Asmus, 2005), internet diskursining o'ziga xos xususiyatlari (Galkin, 2013; Gorina, 2015; Lazareva, 2010; Axrenova, 2016), shuningdek, kompyuter diskursi tahlili (Leontovich, 2015), ilmiy gipermediya diskursiga oid (Yegorova, 2011) hamda tarmoq diskursi va gipermatn aloqasi (Morgun, 2002) kabi muammolarga doir tadqiqotlar mavjud.

Xorij tilshunosligida kompyuter diskursi tahliliga doir Syuzan Xerringning "Computer-mediated discourse analysis: an approach to researching online communities" (2004) nomli maqolasi, Xerring va Androustopouloslarning "Computer-mediated discourse" (2015) nomli qo'llanmasi, Boyd Devisning elektron nutqqa doir "Electronic Discourse: Linguistic Individuals in Virtual Space" (1997) nomli qo'llamasi, Jon Sulerning "Computer and cyberspace "addiction" (2004) kabi ilmiy manbalarda ba'zi muammolar yoritilgan [11].

Shuningdek, ko'plab olib borilgan tadqiqotlar pedagogikada, tilshunoslik va boshqa sohalarida axborot texnologiyalaridan foydalanishga yoki iqtisodiy faoliyat turlarida axborot-kommunikatsiya texnologiyalaridan foydalanish xususiyatlariga bag'ishlangan.

Tadqiqot metodologiyasi. Bilamizki, til jadal rivojlanib bormoqda, zamonaviy tilning rivojlanishi bilan birga sinonimik terminlar, ya'ni bir xil yoki o'xshash ma'noni

anglatib, turli kontekstlarda ishlatiladi, masalan, computer ethics/netiquette (kompyuter etikasi, tarmoq etikasi), cybersecurity/information security (kiberxavfsizlik, axborot xavfsizligi), phishing/spoofing (firibgarlik, soxtalashtirish) va dublet terminlar, ya'ni turli manbalardan kirib kelgan yoki bir vaqtning o'zida bir-birini to'ldiruvchi so'zlar bo'lib, bir ma'noni anglatadi: hard disk va rigid disk (qattiq disk), cloud security/cloud computing security (bulutli xizmatlardagi ma'lumotlarni himoya qilish) kabi terminlarni keltirish mumkin. Bu kabi sohaga kirib kelayotgan terminlarni tadqiq etish, ularning shakllanish omillarini o'rganish muhim sanaladi.

Hozirgi kunda ilm-fandagi mavjud sohalaridan farqli o'laroq axborot texnologiyalari sohasidagi terminlarni shakllanishiga bag'ishlangan tizimli va izchil ilmiy tadqiqotlar mavjud emas. Ushbu mazmunda faqatgina ma'lum darajadagi ishlar, lingvistik va ixtisoslashtirilgan jumallardagi maqolalarni va internet saytlaridagi ma'lumotlarni ko'rish mumkin.

Tahlil va natijalar. Quyida kiberxavfsizlik terminlarining pragmatik xususiyatlariga to'xtalib o'tiladi. Ma'lumki, pragmatika – tilning real dunyoda qanday qo'llanilishini o'rganuvchi fan. Kiberxavfsizlik terminlarining pragmatikasi ularning amaliy qo'llanilishini, kontekstga bog'liq ravishda qanday ma'noga ega bo'lishini o'rganishga qaratilgan. Masalan, kiberxavfsizlikda faol qo'llanuvchi "phishing" (fishing) termini oddiy baliq ovlashni emas, balki internetdagi firibgarlikni anglatib, elektron pochta orqali shaxsiy ma'lumotlarni qo'lga kiritish usulini ifoda etadi. Bu terminning pragmatik talqini uning foydalanuvchilarga yetkazadigan xavfini va uning oldini olish choralarini o'rganishni o'z ichiga oladi.

Demak, pragmatik tahlil o'z mohiyatiga ko'ra tushunchalarning amaliy jihatlarini, ular ishlatiladigan kontekstlarni va ularning funksional jihatlarini o'rganish demakdir. Shunga ko'ra, ba'zi kiberxavfsizlik terminlarining pragmatik tahlillarni keltirishga harakat qilamiz.

Accountability – javobgarlik. Mazkur termin amaliy jihatdan tizimda amalga oshirilgan har bir harakat kim tomonidan va qachon amalga oshirilganligini kuzatish imkonini beradi hamda uning qo'llanilish sohasi asosan, axborot xavfsizligi, IT audit bo'lib, kontekstda tizimdagi harakatlarni kuzatib borish xavfsizlik nazorati va audit jarayonlarida qo'llaniladi.

Adversary – dushman. Ushbu terminning amaliy jihati, tarmoq uchun tahdidga ega bo'lgan subyektlarni aniqlash va ularga qarshi himoya choralarini qo'llash imkonini beradi. Terminning qo'llanilish sohasi asosan, kiberxavfsizlik, tarmoq monitoringi hisoblanadi hamda kontekstda tarmoq xavfsizligi va kiberhujumlarni aniqlash uchun qo'llaniladi.

Data breach - ma'lumotlarning buzilishi. Ruqsatsiz kirish yoki oshkor qilish natijasida maxfiy ma'lumotlarning yo'qolishini anglatadi. Termin amaliy jihatdan kompaniyalar va foydalanuvchilarga katta moliyaviy va huquqiy zarar yetkazadini ifodalaydi.

Adware – reklama dasturi. Mazkur termin amaliy jihatdan foydalanuvchilarga reklama taqdim etadi va marketing maqsadlarida ma'lumotlarni to'playdi. Terminning qo'llanilish sohasi kompyuter xavfsizligi va reklama boshqaruvi bo'lib, kontekstda foydalanuvchi tajribasini buzish hamda maxfiylikni buzish ma'nosini anglatadi.

Cyberattack – kiberhujum. Mazkur termin kompyuter tizimlariga yoki tarmoqlarga qaratilgan ruqsatsiz hujum ma'nosini anglatib, amaliy jihatdan ma'lumotlarni o'g'irlash, buzish yoki tizimni ishdan chiqarishga mo'ljallangan.

Anonymity – anonimlik. Ushbu termin amaliy jihatdan ishtirokchilarga o'zini identifikatsiyalamasdan harakat qilish imkonini beradi. Uning qo'llanilish sohasi kiberxavfsizlik va shaxsiy ma'lumotlar himoyasi bo'lib, kontekstda maxfiylikni ta'minlash, anonim onlayn faoliyat olib borishni anglatadi.

Antibot – antibot. Termin amaliy jihatdan robot-dasturlar va zararli dasturlarni aniqlash hamda yo'q qilish uchun ishlatiladi. U asosan, kiberxavfsizlik va antivirus dasturlarida qo'llanib, kontekstda tarmoq xavfsizligi hamda zararli dasturlarga qarshi himoyani anglatadi.

Encryption – shifrlash. Termin ma'lumotlarni ruqsatsiz o'qishdan himoya qilish uchun kodlash jarayoni ifodalaydi va amaliy jihatdan ma'lumotlar maxfiylikni saqlash va faqat vakolatli foydalanuvchilar uchun ochiqlashni ta'minlaydi.

Ransomware - shantaj dasturi. Ushbu termin foydalanuvchining ma'lumotlarini shifrlab qo'yib, ularni ochish uchun to'lov talab qiladigan zararli dastur ma'nosini anglatib, amaliy jihatdan moliyaviy zarar yetkazish va tizimlar ishini buzishga qaratilgan.

Anti-forensics – anti-kriminalistika. Mazkur termin amaliy jihatdan dalillarni tahlil qilish va tekshirishni qiyinlashtiradi yoki imkonsiz qiladi. Termin kiberxavfsizlik va jinoyat tekshiruvi yo'nalishlarida qo'llanilib, kontekstda jinoyat dalillarini yashirish va yo'q qilish ma'nosini anglatadi.

Malware - zararli dastur. Kompyuterlarga yoki tarmoqlarga zarar yetkazish uchun mo'ljallangan dasturiy ta'minot. Pragmatik xususiyati: Foydalanuvchilarning maxfiy ma'lumotlarini o'g'irlash, tizimlarni ishdan chiqarish yoki ularni manipulyatsiya qilish uchun ishlatiladi.

Anti-spoof – anti-spufing. Terminning amaliy jihati, qonuniy identifikatsiya va autentifikatsiya ma'lumotlarini noqonuniy foydalanishdan himoya qiladi. Termin kiberxavfsizlik va autentifikatsiya tizimlarida qo'llaniladi va kontekstda tizimlarga ruqsatsiz kirishni oldini olish imkoniga ega.

Malware - zararli dastur. Kompyuterlarga yoki tarmoqlarga zarar yetkazish uchun mo'ljallangan dasturiy ta'minot. Pragmatik xususiyati: Foydalanuvchilarning maxfiy ma'lumotlarini o'g'irlash, tizimlarni ishdan chiqarish yoki ularni manipulyatsiya qilish uchun ishlatiladi.

Antivirus – antivirus. Amaliy jihatdan termin viruslarni aniqlash va yo'q qilish uchun ishlatiladi. Terminning qo'llanilish sohasi kompyuter xavfsizligi va antivirus dasturlari bo'lib, kontekstda kompyuter tizimlarini zararli dasturlardan himoya qilish imkonini bildiradi.

Phishing - fishing, firibgarlik. Foydalanuvchini aldab, ularning maxfiy ma'lumotlarini qo'lga kiritish usuli. Pragmatik xususiyati: Elektron pochta yoki soxta veb-saytlar orqali amalga oshiriladi, ko'pincha moliyaviy ma'lumotlarni o'g'irlash maqsadida ishlatiladi.

Arbitrage – arbitraj. Termin amaliy jihatdan kriptografik protokolning talqini bilan bog'liq bahslarni yechishga yordam beradi. Mazkur termin asosan, kriptografiya hamda axborot xavfsizligida qo'llanilib, kontekstda kriptografik jarayonlar va ularning talqinidagi kelishmovchiliklarni bartaraf etish ma'nosida qo'llaniladi.

Xulosa. Ko'rinadiki, kiberxavfsizlik terminologiyasi ko'pincha murakkab va tushunilishi qiyin bo'lgan texnik terminlardan iborat. Bu terminlarni to'g'ri talqin qilish va ulardan foydalanish uchun lingvistik yondashuv zarur. Tahlil natijalari asosida aytish mumkinki, mazkur terminlarning amaliy jihatlarini va kontekstdagi imkoniyatlarini ularni aniq maqsadlarda hamda aniq qo'llanish yo'nalishlarini ko'rsatadi. Shuningdek, terminlarning ma'nosini keng yoritib berish, qo'llanilish imkoniyatlarini aniqlash muhim ahamiyatga egadir.

ADABIYOTLAR

1. Асмус Н.Г. Лингвистические особенности виртуального коммуникативного пространства. Автореф. дисс... канд. филол. наук. – Челябинск, 2005. – 24 с.
2. Ахренова Н.А. Интернет-дискурс как гипертекст. Вестник Московского государственного областного университета (электронный журнал). 2016, No 3.
3. Борковский А.Б. Англо-русский словарь по программированию и информатике (с толкованиями). Издание 2-е, стереотипное. – Москва: «Русский язык», 1989. – 335 с.
4. Егорова Л.А. О проблеме восприятия научного гипермедийного дискурса. Вестник РУДН, серия Лингвистика, 2011, №2.
5. Галкин Д.В. От кибернетических автоматов к искусственной жизни: теоретические и историко-культурные аспекты формирования цифровой культуры. Автореф. дисс... докт. филос. наук. – Томск, 2013. – 51 с.
6. Горина Е.В. Дискурсивная модель интернета. Известия Уральского федерального университета. Сер. 1, Проблемы образования, науки и культуры. 2015. № 2 (138). – С. 22-30.
7. Лазарева Э.А. Дискурсивные защиты как фактор построения интернеткоммуникации // Психолингвистические аспекты изучения речевой деятельности. Екатеринбург, 2010. Вып. 8. – С. 51–59.
8. Леонтович О.А. Метод дискурс-анализа // Научный журнал «Дискурс-Пи» 2015. № 2 (19). – С. 185-187.
9. Моргун Н.Л. Научный сетевой дискурс как тип текста: дисс... канд. филол. наук. – Тюмень, 2002. – 289 с.
10. Реформатский А.А. Введение в языковедение. – Москва: Аспект Пресс, 2010. – 516 с.
11. Herring S.C. Computer-mediated discourse analysis: an approach to researching online communities. March, 2004; Herring S.C. and Androutsopoulos J. Computer-mediated discourse. The Handbook of Discourse Analysis, Second Edition, 2015; Davis B.H. Electronic Discourse: Linguistic Individuals in Virtual Space. SUNY Press, 1997. – 217 с.; Suler J. Computer and cyberspace “addiction”. International Journal of Applied Psychoanalytic Studies 1 (4), 2004. –P. 359-362.