bilan kuzatadi. Tez kunda bola intonatsiyaga e'tibor bera boshlaydi Mayin gapirganda tinchlanadi, keskin intonatsiyaga esa yig'laydi. 2 oylik atrofida gu-gulash, 3-oyning boshida bo‘g‘inlarning talaffuzi paydo bo‘ladi (aga-aga, ta-ta, ba-ba va boshqalar). Bunda tovushlar birikmasi aniq artikulatsiya qilinmaydi. Chug'urlash bosqichining namoyon bo'lish muddatiga kelsak, bu yerda turli fikrlar mavjud: bir guruh mualliflar bu bosqich bola hayotining 2-oyi oxirlarida va 3-oyning boshlarida namoyon bo'ladi.

NATIJALAR

Olib borilgan tadqiqotlar shuni ko'rsatadiki, inson o'z umri davomida oladigan barcha informatsiyaning 70 foizini 5 yoshgacha bo'lgan davrida oladi" kabi fikrlar ham shundan dalolat berib turibdi. Bola ruhiy kamolotining ko'p jihatlari nutq bilan bog'liq ravishda rivojlanadi. Chunki, bola muloqotga kirishishi ya'ni tengdoshlari va kattalar bilan bo'ladigan muloqotlari jarayonida juda ko'plab ma'lumotlarga ega bo'ladi va o'zining ruhiyatini rivojlanish bosqichiga ko'tarib boradi. Shuning uchun, bola hayotining dastlabki birinchi oyidan tarbiya faqat uni parvarish qilish bilan chegaralanmasligi kerak. Bolaning ilk yosh davridan eshitish qobiliyatini tarbiyalash, shuningdek, bolaning emotsional sohasi – jilmayish, kulish, va ovoz tonini uyg'otish lozim. Bularning hammasi birgalikda nutqini rivojlantirishga xizmat qiladi. Asosan, bolalarning nutqiy rivojlanishi uning kattalar bilan individual muloqotida shakllanadi. Bola muloqotga nafaqat emotsional kirishadi, balki so'zlovchining yuzini ham ko'rib turishi kerak. Bog'cha yoshidagi bolalar eng avvalo ko'rgazmali ifodalangan yoki ularni faoliyatlarga jalb etadigan predmetlar, hodisalar, sifatlar, xususiyatlar, munosabatlarning nomlanishini o'zlashtiradi [5].

XULOSA

Xulosa qilib aytganda bolalarda nutqning to'g'ri nuqsonlarsiz rivojlanishi, bolalarning nutqidagi nuqsonlarni vaqtida aniqlashda ota – onalar, tarbiyachilar hamda maktab o'qituvchilaridan katta masuliyat ta'lab etadi.

ADABIYOTLAR RO‘YXATI:

1. Ahmedova Z.M., Ayupova M.Y., Xamidova M.P. Logopedik o‘yin. darsligi, Toshkent, 2007

2. Ayupova M.Y. Logopediya. darslik. Toshkent. O‘zbekiston faylasuflari milliy jamiyati nashriyoti, 2007. - 560 b.

3. Shomahmudova R. To‘g‘ri talaffuzga o‘rgatish va nutq o‘stirish. Toshkent Ilm Ziyo, 2013

4. Shomaxmudova R. Sh. Mo‘minova L. Bolalar nutqidagi nuqsonlar va ularni bartaraf etish. - Toshkent., 1994.

5. Boboeva D.R Tevarak-atrofni o‘rganishda maktabgacha yoshdagi bolalarning bog‘lanishli nutqini rivojlantirish: Ped.fanlari nomzodi. diss.avtoref.- Toshkent, 2001.

AXBOROT XAVFSIZLIGI MUAMMOLARI

Annotatsiya: *Axborot xavfsizligi jamiyatda axborotdan keng foydalanishda muhim ahamiyatga ega hisoblanadi. Ijtimoiy tarmoqlar, internet kabi tushunchlar bilan birga jamiyatga spam, feyk,kompyuter viruslari kabi juda jo'plab tushunchlar ham kirib kelmoqda. Albatta har bir narsanining old va orqa tarafi bor. Demak axborotdan foydalanish jarayonida ham uning qanchalik xavfli va xavfsiz ekanligiga ahamiyat berish muhim hisoblanadi. Hozirgi paytda juda ko'plab bunday misollarni keltirish mumkin. Shunday ekan axborotdan foydalanish madaniyatiga ham kata e'tibor berish kerak bo'ladi.*

Kalit so'zlar:*Axborot xavfsizligi,SMM,kiberjinoyat, konfidentsial xabarlar,axborot ximoyasi*

AXBOROT XAVFSIZLIGI MUAMMOLARI

Bugungi kunda jamiyatni axborotlashtirish muhim ahamiyatga ega bo'lmoqda.Axborotdan foydalanish qanchalik ko'p bo'lsa, uni himoyalash shunchalik muammoga aylanib boraveradi. Kiberjinoyatlardan saqlanish uchun axborotni muxofazalash muhim ahamiyat kasb etadi. Hozirda SMM dan foydalanish jarayonida ham axborot xavfsizligiga oid juda ko'plab muammolar kelib chiqmoqda.

Axborotning muximlik darajasi qadim zamonlardan ma'lum. Shuning uchun xam qadimda axborotni himoyalash uchun turli xil usullar qo'llanilgan. Ulardan biri – sirli yozuvdir. Undagi xabarni xabar yuborilgan manzil egasidan boshqa shaxs o'qiy olmagan. Asrlar davomida bu san'at – sirli yozuv jamiyatning yuqori tabaqalari, davlatning elchixona rezidentsiyalari va razvedka missiyalaridan tashqariga chiqmagan. Faqat bir necha o'n yil oldin hamma narsa tubdan o'zgardi, ya'ni axborot o'z qiymatiga ega bo'ldi va keng tarqaladigan mahsulotga aylandi. Uni endilikda ishlab chiqaradilar, saqlaydilar, uzatishadi, sotadilar va sotib oladilar. Bulardan tashqari uni o'g'irlaydilar, buzib talqin etadilar va soxtalashtiradilar. Shunday qilib, axborotni himoyalash zaruriyati tug'iladi. Axborotni qayta ishlash sanoatining paydo bo'lishi axborotni himoyalash sanoatining paydo bo'lishiga olib keladi.

Axborot xavfsizligining dolzarblashib borishi, axborotning strategik resursga aylanib borishi bilan izohlash mumkin. Zamonaviy davlat infratuzilmasini telekommunikatsiya va axborot tarmoqlari hamda turli xildagi axborot tizimlari tashkil etib, axborot texnologiyalari va texnik vositalar jamiyatning turli jabhalarida keng qo'llanilmoqda (iqtisod, fan, ta'lim, xarbiy ish, turli texnologiyalarni boshqarish va x.k.)

Axborot xavfsizligi deb, ma'lumotlarni yo'qotish va o'zgartirishga yo'naltirilgan tabiiy yoki sun'iy xossali tasodifiy va qasddan ta'sirlardan xar qanday tashuvchilarda axborotning himoyalanganligiga aytiladi.

Ilgarigi xavf faqatgina konfidentsial (maxfiy) xabarlar va xujjatlarni o'g'irlash yoki nusxa olishdan iborat bo'lsa, hozirgi paytdagi xavf esa kompyuter ma'lumotlari to'plami, elektron ma'lumotlar, elektron massivlardan ularning egasidan ruxsat so'ramasdan

foydalanishdir. Bulardan tashqari, bu xarakatlardan moddiy foyda olishga intilish ham rivojlandi.

Axborotning himoyasi deb, boshqarish va ishlab chiqarish faoliyatining axborot xavfsizligini ta’minlovchi va tashkilot axborot zaxiralarining yaxlitliligi, ishonchliligi, foydalanish osonligi va maxfiyligini ta’minlovchi qatiy reglamentlangan dinamik texnologik jarayonga aytiladi.

Axborotning egasiga, foydalanuvchisiga va boshka shaxsga zarar yetkazmokchi bo’lgan nohuquqiy muomaladan xar qanday xujjatlashtirilgan, ya’ni identifikatsiya qilish imkonini beruvchi rekvizitlari qo’yilgan xolda moddiy jismda qayd etilgan axborot ximoyalanishi kerak.

Axborotni ximoyalashning maqsadlari kuyidagilardan iborat:

- axborotning kelishuvsiz chikib ketishi, ugirlanishi, yo’qotilishi, o’zgartirilishi, soxtalashtirilishlarning oldini olish;
- shaxs, jamiyat, davlat xavfsizliligiga bulgan xavf – xatarning oldini olish;
- axborotni yo’q qilish, o’zgartirish, soxtalashtirish, nusxa kuchirish, tusiklash buyicha ruxsat etilmagan xarakatlarning oldini olish;
- xujjatlashtirilgan axborotning mikdori sifatida xukukiy tartibini ta’minlovchi, axborot zaxirasi va axborot tizimiga xar kanday nokonuniy aralashuvlarning kurinishlarining oldini olish;
- axborot tizimida mavjud bulgan shaxsiy ma’lumotlarning shaxsiy maxfiyligini va konfidentsialligini saklovchi fukarolarning konstitutsion xukuklarini ximoyalash;
- davlat sirini, konunchilikka mos xujjatlashtirilgan axborotning konfidentsialligini saklash;
- axborot tizimlari, texnologiyalari va ularni ta’minlovchi vositalarni yaratish, ishlab chikish va kullashda sub’ektlarning xukuklarini ta’minlash.

Hozirda tashqi kommunikatsiya orqali ruxsatsiz foydalanishga atayin qilingan urinishlar bo’lishi mumkin bo’lgan barcha buzilishlarning 10%ini tashkil etadi. Bu kattalik anchagina bo’lib tuyulmasa ham, Internetda ishlash tajribasi ko’rsatadiki, qariyb har bir Internet-server kuniga bir necha marta suqilib kirish urinishlariga duchor bo’lar ekan. Xavf-xatarlar taxlil qilinganida tashkilot korporativ yoki lokal tarmog’i kompyuterlarining xujumlarga qarshi turishi yoki bo’lmaganida axborot xavfsizligi buzilishi faktlarini qayd etish uchun yetarlicha himoyalanmaganligini hisobga olish zarur. Masalan, axborot tizimlarini himoyalash Agentligining (AQSH) testlari ko’rsatadiki, 88% kompyuterlar axborot xavfsizligi nuqtai nazaridan nozik joylarga egaki, ular ruxsatsiz foydalanish uchun faol ishlatishlari mumkin. Tashkilot axborot tuzilmasidan sasofadan foydalanish xollari alohida ko’rilishi lozim.

Xulosa qilib shuni aytish mumkinki, xar qanday axborotdan foydalanishda uning ishonchli va xavfsiz ekanligiga alohida e’tibor berish kerak. Axborot xavfsizligini ta’minlashda esa ishonchli shifrlash usllaridan foydalanish, turli viruslardan himoyalanganligiga ahamiyat berish kerak bo’ladi.