

AXBOROT XAVFSIZLIGI MADANIYATINI SHAKLLANTIRISHNING PSIXOLOGIK OMILLARI: MOTIVATSIYA, MAS’ULIYAT, IDROK, XULQ-ATVOR VA KASBIY QADRIYATLAR

Otaboyev Xaydarali Xusanovich

FVV Akademiyasi magistratura tinglovchisi

Annotatsiya: Mazkur maqolada axborot xavfsizligi madaniyatini shakllantirishning psixologik asoslari, xususan, motivatsiya, shaxsiy mas’uliyat, xavfni idrok etish, xulq-atvor va kasbiy qadriyatlarning o‘zaro aloqadorligi ilmiy-nazariy jihatdan tahlil qilinadi. Raqamli texnologiyalar rivojlanishi sharoitida axborotni himoya qilish faqat texnik vositalar va tashkiliy qoidalar bilan cheklanmasdan, insonning psixologik xususiyatlari, axborotga munosabati hamda kundalik faoliyatidagi xavfsizlik odatlariga ham bog‘liq ekanligi asoslanadi.

Kalit so‘zlar: axborot xavfsizligi, xavfsizlik madaniyati, motivatsiya, shaxsiy mas’uliyat, xavfni idrok etish, kasbiy qadriyatlar, raqamli savodxonlik, psixologik omillar, kiberxavfsizlik.

ПСИХОЛОГИЧЕСКИЕ ФАКТОРЫ ФОРМИРОВАНИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МОТИВАЦИЯ, ОТВЕТСТВЕННОСТЬ, ВОСПРИЯТИЕ, ПОВЕДЕНИЕ И ПРОФЕССИОНАЛЬНЫЕ ЦЕННОСТИ

Отабоев Хайдарали Хусанович

Магистрант Академии МЧС

Аннотация. В данной статье проводится научно-теоретический анализ психологических основ формирования культуры информационной безопасности, в частности взаимосвязи мотивации, личной ответственности, восприятия рисков, поведения и профессиональных ценностей. Обосновывается, что в условиях развития цифровых технологий защита информации зависит не только от технических средств и организационных правил, но и от психологических особенностей человека, его

отношения к информации и привычек безопасного поведения в повседневной деятельности.

Ключевые слова: информационная безопасность, культура безопасности, мотивация, личная ответственность, восприятие рисков, профессиональные ценности, цифровая грамотность, психологические факторы, кибербезопасность.

PSYCHOLOGICAL FACTORS IN DEVELOPING INFORMATION SECURITY CULTURE: MOTIVATION, RESPONSIBILITY, PERCEPTION, BEHAVIOR, AND PROFESSIONAL VALUES

Otaboyev Khaydarali Khusanovich

Master's Student the Academy of the Ministry of Emergency Situations

Abstract. *This article presents a scientific and theoretical analysis of the psychological foundations of developing an information security culture, with particular emphasis on the interrelationship between motivation, personal responsibility, risk perception, behavior, and professional values. It substantiates the view that, in the context of digital technological development, information protection depends not only on technical tools and organizational rules but also on individuals' psychological characteristics, attitudes toward information, and everyday security habits.*

Keywords: *information security, security culture, motivation, personal responsibility, risk perception, professional values, digital literacy, psychological factors, cybersecurity.*

Kirish

Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi va ma'lumotlarning raqamli shaklda saqlanishi axborot xavfsizligini ta'minlash masalasini dolzarb muammoga aylantirmoqda. Davlat boshqaruvi, ta'lim va favqulodda vaziyatlarni bartaraf etish kabi sohalarda axborot resurslarini himoyalash boshqaruv qarorlarining to'g'riligi hamda tashkilot faoliyatining uzluksizligi bilan chambarchas bog'liq. Axborot xavfsizligi axborotning maxfiyligi, yaxlitligi va undan foydalanish imkoniyatini ta'minlashni nazarda tutadi. Biroq bu

maqsadlarga faqat texnik vositalar va me'yoriy hujjatlar orqali erishib bo'lmaydi. Xodimlarning xatti-harakati, xavfni anglash darajasi, qoidalarga munosabati va kasbiy mas'uliyati ham muhim ahamiyatga ega. Masalan, murakkab paroldan foydalanish, shubhali xabarlarini tekshirish va xizmat ma'lumotlarini ruxsatsiz tarqatmaslik insonning kundalik qarorlariga bog'liq. AQSh Milliy standartlar va texnologiyalar instituti tomonidan 2024-yilda e'lon qilingan SP 800-50 Rev. 1 hujjatida kibernetik xavfsizlik bo'yicha ta'lim, xodimlar xulq-atvorini rivojlantirish va xavfsizlik madaniyatini mustahkamlash masalalariga e'tibor qaratilgan [1]. Bu axborot xavfsizligini uzluksiz ta'lim va tashkiliy madaniyat bilan bog'liq jarayon sifatida o'rganish zarurligini ko'rsatadi.

Asosiy qism

Axborot xavfsizligi madaniyati shaxs va tashkilotning axborotni himoyalashga oid bilimlari, e'tiqodlari, qadriyatlari va kundalik xulq-atvorida namoyon bo'ladigan yaxlit tizimdir. U nafaqat xavfsizlik qoidalarini bilish, balki ularni amaliy faoliyatda muntazam bajarishni ham anglatadi. Mazkur madaniyatning shakllanishida uchta o'zaro bog'liq darajani ajratish mumkin: xavfsizlik bo'yicha bilim va xabardorlik; qoidalarga nisbatan ijobiy munosabat; xavfsiz xulq-atvor odatlari. Ushbu darajalar bir-birini to'ldiradi. Xodim xavfsizlik talablarini bilishi mumkin, ammo vaqt tanqisligi yoki ortiqcha ishonuvchanlik sababli ularga amal qilmasligi ehtimoli mavjud. Edgar Sheynning tashkiliy madaniyat haqidagi qarashlaridan kelib chiqib, xavfsizlik qoidalarining samaradorligi ularning rasmiy tasdiqlanishi bilangina emas, balki xodimlar tomonidan umumiy kasbiy me'yor sifatida qabul qilinishi bilan ham belgilanadi [2]. Agar rahbarlar xavfsizlik talablariga o'zlari rioya qilsa va xodimlarning tashabbuslarini qo'llab-quvvatlasa, jamoada ijobiy xavfsizlik muhiti shakllanishi mumkin. Bizning fikrimizcha, axborot xavfsizligi madaniyatining asosiy mezonini qoidalarini yoddan bilish emas, balki ularni kasbiy faoliyatning ajralmas qismi sifatida qabul qilishdir.

Motivatsiya insonni muayyan faoliyatga undaydigan ichki va tashqi omillar tizimidir. Axborot xavfsizligida ichki motivatsiya xavfsizlikni kasbiy qadriyat sifatida qabul qilish, o'z vazifasiga mas'uliyat bilan yondashish va boshqalarga zarar yetkazmaslik istagi bilan bog'liq. Tashqi motivatsiya esa rahbar ko'rsatmalari, xizmat talablari, rag'batlantirish va intizomiy javobgarlik orqali namoyon bo'ladi. Tashqi nazorat xavfsizlik qoidalariga rioya qilishni ta'minlashga yordam beradi. Biroq uzoq muddatli natija uchun xodim talablarning mazmunini tushunishi va



ularni ichki e'tiqod sifatida qabul qilishi lozim. Masalan, shubhali havolani ochmaslik yoki xizmat ma'lumotlarini shaxsiy elektron pochtaga yubormaslik qarori ehtimoliy oqibatlarni anglash va kasbiy mas'uliyatni his qilish bilan bog'liq. Motivatsiyani rivojlantirish uchun xavfsizlik qoidalarining amaliy ahamiyatini tushuntirish, real vaziyatlarga asoslangan mashg'ulotlar tashkil etish va xavfsiz xulq-atvorni rag'batlantirish zarur. Xodimlarga shubhali holatlar haqida xabar berishning aniq va qulay mexanizmlari ham yaratilishi kerak. Shu bilan birga, faqat qo'rqitish va jazolashga asoslangan yondashuv xatolarni yashirishga olib kelishi mumkin. Shu sababli javobgarlik bilan bir qatorda, xatolar sabablarini xolis tahlil qilish va ularni takrorlamaslikka yordam beradigan muhitni shakllantirish muhimdir.

Shaxsiy mas'uliyat insonning o'z harakatlari va qarorlarining oqibatlarini anglashini hamda vazifalarini belgilangan talablar asosida bajarishga intilishini ifodalaydi. Axborot xavfsizligida bu mas'uliyat xizmat hujjatlari, hisob qaydnomalari va axborot resurslaridan ehtiyotkorlik bilan foydalanishda namoyon bo'ladi. Mas'uliyatni uch yo'nalishda ko'rib chiqish mumkin: shaxsiy mas'uliyat - axborot va qurilmalarni himoyalash; kasbiy mas'uliyat - xizmat vazifalarida xavfsizlik talablariga rioya qilish; jamoaviy mas'uliyat - o'z harakatlarining hamkasblar va tashkilotga ta'sirini hisobga olish. Mas'uliyatli xulq-atvorni shakllantirish uchun xodimlarning vazifalari va vakolatlari aniq belgilanishi, xavfsizlik yo'riqnomalari tushunarli bo'lishi hamda hodisalar haqida xabar berish tartibi ishlab chiqilishi lozim. Xodim xatoga yo'l qo'yganida, uni yashirish o'rniga o'z vaqtida xabar berishi muammoni tezroq bartaraf etishga yordam beradi.

Favqulodda vaziyatlar tizimida bu masalaning ahamiyati yanada yuqori. Chunki tezkor boshqaruv va qutqaruv tadbirlarini muvofiqlashtirishda axborotning ishonchliligi, maxfiyligi va o'z vaqtida yetkazilishi muhimdir. Noto'g'ri ma'lumotga tayanish yoki xizmat axborotini ruxsatsiz tarqatish boshqaruv qarorlariga salbiy ta'sir ko'rsatishi mumkin. Bizning nazarimizda, mas'uliyatning muhim belgisi xodimning xavfsizlik talablarini tashqi nazorat mavjud bo'lmagan vaziyatlarda ham bajarishga tayyorligidir.

Xavfni idrok etish insonning tahdid ehtimolini anglash, uning oqibatlarini baholash va tegishli qaror qabul qilish jarayonidir. Axborot xavfsizligida bu shubhali elektron xabarlarini aniqlash, noma'lum manbalardan kelgan fayllarga ehtiyotkorlik bilan munosabatda bo'lish va ma'lumot so'rayotgan shaxsning vakolatini tekshirish orqali namoyon bo'ladi. Xavfni idrok etishga insonning tajribasi, axborot



savodxonligi, hissiy holati va vaqt tanqisligi ta'sir ko'rsatadi. Masalan, rahbar nomidan yuborilgan va zudlik bilan javob berishni talab qiladigan soxta xabar xodimda shubha uyg'otmasligi mumkin. Shu sababli xodimlarni faqat tahdidlar bilan tanishtirish emas, balki shubhali belgilarni aniqlash va ma'lumot manbasini tekshirishga o'rgatish zarur. Icke Ayzanning rejalashtirilgan xulq-atvor nazariyasiga ko'ra, insonning xatti-harakatni bajarish niyatiga uning munosabati, ijtimoiy me'yorlar haqidagi tasavvuri va harakatni amalga oshirish imkoniyatiga bo'lgan ishonchi ta'sir ko'rsatadi [3]. Ushbu yondashuv axborot xavfsizligida ham ahamiyatli: xodim xavfsizlik talabini zarur deb bilishi, jamoa tomonidan qo'llab-quvvatlanishi va uni bajarish uchun yetarli imkoniyatga ega bo'lishi kerak. Xavfni idrok etishni rivojlantirishda vaziyatli tahlil, muammoli savollar, simulyatsion mashqlar va xatolarni xolis muhokama qilish usullaridan foydalanish mumkin. Bunda maqsad xodimlarda ortiqcha qo'rquv uyg'otish emas, balki asosli ehtiyotkorlik va tanqidiy fikrlashni shakllantirishdir.

Axborot xavfsizligi madaniyatining amaliy natijasi kundalik xulq-atvorda namoyon bo'ladi. Xavfsiz xulq-atvorga xizmat qurilmalarini bloklash, ma'lumot yuborishdan oldin qabul qiluvchini tekshirish, himoya vositalaridan to'g'ri foydalanish va shubhali holatlar haqida o'z vaqtida xabar berish kiradi. Bir martalik ma'ruza yoki yo'riqnoma barqaror ko'nikmalarni shakllantirish uchun har doim ham yetarli emas. Xavfsizlik qoidalari amaliy mashqlar va takroriy faoliyat orqali kundalik odatlarga aylanishi kerak. Bunda xodimlar xavfsiz harakatning mazmunini tushunishi va uni bajarish uchun zarur vositalarga ega bo'lishi muhim. Xavfsiz xulq-atvorni rivojlantirishda uch bosqichli yondashuvdan foydalanish mumkin: birinchi bosqichda xodim xavfsizlik talablarini o'rganadi; ikkinchi bosqichda ularni amaliy vaziyatlarda qo'llaydi; uchinchi bosqichda esa xavfsiz harakatlar muntazam takrorlanib, kasbiy faoliyatning barqaror qismiga aylanadi. Rahbarlarning shaxsiy namunasi ham muhimdir. Agar rahbarlar xavfsizlik qoidalariga amal qilsa va xodimlarning tashabbuslarini qo'llab-quvvatlasa, jamoada ijobiy me'yorlar shakllanadi. Shu bilan birga, natijalarni baholashda test ballari bilan cheklanmay, xodimlarning real vaziyatlarda qanday harakat qilishi ham hisobga olinishi lozim.

Kasbiy qadriyatlar insonning mehnat faoliyatida amal qiladigan axloqiy tamoyillari va e'tiqodlarini ifodalaydi. Axborot xavfsizligida halollik, intizom, ishonchlilik, maxfiylikka rioya qilish va xizmat burchiga sadoqat muhim qadriyatlar hisoblanadi. Xizmat ma'lumotlarini ruxsatsiz tarqatmaslik faqat texnik talab emas,



balki ishonchni saqlash va boshqa shaxslarning manfaatlarini hurmat qilish bilan ham bog‘liq. Agar tashkilotda tezlik xavfsizlikdan ustun qo‘yilsa yoki xatolarni yashirish odatiy holga aylansa, xavfsizlik qoidalariga rioya qilish susayishi mumkin. Kasbiy qadriyatlar kundalik faoliyat, jamoaviy muhokamalar, ustoz-shogird munosabatlari va rahbarlarning amaliy namunasi orqali shakllanadi. Shu sababli axborot xavfsizligi masalalarini kasbiy tayyorgarlik dasturlariga kiritish, xodimlarning mas’uliyatli qarorlarini qo‘llab-quvvatlash va ochiq muloqot muhitini yaratish maqsadga muvofiq. 2025-yilda *Computers & Security* jurnalida chop etilgan dalillar tahlilida ham xavfsizlik madaniyatini o‘rganishda xodimlarning munosabati, ta’lim, xulq-atvor va rahbariyatning qo‘llab-quvvatlashi kabi omillarga e’tibor qaratilgan [4]. Bu xavfsizlikni faqat texnik masala sifatida emas, balki inson va tashkilot faoliyati bilan bog‘liq tizim sifatida ko‘rib chiqish zarurligini ko‘rsatadi.

Baholashda so‘rovnoma, suhbat, bilim testlari va vaziyatli topshiriqlardan foydalanish mumkin. Bunda bitta ko‘rsatkichga tayanib yakuniy xulosa chiqarish to‘g‘ri emas. Masalan, xavfsizlik hodisalari haqida xabarlar sonining ortishi xodimlarning xabardorligi va xabar berish madaniyati yaxshilanganini ham anglatishi mumkin. FVV tizimida mazkur mexanizmlarni xizmat axborotini himoyalash, axborot manbalarini tekshirish, rasmiy aloqa kanallaridan foydalanish va shubhali holatlar haqida o‘z vaqtida xabar berishga qaratilgan mashg‘ulotlar orqali amalga oshirish mumkin. Taklif etilgan modelning samaradorligini aniqlash uchun esa uni muayyan tashkilot sharoitida amaliy sinovdan o‘tkazish va natijalarni ilmiy mezonlar asosida baholash lozim.

Xulosa

Axborot xavfsizligi madaniyatini shakllantirish inson omili, texnologik himoya va tashkiliy boshqaruvni uyg‘unlashtirishni talab qiladi. Maqoladagi nazariy tahlil motivatsiya, shaxsiy mas’uliyat, xavfni idrok etish, xavfsiz xulq-atvor va kasbiy qadriyatlar ushbu madaniyatning o‘zaro bog‘liq psixologik omillari ekanini ko‘rsatadi. Motivatsiya xodimlarni xavfsizlik talablariga ongli rioya qilishga undaydi. Shaxsiy mas’uliyat o‘z harakatlarining oqibatlarini anglash va xizmat axborotini ehtiyotkorlik bilan boshqarishda namoyon bo‘ladi. Xavfni idrok etish shubhali holatlarni aniqlash va asosli qaror qabul qilishga yordam beradi. Xavfsiz xulq-atvor esa bilimlarning amaliy faoliyatga aylanishini ta’minlaydi. Kasbiy qadriyatlar - halollik, intizom, ishonchlik va xizmat burchiga sadoqat - ushbu jarayonning ma’naviy asosini tashkil etadi. Maqolada diagnostika, maqsadli ta’lim,

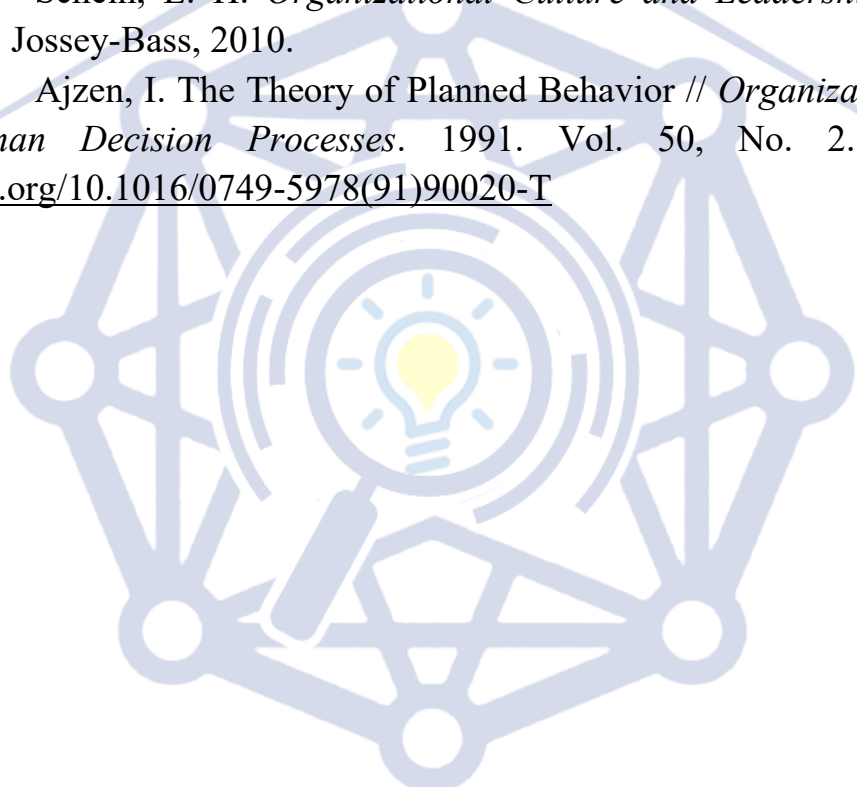


amaliy mashqlar, tashkiliy qo‘llab-quvvatlash, natijalarni baholash va uzluksiz takomillashtirishdan iborat model taklif etildi. Uni amaliyotga joriy etishda xodimlarning kasbiy xususiyatlari, ish sharoitlari va axborot xavfsizligi ehtiyojlarini hisobga olish zarur. Xulosa qilib aytganda, axborot xavfsizligi madaniyatini rivojlantirishning muhim sharti - bilimlarni ichki motivatsiya, shaxsiy mas’uliyat, tanqidiy fikrlash va kasbiy qadriyatlar bilan uyg‘unlashtirishdir. Bu yondashuv, ayniqsa, tezkor qarorlar qabul qiladigan va xizmat axborotining ishonchligi muhim bo‘lgan FVV tizimi uchun alohida ahamiyatga ega.

Foydalanilgan adabiyotlar ro‘yxati:

1. Гафнер В. В. Информационная безопасность. - Rostov-na-Donu: Феникс, 2010. - 324 bet.
2. Власова Л. М. ва бошқалар - Культура безопасности: современный комплекс проблем безопасности. - Москва: Литера, 2012. - 191 bet.
3. Кирсанов К. А., Малявина А. В., Попов Н. В. Информационная безопасность. - Москва: МАЭП, 2000. - 229 bet.
4. Бубнов А. А., Пржегорлинский В. Н., Савинкин О. А. - Основы информационной безопасности. - Москва: Издательский центр «Академия», 2019. - 254 bet.
5. Малюк А. А. Формирование культуры информационной безопасности общества. Журнал «Педагогика», 2009, № 3. – 33-39-betlar.
6. Валитов О. К. Правовая культура и информационная безопасность. // «Вестник Башкирского университета», 2012, т. 17, № 1-1. – 580-585-betlar.
7. Алиева М. Ф. Информационная безопасность как элемент информационной культуры. // «Вестник Адыгейского государственного университета», 2012, № 4 (108). – 97-102-betlar.
8. Селиверстов А. С. К вопросу об актуальности формирования культуры информационной безопасности у курсантов военных вузов. //«Вестник современных исследований», 2018, № 6.3 (21). - 190–192-betlar.
9. Швырев Б. А., Полякова Я. Н. Педагогический процесс формирования культуры информационной безопасности в ФСИН России. «Вестник Уфимского юридического института МВД России», 2024, № 2. - 174–181-betlar.

10. Основы кибер-безопасности. - Toshkent: «Mahalla va oila» nashriyoti, 2021. - 228 bet. ISBN: 978-9943-7778-9-7.
11. Ganiyev S.K., Ganiyev A.A., Xudoyqulov Z.T. Kiberxavfsizlik asoslari. (o`quv qo`llanma). – Toshkent: Muhammad al- Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti. 2020.
12. National Institute of Standards and Technology. *Building a Cybersecurity and Privacy Learning Program*. NIST SP 800-50 Rev. 1. 2024. <https://doi.org/10.6028/NIST.SP.800-50r1>
13. Schein, E. H. *Organizational Culture and Leadership*. 4th ed. San Francisco: Jossey-Bass, 2010.
14. Ajzen, I. The Theory of Planned Behavior // *Organizational Behavior and Human Decision Processes*. 1991. Vol. 50, No. 2. P. 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)



Research Science and
Innovation House