

Qudratov Alijon Normamatovich
Guliston davlat universiteti,
Axborot texnologiyalari kafedrası
katta o'qituvchisi
Abduraimov Dostonbek Egamnazar o'g'li
Guliston davlat universiteti,
Axborot texnologiyalari kafedrası
katta o'qituvchisi

RAQAMLI TRANSFORMATSIYA SHAROITIDA DAVLAT XIZMATCHILARINING KIBERXAVFSIZLIK KOMPETENSIYALARINI RIVOJLANTIRISH MODELİ

Annotatsiya: Mazkur maqolada raqamli transformatsiya sharoitida davlat boshqaruvi tizimida kiberxavfsizlikni ta'minlashda davlat xizmatchilarining kompetensiyalarini rivojlantirish muammolari ilmiy jihatdan tahlil qilingan. Tadqiqotda elektron hukumat va raqamli xizmatlar rivoji bilan bog'liq axborot xavfsizligi tahdidlari tizimli yondashuv asosida ko'rib chiqilgan. Kiberxavfsizlikni ta'minlashda inson omilining hal qiluvchi roli asoslab berilgan. Davlat xizmatchilarining kiberxavfsizlik kompetensiyalari bilimlar, amaliy ko'nikmalar, mas'uliyatli raqamli xulq-atvor va strategik fikrlash komponentlari orqali tavsiflangan. Kompetensiyaviy va ilmiy-tizimli yondashuv asosida kiberxavfsizlik kompetensiyalarini rivojlantirish modeli ishlab chiqilgan. Model uzluksiz kasbiy ta'lim, treninglar va baholash mexanizmlarini o'z ichiga oladi. Tadqiqot natijalari davlat boshqaruvida kiberxavfsizlik madaniyatini shakllantirish zarurligini ko'rsatadi. Mazkur ilmiy ish raqamli davlatni barqaror rivojlantirish strategiyalarini amalga oshirishda amaliy ahamiyatga ega.

Kalit so'zlar: Raqamli transformatsiya, davlat xizmatchilari, kiberxavfsizlik, kompetensiya, axborot xavfsizligi, raqamli hukumat, inson omili, kiberxavfsizlik madaniyati.

Кудратов Алижон
Гулистонский государственный университет,
Кафедра “Информационных технологий”,
Старший преподаватель
Абураимов Достонбек
Гулистонский государственный университет,
Кафедра “Информационных технологий”,
Старший преподаватель

МОДЕЛЬ ДЛЯ РАЗВИТИЯ КОМПЕТЕНЦИЙ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ У ГОСУДАРСТВЕННЫХ СЛУЖАЩИХ В КОНТЕКСТЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация: В статье рассматриваются научные аспекты развития кибербезопасностных компетенций государственных служащих в условиях цифровой трансформации системы государственного управления. Проанализированы угрозы информационной безопасности, возникающие в процессе внедрения электронного правительства и цифровых услуг. Обоснована ключевая роль человеческого фактора в обеспечении кибербезопасности государственных информационных ресурсов. Компетенции государственных служащих в сфере кибербезопасности структурированы по компонентам знаний, практических навыков, ответственного цифрового поведения и стратегического мышления. На основе компетентного и системного подходов разработана модель развития кибербезопасностных компетенций. Модель включает механизмы непрерывного профессионального обучения, практико-ориентированных тренингов и оценки компетенций. Результаты исследования подтверждают необходимость формирования культуры кибербезопасности в государственных органах. Представленные выводы могут быть использованы при реализации стратегий устойчивого развития цифрового государства.

Ключевые слова: Цифровая трансформация, государственные служащие, кибербезопасность, компетенции, информационная безопасность, цифровое правительство, человеческий фактор, культура кибербезопасности.

Kudratov Alijon
Guliston State University,
Department of Information Technologies,
Senior Lecturer
Abduraimov Dostonbek
Guliston State University,
Department of Information Technologies,
Senior Lecturer

A MODEL FOR DEVELOPING CYBERSECURITY COMPETENCIES AMONG PUBLIC SERVANTS IN THE CONTEXT OF DIGITAL TRANSFORMATION

Abstract: This article examines the development of cybersecurity competencies of civil servants in the context of digital transformation of public administration. The study analyzes information security threats arising from the implementation of e-government and digital public services. The decisive role of the human factor in ensuring cybersecurity is substantiated. Cybersecurity competencies of civil servants are structured into knowledge, practical skills, responsible digital behavior, and strategic thinking components. Based on competency-based and systemic approaches, a model for developing cybersecurity competencies is proposed. The model includes mechanisms for continuous professional education, practice-oriented training, and competency assessment. The research findings emphasize the importance of fostering a cybersecurity culture within public sector institutions. The proposed model contributes to strengthening information security and supports the sustainable development of digital government strategies.

Key words: Digital transformation, civil servants, cybersecurity, competencies, information security, digital government, human factor, cybersecurity culture.

KIRISH. XXI asrning ikkinchi choragida global miqyosda raqamli transformatsiya jarayonlari jamiyat hayotining barcha sohalariga, xususan, davlat boshqaruvi tizimiga chuqur kirib bormoqda. Elektron hukumat, raqamli xizmatlar, ma'lumotlarga asoslangan boshqaruv, sun'iy intellekt va bulutli texnologiyalarning joriy etilishi davlat xizmatlarining samaradorligi, shaffofligi va tezkorligini oshirishga xizmat qilmoqda. Shu bilan birga, mazkur jarayonlar axborot xavfsizligi va kiberxavfsizlik masalalarini strategik darajaga olib chiqmoqda.

Davlat boshqaruvi tizimida foydalanilayotgan axborot tizimlari va ma'lumotlar bazalari ko'pincha fuqarolarning shaxsiy ma'lumotlari, moliyaviy axborotlar hamda milliy xavfsizlikka daxldor bo'lgan ma'lumotlarni o'z ichiga oladi. Ushbu resurslarning kiberxavfsizligini ta'minlash faqat texnik choralar bilan emas, balki inson omiliga, ya'ni davlat xizmatchilarining kiberxavfsizlik bo'yicha bilim, ko'nikma va malakalariga ham bevosita bog'liqdir. Statistik ma'lumotlarga ko'ra, kiberhujumlarning katta qismi aynan inson omili bilan bog'liq xatoliklar natijasida yuzaga keladi. Shu sababli davlat xizmatchilarining kiberxavfsizlik kompetensiyalarini tizimli ravishda rivojlantirish dolzarb ilmiy-amaliy muammo hisoblanadi.

Raqamli transformatsiya sharoitida davlat xizmatchilari nafaqat an'anaviy boshqaruv vazifalarini, balki axborot tizimlaridan samarali va xavfsiz foydalanish, kiberxavflarni aniqlash va ularga to'g'ri munosabat bildirish kabi yangi funksiyalarni ham bajarishi talab etiladi. Xalqaro tashkilotlar, jumladan, OECD va BMT tomonidan e'lon qilingan hisobotlarda davlat sektorida kiberxavfsizlik salohiyatini oshirish raqamli hukumatni barqaror rivojlantirishning asosiy sharti sifatida e'tirof etiladi.

Mazkur maqolaning asosiy maqsadi — raqamli transformatsiya sharoitida davlat xizmatchilarining kiberxavfsizlik kompetensiyalarini rivojlantirishga qaratilgan kompleks modelni ilmiy asoslash va uning tarkibiy qismlarini aniqlashdan iborat. Tadqiqot doirasida kiberxavfsizlik kompetensiyalarining mohiyati, ularni shakllantirishga ta'sir etuvchi omillar hamda samarali rivojlantirish mexanizmlari tahlil qilinadi.

ADABIYOTLAR TAHLILI. Raqamli transformatsiya va davlat boshqaruvi tizimida kiberxavfsizlik kompetensiyalarini rivojlantirish masalasi zamonaviy ilmiy tadqiqotlarda ustuvor yo‘nalishlardan biri sifatida e’tirof etilmoqda. Ushbu muammo raqamli hukumat konsepsiyasi, axborot xavfsizligi, inson omili va kompetensiyaviy yondashuv doirasida keng ko‘lamda tahlil qilingan.

Davlat boshqaruvida raqamli transformatsiya jarayonlarini ilmiy asosda o‘rgangan yetakchi tadqiqotchilardan biri Tomasz Janowski hisoblanadi. Uning tadqiqotlarida raqamli hukumat texnologik yangilanish bilan bir qatorda institutsional va kadrlar salohiyatini rivojlantirishni talab qilishi ta’kidlanadi. Olim raqamli transformatsiya muvaffaqiyati davlat xizmatchilarining raqamli va kiberxavfsizlik kompetensiyalariga bevosita bog‘liq ekanini ilmiy asoslab beradi (Janowski, 2015) [1].

Kiberxavfsizlikda inson omilining rolini chuqur tahlil qilgan mashhur mutaxassis Bruce Schneier o‘z asarlarida texnik himoya vositalaridan ko‘ra foydalanuvchilarning xulq-atvori va xabardorligi muhimroq ekanini ta’kidlaydi. Uning fikriga ko‘ra, kiberxavfsizlik madaniyatini shakllantirmasdan turib, davlat sektorida barqaror axborot xavfsizligini ta’minlash mumkin emas (Schneier, 2018) [2].

Kompetensiyaviy yondashuv nazariy asoslarini ishlab chiqqan olimlardan Richard E. Boyatzis kiberxavfsizlik kompetensiyalarini rivojlantirish modelining metodologik asosini tashkil etadi. Boyatzis kompetensiyani bilim, ko‘nikma va xulq-atvorning integratsiyalashgan tizimi sifatida talqin qiladi. Ushbu yondashuv davlat xizmatchilarining kiberxavfsizlikka oid bilimlari bilan bir qatorda ularning mas’uliyatli raqamli xulq-atvorini shakllantirish zarurligini asoslaydi (Boyatzis, 2008) [3].

Axborot xavfsizligi menejmenti va tashkilot xodimlarining roli masalasini Ross Anderson ilmiy jihatdan asoslab bergan. Uning tadqiqotlarida axborot tizimlari xavfsizligini ta’minlashda inson resurslarini boshqarish muhim omil ekanligi ko‘rsatib berilgan. Anderson davlat tashkilotlarida kiberxavfsizlik siyosatini xodimlar kompetensiyalari bilan uyg‘unlashtirish zarurligini ta’kidlaydi (Anderson, 2020) [4].

Davlat sektorida kiberxavfsizlik salohiyatini oshirish masalasi xalqaro tashkilotlar hisobotlarida ham keng yoritilgan. Jumladan, OECD tomonidan e'lon qilingan tahliliy hisobotlarda davlat xizmatchilarining kiberxavfsizlik kompetensiyalarini rivojlantirish raqamli hukumat barqarorligini ta'minlovchi asosiy omil sifatida baholanadi. OECD mutaxassislari kiberxavfsizlikni faqat IT-mutaxassislar vazifasi sifatida emas, balki barcha davlat xizmatchilariga tegishli umumiy kompetensiya deb qarashni taklif etadi.

Shuningdek, "Birlashgan Millatlar Tashkiloti" ning Elektron hukumatni rivojlantirish bo'yicha hisobotlarida davlat sektorida inson kapitalini rivojlantirish kiberxavfsizlik strategiyalarining ajralmas qismi sifatida e'tirof etiladi. BMT ekspertlarining ta'kidlashicha, raqamli transformatsiya jarayonlarida kadrlar tayyorlash va qayta tayyorlash tizimi kuchli bo'lmagan davlatlarda kiberxavflar darajasi yuqori bo'ladi.

Kiberxavfsizlik bo'yicha xalqaro standartlar masalasida ISO/IEC tomonidan ishlab chiqilgan axborot xavfsizligi standartlari muhim nazariy va amaliy asos bo'lib xizmat qiladi. Ushbu standartlarda inson omiliga oid xavflarni boshqarish, xodimlarni muntazam o'qitish va axborot xavfsizligi madaniyatini shakllantirish alohida yo'nalish sifatida belgilangan [5, 6, 7].

Yuqoridagi ilmiy manbalar tahlili shuni ko'rsatadiki, raqamli transformatsiya sharoitida davlat xizmatchilarining kiberxavfsizlik kompetensiyalarini rivojlantirish kompleks va tizimli yondashuvni talab etadi. Mavjud tadqiqotlar asosida ishlab chiqilgan model ushbu ilmiy qarashlarni integratsiyalash orqali milliy davlat boshqaruvi tizimiga moslashtirilgan innovatsion yechim sifatida qaraladi.

TADQIQOT METODOLOGIYASI. Mazkur tadqiqot ilmiy-tizimli yondashuv asosida olib borildi va unda bir qator umumilmiy hamda maxsus tadqiqot metodlaridan foydalanildi. Tadqiqot metodologiyasi quyidagi asosiy yo'nalishlarni qamrab oldi:

Davlat boshqaruvida raqamli transformatsiya, kiberxavfsizlik va kompetensiyaviy yondashuvga oid mahalliy va xorijiy ilmiy adabiyotlar, normativ-huquqiy hujjatlar hamda strategik dasturlar tahlil qilindi. Xususan, kiberxavfsizlik

bo'yicha xalqaro standartlar, jumladan, ISO/IEC tomonidan ishlab chiqilgan axborot xavfsizligi standartlari asosiy nazariy manba sifatida o'rganildi [6, 7].

Davlat xizmatchilarining kiberxavfsizlik kompetensiyalarini rivojlantirish murakkab ko'p komponentli tizim sifatida qaraldi. Ushbu tizim bilim, amaliy ko'nikma, xulq-atvor, axloqiy mas'uliyat va tashkiliy madaniyat elementlarini o'z ichiga olgan holda modellandi.

Xorijiy davlatlar tajribasi, jumladan, rivojlangan raqamli hukumat tizimiga ega mamlakatlarning davlat xizmatchilarini kiberxavfsizlikka tayyorlash modellari taqqoslandi. Ushbu tahlil asosida umumiy tendensiyalar va samarali amaliy mexanizmlar aniqlanib, milliy sharoitga moslashtirildi.

Tadqiqotning asosiy natijasi sifatida davlat xizmatchilarining kiberxavfsizlik kompetensiyalarini rivojlantirish modeli ishlab chiqildi. Model konseptual, funksional va tashkiliy komponentlardan iborat bo'lib, ularning o'zaro aloqasi grafik va mantiqiy bog'lanishlar orqali asoslandi.

TADQIQOT NATIJALARI. O'tkazilgan tadqiqot natijalariga ko'ra, raqamli transformatsiya sharoitida davlat xizmatchilarining kiberxavfsizlik kompetensiyalarini rivojlantirish modeli quyidagi asosiy tarkibiy qismlardan iborat ekanligi aniqlandi [8, 9, 10].



MUHOKAMA. Tadqiqot natijalari shuni ko'rsatadiki, raqamli transformatsiya jarayonlarida kiberxavfsizlik masalasi faqat texnik infratuzilma bilan cheklanib qolmasligi lozim. Davlat xizmatchilarining kompetensiyalarini rivojlantirishga qaratilgan kompleks model inson omilidan kelib chiqadigan xavflarni sezilarli darajada kamaytirishga xizmat qiladi.

Xalqaro tajriba bilan taqqoslaganda, taklif etilgan modelning afzalligi shundaki, u texnik bilimlar bilan bir qatorda axloqiy va xulq-atvor jihatlarini ham qamrab oladi. Bu esa davlat boshqaruvida barqaror kiberxavfsizlik madaniyatini shakllantirishga imkon beradi. Shu bilan birga, modelni amaliyotga joriy etishda tashkiliy va moliyaviy resurslar yetarli darajada ta'minlanishi muhim ahamiyat kasb etadi.

Kelgusida mazkur modelni pilot loyihalar asosida sinovdan o'tkazish, empirik ma'lumotlar asosida takomillashtirish hamda raqamli davlat boshqaruvi strategiyalariga integratsiya qilish maqsadga muvofiqdir.

XULOSA. Xulosa qilib aytganda, raqamli transformatsiya sharoitida davlat boshqaruvi tizimining barqaror va uzluksiz faoliyat yuritishi davlat xizmatchilarining kiberxavfsizlik kompetensiyalarini rivojlantirish darajasiga bevosita bog'liqdir. Davlat sektorida joriy etilayotgan raqamli texnologiyalar axborot resurslarining hajmi va ahamiyatini oshirgan holda, ularni himoyalash masalasini strategik ustuvor yo'nalishga aylantirmoqda. Tadqiqot natijalari shuni ko'rsatadiki, kiberxavfsizlikni ta'minlash faqat texnik vositalar bilan cheklanib qolmasdan, inson omiliga asoslangan kompetensiyaviy yondashuvni talab etadi. Mazkur maqolada ishlab chiqilgan kiberxavfsizlik kompetensiyalarini rivojlantirish modeli bilimlar, amaliy ko'nikmalar, mas'uliyatli raqamli xulq-atvor va strategik fikrlashni o'z ichiga olgan yaxlit tizim sifatida asoslandi. Model davlat xizmatchilarining kiberxavflarni anglash, oldini olish va ularga samarali munosabat bildirish salohiyatini oshirishga xizmat qiladi. Shuningdek, taklif etilgan yondashuv davlat organlarida kiberxavfsizlik madaniyatini shakllantirish va mustahkamlash imkonini beradi. Tadqiqotda aniqlangan rivojlantirish mexanizmlari uzluksiz kasbiy ta'lim va amaliy mashg'ulotlar orqali kompetensiyalarni barqaror rivojlantirishga yo'naltirilgan. Modelning amaliy ahamiyati uning davlat boshqaruvi tizimida joriy etilishi orqali axborot xavfsizligiga oid xatarlarni kamaytirish imkoniyati bilan izohlanadi. Mazkur model raqamli davlatni rivojlantirish strategiyalarini amalga oshirishda samarali ilmiy-amaliy vosita bo'lib xizmat qilishi mumkin. Kelgusida modelni empirik tadqiqotlar asosida sinovdan o'tkazish va milliy sharoitlarga moslashtirish uning ilmiy qiymatini yanada oshiradi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Janowski T. Digital Government Evolution: From Transformation to Contextualization. Government Information Quarterly. <https://doi.org/10.1016/j.giq.2015.07.001>

2. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. *W.W. Norton & Company*. <https://www.schneier.com/books/>
3. Boyatzis R.E. Competencies in the 21st Century. *Journal of Management Development*. <https://doi.org/10.1108/02621710810840730>
4. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. *Wiley*. <https://www.cl.cam.ac.uk/~rja14/book.html>
5. OECD. (2020). Digital Government Index 2019: Results and Key Findings. <https://www.oecd.org/gov/digital-government/>
6. United Nations. (2022). E-Government Survey: The Future of Digital Government. <https://publicadministration.un.org/egovkb>
7. ISO/IEC. (2022). ISO/IEC 27001: Information Security Management Systems. <https://www.iso.org/isoiec-27001-information-security.html>
8. Qudratov, A. (2023). AXBOROT XAVFSIZLIGI FANINI QIZIQTIRUVCHI VA IJODIY TOPSHIRIQLAR ASOSIDA TASHKIL QILISH. Евразийский журнал технологий и инноваций, 1(5), 55-58.
9. Qudratov, A. (2023). PROBLEMS OF DEVELOPING STUDENTS'KNOWLEDGE. Modern Science and Research, 2(4), 729-733.
10. Sayfullayevich, J. U., Normamatovich, Q. A., O'G'Li, B. M. D., & O'G, R. J. G. O. (2024). NEYRON TARMOG 'IDA FAOLLASHTIRISH FUNKTSIYALARINING TAHLILI. Central Asian Journal of Multidisciplinary Research and Management Studies, 1(2), 120-130.
11. Kalandarov, A., Kalandarov, A., Abduraimov, D., & Anorbayev, M. (2024, November). Mathematical model of the coupled problem of thermoelasticity in stresses. In AIP Conference Proceedings (Vol. 3244, No. 1, p. 020013). AIP Publishing LLC.
12. Abduraimov, D. E. (2024). UNVEILING THE STAGES AND PERSPECTIVES OF INTEGRATING ARTIFICIAL INTELLIGENCE SYSTEMS INTO THE EDUCATIONAL PROCESS. Экономика и социум, (4-1 (119)), 102-106.