Kafedra mudiri:

Xudoyqulov Zarif To‘raqulovich

Qabul vaqti: Dushanba-Juma (14:00-16:00 gacha)
Telefon: (+99871) 238-65-38
E-mail: zarif.khudoykulov@tuit.uz

O‘zbekiston Respublikasi Vazirlar Mahkamasi Rayosatining 2016-yil 25-yanvardagi yig‘ilishining 5-son bayoni bilan tasdiqlangan Vazirlar Mahkamasining 2016-yil I yarim yilligi ish rejasining 10-bandiga muvofiq belgilangan vazifa ijrosini ta’minlash maqsadida, hamda vazirlik tomonidan TATUda “Axborot xavfsizligi” fakulteti va fakultet qoshidagi mutaxassislik kafedralarini tashkil etish bo‘yicha takliflarni ko‘rib chiqish yuzasidan, shuningdek, TATUda “Axborot xavfsizligi” fakultetini tashkil etish masalasi O‘zbekiston Respublikasi Axborot kommunikatsiyasi xavfsizligi masalalari bo‘yicha Texnik kengashning majlisining 2016-yil 18-iyuldagi 3-son bayonini va Toshkent axborot texnologiyalari universiteti 2016-yil 29-avgustdagi 1(661)-son Kengashining universitet tashkiliy tuzilmasiga o‘zgartirish kiritish masalasi bo‘yicha Qarori asosida “Kompyuter injiniringi” fakulteti tarkibidagi “Axborot xavfsizligi” kafedrasi “Axborot xavfsizligi” fakulteti tarkibiga o‘tkazildi va fakultet tashkil etildi.

“Axborot xavfsizligi” fakulteti tarkibida “Kriptologiya va diskret matematika” va “Axborot xavfsizligini ta’minlash” kafedralari tashkil etildi. Universitet rektorining 2019-yil 7-martdagi 439-sonli buyrug‘iga asosan kafedra nomi “Kriptologiya” nomiga o‘zgartirildi.

2016-yil 7-sentyabrdan 2019-yil 13-fevraliga qadar kafedra mudir lavozimini t.f.n. O.P.Axmedova bajardi. 2019-yil 13-fevraldan boshlab kafedra mudiri vazifasini PhD, dotsent Z.T.Xudoykulov bajarib kelmoqda.

Kafedra professor-o‘qituvchilari tomonidan bakalavr ta’lim yo‘nalishi va magistratura mutaxassisliklari bo‘yicha tahsil olayotgan talabalar uchun mashg‘ulotlar olib borilmoqda. Kafedra professor-o‘qituvchilari majburiy va tanlov fanlari bo‘yicha ma’ruzalar o‘qib, amaliy mashg‘ulotlar olib boradilar.

Kafedra professor-o‘qituvchilari tomonidan o‘qitiladigan fanlar bo‘yicha darsliklar, o‘quv qo‘llanmalari, laboratoriya va amaliy mashg‘ulotlar uchun uslubiy ko‘rsatmalar, bir qancha ma’ruza materiallari nashr etilgan.

Kafedra faoliyatining asosiy yo‘nalishi talabalarni axborot xavfsizligini ta’minlashning kriptografik usullarini o‘rgatishdan iborat. Kafedra axborot xavfsizligi sohasida, jumladan, ijro hokimiyati organlarida Respublikamizning milliy xavfsizligini ta’minlash bo‘yicha eng muhim vazifalarni hal etishga qodir mutaxassislarni tayyorlaydi.

Kafedra baklavriat ta’lim yo‘nalishi:

5330300 - Axborot xavfsizligi (sohalar bo‘yicha);

60610300 - Axborot xavfsizligi (sohalar bo‘yicha).

Kafedra magistratura mutaxassisliklari:

70610301 - Kriptografiya va kriptoanaliz;

70611004 – Telekommunikatsiya tizimlari va tarmoqlarida axborot xavfsizligi.

Kafedrada olib boriluvchi fanlar:

Bakalavr talabalari uchun:

- Kiberxavfsizlik asoslari;
- Kriptografiya 1;
- Kriptografiya 2;

- Dasturiy vositalar xavfsizligi;
- Foydalanishni boshqarish.

Magistratura talabalari uchun:

- Amaliy kriptografiya;
- Kriptografiya va tarmoq xavfsizligi;
- Dasturlar va ma’lumotlarni himoyalash;
- Tarmoqlarning yuqori xavfsizlik;
- Kriptoanaliz;
- Tarmoq kriminalistikasi;
- Zararli dasturlar tahlili;
- Zamonaviy kriptografiya;
- Kriptografik protokollar;
- Xavfsiz dasturlash (C/C++ tilida).

Kafedra professor-o‘qituvchilari:

- Xudoyqulov Zarif To‘raqulovich – kafedra mudiri, t.f.n., dotsent;
- Haydarov Elshod Dilshod o‘g‘li – dotsent v.b., PhD;
- Mardiyev Ulug‘bek Rasulovich – katta o‘qituvchi;
- Olimov Iskandar Salimboyevich – katta o‘qituvchi;
- Karimov Abduqodir Abdisalomovich – katta o‘qituvchi;
- Imomaliyev Aybek Turapbayevich - katta o‘qituvchi;
- Davronova Lola O‘ktamovna – katta o‘qituvchi;
- Axmedova Nozima Farxod qizi – katta o‘qituvchi;
- Tursunov Otabek Odiljon o‘g‘li – assistent;
- Jabbarov Nuriddin Akbarovich - assistent;
- Qozoqova To‘xtajon Qahramon qizi - assistent;
- Qurbonaliyeva Dilshoda Vali qizi - assistent;
- Daminov Akmal Abdurasulovich – o‘qituvchi-stajiyor;
- Hamidov Sherzod Jalolidding o‘g‘li – tayanch doktorant;
- Bozorov Suhrob Mo‘min o‘g‘li - tayanch doktorant.

Kafedrada faoliyat olib boruvchi o‘rindosh professor-o‘qituvchilar:

- Irgasheva Durdona Yakubdjanovna – DSc, professor;
- Toshev Komil Axmatovich – t.f.n., dotsent;
- Ahmedova Oydin Po‘latovna – t.f.n;
- Allanov Orif Menglimuratovich – PhD.

Kafedraning ilmiy uslubiy ishlari:

1. T.Xudoykulov, I.M. Boyquziyev, O.M.Allanov, U.R.Mardiyev, N.A.Jabbarov. Kriptografik usullar, O‘quv qo‘llanma, -T.: “Lesson-Press”, 2023, -255 b.
2. T.Xudoykulov, I.M. Boyquziyev, O.M.Allanov, I.S.Olimov, O.O.Tursunov, U.U.Tojiakbarova. Kriptografiya 2, O‘quv qo‘llanma, -T.: “Lesson-Press”, 2023, -187 b.
3. T.Xudoykulov, SH.Z.Islomov, U.R.Mardiyev, Kriptografiya 1, O‘quv qo‘llanma, -T.: “Iqtisod-Moliya”, 2021, - 204 b.
4. K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov, Kiberxavfsizlik asoslari, -T.: “Iqtisod-Moliya”, 2021, -228 b.
5. С.К.Ганиев, З.Т.Худойкулов, Н.Б.Насруллаев, Основы кибербезопасности, Учебное пособие, -Т.: “Iqtisod-Moliya”, 2021, 240 с.
6. M.Karimov, J.T.Arziyeva, Z.T.Xudoyqulov, Bir martali parollar asosida foydalanuvchilarni autentifikatsiyalash protokollari, Monografiya, -T.: “Iqtisod-Moliya”, 2021, - 120 b.

7. A.Tashev, Z.T.Xudoyqulov, Yuz tasviri asosida shaxsni identifikatsiyalash va autentifikatsiyalash jarayonining samaradorligini oshirish, Monografiya, -T.:”Nihol print”, 2021 yil, 124 bet.
8. O.Po‘latovna, X.P.Hasanov, M.H.Nazarova, I.U.Xolimtayeva, O.D.Nuritdinov, Axborot xavfsizligi protokollari, O‘quv qo‘llanma, -T.:”Aloqachi”, 2019, 168 bet.
9. Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtayeva, Kriptografiyaning matematik asosi, O‘quv qo‘llanma, -T.:”Aloqachi”, 2019, 192 bet.
10. K.Ganiev, M.M.Karimov, Z.T.Xudoyqulov, M.M.Kadirov. Axborot xavfsizligi bo‘yicha atama va tushunchalarning rus, o‘zbek va ingliz tillaridagi izohli lug‘ati. –T.: «Iqtisod-moliya», - 2017, 480 bet.

Kafedra professor-o‘qituvchilari va ilmiy izlanuvchilarining chop etilgan maqolalar ro‘yhati:

1. Boykuziev I., Angshuman K., Abdurakhimov B., Rupayan D. and Khudoykulov Z. Integral cryptanalysis: a new key determination technique for 3-phase Kuznyechik encryption. Engineering Research Express, 2023, Volume 5, Number 3, -p. 1-11.
2. Khudoykulov Z., Karimov A., Abdurakhmanov R., Mirzabekov M. Authentication in Cloud Computing: Open Problems. 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), 06-08 July 2023, DOI: 10.1109/ICESC57686.2023.10193438.
3. Bozorov S. Optimizing neural network architecture for enhanced attack detection: a comprehensive approach. Innovative Development in Educational Activities, 2(23), 62–74.
4. Elchiyev J., Karimov A.A., Tursunov O.O. Security and privacy issues in cloud computing. Axborotkommunikatsiyalar: tarmoqlar-texnologiyalar – yechimlar respublika jurnali, 4(68)/2023, 35-42 b.
5. Ortiqboyev A.M., Qurbonaliyeva D.V. Axborot xavfsizligida tarmoq stegonografiyasining o‘rni va uni yaratish usullarining qiyosiy tahlili. Axborotkommunikatsiyalar: tarmoqlar-texnologiyalar – yechimlar respublika jurnali, №3(67)/2023, 18-27 б.
6. Xudoyqulov Z.T., Rahmatullayev I.R., Boyqo‘ziyev I.M. Bardoshli statik S-bokslarni generatsiyalash algoritmi. 2023, №3(5), Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali, -C. 57-66.
7. Xudoyqulov Z.T., Rahmatullayev I.R. Dasturiy amalga oshirishga qulay kriptobardoshli statik S-boxlarni generatsiyalash algoritmi. “Milliy standart” ilmiy-texnik jurnali, 2023/4-son, -p.64-68.
8. Xudoyqulov Z.T., Rahmatullayev I.R., Umurzoqov O.Sh. NSA algoritmining akslantirishlari tanlanishining xavfsizlik talablarini bajarilishidagi o‘rni. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali, 2023 № 4(6), -b. 97-101.
9. Xudoyqulov Z.T., Tojiakbarova U.U., Boltayev F.H., Dasturiy ko‘rinishda amalga oshirishga qulay oqimli shifrlash algoritmi, «Axborotkommunikatsiya: Tarmoqlar, Texnologiyalar, Yechimlar» Har chorak ilmiy-texnik jurnal. №1(57)/ 2021 y. –C.35-43.
10. Xudoyqulov Z.T., Karimov A.A., Ortiqboyev A.M., Bulutli hisoblash tizimlarida xavfsizlik muammolarining tahlili, «Axborotkommunikatsiya: Tarmoqlar, Texnologiyalar, Yechimlar» Har chorak ilmiy-texnik jurnal. №2(58)/ 2021 y. –C.36-41.
11. Xudoyqulov Z.T., Tojiakbarova U.U., Ortiqboyev A.M., Elektron ovoz berish protokollarining qiyosiy tahlili, «Axborotkommunikatsiya: Tarmoqlar, Texnologiyalar, Yechimlar» Har chorak ilmiy-texnik jurnal. №3(59)/ 2021 y. –C.56-64.
12. Abduraximov B.F., Xudoyqulov Z.T., Allanov O.M., Islomov Sh.Z., DES algoritmining chiziqli kriptotahlili, «Axborotkommunikatsiya: Tarmoqlar, Texnologiyalar, Yechimlar» Har chorak ilmiy-texnik jurnal. №3(51)/ 2019 y. –C.56-61.
13. Xudoyqulov Z.T., Arziyeva J.T., Ortiqboyev A.M., Bir martali parol generatorlarining tahlili, «Axborotkommunikatsiya: Tarmoqlar, Texnologiyalar, Yechimlar» Har chorak ilmiy-texnik jurnal. №3(51)/ 2019 y. –C.48-55.
14. Karimov M.M., Arziyeva J.T., Xudoykulov Z.T., Анализ метода аутентификации на основе одноразовых паролей, Muhammad al-Xorazmiy avlodlari. Ilmiy-amaliy va axborot-tahliliy jurnal. 4(10)/2019, -C. 3-6.

15. Karimov M.M., Arziyeva J.T., Xudoykulov Z.T., Атаки направленные на методы аутентификации по паролю, Muhammad al-Xorazmiy avlodlari. Ilmiy-amaliy va axborot-tahliliy jurnal. 4(10)/2019, -C. 156-159.
16. Xudoykulov Z., Rustamova S., Polvonov N., Yoriqulov M., Bulutli hisoblash tizimida xavfsizlikni ta'minlash algoritmi, Muhammad al-Xorazmiy avlodlari. Ilmiy-amaliy va axborot-tahliliy jurnal. 3(13)/2020, -C. 30-38.
17. Bakhtiyor Abdurakhimov, Zarif Khudoykulov, Allanov Orif, Ilkhom Boykuziev, Algebraic Cryptanalysis of O'zDSt 1105:2009 Encryption Algorithm, International Conference on Information Science and Communications Technologies ICISCT 2020 Applications, Trends and Opportunities, 4th, 5th and 6th of November 2020, Tashkent Uzbekistan, -C.1-7.
18. Bakhtiyor Abdurakhimov, Zarif Khudoykulov, Allanov Orif, Ilkhom Boykuziev, Differential Collisions in SHA-1, International Conference on Information Science and Communications Technologies ICISCT 2020 Applications, Trends and Opportunities, 4th, 5th and 6th of November 2020, Tashkent Uzbekistan, -C.1-5.
19. Karimov M.M., Khudoykulov Z.T., Arziyeva J.T., A Method of Efficient OTP Generation Using Pseudorandom Number Generators, International Conference on Information Science and Communications Technologies ICISCT 2019, 4th, 5th and 6th of November 2019, Tashkent Uzbekistan, -C.1-4.
20. Abdurakhimov B.F., Khudoykulov Z.T., Allanov O.M., Boykuziev I.M., Analysis of algebraic properties of transformation of O'zDSt 1105:2009 algorithm, International Conference on Information Science and Communications Technologies ICISCT 2019, 4th, 5th and 6th of November 2019, Tashkent Uzbekistan, -C.1-3.
21. Khudoykulov Z.T., Shirinov L.T., Analysis of Security Protocols in Wireless Sensor Networks, International Conference on Information Science and Communications Technologies ICISCT 2019, 4th, 5th and 6th of November 2019, Tashkent Uzbekistan, -C.1-4.
22. Tashev K.A., Khudoykulov Z.T., Arziyeva J.T., Improvement of a Security Enhanced One-time Mutual Authentication and Key Agreement Scheme, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-12, October 2019, -P.5031-5036.
23. Tashev K.A., Khudoykulov Z.T., Islomov Sh.Z., Salimova H.R., Normalization of Facial Occlusion in Face Recognition, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-11, September 2019, -P.2523-2527.
24. Karimov M.M, Tashev K.A., Islomov Sh.Z., Mavlonov O.N. Triangle Method for Fast Face Detection on the Wild. Journal of Multimedia Information System VOL. 5, NO. 1, March 2018 (pp. 15-20).
25. Xudoyqulov Z.T., Allanov O.M., Xolimtoeva I.U. Zamonaviy xesh funksiyalarning xavfsizlik va tezlik xususiyatlari asosida tahlili. Axborotkommunikatsiyalar: Tarmoqlar, Texnologiyalar, Yechimlar. 2(46)2018.
26. Tashev K.A., Khudoykulov Z.T., Islomov SH.Z. Analyzing of face recognition algorithms. Axborotkommunikatsiyalar: Tarmoqlar, Texnologiyalar, Yechimlar. 2(46)2018.
27. Xudoyqulov Z.T., Islomov Sh.Z., Allanov O.M., Mardiyev U.R. A practical implementation of fingerprint based fuzzy commitment scheme. European Science Review. -Austria, Vienna- 2018. № (5-6). -P. 108-112.
28. Xudoyqulov Z.T., Ganiyev S.K., Halimtoeva I.U. Computer's source based (Pseudo) Random Number Generation. International Conference on Information Science and Communications Technologies (ICISCT). 2017. IEEE. – P. 1-6.
29. Xudoyqulov Z.T., Yusupov B.K. Comparative factors of key generation techniques. International Conference on Information Science and Communications Technologies (ICISCT), IEEE, 2016.
30. Ganiyev S.K., Xudoyqulov Z.T. Biometric cryptosystems: open issues and challenges. International Conference on Information Science and Communications Technologies (ICISCT), IEEE, 2016.

Kafedraning rivojlanishidagi hamkorliklar:

- Janubiy Koreya institutlari (KAIST, INXA);
- Rossiyaning yetakchi universitetlari.

Kafedraning rivojlanishidagi soha korxonalari bilan hamkorliklar:

- «UNICON.UZ» MCHJ;
- “Kiberxavfsizlik markazi” DUK.