Head of the department:

Khudoykulov Zarif Turakulovich

Hours: Monday-Friday (14:00-16:00)
Phone: (+99871) 238-65-38
E-mail: zarif.khudoykulov@tuit.uz

For the purpose to ensure the implementation of the plan of tasks for the first half of 2016 (10 appendixes) of the meeting of the Presidium of the Cabinet of Ministers (pr. №5 from 25 January 2016), as well as on the proposal of the Ministry of Development of Information Technologies and Communications of the Republic of Uzbekistan the creation of the faculty "Information security"and the specialized departments as part of the faculty, as well as for the approval of this proposal in the Council on the technical safety of the Ministry of ICT on the development of information technologies and communications of the Republic of Uzbekistan (pr. №3 from 18 July, 2016) and by the decision of the Tashkent University of information Council technologies (dec. №1 (661) from 29 August 2016) established the Faculty of "Information security" with the specialized departments of "Providing information security" and "Cryptology and discrete mathematics" at the department "Information security" of the faculty "Computer engineering".

A specialized department “Cryptology and discrete mathematics” was created within the faculty. In 2019, the department of “Cryptology and Discrete Mathematics” was renamed the department of “Cryptology” (order of the university rector No. 439 dated March 7, 2019).

In 2016-2019, the department was headed by candidate of technical sciences Akhmedova Oydin Pulatovna. Since February 13, 2019, the department has been headed by Doctor of Philosophy in Technical Sciences Khudoykulov Zarifjon Turakulovich.

Professors and teachers of the department conduct classes for students enrolled in bachelor's and master's programs. Teachers of the department give lectures and conduct practical classes in general and selective subjects.

The teaching staff of the department published textbooks, methodological instructions for laboratory and practical classes, and a number of lecture materials on the disciplines taught.

The main activity of the department is training students in cryptographic methods of information security. The department trains specialists capable of solving the most important tasks to ensure the national security of the Republic in the information sphere, and, above all, in executive authorities.

Directions of undergraduate education:

5330300 – Information security (by industry)

60610300 – Information security (by industry)Master's Specialties

List of master's specialties:

70610301 - Cryptography and cryptanalysis;

70611004 - Information security of telecommunication systems and networks.

Subjects of the department:

Bachelor:

- Fundamentals of Cybersecurity;
- Cryptology 1;
- Cryptology 2;

- Software Security
- Access control

Master:

- Applied cryptography;
- Information security in multimedia communication networks;
- Software and data protection;
- Advanced security of networks;
- Information security in optical transmission systems and networks;
- Cryptanalysis;
- Network forensics;
- Malware analysis;
- Cryptographic protocols;
- Secure programming (in C / C ++).

Professors and teachers staff of the department:

- Khudoykulov Zarif Turakulovich - head of Department, PhD;
- Khaidarov Elshod Dilshod ugli – Associate Professor, PhD;
- Mardiyev Ulugbek Rasulovich – teacher;
- Olimov Iskandar Salimboevich – teacher;
- Karimov Abduqodir Abdisalomovich – teacher;
- Imomaliyev Aybek Turapbayevich- teacher;
- Davronova Lola Uktamovna- teacher;
- Axmedova Nozima Farxod qizi- teacher;
- Tursunov Otabek Odiljon ugli – assistant;
- Jabbarov Nuriddin Akbarovich– assistant;
- Qozoqova Tuxtajon Qahramon qizi – assistant;
- Kurbanalieva Dilshod Vali qizi – assistant;
- Daminov Akmal Abdurasulovich – trainee teacher;
- Hamidov Sherzod Jalolidding ugli - PhD student;
- Bazorov Suhrobjon Mumin ugli- PhD

Professors-teachers of the department leading hourly activities:

- Isaev Rixsi Isaxodjaevich – PhD, professor;
- Tashev Komil Axmatovich – PhD, associate professor;
- Irgasheva Durdona Yakubdjanovna – DSc, associate professor;
- Ahmedova Oydin Po’latovna – PhD;
- Allanov Orif Menglimuratovich –

Scientific and methodological work of the department:

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.

Scientific works of the faculty and research staff:

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.

The cooperation of the Department:

- Institutions of South Korea (KAIST, INHA);
- Leading Russian Universities.

Cooperation with enterprises:

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