Заведующий кафедрой:

Худайкулов Зариф Туракулович

Время приема: Понедельник-Пятница (14:00-16:00)
Телефон: (+99871) 238-65-38
E-mail: zarif.khudoykulov@tuit.uz
Краткая история кафедры:

В целях обеспечения выполнения задач, поставленных в соответствии с планом работы Кабинета Министров Республики Узбекистан на первое полугодие 2016 года (10 - пункт) утвержденного на заседания (пр. №3 от 25 января 2016 года) и по рассмотрению предложения Министерство о создание факультета «Информационная безопасность» и специализированных кафедр, а также по одобрению этого предложения в техническом совете по вопросам информационно-коммуникационной безопасности (пр. №3 от 18 июля 2016 года) и на основании решения Совета Ташкентского университета информационных технологий по вопросу изменения организационной структуры университета (№1(661) от 29 августа 2016 года) был создан факультет «Информационная безопасность» и кафедра «Информационная безопасность» была передана из состава факультета «Компьютерный инжиниринг» на факультет.

В составе факультете была создана специализированная кафедры «Криптология и дискретная математика». В 2019 году кафедра «Криптология и дискретная математика» была переименована в кафедру «Криптология» (приказ ректора университета № 439 от 7 марта 2019 года).

В 2016-2019 годах кафедру возглавляла кандидат технических наук Ахмедова Ойдин Пулатовна. С 13 февраля 2019 года кафедру возглавляет доктор философии по техническим наукам Худойкулов Зарифжон Туракулович.

Профессора и преподаватели кафедры ведут занятия для студентов обучающихся на программах бакалавриата, магистратуры. Преподаватели кафедры читают лекции и ведут практические занятия по общим и выборочным предметам.

Профессорско-преподавательским составом при кафедре были изданы учебные пособия, методические указания к лабораторным и практическим занятиям, ряд лекционных материалов по преподаваемым дисциплинам.

Основное направление деятельности кафедры – обучение студентов владению криптографическими методами защиты информации. Кафедра готовит специалистов, способных решать важнейшие задачи по обеспечению национальной безопасности Республики в информационной сфере, и, прежде всего, в органах исполнительной власти.

Направлений образования бакалавриата:

5330300 – Информационная безопасность (по отраслям)

60610300 – Информационная безопасность (по отраслям)

Список специальностей магистратуры:

70610301 - Криптография и криптоанализ;

70611004 - Информационная безопасность телекоммуникационных систем и сетей.

Список дисциплин, преподаваемых на кафедре:

Предметы бакалавриата:

- Основы кибербезопасности;
- Криптография 1;
- Криптография 2;
- Безопасность программных средств
- Управления доступом.

Предметы магистратуры:

- Прикладная криптография
- Криптография и безопасность сети
- Защита программ и данных
- Высокая безопасность сетей
- Криптоанализ
- Сетевая криминалистика
- Анализ вредоносных программ
- Современная криптография
- Криптографические протоколы
- Безопасное программирование (языке C/C++)

Профессорско-преподавательский состав кафедры: основной

- Худойкулов Зариф Туракулович – заведующий кафедрой, PhD, доцент;
- Хайдаров Элшод Дилшод угли – и.о. доцент, PhD;
- Давронова Лола Уктамовна – и.о. доцент, PhD;
- Мардиев Улугбек Расулович – старший преподаватель;
- Олимов Искандар Салимбоевич – старший преподаватель;
- Каримов Абдикодир Абдисаломович – старший преподаватель;
- Имамалиев Айбек Турапбаевич – старший преподаватель;
- Ахмедова Нозима Фарходовна – старший преподаватель;
- Турсунов Отабек Одилжон угли – ассистент;
- Жаббаров Нуриддин Акбарович – ассистент;
- Козокова Тухтажон Кахрамон кизи – ассистент;
- Курбаналиева Дилшода Вали кизи – ассистент;
- Даминов Акмал Абдурасулович – стажёр-преподаватель;
- Хамидов Шерзод Жалолиддин угли – слушатель базовой докторантуры;
- Базоров Сухробжон Мумин угли – слушатель базовой докторантуры.

Профессорско-преподавательский состав кафедры: по совместительству

- Иргашева Дурдона Якубджановна – д.т.н., профессор, DSc
- Ташев Комил Ахматович – к.т.н., доцент
- Ахмедова Ойдин Пулатовна – к.т.н.
- Алланов Ориф Менглимуратович – доцент, PhD

Научно-методические работы кафедры:

1. Худойкулов З.Т., Бойкузиев И.М., Алланов О.М., Мардиев У.Р., Жаббаров Н.А. Криптографические методы (узбекский), Учебник, -Т.: “Lesson-Press”, 2023, -255 с.
2. Худойкулов З.Т., Бойкузиев И.М., Алланов О.М., Олимов И.С., Турсунов О.О., Тожиакбарова У.У. Криптография 2 (узбекский), Учебник, -Т.: “Lesson-Press”, 2023, -187 с.
3. Худойкулов З.Т., Исламов Ш.З., Мардиев У.Р. Криптография 1 (узбекский), Учебник, -Т.: «Iqtisod-Moliya», 2021, - 204 с.
4. Ганиев С.К., Ганиев А.А., Худойкулов З.Т., Основы кибербезопасности (узбекский), Учебник, -Т.: «Iqtisod-Moliya», 2021, - 228 с.

5. С.К.Ганиев, З.Т.Худойкулов, Н.Б.Насруллаев, Основы кибербезопасности, Учебное пособие, -Т.: “Iqtisod-Moliya”, 2021, 240 с.
6. Каримов М.М., Арзиева Ю.Т., Худойкулов З.Т. Протоколы аутентификации пользователей на основе одноразовых паролей, Монография (узбекский), -Т.: «Iqtisod-Moliya», 2021, - 120 с.
7. Ташев К.А., Худойкулов З.Т. Повышение эффективности процесса идентификации и аутентификации на основе изображений лиц, Монография (узбекский), -Т.: «Nihol print», 2021, 124 с.
8. Пулатовна А.О., Хасанов Х.П., Назарова М.Х., Холимтаева И.У., Нуритдинов О.Д. Протоколы информационной безопасности, Учебное пособие (узбекский), -Т.: «Aloqachi», 2019, 168 с.
9. Акбаров Д.Ю., Хасанов П.Ф., Хасанов Х.П., Ахмедова О.П., Холимтаева И.У. Математические основы криптографии, Учебное пособие (узбекский), -Т.: «Aloqachi», 2019, 192 с.
10. Ганиев С.К., Каримов М.М., Худойкулов З.Т., Кадиров М.М. Аннотированный словарь терминов и понятий по информационной безопасности на русском, узбекском и английском языках (узбекский). –Т.: «Iqtisod-Moliya», - 2017, 480 с.

Список научных трудов профессорско-преподавательского и исследовательского состава кафедры:

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.

Сотрудничество по развитии кафедры:

- Институты Южной Кореи (KAIST, INXA);
- Ведущие университеты России.

Сотрудничество с отраслевыми предприятиями по развитии кафедры:

- «UNICON.UZ» ООО;
- «Центр кибербезопасности» ГУК;