

Заведующий кафедрой:

Худайкулов Зариф Туракулович

Время приема: Понедельник-Пятница (14:00-16:00)

Телефон: (0371)-238-65-38

E-mail: zarif.xudoyqulov@mail.ru

С целью обеспечения выполнения задач плана за первое полугодие 2016 года (10 приложение) работы заседания Президиума Кабинета Министров Республики Узбекистан (пр. №5 от 25 января 2016 года), а также по предложению Министерства по развитию информационных технологий и коммуникации Республики Узбекистан создание факультета «Информационная безопасность» и специализированных кафедр в составе этого факультета, а также по одобрению этого предложения в техническом совете по безопасности ИКТ Министерства по развитию информационных технологий и коммуникации Республики Узбекистан (пр. №3 от 18 июля 2016 года) и по решению Совета Ташкентского университета информационных технологий (пр. №1 (661) от 29 августа 2016 года) создан факультет «Информационная безопасность» с специализированными кафедрами «Обеспечение информационной безопасности» и «Криптология и дискретная математика» на базе кафедры «Информационная безопасность» факультета «Компьютерный инжиниринг».

Приказом ректора университета № 439 от 7 марта 2019 года кафедра переименована в «Криптология». Заведующей кафедрой с 7 сентября 2016 г. по 13 февраля 2019 г. к.т.н. О.П. Ахмедова. С 13 февраля 2019 года заведующим кафедрой является доцент, PhD З.Т. Худойкулов. В 2021-2022 учебном году кафедре работают профессор, к.т.н. Р.Исаев, доцент, DSc, Д.Иргашева, доцент, к.т.н. К.Ташев, к.т.н. О. Ахмедова, PhD, О.Алланов по совместительству, в основном штате, старший преподаватель У. Мардиев, ассистенты И. Олимов, А. Каримов, О. Турсунов, У. Тоджиабарова и докторанты и стажер-исследователи кафедры, И. Холимтоева, А. Имомалиев, Л. Давронова, Н. Ахмедова, Ш. Хамидов, С. Бозоров.

В 2021-2022 учебном году профессора-преподаватели кафедры проводят лекции и практические занятия по предметам и выборочным предметам специальности, магистрантам «Прикладная криптография», «Информационная безопасность в мультимедийных сетях», «Программы и защита данных», «Высокая безопасность сетей», «Информационная безопасность в системах и сетях оптической передачи», «Криптоанализ», «Сетевая криминалистика», «Анализ вредоносных программ», «Криптографические протоколы», «Безопасное программирование (языке C/C++)», бакалаврам «Основы кибербезопасности», «Криптография 1», «Криптография 2».

В 2021 году преподаватели кафедры издали учебники «Основы кибербезопасности» (на узбекском и русском языках), «Криптография 1». Также получили учёные степени Д. Иргашева DSc и О. Алланов PhD.

По направлению бакалавриатуры:

- 5330300 - Информационная безопасность

По специальностям магистратуры:

- 5A330301 - Криптография и криптоанализ
- 5A350104 - Информационная безопасность телекоммуникационных систем и сетей.

Учебные дисциплины, читаемые на кафедре

По направлению бакалавриатуры:

- Информационная безопасность
- Стеганографические методы
- Безопасность баз данных
- Криптографические методы
- Протоколы информационной безопасности
- Идентификация и аутентификация

По специальности магистратуры:

- Прикладного криптографии и криптоанализ
- Разработка безопасных программных средств
- Защиты информации в оптических сетях и системах
- Методы и средства криптографической защиты информации
- Разработка криптографической инфраструктуры и ее эксплуатация

Профессорско-преподавательский состав кафедры

- Худойкулов Зариф Туракулович – заведующий кафедрой, к.т.н.
- Мардиев Улугбек Расулович – старший преподаватель
- Олимов Искандар Салимбоевич - ассистент
- Каримов Абдикодир Абдисаломович - ; ассистент
- Турсунов Отабек Одилжон угли - ассистент
- Тожиакбарова Умида Усмонжоновна - ассистент
- Давронова Лола Уктамовна - слушатель базовой докторантуре
- Холимтаева Икбола Убайдуллаевна - слушатель базовой докторантуре
- Хамидов Шерзод Жалолиддин угли - стажер-исследователь
- Базоров Сухробжон Мумин угли - стажер-исследователь

Профессоры-преподаватели кафедры ведущие почасовую деятельность:

- Исаев Рихси Исаходжаевич - к.т.н., профессор
- Ташев Комил Ахматович - к.т.н., доцент
- Иргашева Дурдона Якубджановна - к.т.н., доцент
- Ахмедова Ойдин Пулатовна - к.т.н.
- Алланов Ориф Менглимуратович - PhD
-

Научно-исследовательские работы:

- Ф-706-17 – Исследование применения биометрико – криптографических технологий в информационных системах. Руководитель: Иргашева Д.Я.

Научно-методические работы кафедры:

1. Худойкулов З.Т., Исламов Ш.З., Мардиев У.Р. Криптография 1 (узбекский), Учебник, -Т .: «Iqtisod-Moliya», 2021, - 204 с.
2. Ганиев С.К., Ганиев А.А., Худойкулов З.Т., Основы кибербезопасности, Учебник, -Т .: «Iqtisod-

- Moliya», 2021, - 228 с.
3. С.К.Ганиев, З.Т.Худойкулов, Н.Б.Насруллаев, Основы кибербезопасности (узбекский), Учебное пособие, -Т.: «Iqtisod-Moliya», 2021, 240 с.
 4. Каримов М.М., Арзиева Ю.Т., Худойкулов З.Т. Протоколы аутентификации пользователей на основе одноразовых паролей, Монография (узбекский), -Т.: «Iqtisod-Moliya», 2021, - 120 с.
 5. Ташев К.А., Худойкулов З.Т. Повышение эффективности процесса идентификации и аутентификации на основе изображений лиц, Монография (узбекский), -Т.: «Nihol print», 2021, 124 с.
 6. Пулатовна А.О., Хасанов Х.П., Назарова М.Х., Холилтаева И.У., Нуритдинов О.Д. Протоколы информационной безопасности, Учебное пособие (узбекский), -Т.: «Aloqachi», 2019, 168 с.
 7. Акбаров Д.Ю., Хасанов П.Ф., Хасанов Х.П., Ахмедова О.П., Холилтаева И.У. Математические основы криптографии, Учебное пособие (узбекский), -Т.: «Aloqachi», 2019, 192 с.
 8. 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.
 9. Ганиев С.К., Каримов М.М., Ташев К.А.. Информационная безопасность. Учебник (узбекский). -Т.: «Fan va texnologiya», 2016, 372 с.
 10. Ганиев С.К., Каримов М.М., Ташев К.А.. Информационная безопасность. Безопасность информационных и коммуникационных систем. Учебное пособие (узбекский). -Т.: «Aloqachi», 2008, 382 с.

Научные труды профессорско-преподавательского и исследовательского состава:

1. 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. -С.35-43.
2. 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. -С.36-41.
3. 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. -С.56-64.
4. 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. -С.56-61.
5. 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. -С.48-55.
6. 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, -С. 3-6.
7. 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, -С. 156-159.
8. 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, -С. 30-38.
9. 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.
10. 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.
 11. 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.
 12. 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.
 13. 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.
 14. 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.
 15. 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.
 16. 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).
 17. 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.
 18. Tashev K.A., Khudoykulov Z.T., Islomov SH.Z. Analyzing of face recognition algorithms. Axborotkommunikatsiyalar: Tarmoqlar, Texnologiyalar, Yechimlar. 2(46)2018.
 19. 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.
 20. 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.
 21. Xudoyqulov Z.T., Yusupov B.K. Comparative factors of key generation techniques. International Conference on Information Science and Communications Technologies (ICISCT), IEEE, 2016.
 22. Ganiyev S.K., Xudoyqulov Z.T. Biometric cryptosystems: open issues and challenges. International Conference on Information Science and Communications Technologies (ICISCT), IEEE, 2016.
 23. Irgasheva D.Ya., Rustamov F. Digital signature electron commerce, TATU xabarlari (Vestnik) (1(33)) 2015 yil, 96-100 bet.
 24. Irgasheva D.Y. Role model with zone differentiation of access IJRET: International Journal of Research in Engineering and Technology. Volume:05. Issue:05, May 2016. <http://ijret.esatjournals.org>. eISSN-2319-1163, pISSN 2321-7308.
 25. Д.Я.Иргашева А.К.Усманов Разработка ролевой модели с зональным разграничением доступа Международный научный журнал «Наука и Мир» (№6 (34), июнь).
 26. Karimov, K.Tashev, Sh.Islomov. Increasing accuracy and reducing time of face recognition with Euclid norm. International Journal of Recent and Innovation trends in Computing and

Свидетельство об официальной регистрации программы для ЭВМ

- Tashev K.A., Xudoyqulov Z.T., Arziyeva J.T., Arziyev A.T., Yoriqulov M., Rustamova S.R., Secure SMS authenticator, № DGU 07387,12.2019.
- Tashev K.A., Xudoyqulov Z.T., Arziyeva J.T., Arziyev A.T., Yoriqulov M., Rustamova S.R., Secure OTP Authenticator, № DGU 07386,12.2019.
- Xudoyqulov Z.T., Arziyeva J.T., Arziyev A.T., Yoriqulov M., Secure OTP Reader, № DGU 07388,12.2019.
- Abduraximov B.F., Allanov O.M., Boykuziyev I.M., Xudoyqulov Z.T., Karimov Z.T., Olimov I.S., Xamidov Sh.J., Bozorov A.S., Qurbanova F.Ch., "O'zDST 1105:2009 shifrlash algoritmini algebraik kriptotahlil uchun ishlab chiqilgan dasturiy ta'minoti", № DGU 07494, 08.01.2020.
- Ganiyev S.K., Xudoyqulov Z.T., Zokirov O.Yo., Abduraxmonov A.A., Xolimtoyeva I.U., Koraboyev E.A., Shakarov M.A., "Mobile CC Authentication dasturiy vositasi", № DGU 09367, 11.11.2020.
- Ganiyev S.K., Xudoyqulov Z.T., Zokirov O.Yo., G'ulomov Sh.R., Nasrullayev N.B., Abduraxmonov A.A., CC Authentication dasturiy vositasi, № DGU 09196, 19.10.2020.
- Ganiyev S.K., Toshev K.A., Irgasheva D.Ya., Xudoyqulov Z.T., Gaipnazarov R.T., Rustamova S.R., CAC - foydalanishni cheklash tizimi, № DGU 09478, 25.11.2020.
- Ganiyev S.K., Toshev K.A., Irgasheva D.Ya., Xudoyqulov Z.T., Islomov Sh.Z., Rustamova S.R., RBAC - foydalanishni cheklash tizimi, № DGU 09608, 07.12.2020.
- Tashev K.A., Xudoyqulov Z.T., Nasrullayev N.B., Yoriqulov M.R., Shakarov M.A., Raxmonqulova M.R., YANGI ANTIVIRUS, № DGU 10671, 30.03.2021.
- Ganiev S.K., Xudoyqulov Z.T., Normuminov F.Q., Xolimtoeva I.U., Davronova L.O', Imamaliyev A.T., Allanov O.M., Karimov A.A., Eshonqulov N.D. WIN RNG, № DGU 05402, 06.2018.
- Tashev K.A., Irgasheva D.Ya., Axmedova O.P., Xudoyqulov Z.T., Islomov SH.Z., Mardiyev U.R., Allanov O.M., Ostonov M.B., BIO KEY BINDING SYSTEM, № DGU 05725, 24.10.2018.
- Tashev K.A., Irgasheva D.Ya., Axmedova O.P., Xudoyqulov Z.T., Islomov SH.Z., Mardiyev U.R., Safarov A.R., Axmadjonov A.M., Ergashev M.M., BIO KEY RELEASE, DGU 05401, 13.06.2018.

Договора о сотрудничестве кафедры с зарубежными странами:

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

Договора о сотрудничестве кафедры с предприятиями и организациями отрасли:

- "UNICON.UZ" DUK
- «Центр кибербезопасности» ГУК;