



Формирование кадрового потенциала в области кибербезопасности в Республике Узбекистан

Аюбджанова Венера Усмановна

Актуальность и статистика состояния кибербезопасности в Республике Узбекистане

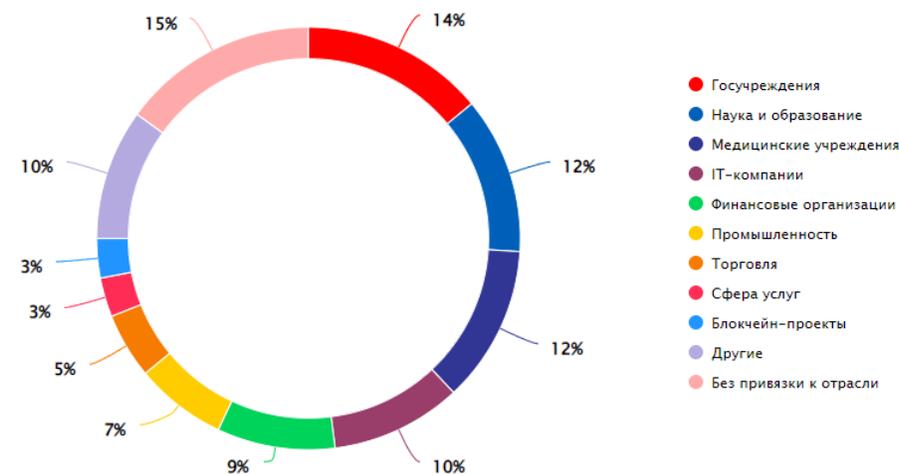
Увеличение числа кибератак на государственные информационные ресурсы и системы, на промышленные сегменты включая объекты критической информационной инфраструктуры, требует необходимости в усилении мер кибербезопасности и подготовке высококвалифицированных кадров и специалистов для противодействия новым видам угроз.

2022 г. < 10 млн. кибератак.

2023 г. < 11 млн. кибератак.

2024 г. < 12,5 млн. кибератак.

В условиях быстро меняющихся цифровых технологий, увеличения числа киберугроз, вопрос о непрерывной подготовке и переподготовке кадров и специалистов становится первостепенной задачей государства.



Категории жертв среди организаций

В рамках стратегии «Цифровой Узбекистан 2030», принятой в октябре 2020 года, особое внимание уделяется развитию цифровой экономики и электронному правительству, ставя в приоритет интеграцию ИКТ в образование и промышленную индустрию.

**Согласно Постановления Президента
Республики Узбекистан №17 от 22 января
2025 года**

**«О мерах по внедрению системы
профессиональной подготовки кадров для
сферы противодействия преступлениям,
совершаемым с использованием цифровых
технологий»**

в учебных заведениях активно создаются и внедряются программы по подготовке и переподготовке кадров в области информационной и кибербезопасности.



**Постановление Президента
№ ПП-4851 от 6 октября 2020 года.**
Совершенствование системы
подготовки кадров в области
информационных технологий, развитие
и интеграция научных исследований с
IT-индустрией.



Постановление Президента Республики Узбекистан

№ ПП-51 направлено на развитие IT-сферы в стране и поддержку специалистов, стремящихся получить международные IT-сертификаты, предусматривает частичное возмещение расходов, связанных с сертификацией, что стимулирует развитие профессиональных навыков и конкурентоспособности на мировом рынке труда.



Правительство компенсирует до **60% расходов**, потраченных на получение международных IT-сертификатов, что стимулирует молодежь развиваться в этой сфере.

МЕЖДУНАРОДНЫЕ СЕРТИФИКАТЫ

- Microsoft Certified Solutions Expert (MCSE)
- Certified Information Systems Security Professional (CISSP)
- AWS Certified Solutions Architect
- Cisco Certified Network Associate (CCNA)

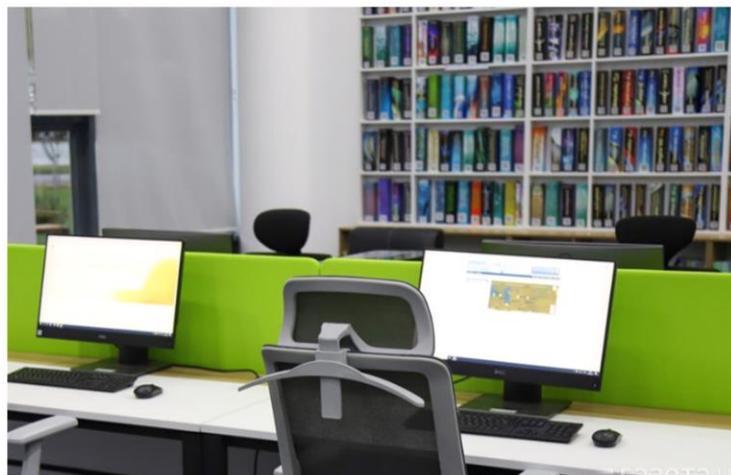


Постановлением Президента от 20.01.2025 г. № ПП-14



Создан Государственный Университет «Cyber University»
Объявлен прием студентов в ВУЗ, который будет готовить специалистов в области информационной и кибербезопасности, таких как: разработчик программного обеспечения систем защиты, эксперт ИБ, специалист по КБ, пентестер, аналитик безопасности и другие.

При Университете будут проводится курсы по переподготовке и повышению квалификации в сфере информационной и кибербезопасности.



Формирование будущих специалистов в сфере кибербезопасности

В нижеприведенных учебных заведениях открылись новые направления по подготовке бакалавров, магистров, проводятся научные исследования в области цифровых технологий, искусственного интеллекта и кибербезопасности.



Ташкентский университет информационных технологий имени Мухаммада ал-Хоразми



Университет Инха в городе Ташкенте



Национальный университет Узбекистана имени Мирзо Улугбека



Ташкентский государственный технический университет имени Ислама Каримова



Туринский политехнический университет в Ташкенте



Цифровой университет Японии



Университет Амита в Ташкенте



Частные компании проводят курсы по следующим направлениям:

- сетевые технологии и безопасность;
- этический хакинг; аналитика ИБ;
- системное администрирование;
- аудит информационной безопасности;
- искусственный интеллект и машинное обучение;
- форензика; цифровая криминалистика и другие.

За последние годы **киберсорязания** в Узбекистане стали важной частью подготовки специалистов в области ИТ и кибербезопасности, такие мероприятия помогают выявлять таланты, развивать навыки и укреплять позиции страны в цифровом мире. Соревнования становятся масштабнее привлекая и международных участников.

Uzbek Cyber Security Challenge 2023(UZCERT с IT Park)

Участники решали задачи по защите информационных систем, обнаружению уязвимостей и защите данных.
CTF по категории:Сетевое администрирование и безопасность.

Hackathon IT Park 2023 (IT Park) посвященный разработке приложений и решений в области кибербезопасности и цифровизации. Было представлено более 50 проектов, направленных на повышение безопасности данных и оптимизацию ИТ-инфраструктуры

Uzbekistan National CTF 2024 (МИНЦИФРЫ)

Участники решали задачи в области криптографии, защиты сетей и анализа вредоносных программ. В соревновании приняли участие более 100 команд, включая студентов, ИТ-специалистов и начинающих энтузиастов.

Cybersecurity Youth Forum 2024

Форум, включал киберсорязания для школьников и студентов с целью популяризации ИТ-образования, проводились мини-хакатоны и обучающие семинары по направлениям: основы защиты данных, киберэтика, программирование.

UzHack 2025

(IT Park и UZCERT) разработка инновационных решений для защиты данных и киберзащиты. Участвовали и узбекские команды и международные команды. Киберсорязания проводились по направлениям: Искусственный интеллект в кибербезопасности. Автоматизация обнаружения угроз. Разработка инструментов для защиты IoT . Призовой фонд составил \$50,000.

Central Asia Cyber Summit 2025

(Центр Кибербезопасности Республики Узбекистан)

Международный региональный саммит по кибербезопасности, включающий соревнования между командами из стран Центральной Азии. Реальные сценарии кибератак, моделирование угроз, защита критически важной инфраструктуры.



Тенденции и анализ проводимых киберсорязаний



Rector's Cup-2025



Киберсоревнования «CYBERKENT»



«Олимпиада СТФ по кибербезопасности» в ТУИТ



CTF хакатон в Центре Молодежи г.Нукус



Кибер Клубы-сообщества молодых специалистов, готовых защищать интересы государства в цифровом пространстве

В 2022 году при «Центре Кибербезопасности» был организован и активно развивается «Кибер Клуб», состоящий из одаренной молодежи, основное назначение которого заключается в исследовании уязвимостей информационных ресурсов и систем доменной зоны uz.



Члены Клуба Кибербезопасности участвуют в различных национальных и международных мероприятиях, конкурсах, обмениваются опытом и знаниями, а также учувствуют от имени нашего государства на соревнованиях в области кибербезопасности за честь нашей страны.



Проводятся ежегодно Международный Саммиты по кибербезопасности

С 2023 года Центром Кибербезопасности Республики Узбекистан проводятся международные саммиты, целью является создание международной интерактивной площадки высокого уровня для обмена опытом, демонстрация современных решений и открытие новых возможностей на взаимовыгодных условиях.



В рамках саммита проводятся киберучения на основе смоделированного киберполигона города, где команды RED TEAM и BLUE TEAM взламывают и защищают инфраструктуру.

Согласно международного **рейтинга Национальный Индекс Кибербезопасности** в Республике Узбекистан продолжает улучшать свои позиции: внедряются современные меры по защите критически важных объектов инфраструктуры, проводится обучение населения и непрерывная подготовка специалистов в области информационных технологий, искусственного интеллекта, информационной и кибербезопасности.

Дальнейшие планы развития информационной и кибербезопасности в Республике Узбекистан

- ☑ Развитие национальной системы киберзащиты
- ☑ Развитие национальной системы исследований уязвимостей (киберразведки)
- ☑ Развитие национальной системы киберрезистентности (киберустойчивости)
- ☑ Развитие национальной системы киберпрофилактики (кибергигиена)
- ☑ Развитие научно-технической базы в прогрессивных направлениях цифровых технологий
- ☑ Развитие кадрового потенциала



Спасибо за внимание!



Республика Узбекистан,
100115, г. Ташкент, ул. Тараса Шевченко, 20



Телефон: (99871) 203 55 11
Факс: (99871) 277 70 66



E-mail: info@csec.uz
Веб-сайт: www.csec.uz