ISSN 3060-4567

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Шамсиева Юлдузхон Файзиддиновна

Ташкентский государственный экономический университет

Аннотация: *В данной статье рассматриваются актуальные вопросы обеспечения информационной безопасности в условиях ускоренной цифровизации всех сфер общества. Особое внимание уделяется анализу угроз, возникающих в киберпространстве, таких как хакерские атаки, фишинг, вредоносные программы и утечка персональных данных. Описаны основные принципы и методы защиты информации, включая использование криптографических технологий, межсетевых экранов, систем обнаружения вторжений и политик информационной безопасности на уровне организаций. Рассматриваются международные стандарты и нормативные документы в области информационной безопасности. Также проанализированы подходы к подготовке кадров и повышение киберграмотности населения как ключевого фактора эффективной защиты информационного пространства. Статья подчеркивает необходимость комплексного подхода и государственно-частного партнерства для обеспечения устойчивой и безопасной цифровой среды.*

Ключевые слова*: информационная безопасность, киберугрозы, защита данных, цифровая безопасность, криптография, фишинг, киберграмотность, нормативные стандарты, кибербезопасность.*

Информационная безопасность представляет собой совокупность мер, направленных на защиту информации от несанкционированного доступа, разрушения, изменения, блокирования, копирования, распространения и других угроз. В условиях стремительной цифровизации и расширения киберпространства информационная безопасность становится ключевым элементом национальной и международной безопасности. Современные

ISSN 3060-4567

угрозы информационной безопасности включают в себя кибератаки, вирусные и вредоносные программы, фишинг, утечки персональных данных, атаки с использованием программ-вымогателей и социальную инженерию. Эффективная защита от этих угроз требует комплексного подхода, включающего технические, организационные и правовые меры. Технические средства защиты включают межсетевые экраны, антивирусные программы, системы обнаружения и предотвращения вторжений, технологии шифрования и резервного копирования. Организационные меры предусматривают создание политик информационной безопасности, обучение персонала и проведение аудитов. Правовые меры регулируются законами и международными стандартами, такими как ISO/IEC 27001.

Большое значение имеет развитие киберграмотности среди населения, особенно в условиях роста числа пользователей интернет-услуг. Образование и повышение осведомлённости помогают формировать культуру безопасного поведения в цифровой среде. Таким образом, обеспечение информационной безопасности требует постоянного совершенствования технических решений, международного сотрудничества, нормативно-правовой базы и широкого вовлечения общества в процессы цифровой трансформации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Конституция Республики Узбекистан. – Ташкент: «Ўзбекистон», 2023.
2. Мирзиёев Ш.М. Стратегия развития Новой Узбекистан: продолжение реформ, уверенное движение вперёд. – Ташкент: «Ўзбекистон», 2022.
3. Государственная программа «Цифровой Узбекистан – 2030». – Министерство цифровых технологий РУз, 2021.
4. Гостев А.А. Информационная безопасность: теория и практика. – Москва: Юрайт, 2022.
5. Бочаров Д.В. Основы кибербезопасности. – Санкт-Петербург: Питер, 2021.
6. Соловьёв В.Д. Криптография и защита информации. – Москва: Форум, 2020.
7. Грачёв С.В. Современные угрозы информационной безопасности. – Москва: Академия, 2023.

8. ISO/IEC 27001:2022 — Международный стандарт по управлению информационной безопасностью.

9. Антипов С.Н. Киберграмотность и цифровая безопасность. – Екатеринбург: УрФУ, 2023.

10. Лукьяненко К.А. Политика информационной безопасности в организациях. – Казань: Казанский университет, 2021.