VOLUME-3, ISSUE-6

ОЦЕНКА ЭФФЕКТИВНОСТИ ВНЕДРЕНИЯ НАЦИОНАЛЬНЫХ СТАНДАРТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГЛОБАЛЬНЫЙ КОНТЕКСТ

Турдиалиева Махзуна Мухторалиевна
соискатель,
Ташкентский химико-технологический институт
Республика Узбекистан, г. Ташкент
E-mail: zdaminkhonova@gmail.com

Рахмонбердиева Лобар Баходир кизи
студентка,
Ташкентский химико-технологический институт
Республика Узбекистан, г. Ташкент
Маматкулов Жавохир Аброр угли
студент,
Ташкентский химико-технологический институт
Республика Узбекистан, г. Ташкент

Аннотация: В данной статье рассматриваются подходы к оценке эффективности внедрения национальных стандартов в области информационной безопасности в условиях глобализации. Анализируется международный и национальный опыт, включая Узбекистан, с целью выявления факторов, влияющих на успешность реализации стандартов. Делается акцент на важности гармонизации национальных и международных нормативов для повышения устойчивости цифровой среды.

Ключевые слова: информационная безопасность, стандартизация, национальные стандарты, эффективность, киберугрозы, ISO, O‘zDSt.

ASSESSMENT OF THE EFFECTIVENESS OF THE IMPLEMENTATION OF NATIONAL STANDARDS IN THE FIELD OF INFORMATION SECURITY IN THE GLOBAL CONTEXT

Turdialieva Makhzuna Mukhtoralievna
applicant,
Tashkent Institute of Chemical Technology
, Republic of Uzbekistan, Tashkent
E-mail: zdaminkhonova@gmail.com

Rakhmonberdieva Lobar Bahodir qizi
student,
Tashkent Institute of Chemical Technology
, Republic of Uzbekistan, Tashkent

Abstract: This article discusses approaches to assessing the effectiveness of the implementation of national standards in the field of information security in the context of globalization. The international and national experience, including Uzbekistan, is analyzed in order to identify factors influencing the success of standards implementation. The emphasis is placed on the importance of harmonizing national and international standards to enhance the sustainability of the digital environment.
Key words: information security, standardization, national standards, efficiency, cyber threats, ISO, O'ZDST

Информационная безопасность (ИБ) в условиях цифровой трансформации экономики становится критическим элементом как государственной, так и корпоративной политики. Растущий объём киберугроз требует наличия чётко структурированной системы регулирования и защиты информации. Одним из ключевых инструментов в этой сфере выступает стандартизация. Эффективное внедрение национальных стандартов ИБ напрямую влияет на защищённость цифровых инфраструктур. Однако на сегодняшний день стоит вопрос: насколько эти стандарты действенны и соответствуют глобальным требованиям? [9]

Национальные стандарты информационной безопасности. общее представление

Национальные стандарты ИБ представляют собой нормативные документы, регулирующие методы защиты информации, порядок проведения аудита, требования к ИТ-инфраструктурам и персоналу. В Узбекистане базовым является стандарт O‘zDSt 1106:2009, [1] а также законы «Об информации» [2] и «О кибербезопасности» [3]. Подобные документы устанавливают минимальные требования к обеспечению конфиденциальности, целостности и доступности информации.

Международный контекст

Международные стандарты, такие как ISO/IEC 27001[4] и NIST SP 800 [6], служат ориентиром для многих стран в разработке собственных систем ИБ. Они охватывают широкий спектр требований: от политики безопасности до технической реализации. В отличие от некоторых локальных стандартов, они обеспечивают высокую степень совместимости и масштабируемости [5].

Методология оценки эффективности внедрения

Существует несколько подходов к оценке эффективности внедрения стандартов ИБ [7]

Сравнительный анализ числа киберинцидентов до и после внедрения стандартов;

Аудит соответствия международным и национальным нормам;

Оценка уровня цифровой зрелости организаций;

Интервью и опросы специалистов в области информационной безопасности;

Мониторинг исполнения требований стандартов в государственных и частных структурах [8].

Примеры внедрения стандартов в разных странах

В США стандарт NIST SP 800 является обязательным для всех федеральных агентств и служит ориентиром для частных компаний. Его внедрение привело к снижению числа инцидентов на 25% в течение первых трёх лет[6].

В странах ЕС гармонизация происходит через GDPR и ENISA [7], что обеспечивает высокую степень скоординированности мер. В Китае — национальные стандарты независимы и строго централизованы.

В Узбекистане, начиная с 2017 года, активизировалась деятельность по цифровой трансформации, в том числе в сфере ИБ. Созданы CERT.UZ [8], Госинспекция по контролю в сфере ИКТ, и начато внедрение модели Zero Trust в ключевых инфраструктурах [10].

Проблемы и вызовы

Отставание стандартов от технического прогресса;

Недостаточная подготовка специалистов в области ИБ;

Отсутствие единой международной платформы для обмена опытом;

Разрыв между требованиями законодательства и практикой внедрения на местах [9].

Рекомендации по повышению эффективности

Адаптация национальных стандартов к международным (ISO, ITU);

Проведение обязательной сертификации специалистов и организаций;

Разработка показателей KPI для оценки выполнения стандартов;

Укрепление международного сотрудничества в рамках ШОС, ООН и др.;

Регулярное обновление нормативно-правовой базы с учётом развития технологий.

Заключение.

Эффективность внедрения национальных стандартов ИБ зависит от множества факторов: уровня подготовки кадров, степени зрелости ИТ-сферы, международного сотрудничества. Для Узбекистана важным шагом является не только адаптация к ISO/IEC, но и создание гибкой, динамичной нормативной среды. Глобальный подход и активное участие в международных цифровых инициативах станут залогом повышения защищённости государства в условиях нарастающих киберугроз.

Список использованной литературы

1. O‘zDSt 1106:2009. Информационная безопасность. Основные положения.
2. Закон Республики Узбекистан «Об информации» от 11 декабря 2003 года.
3. Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года.
4. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection.
5. ITU Global Cybersecurity Index, 2022.
6. NIST SP 800-53 Rev. 5. U.S. Department of Commerce.
7. ENISA Threat Landscape 2023.
8. CERT.uz – Центр реагирования на компьютерные инциденты Узбекистана.
9. Соловьёв, В.Д. Информационная безопасность: теория и практика. – М.: КноРус, 2021.
10. Бобоев А.Ш. Современные аспекты кибербезопасности в Узбекистане. Журнал «Цифровая экономика», 2023.