Французов Иван Александрович
студент
Шумилов Никита Дмитриевич
студент
Научный руководитель
Филипская Анастасия Вадимовна
старший преподаватель
ФГБОУ ВО «МИРЭА – Российский технологический университет»
г. Москва

ВЛИЯНИЕ АНГЛОЯЗЫЧНОЙ ДОКУМЕНТАЦИИ НА МЕЖДУНАРОДНЫЕ СТАНДАРТЫ КИБЕРБЕЗОПАСНОСТИ

Аннотация: *в статье исследуется, как англоязычная документация влияет на международные стандарты кибербезопасности (ISO, NIST, CIS, ENISA). Практически все ключевые стандарты разрабатываются на английском, что позволяет унифицировать требования, но создаёт трудности при локализации. Авторами обсуждаются основные исторические этапы создания стандартов (ISO/IEC 27001, NIST SP 800-серия, CIS Controls), роль английского как рабочего языка глобальной ИБ-экспертизы, проблемы перевода (на примере российских ГОСТ), примеры внедрения стандартов в разных странах, а также влияние на образование и подготовку кадров.*

Ключевые слова: *кибербезопасность, международные стандарты ИБ, англоязычная документация, ISO/IEC 27001, NIST, CIS Controls, ENISA, СУИБ, локализация, перевод стандартов, подготовка специалистов.*

Введение.

Глобальная цифровизация предъявляет единые требования к защите информации: международные стандарты информационной безопасности (ИБ) служат основой для построения систем управления безопасностью (СУИБ). Например, ISO/IEC 27001 описывает требования к СУИБ, и по последнему отчёту ISO на него приходится более 70 тыс. сертифицированных предприятий в 150 странах.

Подобную роль в США выполняют стандарты NIST. Международные организации (ENISA в ЕС, CIS в США) также выпускают руководства и контрольные списки.

Практически все эти документы публикуются в оригинале на английском. Английский язык стал де-факто языком ИБ-стандартов: он обеспечивает единые определения и высокую оперативность обновлений. С другой стороны, отсутствие мгновенных переводов создаёт барьер: специалисты из непривилегированных англоязычностью стран вынуждены работать с оригиналами или ждать локализаций. Введение подводит читателя к проблематике работы с англоязычными стандартами и объясняет, почему важно изучать именно их содержимое.

История развития стандартов ИБ.

Классические стандарты ИБ возникли начиная с конца 1990-х годов. В 2005 г. опубликован первый выпуск ISO/IEC 27001, и в последующие годы его пересмотрели (ISO/IEC 27001:2013, а в 2022 – ISO/IEC 27001:2022). Это основной стандарт по СУИБ, на который ссылаются многие организации. В США и иных странах в 2000-х сформировался комплекс NIST: SP 800-53 впервые вышел в 2005 г. и к 2020 уже имел 5 ревизию; SP 800-171 (защита CUI) – в 2016 г., обновлён до Rev.2 в 2020. Технические контрольные списки (CIS Controls) появились в 2008 г., последнее крупное обновление (v7.1) – в 2019, затем в 2021 выпущена v8. Для ЕС характерны проекты стандартизации сертификации ИКТ (от ENISA), развивающиеся после создания ENISA в 2004 г. (например, европейская схема EUCC на основе Common Criteria). Таким образом, киберстандарты ИБ постоянно эволюционировали, сохраняя англоязычную основу.

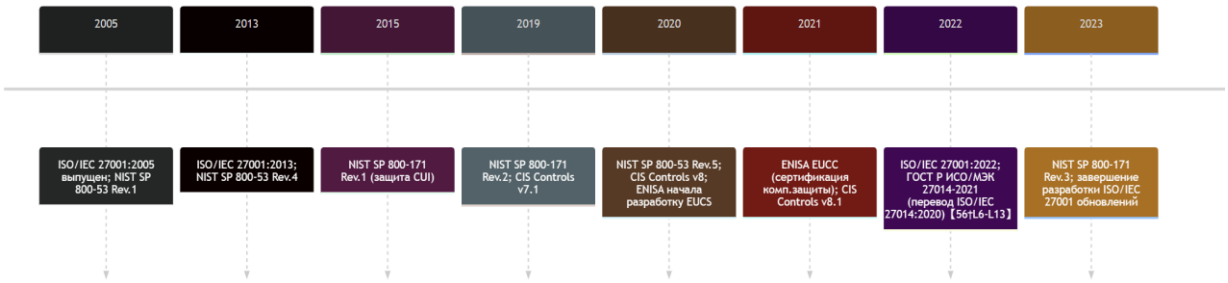

Рис. 1. Хронологическая шкала развития международных стандартов в области кибербезопасности за период с 2005 по 2023 год

Роль английского языка.

Английский язык обеспечивает единство терминологии и оперативность обмена опытом. Международные стандарты публикуются на английском, а все пересмотры и новые рекомендации сразу появляются в оригинале. Это означает, что доступ к «первичным» требованиям возможен только через англоязычные источники. Европейское агентство ENISA подчёркивает, что новые схемы сертификации строятся «на основе международных стандартов», и сотрудничество с ISO, CEN, ETSI помогает обеспечить согласованность подходов. Аналогичным образом, меры контроля CIS представлены на английском языке в виде приоритетного набора защитных механизмов, на которые ссылаются различные концептуальные основы. Таким образом, Английский язык служит языком межнационального общения для стандартов кибербезопасности, обеспечивая широкую совместимость. В то же время для специалистов в странах со слабым уровнем знания английского языка это становится препятствием: им приходится учить профессиональную терминологию на английском, а при отсутствии перевода полагаться на устаревшие версии или сторонние обзоры.

Проблемы перевода и локализации.

Официальные переводы стандартов делаются национальными органами, но всегда с задержкой. Например, ISO/IEC 27001:2013 официально принят в РФ как ГОСТ Р ИСО/МЭК 27001-2021. Аналогично, ISO/IEC 27014:2020 был выпущен в России как ГОСТ Р ISO/IEC 27014-2021. Однако более свежие версии (как ISO/IEC 27001:2022) на момент настоящего исследования ещё не были переведены. В результате российским ИТ-специалистам часто приходится одновременно пользоваться англоязычным текстом ISO и русским ГОСТ (с возможными расхождениями). Это же справедливо и для других стран СНГ и Восточной Европы. Перевод сложных технических стандартов требует участия экспертов, из-за чего возможны неточности терминологии. Отдельные термины просто не

имеют точных аналогов. Взаимосвязь международных и национальных норм часто проводится через «стандарт-корреляцию»: национальные регуляторы связывают свои требования с международными стандартами, но формулировки всё же различаются.

Внедрение стандартов и подготовка специалистов.

В разных странах правила интегрируют международные стандарты по-разному. Практически повсеместно ISO/IEC 27001 признаётся «скелетом» СУИБ большинства организаций. В США и ЕС распространены добровольная сертификация по ISO/IEC и обязательное следование NIST для госсектора, тогда как в России законодательство часто задаёт национальные требования, а следование ISO носит добровольный характер, если только не требуется сертификация ГОСТ. При этом российские ГОСТы по ИБ фактически повторяют требования ISO, облегчая международное признание сертификатов. Для подготовки кадров влияние английского также заметно: большинство учебников, курсов и сертификатов по ИБ (CISSP, CISA, СУИБ-курсы) базируются на англоязычных стандартах. Знание английского позволяет специалисту быстро применять новые международные наработки. В то же время выявляется недостаток англоязычных материалов на родном языке – это тормозит распространение передовых практик в бизнесе и государственном секторе.

Заключение.

Англоязычная документация остаётся основой глобальных стандартов кибербезопасности, унифицируя подходы к ИБ в разных странах. Её влияние проявляется в единстве терминологии и быстрых обновлениях требований. Вместе с тем отсутствие мгновенных переводов создаёт трудности: специалисты вынуждены работать с оригиналами или ждать локализаций. Для преодоления «языкового барьера» важно одновременно углублять владение английским среди ИБ-кадров и расширять качественные переводы международных стандартов. Это обеспечит доступность знаний и укрепит эффективность мер кибербезопасности в масштабе стран и организаций.

References

1. ACM. ACM Digital Library – Cybersecurity and Information Policy Research. URL: https://dl.acm.org (date of request: 02.05.2026).

2. European Union Agency for Cybersecurity. ENISA Threat Landscape 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (date of request: 02.05.2026).

3. IEEE. Cybersecurity Standards and Practices (IEEE Xplore Digital Library). URL: https://ieeexplore.ieee.org (date of request: 02.05.2026).

4. International Organization for Standardization. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems. URL: https://www.iso.org/standard/27001 (date of request: 02.05.2026).

5. National Institute of Standards and Technology. NIST Cybersecurity Framework (CSF 2.0). URL: https://www.nist.gov/cyberframework (date of request: 02.05.2026).

6. National Institute of Standards and Technology. NIST Special Publication 800–53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (date of request: 02.05.2026).