

Для цитирования

Лившиц И.И. Устойчивое развитие вузов Российской Федерации / III Научно-практическая конференция «Стандартизация: траектория науки», Москва, 15 октября 2025 года // Информационно-экономические аспекты стандартизации и технического регулирования. 2025. № 6(87). С. 413–416.

УДК 004.094

УСТОЙЧИВОЕ РАЗВИТИЕ ВУЗОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Лившиц И.И., д-р техн. наук, ФГБУ «Университет ИТМО», Россия, Санкт-Петербург

Рассматривается актуальная проблема – оценка устойчивого развития учебного процесса в высших учебных заведениях (вузах) Российской Федерации и обеспечение требований информационной безопасности (ИБ). Представляется целесообразным рассматривать устойчивое развитие вузов не как отдельный процесс или как набор разрозненных процессов, а как «встроенное качество» известных систем менеджмента: системы менеджмента качества (СМК) в соответствии с требованиями ISO 9001 и системы менеджмента для образовательной организации (СМОО) по требованиям ISO 21001. Для обеспечения устойчивого развития крайне важно и обеспечить принцип «встроенного качества», и реализовать практические аспекты обеспечения ИБ.

Ключевые слова: устойчивое развитие, аудит, система менеджмента качества, система менеджмента образовательных учреждений, процесс, информационная безопасность, риски, стандарт.

SUSTAINABLE DEVELOPMENT OF UNIVERSITIES IN THE RUSSIAN FEDERATION

Livshitz I.I., Doctor of Technical Sciences, ITMO University, St.Petersburg

An actual problem is considered – the assessment of the sustainable development of the educational process in Higher education institutions of the Russian Federation and ensuring the requirements of information security. It seems advisable to consider the sustainable development of Universities not as a separate process or as a set of disparate processes, but as the "built-in quality" of well-known management systems: quality management systems (QMS) in accordance with the requirements of ISO 9001 and management systems for educational organizations (MSEO) according to the requirements of ISO 21001. To ensure sustainable development, it is extremely important to ensure the principle of "built-in quality" and implement practical aspects of information security.

Keywords: sustainable development, audit, quality management system, educational institutions management system, process, information security, risks, standard.

Введение

Для обеспечения устойчивого развития для вузов возможно применение различных систем менеджмента, например «универсального» ISO 9001:2015¹ и «специализированного» ISO 21001:2018². С учетом практики аудитов автора можно полагать, что одним из ключевых факторов обеспечения устойчивого развития в вузах является реализация требований ИБ [1,2]. Этот аспект крайне важен – известна нехватка квалифицированных кадров и общая проблема увеличения выпуска необходимого количества специалистов в области ИБ [2, 3, 4]. Соответственно, без специалистов достаточного уровня в сфере ИБ не представляется возможным обеспечить требуемый уровень ИБ в современной ИТ-инфраструктуре вуза, что, в свою очередь, существенно влияет на достижение позитивных результатов устойчивого развития всей отрасли образования в РФ [5, 6, 7].

¹ <https://www.iso.org/standard/62085.html>

² <https://www.iso.org/standard/66266.html>

Постановка задачи – формирование оценки выполнения требований ИБ в составе СМК и/или СМОО для вузов. В представленной публикации рассмотрены методы решения задачи – системный анализ, структурный анализ, теория принятия решений, современные стандарты (в том числе стандарты риск-менеджмента).

Анализ инцидентов безопасности вузов

По оценке экспертов Positive Technologies³, количество успешных атак в РФ в 2024 году относительно 2023 года выросло более чем в 2 раза. Представляется целесообразным привести несколько примеров значимых инцидентов (успешных кибератак, прерывания нормального функционирования и пр.) для вузов в мире:

- 1) атака на университет Блуфилда⁴ (США);
- 2) атака на университет Технион⁵ (Израиль);
- 3) атака на Цюрихский университет⁶ (Швейцария);
- 4) атака на Манчестерский университет⁷ (Великобритания).

Специфика применения ISO 21001

В отличие от популярного стандарта ISO серии 9001 стандарт ISO серии 21001 пока не очень распространен в мире. Для целей данной публикации предлагается рассмотреть доступную статистику по сертификации в мире на базе актуального отчета ISO Survey за 2023 год для ISO 9001, в аналитике которого введен код (Sector number) 37 для отрасли «образование» (Education). В файле (ISO-CASCO_1.ISO Survey 2023 results – number of certificates and sites per country and the number of sectors overall) содержится информация по статистике сертификации по требованиям ISO 9001 для кода 37 – всего таких сертификатов 11 202 из 837 978, что составляет только 1,34%. Для обеспечения устойчивого развития вузы должны существенно изменить свою приверженность к демонстрации лучших практик и реально применимых мер в области обеспечения ИБ.

Оценивание требований ISO 21001 и требования реализации ИБ

Представляется полезным представить оценку требований ISO серии 21001, выполнение которых, объективно, существенно для обеспечения ИБ в вузе. Прежде всего рассмотрим общие факторы ISO серии 9001 и ISO серии 21001, которые содержат общие требования к должному обеспечению ИТ-инфраструктуры в аспекте ИБ, например:

- обеспечение безопасной инфраструктуры (п. 7.1.3.2);
- обеспечение требований к ИТ-инфраструктуре (например, п. 7.1.3.3, 7.5.3.2 b), (8.5.1.1 d) в аспекте ИБ.

Далее рассмотрим оценку требований по ISO серии 21001, применимых для обеспечения ИБ в вузе (см. табл.).

³ <https://www.kommersant.ru/doc/7480689?from=trends>

⁴ <https://www.securitylab.ru/news/537985.php>

⁵ <https://www.securitylab.ru/news/536418.php>

⁶ <https://www.securitylab.ru/news/536310.php>

⁷ <https://www.securitylab.ru/news/539183.php>

Пункт	Раздел	Требование	Фактор
0.4	Введение	к) безопасность и защита данных (data security and protection)	Важно для управления рисками ИБ, невыполнение может привести к компрометации данных
4.2	Среда организации	Эти заинтересованные стороны должны включать: – обучающихся; – других выгодоприобретателей; – персонал организации.	Важно для защиты данных заинтересованных сторон
5.1.1	Лидерство	к) поддержки устойчивой реализации видения образования и соответствующих методологий образования;	Важно для отражения в высших документах вуза (уставе, стандартах и пр.) лидерство в обеспечении ИБ
6.2.2	Планирование	При планировании достижения целей образовательной организации она должна определить и кратко описать в своем стратегическом плане:	Важно разработать специальный документ, учитывающий требования в аспекте обеспечения ИБ
7.5.3.1	Поддержка	б) ее адекватной защиты (например, от несоблюдения конфиденциальности, от ненадлежащего использования, потери целостности или непреднамеренного изменения)	Очень важно для любого вуза, поскольку есть риск утечки ценной информации, учебных программ и пр.
8.1.1	Операционная деятельность	Организация должна управлять запланированными изменениями и анализировать последствия непредусмотренных изменений, предпринимая, при необходимости, действия по смягчению любых негативных воздействий	Очень важно для любого вуза, поскольку есть риск непрерывных изменений в аспекте ИБ

Вывод

В представленной публикации рассматривается актуальная проблема – оценка устойчивого развития учебного процесса в вузах Российской Федерации и обеспечение требований ИБ. Новизна представленной публикации заключается в объективных примерах применения известных стандартов (ISO 9001 или ISO 21001) для результативного выполнения соответствующих требований и обеспечения устойчивого развития вузов. Полученные результаты могут быть применены заинтересованными сторонами в рамках общего процесса обеспечения устойчивого развития для вузов.

Список литературы

1. Лившиц И.И. Управление качеством в дистанционном режиме обучения на примере практики в университете ИТМО // Менеджмент качества. 2022. № 1. С. 68–77.
2. Лившиц И.И. Об актуальных проблемах образования в области информационной безопасности // Автоматизация в промышленности. 2019. № 9. С. 10–13.
3. Лившиц И.И. Оценка необходимости совершенствования действующей процедуры подготовки квалифицированных кадров в области информационной безопасности // Газовая промышленность. 2024. № 9 (871). С. 200–205.
4. Лившиц И.И. Проблемы подготовки специалистов в области информационной безопасности // Вестник Дагестанского государственного технического университета. Технические науки. 2024. Т. 51. № 1. С. 13–131.
5. Лившиц И.И., Неклюдов А.В. Методика оптимизации программы аудитов информационной безопасности // В сборнике: Комплексная защита информации. Материалы XXII научно-практической конференции. 2017. С. 135–139.
6. Лившиц И.И., Неклюдов А.В. Методика мгновенных аудитов информационной безопасности // В сборнике: Комплексная защита информации. Материалы XXII научно-практической конференции. 2017. С. 139–142.

7. Лившиц И.И. Методика технического аудита безопасности собственной службы Service Desk // Стандарты и качество. 2024. № 6. С. 102–107.

References

1. Livshitz I.I. Quality management in distance learning using the example of practice at ITMO University // Quality management. 2022. No. 1. pp. 68–77.
2. Livshitz I.I. On current issues of education in the field of information security // Automation in industry. 2019. No. 9. pp. 10–13.
3. Livshitz I.I. Assessment of the need to improve the current procedure for training qualified personnel in the field of information security // Gas industry. 2024. No. 9 (871). pp. 200–205.
4. Livshitz I.I. Problems of training specialists in the field of information security // Bulletin of Dagestan State Technical University. Technical sciences. 2024. Vol. 51. No. 1. pp. 123–131.
5. Livshitz I.I., Neklyudov A.V. Methodology for optimizing the information security audit program // In the collection: Comprehensive information protection. Materials of the XXII scientific and practical conference. 2017. pp. 135–139.
6. Livshitz I.I., Neklyudov A.V. Methodology of instant information security audits // In the collection: Comprehensive information protection. Materials of the XXII scientific and practical conference. 2017. pp. 139–142.
7. Livshitz I.I. Methodology of technical security audit of own Service Desk // Standards and quality. 2024. No. 6. pp. 102–107.