ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.021, 004.42, 004.074

DOI: 10.21822/2073-6185-2025-52-3-71-76 Оригинальная статья/ Original article

К вопросу обеспечения требований информационной безопасности в ВУЗе

И.И. Лившиц
Национальный исследовательский университет ИТМО,
197101, г. Санкт-Петербург, Кронверкский пр., д. 49, Россия

Резюме. Цель. В представленной публикации рассматривается актуальная проблема – обеспечение требований информационной безопасности (ИБ) при обеспечении учебного процесса в высших учебных заведениях (ВУЗ) Российской Федерации. **Метод.** Представляется целесообразным рассматривать обеспечение требований ИБ не как отдельный процесс, а как «встроенное качество» известных систем менеджмента, например, системы менеджмента качества (СМК) в соответствии с требованиями ISO 9001 или специализированной системы менеджмента для образовательной организации (СМОО) по требованиям ISO 21001. **Результат.** Доказано, что для обеспечения ИБ требуется только «целевая» система менеджмента в соответствии с требованиями ISO 27001, но в действительности, как показала практика автора по аудитам ВУЗов, это не единственный оптимальный вариант. Новизна представленной публикации заключается в объективных примерах как могут быть применены хорошо известные стандарты (например ISO 9001 или ISO 21001) с минимальными издержками и с результативным выполнением соответствующих требований. **Вывод.** Реализация принципа «встроенного качества» в аспекте обеспечения ИБ, получившая достаточное подтверждение при апробации в ВУЗах, дает практический базис для экспертов (консультантов и аудиторов) выбора и реализации стратегического направления в области оценки соответствия. Полученные результаты могут быть применимы всеми заинтересованными сторонами, стремящимися обеспечить требуемый уровень ИБ в рамках общего процесса обеспечения результативной СМК или СМОО для ВУЗов.

Ключевые слова: система менеджмента, система менеджмента информационной безопасности, система менеджмента образовательных учреждений, процесс, информационная безопасность, внутренние аудиты, риски, стандарт

Для цитирования: И.И. Лившиц. К вопросу обеспечения требований информационной безопасности в ВУЗе. Вестник Дагестанского государственного технического университета. Технические науки. 2025;52(3):71-76. DOI:10.21822/2073-6185-2025-52-3-71-76

On the issue of ensuring information Security requirements at the University

I.I. Livshits
National Research University ITMO,
49 Kronverksky Ave., St. Petersburg 197101, Russia

Abstract. Objective. This publication addresses a pressing issue: ensuring information security (IS) requirements for the educational process at higher education institutions (HEIs) in the Russian Federation. **Method.** It appears appropriate to consider IS compliance not as a separate process, but as an "integrated quality" of established management systems, such as a quality management system (QMS) compliant with ISO 9001 or a specialized management system for an educational organization (SMEO) compliant with ISO 21001. **Result.** It has been demonstrated that IS compliance requires only a "targeted" management system compliant with ISO 27001. However, as the author's experience in auditing HEIs has shown, this is not the only optimal option. The novelty of this publication lies in its objective examples of how well-known standards (e.g., ISO 9001 or ISO 21001) can be applied with minimal costs and effective compliance with relevant requirements. **Conclusion.** The implementation of the "built-in quality" principle in terms of information security assurance, which has been sufficiently confirmed during testing at

universities, provides a practical basis for experts (consultants and auditors) in selecting and implementing a strategic direction in the field of conformity assessment. The obtained results can be applied by all stakeholders striving to ensure the required level of information security as part of the overall process of ensuring an effective QMS or ISMS for universities.

Keywords: management system, information security management system, educational institution management system, process, information security, internal audits, risks, standard

For citation: I.I. Livshits. On the issue of ensuring information Security requirements at the University. Herald of the Daghestan State Technical University. Technical Sciences. 2025; 52(3):71-76. (In Russ) DOI:10.21822/2073-6185-2025-52-3-71-76

Введение. В настоящее время для ВУЗов возможно создание систем менеджмента в соответствии с требованиями различных стандартов, например «универсального» ISO 9001:2015 [1] и «специализированного» ISO 21001:2018 [2].

Также известно, что в деятельности современных ВУЗов необходимо учитывать нескольких «комплексов» различных требований, например национальных, отраслевых и/или международных.

Для ВУЗов, минимально требуются:

- национальные требования (например, лицензирование в установленном порядке);
- отраслевые требования (например, для авиационных учебных заведений требуются авиатренажеры (Boeing, Airbus и пр.) и техническая база для изучения авиационных двигателей (Д30, ВК-2500 и пр.);
- международные требования: сертифицированные учебные центры (например, аккредитация IATA, EALTS), международные сертификаты ICAO (управление воздушным движением и аэронавигация), ISAGO (наземное обслуживание) и пр.

Вопросы обеспечения ИБ получили существенный импульс для вдумчивого изучения во время эпидемии Covid-19, когда почти все ВУЗы в мире были вынуждены перевести учебный процесс в дистанционный формат [02,13,14].

В равной мере можно отметить влияние возросшей потребности в привлечении квалифицированных кадров и известных проблем, связанных с незначительным увеличением выпуска специалистов в области ИБ [15,16,17].

Соответственно, в настоящее время имеются существенные риски реализации программы аудитов систем менеджмента в ВУЗах, что, в свою очередь, существенно влияет на реализацию программы внутренних аудитов (в том числе и аудитов ИБ) [18, 19, 20].

Влияние современных угроз ИБ на ВУЗы, объективно, является одним из ярко выраженных негативных трендов развития ИТ, что безусловно требует принятия соответствующих результативных мер для защиты чувствительной информации, прежде всего – персональных данных (ПДн).

Объективно, для решения поставленной задачи может быть применим специальный стандарт ISO/IEC 27001[3], который предусматривает все необходимые требования для защиты ценных активов, а также содержит приложение А (обязательное) с перечнем мер защиты («контролей»), которые могут быть применены в конкретном ВУЗе с учетом установленных требований (национальных, отраслевых и/или международных). Однако разработка, внедрение и сертификация системы менеджмента ИБ в ВУЗе может оказаться долгосрочным и дорогостоящим процессом и, следует признать, в настоящее время практически не применяется.

Постановка задачи. В представленной публикации предложен иной вариант решения поставленной задачи – исследование возможности обеспечения ИБ в ВУЗе на базе более известных систем менеджмента – СМК м СМОО соответственно.

Целью исследования является формирование оценки выполнения требований ИБ в составе СМК и/или СМОО для ВУЗов.

Методы исследования. В представленной публикации рассмотрены методы решения задачи – системный анализ, структурный анализ, теория принятия решений, современные стандарты (в том числе стандарты риск-менеджмента).

По оценке экспертов Positive Technologies [4], количество «успешных» атак в РФ в 2024 г. относительно 2023 г. выросло более чем в 2 раза. Более интересно рассмотреть статистику по доли критичных инцидентов – примерно в 10% от общего числа кибератак, при этом «критичность» определялась тем, что атака привела к остановке работы, прерывания ИТ сервисов или потере чувствительных данных (информация о клиентах, партнерах и сотрудниках).

Представляется целесообразным привести несколько примеров значимых инцидентов («успешных» кибератак, компрометации ПДн, прерывания нормального функционирования и пр.) конкретно для ВУЗов в мире:

- атака на университет Блуфилда [5] (США), украдены более 1,2 Тбайт критичных данных;
- атака на университеты Кореи [6];
- атака на университет Технион [7] (Израиль);
- атака на Цюрихский университет [8] (Швейцария);
- атака на Манчестерский университет [9] (Великобритания);
- атака на серверы Санкт-Петербургского государственного университета [10].

Специфика применение ISO 21001. В отличие от хорошо известного и самого популярного стандарта ISO серии 9001 (более 800 тысяч сертификатов за 2023 г.), стандарт ISO серии 21001 пока не очень распространён в мире и на дату подготовки публикации в отчете ISO Survey за 2023 отдельно стандарт не рассматривается.

Для целей данной публикации предлагается рассмотреть доступную статистику по сертификации в мире на базе актуального отчета ISO Survey за 2023 [11] 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 детальная информация по статистике сертификации по требованиям ISO 9001 для кода 37 – всего таких сертификатов 11.202 из 837.978, что составляет около 1,34%.

В абсолютном сравнении 11 тысяч сертификатов только для образовательных организаций в мире это весьма значительный объем, больше, чем, например, популярный ISO/IEC 20000 – 3.670 или ISO 37001 – 7.894 сертификатов соответственно.

Примечательно, что в том же файле (ISO-CASCO_1.ISO Survey 2023 results - number of certificates and sites per country and the number of sectors overall) содержится детальная информация по статистике сертификации по требованиям ISO/IEC серии 27001 также для кода 37 – всего таких сертификатов 207.

Определенно, этот незначительный (по сравнению с другими стандартами) показатель требует дальнейшего изучения.

Рассмотрим специальный отчет по распределению сертификатов по кодам в файле (ISO-CASCO_2. ISO Survey 2023 results - number of sectors by country for each standard). Тройка лидеров по сертификации систем менеджмента ИБ для кода 37 – отрасли образование (Education) выглядит следующим образом:

- 39 – Япония;
- 29 – Испания;
- 26 – Греция.

Обсуждение результатов. Оценивание требований ISO 21001 в аспекте 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 (табл. 1).

Таблица 1. Оценка требований ISO 21001, применимых для обеспечения ИБ в ВУЗе
Table 1. Assessment of ISO 21001 requirements applicable to ensuring information security in a university

Раздел Section	Пункт Item	Требование Requirement	Фактор Factor
Введение Introduction	0.4	k) безопасность и защита данных (data security and protection)	Важно для управления рисками ИБ, невыполнение может привести компрометации ПДн
Среда организации Organizational Environment	4.2	Эти заинтересованные стороны должны включать: — обучающихся; — других выгодоприобретателей; — персонал организации.	Важно для точного учёта ПДн указанных заинтересованных сторон, которые необходимо защищать
Лидерство Leadership	5.1.1	k) поддержки устойчивой реализации видения образования и соответствующих методологий образования;	Важно для отражения в высших документах ВУЗа (Уставе, Политиках, Стандартах и пр.) роли лидерства в аспекте обеспечения ИБ
	5.2.1	g) включает в себя обязательство соответствовать социальной ответственности организации;	
	5.3	h) обеспечения того, что все процессы обучения интегрированы, вне зависимости от метода их предоставления;	
Планирование Planning	6.2.2	При планировании достижения целей образовательной организации, она должна определить и кратко описать в своём стратегическом плане;	Важно разработать специальный документ, учитывающий требования в аспекте обеспечения ИБ
Поддержка Support	7.1.2.1	c) персонал внешних поставщиков, работающих совместно или содействующих организации	Важно разработать специальный документ, учитывающий требования в аспекте обеспечения ИБ иностранных преподавателей (например, в рамках академической мобильности)
	7.1.3.3	Если применимо, должна быть предоставлена инфраструктура … Примечание 1. Инфраструктура может включать цифровое пространство.	Целесообразно принять во внимание стандарт ИБ ISO/IEC 27001 и/или ISO/IEC 27032 в области кибербезопасности
	7.1.6	При рассмотрении изменяющихся потребностей и тенденций организация должна оценивать текущий уровень знаний. Примечание 2. Знания организации могут быть основаны на: — внутренних источниках … — внешних источниках ...	Важно обеспечить «классический подход» разделения внешних и внутренних факторов в аспекте обеспечения ИБ
	7.1.6.2	Образовательные ресурсы должны: b) подвергаться анализу через запланированные промежутки времени для обеспечения их актуальности;	Важно для любого ВУЗа, поскольку есть риск проиграть конкурентам
	7.5.3.1	b) её 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.

Операционная деятельность Operations	8.1.1	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
	8.4.3	Организация должна сообщать внешним поставщикам свои требования в отношении: c) компетентности, включая все необходимые квалификации персонала;	Очень важно для любого ВУЗа, поскольку важно обеспечить защиту ПДн
	8.5.5	c) при каких условиях данные обучающихся могут быть предоставлены третьим сторонам;	Очень важно для любого ВУЗа, поскольку важно обеспечить защиту ПДн

Вывод. В представленной публикации предложены основные результаты процесса обеспечения требований ИБ при выполнении учебного процесса в ВУЗах Российской Федерации.

Новизна представленной публикации заключается в объективных примерах применения известных стандартов (например ISO 9001 или ISO 21001) для результативного выполнения соответствующих требований в области ИБ.

Полученные результаты могут быть применены заинтересованными сторонами, стремящимися обеспечить требуемый уровень ИБ в рамках общего процесса обеспечения результативной СМК или СМОО для ВУЗов.

Библиографический список:

1. https://www.iso.org/standard/62085.html
2. https://www.iso.org/standard/66266.html
3. https://www.iso.org/standard/27001
4. https://www.kommersant.ru/doc/7480689?from=trends
5. https://www.securitylab.ru/news/537985.php
6. https://cyberresilience.com/threatintel/apt-group-kimsuky-targets-university-researchers/?utm_source=se%D1%81uritylabru
7. https://www.securitylab.ru/news/536418.php
8. https://www.securitylab.ru/news/536310.php
9. https://www.securitylab.ru/news/539183.php
10. https://www.kommersant.ru/doc/7381376?ysclid=m8po0siqqx875956208
11. https://www.iso.org/the-iso-survey.html
12. Лившиц И.И. Обеспечение безопасности персональных данных в условиях дистанционного режима // Энергобезопасность и энергосбережение. 2022. № 1. С. 57-62.
13. Лившиц И.И. Результаты применения воронки рисков в полном дистанционном режиме обучения // Энергобезопасность и энергосбережение. 2021. № 2. С. 46-50.
14. Лившиц И.И. Управление качеством в дистанционном режиме обучения на примере практики в университете ИТМО // Менеджмент качества. 2022. № 1. С. 68-77.
15. Лившиц И.И. Об актуальных проблемах образования в области информационной безопасности // Автоматизация в промышленности. 2019. № 9. С. 10-13.
16. Лившиц И.И. Оценка необходимости совершенствования действующего порядка подготовки квалифицированных кадров в области информационной безопасности // Газовая промышленность. 2024. № 9 (871). С. 200-205.
17. Лившиц И.И. Проблемы подготовки специалистов в области информационной безопасности // Вестник Дагестанского государственного технического университета. Технические науки. 2024. Т. 51. № 1. С. 123-131.
18. 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.
19. 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.

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

References:

1. https://www.iso.org/standard/62085.html
2. https://www.iso.org/standard/66266.html
3. https://www.iso.org/standard/27001
4. https://www.kommersant.ru/doc/7480689?from=trends
5. https://www.securitylab.ru/news/537985.php
6. https://cyberresilience.com/threatintel/apt-group-kimsuky-targets-university-researchers/?utm_source=se%D1%81uritylabru
7. https://www.securitylab.ru/news/536418.php
8. https://www.securitylab.ru/news/536310.php
9. https://www.securitylab.ru/news/539183.php
10. https://www.kommersant.ru/doc/7381376?ysclid=m8po0siqqx875956208
11. https://www.iso.org/the-iso-survey.html
12. Livshits I.I. Ensuring the Security of Personal Data in Remote Learning. *Energy Safety and Energy Saving*. 2022;1:57-62. (In Russ)
13. Livshits I.I. Results of Applying the Risk Funnel in Full Distance Learning. *Energy Safety and Energy Saving*. 2021;2: 46-50. (In Russ)
14. Livshits I.I. Quality Management in Distance Learning: An Example of Practice at ITMO University. *Quality Management*. 2022;1: 68-77. (In Russ)
15. Livshits I.I. On Current Issues of Education in the Field of Information Security. *Automation in Industry*. 2019; 9:10-13. (In Russ)
16. Livshits I.I. Assessing the Need to Improve the Current Procedure for Training Qualified Personnel in the Field of Information Security. *Gas Industry*. 2024;9 (871):200-205. (In Russ)
17. Livshits I.I. Problems of Training Specialists in the Field of Information Security. *Herald of the Dagestan State Technical University. Technical Sciences*. 2024;51(1):123-131. (In Russ)
18. Livshits I.I., Neklyudov A.V. Methodology for Optimizing the Information Security Audit Program. In the collection: Comprehensive Information Protection. Proceedings of the XXII scientific and practical conference. 2017:135-139. (In Russ)
19. Livshits I.I., Neklyudov A.V. Methodology for Instant Information Security Audits. In the collection: Comprehensive Information Protection. Proceedings of the XXII scientific and practical conference. 2017: 139-142. (In Russ)
20. Livshits I.I. Methodology for technical security audit of own Service Desk. *Standards and quality*. 2024;6:. 102-107. (In Russ)

Сведения об авторе:
Лившиц Илья Иосифович, доктор технических наук, профессор практики, Livshitz.i@yandex.ru
Information about author:
Ilya I. Livshits, Dr. Sci.(Eng.), Prof. of Practice; Livshitz.i@yandex.ru

Конфликт интересов/Conflict of interest.
Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.
Поступила в редакцию/Received 18.06. 2025.
Одобрена после рецензирования/Reviced 22.07.2025.
Принята в печать/ Accepted for publication 30.08.2025.