Лабороторна робота №6
"Стандарти в інформаційній сфері"

Мета роботи: Отримати практичні навички аналізу стандартів інформаційної сфери та їх застосування для оцінки якості інформаційних систем.

Основні завдання:

Дослідити та класифікувати види стандартів, що діють в інформаційній сфері.

Проаналізувати обрану інформаційну систему (або її опис) на предмет відповідності вимогам конкретних стандартів.

Сформулювати висновки щодо ролі стандартизації для управління якістю інформаційних систем.

🔍 Теоретична частина. Класифікація стандартів в інформаційній сфері

Завдання: На основі рекомендованих джерел та самостійного пошуку, заповніть таблицю класифікації стандартів. Для кожного виду наведіть 1-2 конкретних приклади з коротким описом їх призначення.

Вид стандарту	**Призначення**	**Приклади**	**Сфера застосування**
1. Міжнародні стандарти інформаційної безпеки	Забезпечення конфіденційності, цілісності та доступності інформації. Надають рамки для побудови системи управління інформаційною безпекою (СУІБ).	- **ISO/IEC 27001** — визначає вимоги до СУІБ для сертифікації. - **ISO/IEC 27002** — практичні правила та контрольні заходи для безпеки інформації.	Підприємства будь-якого розміру та галузі, що прагнуть системно керувати ризиками безпеки інформації.
2. Національні стандарти (ДСТУ)	Нормативне регулювання в Україні у сферах інформації, документації та побудови систем.	- **ДСТУ 5034:2008** — визначає термінологію науково-інформаційної діяльності. - **ДСТУ 3396.1-96** — визначає порядок проведення робіт з технічного	Організації та установи України, технічні комітети, архіви, бібліотеки.

Вид стандарту	Призначення	Приклади	Сфера застосування
		захисту інформації.	
3. Галузеві стандарти	Забезпечення безпеки та надійності в конкретних, критично важливих галузях економіки.	- **PCI DSS** — стандарт безпеки даних індустрії платіжних карток для захисту фінансових транзакцій.	Фінансові установи, торговці, що обробляють платежі картками.
4. Стандарти з управління проектами та життєвим циклом	Регламентація процесів створення, впровадження та супроводу інформаційних систем.	- **ГОСТ 34.602-89** — вимоги до змісту технічного завдання на створення автоматизованої системи. - **РД 50-34.698** — вимоги до змісту документів на автоматизовані системи.	Розробники, замовники та експлуатаційні служби автоматизованих систем.

💻 Практична частина. Аналіз інформаційної системи на відповідність стандартам

Завдання: Виберіть будь-яку реальну або гіпотетичну інформаційну систему
Варіанти – обирати з варіантів лабороторної роботи № 5
Проаналізуйте її, використовуючи нижченаведену схему.

1. Опис об'єкта аналізу:
Назва системи: *Наприклад, "Інформаційна система приймальної комісії ВНЗ"*.
Основне призначення: *Збір, зберігання та обробка заяв від абітурієнтів, формування рейтингових списків*.
Ключові компоненти: *Веб-інтерфейс для абітурієнтів, база даних з персональною інформацією, модуль формування звітів*.

2. Аналіз відповідності стандартам:
ISO/IEC 27001 (Безпека інформації):

Критерій: Наявність документованої політики безпеки інформації та процесів управління ризиками.
Статус відповідності: ⚠️ *Частково відповідає.*
Обґрунтування: *Система має механізми авторизації та шифрування даних, що відповідає принципам стандарту. Однак відсутній документований огляд ризиків безпеки для цієї конкретної системи.*
ДСТУ 5034:2008 (Термінологія):
Критерій: Чітке визначення понять "заявка", "рейтинг", "особиста справа" в описі системи.
Статус відповідності: ❌ *Не відповідає.*
Обґрунтування: *Внутрішня документація системи використовує терміни, що відрізняються від загальноприйнятих в освітній сфері, що може призвести до непорозумінь.*
Принципи якості інформаційних систем (на основі):
Критерій: Підтримка прийняття рішень на операційному (обробка заяв) та тактичному (аналіз вступної кампанії) рівнях.
Статус відповідає: ✅ *Повністю відповідає.*
Обґрунтування: *Система ефективно автоматизує операційні завдання та надає керівництву аналітичні звіти для прийняття стратегічних рішень щодо набору.*

3. Висновки та рекомендації щодо вдосконалення системи:
Головний висновок: Система функціонально ефективна, але потребує покращення в частині формалізації процесів управління безпекою та уніфікації термінології.
Рекомендації:
Розробити та затвердити *Політику безпеки інформації* для системи, провести оцінку ризиків.
Привести терміни, що використовуються в інтерфейсі та документації, у відповідність до національних стандартів (ДСТУ) та галузевих норм.
Запровадити процедуру регулярного аудиту журналів подій системи для забезпечення відстежуваності дій.

✅ Питання для самоперевірки

Чим відрізняються стандарти **ISO/IEC 27001** та **ISO/IEC 27002** за своїм призначенням?
Яку практичну користь для розробника системи несе **ГОСТ 34.602-89**?
Навіщо інформаційній системі управління відповідати принципам, описаним у?

📚 Список використаних джерел

Вікіпедія. Стандарти інформаційної безпеки посилання .
Міжнародні стандарти інформаційної безпеки посилання.
LibreTexts. Інформаційні системи управління посилання.
Вікіпедія. Список нормативних документів щодо інформаційної безпеки в Україні посилання.

Терещенко Л. Принципи класифікації управлінських інформаційних систем посилання.
ДСТУ 5034:2008 Інформація і документація. Науково-інформаційна діяльність посилання.