**PDCA-цикл как инструмент в контексте СМИБ**

|  |
| --- |
| **ЗАДАНИЕ** |
| Как отмечалось в 1-ой сессии, PDCA-цикл встроен в структуру системы менеджмента. Хотя эта связь между различными этапами PDCA не так заметна, как в первом издании ISO/IEC 27001, ее все же можно проследить и в текущей версии ISO/IEC 27001.  Теперь, когда мы освежили знания о структуре и содержании стандарта, ваша задача — просмотреть разделы ISO/IEC 27001 и распределить их по различным фазам PDCA-цикла.  Например, пункт 4.1. относится к этапу планирования, поскольку организация собирает информацию о себе для создания своей системы. Является ли это единственной ролью 4.1 или она применима и в другие периоды цикла, не связанные с первоначальным планированием системы. Если да, меняется ли ассоциация фаз? Представьте обоснование своего выбора.  Обратите внимание, что один раздел может иметь более одной ассоциированной фазы. |

|  |
| --- |
| **ВРЕМЯ** |
| 30 минут на подготовку  15 минут общее обсуждение |

|  |
| --- |
| **РЕЗУЛЬТАТЫ** |
| Заполненная таблица в соответствии с условиями задания. |

|  |
| --- |
| **МЕТОД ОЦЕНКИ** |
| По готовности, вы представите результат в общем обсуждении поочередно. Преподаватель даст обратную связь и сфокусирует внимание на важных моментах. |

| **Раздел ISO/IEC 27001:2022** | **Выбор фазы PDCA** | **Обоснование** |
| --- | --- | --- |
| 4.1 Understanding the organization and its context  **Понимание организации и её контекста** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 4.2 Understanding the needs and expectations of interested parties  **Понимание потребностей и ожиданий заинтересованных сторон** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 4.3 Determining the scope of the information security management system  **Определение области применения системы менеджмента информационной безопасности** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 4.4 Information security management system  **Система менеджмента информационной безопасности** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 5.1 Leadership and commitment  **Лидерство и приверженность** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 5.2 Policy  **Политика** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 5.3 Organizational roles, responsibilities and authorities  **Организационные обязанности, ответственность и полномочия** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 6.1 Actions to address risks and opportunities  **Действия по работе с рисками и возможностями** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 6.2 Information security objectives and planning to achieve them  **Цели в области информационной безопасности и планирование их выполнения** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 6.3 Planning of changes  **Планирование изменений** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 7.1 Resources  **Ресурсы** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 7.2 Competence  **Компетентность** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 7.3 Awareness  **Осведомлённость** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 7.4 Communication  **Обмен информацией** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 7.5 Documented information  **Документированная информация** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 8.1 Operational planning and control  **Планирование и управление операциями** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 8.2 Information security risk assessment  **Оценка рисков информационной безопасности** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 8.3 Information security risk treatment  **Обработка рисков информационной безопасности** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 9.1 Monitoring, measurement, analysis and evaluation  **Мониторинг, измерение, анализ и оценка** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 9.2 Internal audit  **Внутренний аудит** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 9.3 Management review  **Анализ со стороны руководства** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 10.1 Continual improvement  **Непрерывное улучшение** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| 10.2 Nonconformity and corrective action  **Несоответствия и корректирующие действия** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |
| Annex A  **Приложение А** | Plan (**P**)  Do (**D**)  Check (**C**)  Act (**A**) |  |

**Пожалуйста, передайте этот лист своему преподавателю по завершении упражнения.**