

Управление документами и записями

написано Александр Астахов | 10 июня, 2023

Для эксплуатации и сопровождения СУИБ необходима полная, доступная и корректная документация, а также контролируемый процесс управления документами, область действия и уровень детализации которого для разных организаций может варьироваться. Ответственность за осуществление надзора над процессом управления документацией должна быть четко определена и согласована.

Требования к управлению документами и записями содержатся в ISO 27001. Эти требования полностью соответствуют требованиям, предъявляемым к документации другими стандартами систем управления, такими как ISO 9001. Они помогают комбинировать различные системы управления и согласованно применять необходимые механизмы контроля документации. Эффективный контроль документов способствует согласованному распространению информации, устраняя неразбериху в отношении состояния СУИБ.

Управление документами и записями:

- *контроль и защита документов и записей;*
- *утверждение, анализ и корректировка документов;*
- *идентификация изменений и статуса текущих версий;*
- *обеспечение доступности, передачи, хранения и уничтожения документов и записей;*
- *идентификация устаревших документов и документов, имеющих внешнее происхождение;*
- *контроль над распространением документов;*
- *предотвращение непреднамеренного использования устаревших документов.*

Документация включает в себя политики, стандарты, руководства, процедуры, списки проверки, реестр рисков и другие документы, используемые для поддержки СУИБ. В ISO 27001 содержится список документации, которая в обязательном порядке должна быть разработана. Он включает в себя:

- документированные положения политики безопасности и цели контроля;
- область действия СУИБ;
- процедуры и механизмы контроля, поддерживающие СУИБ;
- описание методологии оценки рисков;
- отчет об оценке рисков;
- план обработки рисков;
- документированные процедуры, которые необходимы для обеспечения эффективного планирования, выполнения и контроля процессов информационной безопасности и описывающие, как измерять эффективность механизмов контроля;
- записи о процессах СУИБ;
- декларация о применимости механизмов контроля.

Эта, а также любая другая, документация и записи, необходимые для эксплуатации СУИБ и предоставления свидетельств ее корректного и эффективного функционирования, должны поддерживаться в актуальном состоянии. Некоторая документация, относящаяся к исполнению механизмов контроля СУИБ, может находиться в области ответственности функциональных подразделений, не относящихся к информационной безопасности.