ISO/IEC 27001:2022 и ISO/IEC 27002:2022: Ключевые обновления и идеи

написано GlobalTrust.ru | 16.05.2024

Международный стандарт на системы менеджмента информационной безопасности ISO 27001 и сопутствующий ему стандарт ISO 27002 были обновлены в 2022 году. В этой статье рассказывается о наиболее заметных изменениях этих стандартов.

Изменения ISO/IEC 27001:2022

ISO 27001:2022 существенно не отличается от ISO 27001:2013, но есть некоторые заметные изменения. Однако большинство из них относятся к Приложению SL, структуре высокого уровня, общей для всех новых стандартов систем менеджмента ISO, а не к информационной безопасности:

- **Контекст и область действия.** Теперь вы должны определить «релевантные» требования заинтересованных сторон и определить, какие требования будут удовлетворяться посредством СМИБ, которая теперь должна явно включать в себя «необходимые процессы и их взаимодействие».
- **Планирование.** Цели информационной безопасности теперь должны контролироваться и «быть доступными в виде документированной информации». Появился новый подраздел, посвященный планированию изменений в СМИБ. Здесь не указаны какие-либо процессы, которые должны быть включены, поэтому вам следует определить, как вы можете продемонстрировать, что изменения в

СМИБ действительно были запланированы.

- **Поддержка.** Требования по определению того, кто будет коммуницировать, и процессы осуществления коммуникации были заменены требованием определить, «каким образом следует коммуницировать».
- **Операции.** Требование планировать способы достижения целей информационной безопасности было заменено требованием установить критерии для процессов реализации действий, определенных в разделе 6, и управлять этими процессами в соответствии с этими критериями. От организаций теперь требуется контролировать «предоставляемые из-вне процессы, продукты или услуги», имеющие отношение к СМИБ.
- **Приложение.** Приложение А было пересмотрено для приведения его в соответствие с ISO 27002:2022. Механизмы контроля согласно Приложению А обсуждаются в разделе ниже.

Каковы изменения контроля в Приложении А?

Некоторые механизмы контроля Приложения А были объединены, а также было добавлено 11 новых:

- Несмотря на то, что никакие контроли не были удалены, в ISO 27001:2022 перечислено только 93 контроля, а не 114 как в ISO 27001:2013. Это связано с большим количеством объединенных контролей (24 вместо 56).
- Эти контроли сгруппированы в 4 «темы», а не в 14 областей контроля, как раньше. Они включают в себя:
    - Кадровые (8 контролей)
    - Организационные (37 контролей)
    - Технологические (34 контроля)
    - Физические (14 контролей)

- Совершенно новые контроли:
    - Разведка угроз

        - Информационная безопасность при использовании Облачных сервисов
        - Готовность ИКТ к обеспечению непрерывности бизнеса
        - Мониторинг физической безопасности
        - Управление конфигурацией
        - Удаление информации
        - Маскирование данных
        - Предотвращение утечки данных
        - Мониторинг активности
        - Веб-фильтрация
        - Безопасное кодирование

- В ISO 27002 контроли также имеют пять типов «атрибутов», чтобы их было легче классифицировать:
    - Тип контроля (превентивный, детектирующий, корректирующий)
    - Свойства информационной безопасности (конфиденциальность, целостность, доступность)
    - Концепции кибербезопасности (идентификация, защита, обнаружение, реагирование, восстановление)
    - Операционные возможности (стратегическое управление, управление активами и т. д.)
    - Домены безопасности (стратегическое управление и экосистема, защита, оборона, устойчивость)

Что изменилось в ISO 27002?

Фраза «свод правил» (“code of practice”) была исключена из названия обновленного стандарта ISO 27002. Это лучше отражает его цель как эталонного набора мер по обеспечению информационной безопасности.

Сам стандарт значительно длиннее предыдущей версии, а элементы управления были переупорядочены и обновлены, как описано в разделе выше.

Как обновление ISO 27001 повлияет на вашу организацию?

Если вы находились на стадии внедрения предыдущей версии стандарта, не паникуйте. Органы по сертификации, скорее всего, предложат сертификацию по стандарту ISO 27001:2022 всего через шесть месяцев после его публикации. Кроме того, стандарт ISO 27001:2013 будет сохранен еще на три года, так что ваша работа по внедрению стандарта 27001:2013 не пропадет. Однако вы можете использовать новые контроли согласно Приложению A из ISO 27001:2022 в качестве альтернативного набора контролей.

Если вы уже сертифицированы по стандарту ISO 27001:2013, помните, что у вас будет время («Переходный период») для полного перехода на новые требования. Однако лучший момент для этого — перед следующим внутренним аудитом , независимо от того, прошли ли вы сертификацию давным давно или только находитесь в процессе сертификации.

Внутренний аудит ISO 27001 включает детальную оценку СМИБ вашей организации, чтобы убедиться в ее соответствии критериям стандарта. Это позволит вам оценить, правильно ли вы отразили в СМИБ изменения, не подвергая риску статус вашей сертификации. Рекомендуется проведение внутреннего аудита как минимум за три месяца до проведения внешней оценки. Это позволит выявить любые потенциальные несоответствия и исправить их до прихода внешнего оценщика.