Декларация о применимости механизмов контроля

написано Александр Астахов | 11 июня, 2023

Оценка рисков позволяет двигаться от анализа потенциальных проблем к формулировке конкретных требований безопасности, применимых к организации. Для контроля реализации этих требований необходимо знать, где организация находится в данный момент и где она хочет быть завтра. Определение и контроль выполнения требований безопасности в соответствии с ISO 27001 осуществляется в форме «Декларации о применимости механизмов контроля».

*Декларация о применимости механизмов контроля*предназначена для отображения требований безопасности, устанавливаемых международным стандартом ISO 27001, а также любых других требований безопасности на требования безопасности организации, идентифицированные в результате оценки рисков. Декларация о применимости может служить основой для разработки плана обработки рисков. Любые исключения из Декларации о применимости механизмов контроля, описанных в стандарте ISO 27001, а также в других стандартах и нормативных документах, применимых к организации, должны быть обоснованы.

№	Область контроля	Механизм контроля	Текущее состояние	Комментарий или обоснование для исключения механизма контроля
A.5 Политика безопасности				
A.5.1 Политика информационной безопасности Цель: Обеспечить управление и поддержку в области информационной безопасности со стороны руководства организации в соответствии с требованиями бизнеса, относящимися к делу законами и нормативными актами.				
A.5.1.1	Документированная политика информационной безопасности	Документированная политика информационной безопасности должна быть утверждена руководством, опубликована и доведена до сведения всех сотрудников организации и имеющих к ней отношение внешних сторон.	QY	Документированная политика безопасности утверждена руководством и доведена до сведения сотрудников под роспись. Необходимо пересмотреть содержание политики безопасности в соответствии с требованиями ISO 27001.
A.5.1.2	Пересмотр политики информационной безопасности	Политика информационной безопасности должна пересматриваться через запланированные интервалы времени, а также в случае влияющих на нее существенных изменений, чтобы обеспечить ее непрерывное соответствие реальному положению дел, достаточность и эффективность.	N	Пересмотр политики безопасности не производился.
A.6 Организация информационной безопасности				
A.6.1 Внутренняя организация Цель: Управлять информационной безопасностью в организации.				

Декларация о применимости не только описывает все применимые к организации требования безопасности, но также определяет

текущее состояние выполнения этих требований, являясь одновременно и *отчетом о несоответствиях* организации требованиям безопасности. Это основной документ, используемый аудиторами при проведении проверок реализации механизмов контроля, оценки соответствия организации стандартам и сертификационных мероприятиях.

Данный документ актуализируется по мере возникновения новых рисков, переоценки существующих рисков, изменения требований законодательства, а также по мере реализации мер по обработке рисков.

Для оценки текущего уровня соответствия по каждой области контроля используется несложная формула. Состояние механизма контроля оценивается по качественной трехзначной шкале. В случае необходимости эта шкала может быть расширена, а формула слегка усложнена с тем, чтобы учитывать относительные веса механизмов контроля.

Текущее состояние механизма контроля (или процесса) может быть следующим:

Y– реализован полностью

QY– реализован частично

N– не реализован

NA– не применяется (например, по причине низкого уровня риска, осознанно принимаемого руководством)

?– применимость механизма контроля не определена, требуется дополнительное исследование

Уровень соответствия требованиям для каждой области контроля (группы процессов) рассчитывается по формуле:

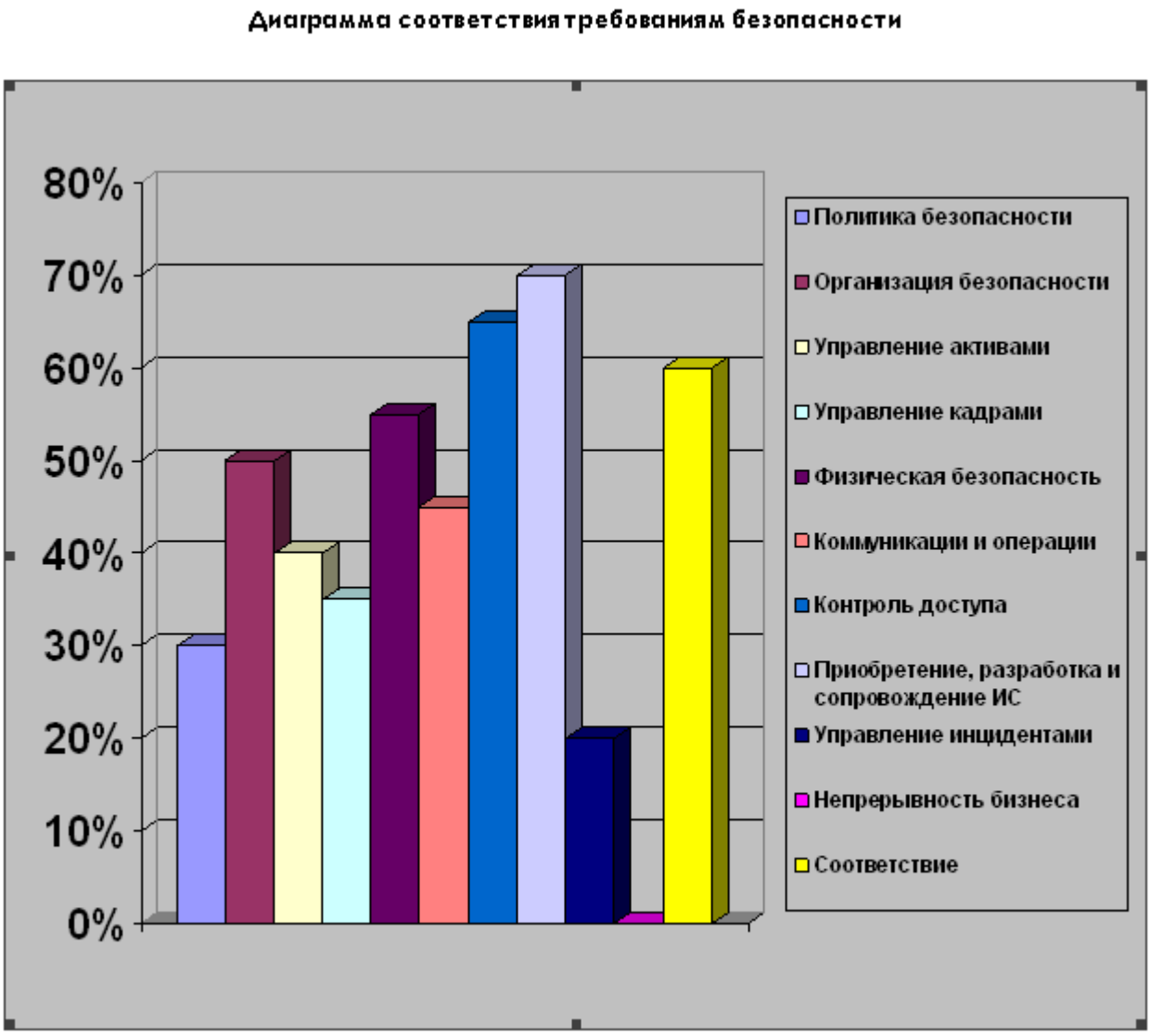
[∑n (Состояние контроля)] / (2n) x 100%,

где **n** – количество механизмов контроля, находящихся в

состоянии **Y, QY** или **N.**

Состояние контроля может принимать одно из трех значений: **Y = 2, QY = 1, N = 0.**

Диаграмма соответствия организации требованиям безопасности по областям контроля, определяемым в стандарте ISO 27001, с учетом существующих рисков, приведена на рисунке.



Для достижения оптимального уровня возврата инвестиций в информационную безопасность организация должна стремиться к полному соответствию требованиям, сформулированным в Декларации о применимости.

Отметим, что даже полное соответствие организации своей Декларации о применимости не означает того, что все риски

обработаны и План обработки рисков больше не нужен. Практически все контрмеры требуют не только внедрения, но и непрерывной деятельности по поддержанию этих контрмер в рабочем состоянии, включающей в себя эксплуатацию, администрирование, мониторинг, корректировку и совершенствование. Все эти мероприятия должны быть отражены в Плане обработки рисков.

Поэтому даже если организация внедрила все механизмы контроля, описанные в ее Декларации о применимости, то План обработки рисков ей все равно необходим. Кроме того, ситуация с рисками непрерывно изменяется, так же как изменяется и отношение руководства организации к определенным рискам, поэтому описанный в Декларации о применимости состав механизмов контроля не остается неизменным.