Идентификация организационных уязвимостей

написано Александр Астахов | 10 июня, 2023

К *организационным уязвимостям* относятся любые слабости защиты, не являющиеся слабостями технических или программных средств.

Для идентификации организационных уязвимостей проводится проверка источников этих уязвимостей, к которым относятся:

- процессы управления безопасностью;
- организационная структура, распределение ролей и ответственности;
- документированные процедуры и записи;
- квалификация, осведомленность и обученность персонала;
- физические меры защиты и физическое окружение;
- соответствие требованиям законодательства, нормативной базы, договоров, стандартов и бизнеса.

Организационные уязвимости обычно заключаются в отсутствии или неправильном применении механизмов контроля. Поэтому основным источником идентификации организационных уязвимостей служит международный стандарт ISO 27001, т.к. этот стандарт содержит наиболее полное высокоуровневое описание того, что должно быть сделано для защиты информационных активов. Если чего-то не хватает, то это может рассматриваться в качестве потенциальной уязвимости. Международный стандарт ISO 27002 содержит подробное описание областей и механизмов контроля. Выпускаемые Британским институтом стандартов руководства по аудиту и внедрению СУИБ BIP 0072 и BIP 0073 описывают, каким образом можно оценивать соответствие ISO 27001 и идентифицировать организационные уязвимости.

Еще одним источником идентификации организационных уязвимостей служит анализ законодательной и нормативной базы в области

информационной безопасности.

Источники идентификации потенциальных организационных уязвимостей:

- ***ISO 27001, разделы 4-8,*** *– определяют требования и процессы СУИБ;*
- ***ISO 27001, приложение А,*** *– определяет 11 областей и 137 механизмов контроля;*
- ***ISO 27002*** *– подробно описывает 11 областей и 137 механизмов контроля;*
- ***BIP 0072*** *– содержит опросники для проверки соответствия требованиям ISO 27001;*
- ***BIP 0073*** *– предоставляет дополнительное руководство по внедрению и аудиту механизмов контроля;*
- *применимая законодательная и нормативная база.*

Оценка процессов СУИБ на соответствие ISO 27001

Разделы 4–8 международного стандарта ISO 27001 определяют обязательные (читай – наиболее важные с точки зрения передового опыта и здравого смысла) элементы СУИБ, такие как политика безопасности, оценка и обработка рисков, аудиты, анализ со стороны руководства, анализ эффективности, корректирующие и превентивные меры и т.п. Отсутствие этих элементов почти всегда свидетельствует о наличии серьезных уязвимостей.

Для анализа данных организационных уязвимостей составляется таблица соответствия, в которой для каждого требования, содержащегося в стандарте ISO 27001, отмечается текущее состояние с выполнением этого требования, а также дается описание свойственных организации особенностей в интерпретации этого требования и существующих затруднений с его выполнением.

Оценочные мероприятия включают в себя интервьюирование персонала, сбор и анализ свидетельств надлежащего функционирования СУИБ, анализ полноты и правильности реализации механизмов контроля, описанных в стандарте. Результаты анализа заносятся в оценочную таблицу, фрагмент которой показан на рисунке.

№	Требование стандарта	Текущее состояние	Комментарии
4	**Система управления информационной безопасностью**		
4.1	Общие требования		
	Организация должна создать, внедрить, эксплуатировать, осуществлять мониторинг, анализировать, сопровождать и совершенствовать документированную СУИБ в контексте общих бизнес активностей и рисков организации. В этом Международном стандарте используется процесс, основанный на модели ПРПД, показанной на рисунке 1.		
4.2	Создание и управление СУИБ		
4.2.1	**Создание СУИБ**		
a)	Определить область действия и границы СУИБ в терминах характеристик бизнеса, организации, ее расположения, ресурсов и технологий, а также включая детальную информацию и обоснование для любых исключений из области действия (см. 1.2).		
b)	Определить политику СУИБ в терминах характеристик бизнеса, организации, ее расположения, ресурсов и технологий, которая: 1. включает в себя основу для определения ее целей и устанавливает общее направление и принципы дехтельности по отношению к информационной безопасности; 2. учитывает требования бизнеса и требования законодательной или нормативной базы, а также контрактные обязательства в области безопасности; 3. объединяется со стратегическим контекстом управления рисками в организации, в котором будет происходить создание и сопровождение СУИБ; 4. устанавливает критерии для оценивания рисков (см. 4.2.1c)); и 5. утверждена руководством. ПРИМЕЧАНИЕ: В этом Международном стандарте политика СУИБ рассматривается в качестве надмножества политики информационной безопасности. Эти политики могут быть описаны в одном документе.		

Целесообразность использования механизмов контроля, перечисленных в приложении А стандарта ISO 27001 и далее подробно описанных в стандарте ISO 27002, должна определяться по результатам оценки рисков. Однако отсутствие любого из этих механизмов контроля может рассматриваться на данном этапе в качестве потенциальной уязвимости, т.к. это ослабляет защиту активов.

Для анализа этой группы уязвимостей также используется оценочная таблица, фрагмент которой показан на рисунке. Левая часть этой таблицы полностью повторяет структуру Приложения А стандарта ISO 27001, а в правой части отмечается текущий статус реализации соответствующих механизмов контроля, описываются особенности реализации этих механизмов, а также

приводится обоснование исключений некоторых механизмов контроля там, где это необходимо.

Как мы увидим далее, именно эта оценочная таблица будет выполнять роль Декларации о применимости механизмов контроля – важнейшего документа СУИБ, вокруг которого в последующем будет строиться обработка рисков и аудиты.

№	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.		
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.		
A.6 Организация информационной безопасности				
A.6.1 Внутренняя организация Цель: Управлять информационной безопасностью в организации.				
A.6.1.1	Приверженность руководства информационной безопасности	Руководство должно активно поддерживать безопасность в организации путем четкого управления, демонстрируемой приверженности, явного назначения и подтверждения ответственности за информационную безопасность.		
A.6.1.2	Координация информационной безопасности	Действия по обеспечению информационной безопасности должны координироваться представителями из различных частей организации с соответствующими ролями и должностными обязанностями.		

Результатом идентификации организационных уязвимостей является отчет о несоответствиях, в котором для каждой области контроля определяется степень соответствия, перечисляются существующие механизмы безопасности, сильные и слабые стороны, а также даются рекомендации по усилению защиты.

На следующем рисунке приведен фрагмент таблицы с описанием уязвимостей для области контроля «Управление активами».

Таблица. Оценка достижения цели контроля «Управление активами»

Цель контроля:	Обеспечить и поддерживать надлежащий уровень защиты активов организации.Все активы должны быть учтены и иметь назначенного владельца. Также должна быть определена ответственность за сопровождение этих активов и обеспечение их безопасности.

Уровень соответствия:	Низкий (40%)
Свидетельства соответствия:	Политика безопасности организации определяет права доступа к основным категориям информационных и ИТ активов на уровне файловых папок, ИТ сервисов и программных модулей. Права доступа периодически проверяются и пересматриваются.Политика безопасности определяет правила допустимого использования активов, которые внедрены и соблюдаются на практике.Перечень конфиденциальной информации оформлен в виде приложения к Политике безопасности.
Несоответствия:	Отсутствует реестр информационных активов.Владельцы активов не идентифицированы явным образом.Отсутствуют правила маркирования и обращения с конфиденциальными документами, а также схема их классификации.
Рекомендации:	Сформировать и поддерживать в актуальном состоянии реестр активов.Назначить владельцев для каждого активов и определить их ответственность за активы.Определить общую схему классификации информации по критериям конфиденциальности, целостности и доступности.Разработать и внедрить правила маркировки и обращения с конфиденциальными документами.