Общие недостатки и ограничения коммерческих программных продуктов

написано Александр Астахов | 11 июня, 2023

Недостатки, свойственные многим программным продуктам, предназначенным для управления рисками, ограничивают их практическое применение. К числу наиболее распространенных недостатков следует отнести:

- неполную совместимость с международными стандартами – например, очень мало продуктов было разработано специально для ISO 27001;
- неполный охват активов. Большинство продуктов сосредоточиваются только на ИТ активах, игнорируя остальные виды активов, которые, однако, не менее важны для информационной безопасности;
- сложность использования. Многие продукты слишком сложны в использовании;
- затруднение процесса осознания рисков, т.к. расчет рисков выполняется автоматически и скрыт от пользователя;
- те или иные проблемы с отображением русского языка, характерные для большинства импортных программных продуктов.

Обнаружить продукт, лишенный всех перечисленных недостатков и в то же время полностью соответствующий требованиям международных стандартов, достаточно сложно. Не говоря уже о том, что многие продукты, позиционируемые разработчиками как средства для оценки или управления рисками, на самом деле таковыми не являются, т.к. не реализуют ни методологии оценки рисков, ни алгоритма их вычисления, а предоставляют лишь средства представления и хранения данных о рисках, оставляя

анализ и оценивание рисков, по существу, на откуп пользователю.

Многие известные продукты либо не позволяют проводить полноценной оценки рисков (Cobra), а скорее являются средствами для анализа несоответствий требованиям стандарта ISO 27001 (gap analysis), либо включают в себя слабые средства оценки рисков, не полностью соответствующие требованиям ISO 27001, хотя в них много другого функционала (Callio Secura), либо являются слишком сложными в использовании, дорогими и некастомизируемыми (CRAMM).

Можно было бы выделить из этого списка RA2 the art of risk как инструмент полностью соответствующий требованиям ISO 27001 (его разработчики являются авторами этого международного стандарта), однако он не позволяет сравнивать между собой результаты оценок, что было бы необходимо для крупной организации, содержит крайне примитивные средства построения модели активов и редактирования текстовой информации, затрудняющие его использование, а также неправильно отображает русские буквы в отчетах.

Нас также в целом устраивает RiskWatch, однако он, как и многие другие продукты, не был специально разработан для ISO 27001, а его цена довольно высока.

Можно было бы обратить внимание на новый продукт vsRisk британской компании IT Governance. Он позволяет получать по результатам оценки рисков полноценную Декларацию о применимости в полном соответствии с требованиями ISO 27001. Однако vsRisk также неправильно отображает русские буквы и содержит ряд других существенных недостатков, затрудняющих его практическое применение и которые разработчики обещали устранить когда-нибудь в следующих версиях продукта.