

большинство МВИ из этих реестров на сегодняшний день частично или полностью уже не соответствуют требованиям, предъявляемым к ним (ГОСТ 8.010 и т.д.). В связи с этим, реестры были актуализированы. При этом, к примеру, в Республике Беларусь государственный реестр МВИ «опустел» почти на 30 % от изначального состояния (на 1 января 2015 года). В свою очередь, это привело к формированию значительной проблемы для ряда лабораторий Республики Беларусь, работающих в сфере законодательной метрологии и применявших исключенные методики.

К сожалению, в Республике Беларусь до сих пор не организована грамотная работа по актуализации реестра МВИ, начиная от информирования организаций об исключении методики из реестра до общего планирования работ по его актуализации. Поэтому сотрудники лабораторий отечественных предприятий занимаются решением данного вопроса самостоятельно. С одной стороны, это имеет ряд положительных моментов – реестр постепенно актуализируется, а с другой стороны, формируют ряд проблемных областей – дублирование работ по разработке МВИ, низкая результативность работ и т. д.

УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ МЕНЕДЖМЕНТА РИСКОВ

Студент гр. 11305315 Прихач И. В.

Ст. преподаватель Павлов К. А.

Белорусский национальный технический университет

Метод анализа и оценки рисков информационной безопасности, описанный в СТБ ISO/IEC 27005-2012 «Информационные технологии. Методы обеспечения безопасности. Менеджмент рисков информационной безопасности», более полно отражают специфику работы с системой менеджмента информационной безопасности, нежели стандарты ISO серии 31000.

В соответствии с положениями СТБ ISO/IEC 27005 обработка рисков информационной безопасности рассматривается как итеративный процесс, что предоставляет возможность повысить уровень детализации оценки рисков при каждой последующей итерации.

Процесс оценки рисков информационной безопасности предлагает определенную поэлементную процедуру описания рисков информационной безопасности, которая включает проведение инвентаризации активов организации, выявление их уязвимостей и угроз, а также определение последствий от реализации угроз в отношении активов и оценки влияния реализуемых и внедряемых мер на последствия для активов организации.

Определение существующих мер защиты является следующим этапом в управлении рисками информационной безопасности. Здесь же рассматривается вопрос о разработке и внедрении мер в отношении рисков, для которых в текущем состоянии системы менеджмента информационной безопасности не реализуются защитные меры.

Процесс менеджмента риска информационной безопасности и связанные с ним действия соответствуют текущим обстоятельствам и соблюдаются. В связи с этим, итоговый перечень рисков и их факторов (угрозы, уязвимости, вероятность возникновения, последствия и пр.) может и должен постоянно пересматриваться организацией в рамках мониторинга рисков.

Результаты введения мер защиты отражаются в документированной информации системы менеджмента информационной безопасности организации, называемой «Заявление о применимости» (SoA – Statement of applicability).

Методология, описанная в СТБ ISO/IEC 27005, довольно сложна и требовательна к затратам ресурсов, но она позволяет получить более полную исходную информацию о состоянии информационной безопасности в организации, что, в свою очередь, приводит к более корректному планированию внедрения или управлению системой менеджмента информационной безопасности, соответствующей требованиям СТБ ISO/IEC 27001.

УДК 005.6

ISO/IEC СЕРИИ 9000 КАК ИНСТРУМЕНТ ФОРМИРОВАНИЯ СМК ДЛЯ ОРГАНИЗАЦИЙ, РАБОТАЮЩИХ В СФЕРЕ ИТ

Студент гр. 11305315 Абдыев А. Д.

Ст. преподаватель Павлов К. А.

Белорусский национальный технический университет

В настоящее время автоматизация стала одним из ключевых методов и ресурсов функционирования любой организации: автоматизация бизнес-процессов, внедрение различные информационные системы, электронного документооборота и т.д. Связи с чем, появилось довольно большое количество ИТ-организаций, которые предоставляют услуги по разработке конкретных информационных систем и программных решений.

Данная категория объектов проектирования и производства не укладывается в общее понятие «материальной продукции. С другой стороны, данные разработки не совсем являются услугой, потому что на выходе получается конкретный ресурс, требующий, в том числе, соответствующего обслуживания. Поэтому организации, работающие в ИТ-сфере, столкнулись с определенной ситуацией: следуя принципу удовлетворенности потребителя и формируя СМК на базе стандартов ISO серии 9000, они не могут полностью