УДК 004.056:65.012.8

ДОКУМЕНТИРОВАНИЕ НА ЭТАПАХ РАЗРАБОТКИ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Т.В. БЕЛОУС, Р.В. ПАРШУКОВА, А.М. ПРУДНИК

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
aleksander.prudnik@bsuir.by

Приводится обоснование разработки, а также практические аспекты внедрения системы менеджмента информационной безопасности (СМИБ) для государственных учреждений в соответствии со стандартом СТБ ISO/IEC 27001:2011 «Системы менеджмента информационной безопасности. Требования».

Ключевые слова: информационная безопасность, СМИБ, ISO 27000, оценка рисков, аудит.

СМИБ является частью общей системы управления организации, которая основана на оценке рисков, и предназначена для реализации, эксплуатации, мониторинга и совершенствования ИБ. Реализация СМИБ предполагает использование в качестве руководства для разработки стандартов Международной организации по стандартизации серии ISO 27000 [1], которая в настоящее время насчитывает более 50 стандартов (с учетом стандартов, находящихся на стадии разработки).

Методология реализации СМИБ, как и прочих систем менеджмента (качества, окружающей среды и др.), основана на цикле PDCA (Plan-Do-Check-Act — четырехэтапный итерационный метод решения проблем, используемый для улучшения бизнес-процессов).

К основным достоинствам разработки и внедрения СМИБ принято относить [2]:

– способность организации соответствовать различным требованиям по защите данных, особенно, если данная организация является государственным учреждением, финансовой организацией или учреждением здравоохранения;

– преимущество перед конкурентами;

– снижение расходов, вызванных инцидентами ИБ;

– оптимизация ведения бизнеса — четко определяются обязанности и ответственность сотрудников, а также права доступа к информационным активам.

Перед разработкой СМИБ должны быть выполнены следующие этапы (здесь и далее после наименований этапов в скобках приводятся основные документы, которые должны быть разработаны на данном этапе):

– получение одобрения руководства для реализации СМИБ (описание стандартов, применяемых к организации, описание предварительной области действия СМИБ, определение ролей и сфер ответственности в области СМИБ);

– разработка плана проекта, которая предполагает определение области применения СМИБ (описание производственных процессов и сфер ответственности в области действия СМИБ и за ее пределами; описание информационных систем и телекоммуникационных сетей в области применения СМИБ и за ее пределами);

– определение требований, которым должна соответствовать СМИБ, определение информационных активов организации и получение данных по текущему состоянию ИБ в рамках области применения СМИБ (список основных процессов, функций, объектов, информационных систем, коммуникационных сетей; требования организации, касающиеся конфиденциальности, доступности и целостности; перечень уязвимостей в организации; классификация процессов и активов);

– определение методологии оценки рисков, оценка рисков и выбор вариантов действий с рисками (уменьшение, передача, принятие), а также выбор средств управления ими (перечень целей и средств управления рисками; документированная оценка риска высокого уровня; утвержденная методология оценки риска, совмещенная с контекстом стратегического менеджмента риска в организации).

Непосредственно разработка СМИБ предполагает:

– разработку конечной структуры организации с описанием ролей и сфер ответственности (структура организации, роли и сферы ответственности);

– разработка основы для документации СМИБ (обобщенная база записей и документации по СМИБ, хранилища и шаблоны записей);

– разработку политик ИБ (политики ИБ);

– разработку процедур обеспечения ИБ (процедуры ИБ);

– разработку систем ИБ информационных и коммуникационных технологий и физических объектов, в том числе план внедрения средств управления (план внедрения средств управления, связанных с безопасностью ИКТ и физических объектов);

– разработку средств управления;

– план проверок, проводимых руководством, т.е. список исходных данных для осуществления проверки и ее процедуры, включая аспекты аудита, мониторинга и измерения (список исходных данных для осуществления проверки руководством, процедуры проверки руководством, включая аспекты аудита, мониторинга и измерения);

– разработка программы обучения, образования и информирования персонала организации в области ИБ, в т.ч. материалы для обучения в области ИБ, само обучение в области ИБ, включая разъяснение функций и ответственности, планы обучения и записи результатов обучения, образования и информирования в области ИБ (материалы для обучения в области ИБ; формирование обучения в области ИБ, включая должностные обязанности и ответственность; планы обучения, образования и информирования в области ИБ; документирование результатов обучения и образования в области ИБ);

– разработка конечного плана проекта СМИБ.

После разработки и внедрения СМИБ организации надлежит выполнить процедуры мониторинга и анализа, провести внутренний и внешний аудиты, произвести измерение результативности средств управления с целью определения их соответствия требованиям безопасности, а также выполнить оценки рисков.

Заключительными действиями являются разработка процедур по корректирующим и предупреждающим действиям, проверка соответствия СМИБ по контрольной таблице стандарта ISO 27003[1] и проведение внешнего аудита СМИБ [3].

Список литературы

1. ISO – ISO Standards – ISO/IEC JTC 1/SC 27 – IT Security techniques — Режим доступа http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306. Дата доступа 11.01.2014.

2. Four key benefits of ISO 27001 implementation [Электронный ресурс]. — Режим доступа http://blog.iso27001standard.com/2010/07/21/four-key-benefits-of-iso-27001-implementation/. Дата доступа 11.01.2014.

3. СТБ ISO/IEC 27001:2011. Системы менеджмента информационной безопасности. Требования. Введ. 2012-01-01. Минск: БелГИСС, 2012. 36 с.

[1] В настоящее время СТБ ISO/IEC 27003 «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности» находится на стадии завершения рассмотрения.