защиты информации. При этом данный выходной продукт связан с энергетическими и финансовыми затратами, так что возможна количественная оценка затрат на единицу различающей информации, в том числе, и в интегральном выражении. Возможность же количественной оценки потерь различающей информации в процессе принятия решения позволяет оценивать эти потери при поэтапной обработке информации и осуществлять оптимизацию как в отдельных звеньях цепи поэтапной обработки информации, так и системы защиты в целом.

ПРАКТИЧЕСКИЕ АСПЕКТЫ ВНЕДРЕНИЯ СИСТЕМ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Рассматриваются практические аспекты внедрения системы менеджмента информационной безопасности (СМИБ) в соответствии со стандартом СТБ ISO/IEC 27001:2011 «Системы менеджмента информационной безопасности. Требования». СМИБ — это часть общей системы управления организации, которая основана на оценке рисков, и которая 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.

Перед разработкой СМИБ должны быть выполнены следующие этапы:

– получение одобрения руководства для реализации СМИБ;

– разработка плана проекта, которая предполагает определение области применения СМИБ;

– определение требований, которым должна соответствовать СМИБ, определение информационных активов организации и получение данных по текущему состоянию ИБ в рамках области применения СМИБ;

– определение методологии оценки рисков, оценка рисков и выбор вариантов действий с рисками (уменьшение, передача, принятие), а также выбор средств управления ими.

Непосредственно разработка СМИБ предполагает:

– разработку конечной структуры организации с описанием ролей и сфер ответственности;

– разработку политик ИБ;

– разработку процедур обеспечения ИБ;

– разработку систем ИБ информационных и коммуникационных технологий и физических объектов, в том числе план внедрения средств управления;

– разработку средств управления;

– план проверок, проводимых руководством, т.е. список исходных данных для осуществления проверки и ее процедуры, 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;

– 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, произвести проверку полного соответствия СМИБ по контрольной таблице стандарта ISO 27003 и провести внешний аудит СМИБ.

Литература

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.