СЕКЦИЯ 1. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДЫ ОЦЕНКИ КАЧЕСТВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

А.А. НАВРОЦКИЙ, О.В. ГЕРМАН, Л.С. СТРИГАЛЕВ

В широком спектре проблем безопасности современных автоматизированных систем (АС) различного назначения все большую значимость приобретают методы адекватной оценки качества систем и средств информационной безопасности. Что обусловлено как всевозрастающей сложностью технологических процессов АС, включая средства обеспечения безопасности, так и стоимостью самой защищаемой информации. В этих условиях методы оценки качества информационной безопасности необходимы не только для повышения защищенности и снижения затрат на безопасность АС, но и для мониторинга состояния АС.

Необходимость адекватной оценки качества информационной безопасности предъявляет к названным методам определенную совокупность требований. В числе которых: измеримость показателей качества, чувствительность показателей к существенным параметрам АС и внешней среды, оценка предельных возможностей средств защиты, возможность оценки качества поэтапной обработки информации в технологической цепочке системы зашиты информации. Названные оценки необходимы при разработке, выборе и эксплуатации средств защиты информации.

В докладе обсуждаются достоинства, недостатки и ограничения методов оценки качества средств информационной безопасности, отвечающих названным выше требованиям. Эти методы основаны на количественной оценке качества функционирования средств безопасности и позволяют учитывать энергетические и финансовые затраты, оценивать потери при принятии решения, что дает возможность оптимизировать данные потери по различным критериям, в том числе и с учетом прагматических особенностей АС как в условиях параметрической, так и непараметрической неопределённости.

КРИТЕРИИ ОПТИМИЗАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

А.А. НАВРОЦКИЙ, О.В. ГЕРМАН, Л.С. СТРИГАЛЕВ

Классические критерии оптимальности, такие как критерий идеального наблюдателя, минимума среднего риска, Неймана–Пирсона и др. не обладают свойством аддитивности и поэтому они практически не применимы для конструктивного решения задач оптимизации поэтапной обработки информации.

Указанного недостатка лишена логарифмическая мера отношения правдоподобия (различающая информация) усреднение которой позволяет получить критерий максимума различающей информации эквивалентный частному случаю критерия минимального среднего риска. Используя этот опорный информационный критерий посредством введения весовых коэффициентов можно получить эквиваленты не только других классических критериев, в том числе и последовательный критерий Вальда, но и специфические информационные критерии. Например, такие критерии как критерий максимальной взвешенной информации, критерий максимума полезной информации. Значительные преимущества информационные методы имеют и при решении задач оптимизации в условия параметрической и непараметрической неопределенности.

Основное достоинство этих критериев состоит в том, что различающая информация по существу является «выходным продуктом» для объектов определенного класса средств

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.