электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 621.322

Минимизация ресурсов при проведении аудита системы менеджмента информационной безопасности

Пульман Н.И., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Шахалов И.Ю., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
bauman@bmstu

В настоящее время существует проблема защиты информационной безопасности (ИБ) в организации. Причиной данной проблемы является тенденция быстрого развития организаций и соответственно увеличение объема данных, которые хранятся и обрабатываются в информационной системе (ИС). Рост объема данных ведет к усложнению ИС, а значит неизбежно появление уязвимостей, обнаруживаемых в ней и рисков в области ИБ. Успешная деятельность организации напрямую зависит от системы защиты информации и одним из путей решения проблемы защиты ИБ является построение СМИБ.

СМИБ представляет собой часть общей системы менеджмента организации и основывается на подходе бизнес-рисков при создании, внедрении, функционировании, мониторингу и улучшении ИБ. Современная СМИБ организации является сложной технической системой, которая постоянно совершенствуется для того, чтобы благополучно решать задачи по обеспечению ИБ.

Проведение аудита – это ключевой этап в системе построения и использования СМИБ. Аудит ИБ является обязательным механизмом контроля для любой организации и позволяет получить объективную оценку состояния безопасности функционирования системы, оценить и спрогнозировать риски, а также управлять влиянием рисков на бизнес-процессы организации. Регулярный контроль в виде аудита способствует продвижению организации к построению наиболее эффективной СМИБ.

В области ИБ есть ряд стандартов, содержащих требования по созданию СМИБ организации. Наиболее известные из них: международный стандарт ISO/IEC 27001:2005 (Российский аналог ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология.

Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"), и новый международный стандарт ISO/IEC 27001:2013 "Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования".

Основная задача аудита – это подтверждение конфиденциальности (обеспечения доступности информации только для тех пользователей ИС, которые имеют соответствующие полномочия), целостности (обеспечения точности и полноты информации, а также методов ее обработки) и доступности (обеспечения доступа к информации пользователям ИС, которые имеют соответствующие полномочия, когда это необходимо) информации, обрабатывающейся в ИС организации.

Во время выполнения аудиторских работ также решаются следующие задачи:

- анализ структуры организации;
- анализ защищаемой области деятельности и организационно-распорядительных документов;
- анализ структуры и функциональных особенностей, используемых информационных технологий автоматизированной системы сбора, обработки, передачи и хранения информации;
- проверка выполнения требований стандарта к СМИБ;
- разработка комплексных рекомендаций по методологическому, организационно-управленческому, технологическому, техническому и аппаратно-программному обеспечению для создания, построения или совершенствования СМИБ.

В большинстве случаев решение перечисленных задач сводится к выполнению четырех этапов, а именно:

- планирование аудита;
- планирование мероприятий по аудиту (разработка, согласование и утверждение планов мероприятий);
- проверка на соответствие требованиям стандарта;
- систематизация результатов обследования и формирование отчетности.

Планирование аудита. На данном этапе осуществляется сбор организационно-распорядительных документов, отраслевых стандартов, недокументированных проектных решений и других рабочих материалов, касающихся вопросов создания СМИБ и ИС организации, способствующих использованию механизмов и средств обеспечения ИБ. Разработка, согласование и утверждение планов мероприятий по аудиту.

Проверка на соответствие требованиям стандарта. Этот этап включает: определение области деятельности и ключевые бизнес-процессы организации, которые необходимо защитить в первую очередь; проведение анкетирования и интервьюирования сотрудников организации, анализ организационно-распорядительных и нормативных документов и анализ ИБ на соответствие стандарта.

Оценка рисков ИБ. Аналитический и инструментальный анализ автоматизированной системы и информационных ресурсов организации. Проведение консультаций со специалистами, оценка соответствия фактического уровня безопасности информации и анализ рисков.

Систематизация результатов обследования и формирование отчетности. Предоставление итогового отчета руководству организации.

Сегодня существует довольно много организаций, которые предлагают услугу проведения аудита СМИБ. Некоторые из них придерживаются практики разделения специалистов на две группы: группу аудита и группу технических специалистов. Группа аудита проверяет соответствие СМИБ клиента стандарту ISO 27001, а технические специалисты ищут уязвимости в операционных системах и системах управления базами данных, а также в настройках сетевого оборудования, используя сетевые сканеры уязвимостей и специальные скрипты. В результате проделанной работы, клиент получает отчет с рекомендациями, который состоит из двух отдельных частей – требований ISO 27001 и рекомендаций по устранению технических уязвимостей.

При реализации процесса проведения аудита СМИБ привлекаются сотрудники организации, осуществляется доступ к документам организации и ее базе данных, изучается имеющаяся в организации автоматизированная информационная система, а это все влечет за собой определенный расход временных и трудовых ресурсов, а также материальных затрат.

Таким образом, в данной статье рассматривается важная и актуальная задача минимизации экономических и временных ресурсов путем автоматизации наиболее трудоемких этапов при проведении аудита СМИБ.

Пусть:

$O = \{o_1, \dots, o_n\}$ – множество объектов проверки,

$N = \{1, 2, \dots, n\}$ – множество индексов объектов проверки.

$T(O)$ – время, затраченное на проведение аудита СМИБ на множестве объектов проверки O.

t_1 – время, которое необходимо затратить на планирование мероприятий для проведения аудита.

t_2 – время, которое необходимо затратить на проведение опроса сотрудников.

t_3 – время, которое необходимо затратить на анализ СМИБ.

t_4 – время, которое необходимо затратить на подготовку отчетной документации о проведении аудита СМИБ.

t_{o_i} – время, которое необходимо затратить на проведение аудита o_i объекта проверки.

$C(O)$ – стоимость аудита СМИБ на множестве объектов проверкиO.

c_{o_i} – стоимость на проведение аудита o_i объекта проверки.

Требуется минимизировать временные затраты на проведение аудита при ограниченных материальных затратах организации.

Введем следующий показатель стоимости проведения аудита:

$$C(O) = \sum_{i=1}^{n} c_i = \sum_{i=1}^{n} t_{o_i} \cdot \rho \quad (1)$$

Где ρ – затраты (человек/часы) на проведение аудита. Время, которое необходимо затратить организации на проведение аудита СМИБ, складывается из времени проведения аудита i-ого объекта проверки.

$$T(O) = \sum_{i=1}^{n} t_{o_i} \quad (2)$$

Время на i-ый объект оценки в свою очередь состоит из суммы:

$$t_{o_i} = t_1 + t_2 + t_3 + t_4 \quad (3)$$

В результате получаем, что необходимо свести к минимуму время, требуемое для проведения аудита при заданном уровне стоимости ($C_{зад}$):

$$\begin{cases} T(O) = \sum_{i=1}^{n} t_{o_i} \rightarrow min_{\{\text{средства автом}\}} \\ \sum_{i=1}^{m} c_{o_i} \leq C_{зад} \end{cases} \quad (4)$$

Список литературы

1. Акулов О.А., Баданин Д.Н., Жук Е.И., Медведев Н.В., Квасов П.М., Троицкий И.И. Основы информационной безопасности: учеб. пособие. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. 161 с.
2. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1(2). С.67-73.
3. Лившиц И.И. Оценка систем менеджмента информационной безопасности // Менеджмент качества. 2013. № 1. С. 22-34.
4. Шахалов И.Ю., Дорофеев А.В. Основы управления информационной безопасностью современной организации // Правовая информатика. 2013. № 3. С. 4-14.