УДК 681.3:004.9

И. В. Найханова

АУДИТ СИСТЕМ МЕНЕДЖМЕНТА КАЧЕСТВА И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассмотрены вопросы аудита систем менеджмента информационной безопасности. Проанализированы современные стандарты в области менеджмента информационной безопасности.

Email: i.naykhanova@cnpo.ru

Ключевые слова: информационная безопасность, системы менедж–мента информационной безопасности.

Сегодня проведение аудита систем управления информационной безопасностью (ИБ) является необходимым и востребованным мероприятием [1–3]. Ряд организаций, бизнес которых тесно связан с использованием информационных технологий, например банки, нефтяные, газовые, энергетические и телекоммуникационные компании, в последнее время стали активнее практиковать проведение аудита систем управления информационной безопасностью (СУИБ).

Аудит СУИБ может быть инициирован руководством компании (внутренний аудит СУИБ), ее контрагентами (например, аудит системы ИБ может быть требованием клиента или пунктом в контракте), а также третьей стороной — контролирующими органами и пр. (аудиты, проводимые независимыми органами сертификации).

Сертификация СУИБ позволяет получить обоснованные гарантии того, что в проверяемой организации создана, внедрена и функционирует система управления информационной безопасностью, отвечающая требованиям стандартов. Сертификация СУИБ гарантирует, что в организации проведена оценка рисков, определен и внедрен комплекс средств управления этими рисками, осуществляется мониторинг и анализ функционирования СУИБ, ее сопровождение и совершенствование, выполнены основные требования, предъявляемые к документации на СУИБ, и т. д. Кроме того, сертификация подтверждает, что руководство организации продемонстрировало поддержку процессов и усилий, связанных с планированием, внедрением, эксплуатацией, контролем, сопровождением и модернизацией СУИБ в соответствии с требованиями стандартов [4].

Количество сертифицированных предприятий постоянно растет. Это объясняется в том числе и тем, что статус стандарта BS 7799 вырос до уровня международного стандарта ISO 27001.

Отметим, что анализ защищенности современных организаций от угроз информационной безопасности — работа сложная, многоплановая и трудоемкая. Нужно выбрать действительно необходимые для компании защитные меры, включающие не только специализированный инструментарий, но и комплекс нормативно-распорядительных документов.

Согласно российским стандартам — ГОСТ 17799–2005 и ГОСТ 27001–2006, СУИБ трактуется как часть общей системы управления, основанной на оценке бизнес-рисков и предназначенной для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ. С этой точки зрения представляет интерес провести сравнительный анализ ГОСТ Р ИСО 9001 и ГОСТ 17799–2005 и 27001–2006.

Сравнительный анализ. ГОСТ 17799–2005 и 27001–2006 совместимы со стандартом ГОСТ Р ИСО 9001. Если в организации уже внедрены системы менеджмента в соответствии со стандартом ГОСТ Р ИСО 9001, то обеспечить выполнение требований стандартов 17799–2005 и 27001–2006 в рамках существующих систем менеджмента значительно легче.

Рассмотрим аспекты, которые подтверждают данное утверждение.

ГОСТ 17799–2005 и 27001–2006, как и ГОСТ Р ИСО 9001, содействуют утверждению процессного подхода. Каждый стандарт имеет свою модель взаимосвязи процессов. На рис. 1 и 2 приведены модели, соответствующие ГОСТ Р ИСО 9001 и ГОСТ 27001–2006.

Рис. 1. Модель системы менеджмента качества, основанной на процессном подходе (ГОСТ Р ИСО 9001)

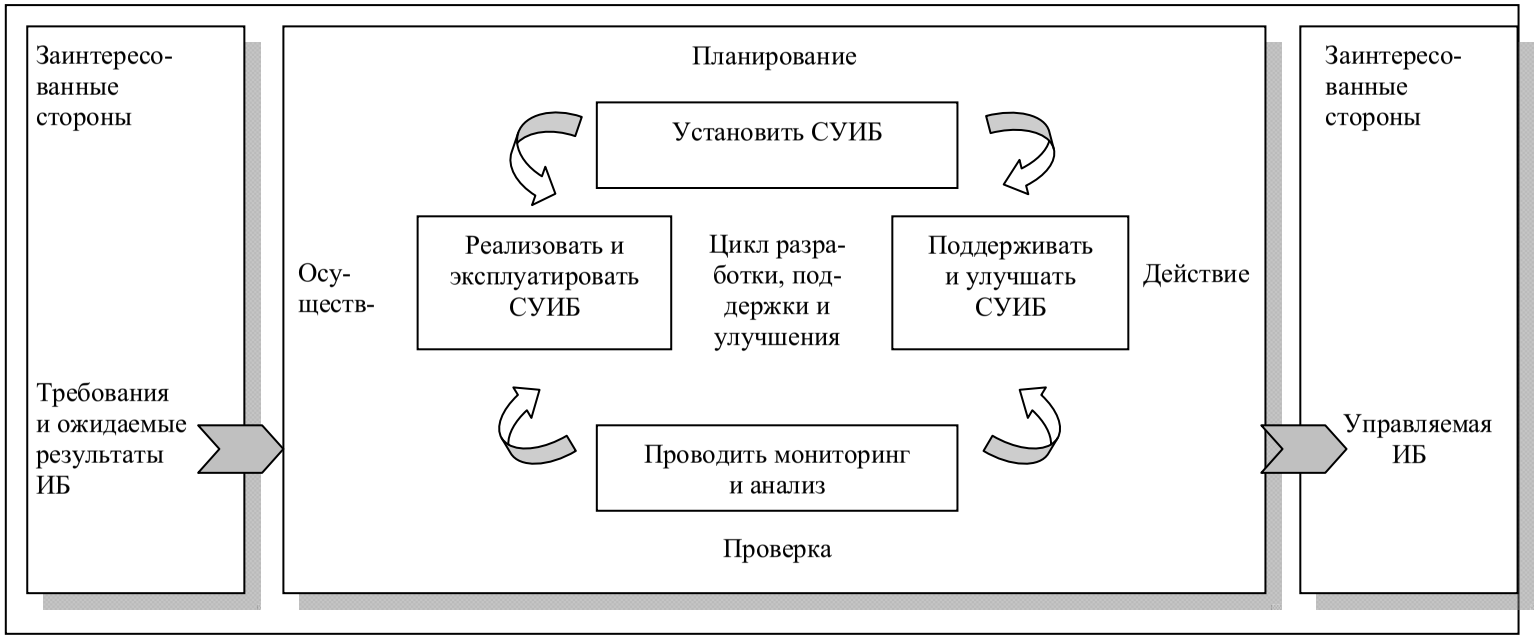

Рис. 2. Применение модели ПРПД к процессам СУИБ (ГОСТ 27001–2006)

Приведенная на рис. 1 модель системы качества (ГОСТ Р ИСО 9001), основанная на процессном подходе, иллюстрирует связи между процессами и показывает, что потребители играют существенную роль при определении входных данных. Мониторинг удовлетворенности потребителей требует оценки информации и восприятия потребителями выполнения их требований. Эта модель охватывает основные требования, не детализируя их. Кроме того, она может быть применена ко всем процессам цикла PDCA (plan — do — check — act), который кратко описывается следующим образом:

1) *планирование* (plan) — разработка цели и процессов, необходимых для достижения результатов в соответствии с требованиями потребителей и политикой организации;

2) *осуществление* (do) — внедрение процессов;

3) *проверка* (check) — постоянный контроль и измерение процессов и продукции в сравнении с политикой, целями и требованиями на продукцию, сообщение о результатах;

4) *действие* (act) — действия по улучшению показателей процессов.

В стандарте ГОСТ 27001–2006 принята модель планирование — реализация — проверка — действие (ПРПД), которая применяется для структурирования всех процессов СУИБ. Ясно, что эта модель вполне соответствует модели PDCA согласно ГОСТ Р ИСО 9001. В данном случае термин «осуществление» и термин «реализация» можно считать синонимами. Отметим также, что в ГОСТ 27001–2006 и ГОСТ 17799–2005 термин «заинтересованные стороны» понимается несколько шире, так как кроме потребителей в заинтересованные стороны могут входить, например, контролирующие органы.

Таким образом, в принципе существует возможность провести аудит СУИБ и на основе ГОСТ Р ИСО 9001. Однако это будет намного сложнее, так как в отличие от этого стандарта в ГОСТ 27001–2006 и ГОСТ 17799–2005 подробно описаны требования именно к СУИБ.

СУИБ получает в качестве входных данных требования информационной безопасности и ожидаемые результаты заинтересованных сторон и за счет применения необходимых мер и процессов генерирует правила информационной безопасности, которые отвечают этим требованиям и ожиданиям (рис. 2).

Модель ПРПД отражает принципы, установленные в руководстве OECD (2002) по управлению информационной безопасностью информационных систем и сетей. Этот стандарт описывает четкую модель для реализации определяемых им принципов оценки рисков, проектирования и внедрения механизмов безопасности, управления безопасностью и ее переоценки.

По сути, ГОСТ 17799–2005 является практическим руководством по созданию системы обеспечения ИБ организации и определяет 133

регулятора ИБ (меры, средства, механизмы, контрмеры), сгруппированные по 11 разделам. Стандарт может стать основой для разработки, например, корпоративной политики безопасности или торгового соглашения между компаниями. Поскольку он носит сугубо рекомендательный характер, экспертиза организаций по нему не предусматривается. Сертификация систем менеджмента качества и информационной безопасности проводится на соответствие ГОСТ 27001–2006, который определяет комплекс требований (вытекающих из ГОСТ 17799–2005) и формирует спецификации для создания, внедрения, эксплуатации, мониторинга, пересмотра, сопровождения и совершенствования этих систем. Наличие сертификации, согласно ГОСТ 27001–2006, позволяет наглядно показать деловым партнерам, инвесторам и клиентам, что в компании налажено эффективное управление ИБ, а это, в свою очередь, способствует росту капитализации компании.

Сам факт выполнения компанией требований ГОСТ 17799–2005 и ГОСТ 27001–2006 обеспечивает ей серьезное конкурентное преимущество на цивилизованном рынке. Сертификация системы управления ИБ – один из этапов сертификации качества всей системы менеджмента качества организации, при этом управление информационной безопасностью, несомненно, является одной из важнейших задач менеджмента. Осуществляя, например, сертификацию продуктов в соответствии с ГОСТ 15408–2002 и сертификацию системы управления ИБ, российские предприятия смогут сделать серьезную заявку на участие в безопасном глобальном информационном пространстве.

Недостаток отечественной нормативной базы ИБ состоит в отсутствии российского стандарта по рискам, так как имеется ГОСТ 27001–2006, в котором заданы требования к СУИБ, и ГОСТ 17799–2005, где имеются примеры по среде и системам ИБ, но, к сожалению, нет руководства по оценке и управлению рисками. Тем не менее аудит систем информационной безопасности лучше проводить в соответствии с ГОСТ 17799–2005 и ГОСТ 27001–2006.

СПИСОК ЛИТЕРАТУРЫ

1. Медведев Н. В., Квасов П. М., Цирлов В. Л. Стандарты и политика информационной безопасности автоматизированных систем // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2010. № 1. – С. 103–111.
2. Марков А. С., Миронов С. В., Цирлов В. Л. Разработка политики безопасности организации в свете новейшей нормативной базы // Защита информации. Конфидент. 2004. № 2. – С. 20–28.
3. Марков А. С., Цирлов В. Л. Управление рисками — нормативный вакуум информационной безопасности // Открытые системы. СУБД. 2007. № 8. – С. 63–67.
4. О внедрении ГОСТ ИСО/МЭК 17799 и 27001 / А.С. Марков и др. // Информационная безопасность. 2006. № 3/4.

Статья поступила в редакцию 19.10.2011