ренние и внешние расходы (реклама, дешевый офис и т.п.), некоторые виды деятельности, производят временную заморозку инвестиционных проектов, пересматривают должностные обязательства, сокращают рабочее время, экономят на закупке и доставке сырья и т.д.

На начало 2009 года центр аналитических исследований «Анкор» провел экспресс-исследование с целью изучить реакцию компаний на экономический кризис. По данным опроса, 51% компаний пересмотрели должностные обязанности работников, 48% изменили организационную структуру с точки зрения оптимизации, 38% заморозили свои инвестиционные проекты, 35% сократили некоторые виды деятельности, 59% сократили свои внутренние расходы не связанные с персоналом.

В этих условиях следует вести контроль принятых мер, чтобы они эффективно исполнялись, и не наносили вред, как предприятию, так и его конкурентоспособности на рынке.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. http://biz.liga.net/articles/EA090027.html

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Ганиева Э.Ш., студентка, гр. УА-401, НАПКС
Научный руководитель: Фролов В.И., к.э.н., доцент

В настоящее время информация является одним из самых ценных ресурсов в любой компании, организации, предприятии, а для некоторых — и основным производственным ресурсом, ведь от сохранности информации и бесперебойного доступа к ней нередко зависят важные технологические и бизнес-процессы. Информационные технологии оказывают существенное влияние на производственные процессы предприятий.

Для того чтобы оценить реальное состояние защищенности ресурсов ИС и ее способность противостоять внешним и внутренним угрозам безопасности, необходимо регулярно проводить аудит информационной безопасности.

Целью данной статьи является рассмотрение тонкостей аудита, выявление задач, которые достигаются в процессе аудита информационной безопасности предприятия, а также выявление проблем и перспектив аудита.

По поводу аудита информационных систем в мире накоплен колоссальный опыт. Он обобщен известной организаций ISACA (Information Systems and Control Associations, www.isaca.org) и сформирован в виде соответствующих нормативов и методик под общим названием COBIT (Control Objectives for Information and related Technologies — Задачи управления для информационных и связанных с ними технологий).

Собственно же аудит заключается в:

1) изучении текущего состояния и планов развития информационных технологий на конкретном предприятии;

2) сравнении результатов с тем, как должны работать информационные системы в идеальном (оптимальном) состоянии (то есть с соответствующими стандартами в данной области);

3) выработке рекомендаций для данного предприятия — что необходимо сделать, чтобы максимально приблизиться к указанным стандартам.

В число задач, которые решаются в ходе проведения аудита информационной безопасности входят:

- сбор и анализ исходных данных об организационной и функциональной структуре ИТС организации, необходимых для оценки состояния информационной безопасности;
- анализ существующей политики обеспечения информационной безопасности на предмет полноты и эффективности;
- анализ информационных и технологических рисков связанных с осуществлением угроз информационной безопасности;
- осуществление тестовых попыток несанкционированного доступа к критически важным узлам ИС и определение уязвимости в установках защиты данных узлов;
- формирование рекомендаций по разработке (или доработке) политики обеспечения информационной безопасности на основании анализа существующего режима информационной безопасности;
- формирование предложений по использованию существующих и установке дополнительных средств защиты информации для повышения уровня надежности и безопасности ИС организации [3].

Казалось бы, все просто — начать и закончить, но на пути постоянно возникают сложности. Первая и самая главная — стоимость работ. Действительно, трудно предположить, что будет дешевой работа группы высокопрофессиональных ИТ-специалистов, которые проведут:

- анкетирование специалистов по отдельным направлениям;
- интервью с ключевыми работниками;

• изучение имеющейся нормативной документации, организационной структуры, принципов управления ИТ;
• выборочное или массовое тестирование аппаратного обеспечения, производительности сети;
• анализ накопленной информации;
• выработку соответствующих экспертных оценок и рекомендаций;
• подготовку развернутого отчета по результатам работ.

Соответственно, когда руководство предприятия-заказчика плохо представляет себе конкретные результаты работ, платить значительные суммы никто не захочет. Дополнительный негатив вносят специалисты по аудиту, которые формируют отчет в виде типового рапорта, слепо следуя имеющимся методикам. Например:
• нет классификации данных — необходимо произвести классификацию данных;
• отсутствует политика NN — следует разработать политику NN;
• не произведена оценка рисков — провести оценку рисков.

В рассматриваемой группе предприятий с высокой степенью вероятности будет отсутствовать большинство из требуемых стандартами пунктов. При получении отчета с простой констатацией отсутствия и рекомендациями о том, что необходима дальнейшая работа (без детальной приоритизации, развернутого плана действий, проектов требуемых нормативов, выписок из используемых стандартов и методик), у руководителя организации сложится весьма негативное мнение об аудите. Если окажется, что итоговый отчет представлен в виде двух-трех томов по 500 страниц, основную часть которых занимают рассуждения о преимуществе трехзвенной архитектуры перед файл-сервером и о перспективах развития беспроводных технологий, то, скорее всего, отчет окажется в пыльном шкафу, изученным и использованным процентов на десять [2].

Аудит информационной безопасности можно разделить на два вида:
• экспертный аудит информационной безопасности, в ходе которого выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в процедуре аудита;
• аудит информационной безопасности на соответствие международному стандарту ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», разработанному Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC) на основе британского стандарта BS 7799-2:2002 «Системы управления информационной безопасностью. Спецификация и руководство по применению».

Цель проведения экспертного аудита информационной безопасности — оценка состояния безопасности ИС и разработка рекомендаций по применению комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных и других ресурсов ИС от угроз информационной безопасности.

Экспертный аудит информационной безопасности позволяет принять обоснованные решения по использованию мер защиты, необходимых для отдельно взятой организации, оптимальных в соотношении их стоимости и возможности осуществления угроз нарушения информационной безопасности.

Аудит информационной безопасности на соответствие международному стандарту ISO/IEC 27001:2005 представляет собой перечень требований к системе менеджмента информационной безопасности (СМИБ), обязательных для сертификации. Стандарт устанавливает требования к разработке, внедрению, функционированию, мониторингу, анализу, поддержке и совершенствованию документированной СМИБ в контексте существующих бизнес-рисков организации [4].

Аудит включает в себя следующие последовательные этапы выполнения работ:

1 этап. Подготовка договорной и исходно-разрешительной документации. На данном этапе создается рабочая группа, куда входят представители заказчика и аудитора, назначаются ответственные лица за выполнение аудита ИС с обеих сторон. Определяются системные границы проведения аудита. Отмечаются проблемные ситуации (известные аппаратные и программные сбои, автоматизированные функции, эффективность выполнения которых недостаточна и т.д.).

2 этап. Сбор исходных данных. Осуществляется сбор информации о текущем состоянии информационных технологий. Методы получения данной информации, раскрывающей все нюансы функционирования ИС, включают анкетирование и интервьюирование по заданным направлениям, сбор необходимых сведений о программном и аппаратном обеспечении.

3 этап. Анализ информации. На данном этапе осуществляется процесс анализа информации. Кроме того, в случае если данные оказываются недостоверными или устаревшими, производится уточнение исходных данных. Таким образом, осуществляется итерационный процесс, включающий следующие шаги: сбор информации, анализ информации, уточнение информации и повтор анализа информации.

4 этап. Выработка рекомендаций. На основе результатов проведенного анализа, вырабатываются рекомендации (основные — для высшего руководства, детальные — для среднего звена) с указанием ожидаемого эффекта, сопутствующих рисков и ориентировочного бюджета. После предварительного согласования с Заказчиком рекомендации проверяются на выполнимость и актуальность с учетом рисков внедрения.

5 этап. Контроль выполнения рекомендаций. На данном этапе осуществляется контроль над проектной организацией, реализующей рекомендации [5].

В качестве объекта аудита может выступать как ИС организации в целом, так и ее отдельные сегменты, обеспечивающие обработку информации, которая подлежит защите.

Аудит может проводиться как силами штатного персонала (внутренний аудит), так и путем привлечения независимых специалистов (внешний аудит). Использование внешнего аудита имеет следующие преимущества:

- представляет собой независимое исследование, что повышает степень объективности результатов;
- проводится силами специалистов, не связанных ранее с предприятием-заказчиком и поэтому имеющих свежий взгляд на все имеющиеся проблемы, что автоматически повышает достоверность результатов.

Привлечение собственных специалистов отвлекает их от основной деятельности. Это сказывается как на качестве их текущей работы, так и на качестве результатов аудита.

Использование внешнего аудита позволяет не отвлекать имеющихся специалистов компании от текущих работ и не снижать на время аудита степень обработки запросов сотрудников компании;

Использование отработанных методик позволит провести аудит и быстрее и качественнее, что в свою очередь позволит сократить затраты на аудит и позволит быстрее повысить уровень защищенности ИТ-инфраструктуры по сравнению с внутренним аудитом;

Проведение аудита требует наличия специалистов высокой квалификации, имеющих не только опыт работы с самым разнообразным программным и аппаратным обеспечением, но и опыт проведения аудита.

Результатом аудита является создание пакета документов, содержащего детализированные данные о состоянии сети и ряд рекомендаций по улучшению качества работы, повышения надежности, производительности, защищенности и эффективности предоставления услуг. Содержание предоставляемой документации в значительной степени зависит от пожеланий заказчика, имеющейся ИТ-инфраструктуры и также организационной структуры компании-заказчика.

Аналитический отчет является основным отчетным документом об аудите. Его назначение и структура согласуются одновременно с определением целей аудита [6].

В условиях растущих темпов бизнеса становятся все более необходимыми проведение высокоуровневого аудита информационных систем, методов и средств безопасности, построение моделей оценки рисков. Следует ожидать постепенного слияния аудита с процессом сопровождения системы и переход к аудиту на постоянной основе. Высокоуровневый аудит становится командным видом «спорта», в основе которого — гармоничные конструктивные взаимоотношения между всеми заинтересованными сторонами [5; 6].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. http://www.itshop.com.ua.
2. http://www.am-soft.ua/site.php/page5068.html
3. http://www.it.techexpert.ua/consult/audit
4. http://www.it.techexpert.ua/consult/infoSequrity/auditonISO
5. http://www.leta.ru/audit_is
6. http://www.alatus.ru

НАЛОГ С ДОХОДОВ ФИЗИЧЕСКИХ ЛИЦ В ЗАРУБЕЖНЫХ СТРАНАХ

Горишняя Д.В., студентка, гр. ФИН-401, НАПКС
Научный руководитель: Сушкова Е.Е., ассистент

Центральное место в системе налогообложения принадлежит налогу на доходы физических лиц, который регулируется Законом Украины «О налоге с доходов физических лиц» №889-IV от 22.05.2003 г. Как и любой другой налог, подоходный налог является одним из экономических рычагов государства, с помощью которого оно пытается решить различные разнонаправленные задачи: 1) обеспечения достаточных денежных поступлений в бюджеты всех уровней; 2) регулирование уровня доходов населения и соответственно структуры личного потребления и сбережений граждан; 3) стимулирование наиболее рационального использования получаемых доходов; 4) помощь наименее защищенным категориям населения.

Подоходное налогообложение обладает большими возможностями воздействия на уровень реальных доходов населения, позволяет с помощью системы льгот, выбора объекта и ставок налогообложения стимулировать стабильные доходы бюджета за счет повышения ставок налога по мере роста заработков граждан.

Цели взимания и основные черты подоходного налога в Украине во многом схожи с принятыми во многих промышленно развитых странах аналогичными налогами. Его место в налоговой системе определяется следующими факторами: