А. П. Курило,
Банк России,
А. И. Толстой (к. т. н., доцент),
Московский инженерно-физический институт (государственный университет)

ПОВЫШЕНИЕ КВАЛИФИКАЦИИ СПЕЦИАЛИСТОВ БАНКА РОССИИ В ПОДДЕРЖКУ ВНЕДРЕНИЯ КОМПЛЕКСА СТАНДАРТОВ БАНКА РОССИИ «ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Введение

Развитие и укрепление банковской системы (БС) РФ, а также обеспечение эффективного и бесперебойного функционирования платежной системы РФ является целями деятельности Банка России. Одним из условий для достижения этих целей является обеспечение необходимого и достаточного уровня информационной безопасности (ИБ) каждой организации БС РФ, в том числе ИБ Банка России.

Требуемый уровень ИБ может быть достигнут только на основе комплексного подхода, предполагающего планомерное использование правовых, организационных, программно-аппаратных и других мер обеспечения ИБ на единой концептуальной и методической основе. Именно поэтому с 2001 года в Банке России были развернуты работы по разработке Комплекса стандартов, направленных на создание такой концептуальной и методической базы.

Основополагающим стандартом Комплекса стандартов стал стандарт Банка России «Обеспечение ИБ организаций БС РФ. Общие положения», который был введен в действие в декабре 2004 года. Начавшийся с этого момента начался процесс внедрения стандарта в Банке России состоял из многих этапов. В 2004 году начинается работа над подготовкой Политики безопасности Банка России, которая впитала в себя многие положения этого стандарта. Параллельно была проведена работа по апробации стандарта в одном из структурных подразделений Банка России. В 2005 году проведена апробация стандарта в опытной зоне внедрения, состоящей из 12 структурных подразделений Банка России. В 2007 году по результатам апробации вводится в действие вторая редакции стандарта, а также документ «Основные направления политики ИБ Банка России». В 2007 году разрабатываются и утверждаются модели угроз и нарушителей, отражающие требования стандарта, а также вводятся в действия два новых стандарта и два руководства по стандартизации, посвященные аудиту ИБ, методике оценки соответствия требованиям стандарта, методике самооценки ИБ и требованиям к документации по обеспечению ИБ.

Таким образом, в настоящее время комплекс стандартов по ИБ образован следующими нормативными документами:

1) стандарт Банка России СТО БР ИББС 1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»;

2) стандарт Банка России СТО БР ИББС-1.1 «Обеспечение ИБ организаций БС РФ. Аудит ИБ»;

3) стандарт Банка России СТО БР ИББС-1.2 «Методика оценки соответствия ИБ организаций БС РФ требованиям СТО БР ИББС–1.0»;

4) рекомендации в области стандартизации Банка России РС БР ИББС-2.0 «Методические рекомендации по документации в области обеспечения ИБ в соответствии с требованиями СТО БР ИББС-1.0»;

5) рекомендации в области стандартизации Банка России РС БР ИББС-2.1 «Руководство по самооценке соответствия ИБ организаций БС РФ требованиям СТО БР ИББС–1.0».

На 2008 г. планируется внедрение новой редакции стандарта СТО БР ИББС-1.0, коррекция стандарта СТО БР ИББС-1.2 и разработка двух рекомендаций, посвященных методике оценки рисков ИБ и методике классификации активов.

Следует отметить, что при внедрении Комплекса стандартов определенную роль играет проведение обучения по программам, отражающим основные положения стандартов и представляющим имеющийся опыт использования стандартов. В данном случае решается две задачи. Во-первых, ознакомление специалистов с существующей нормативной базой и доведение до них информации, необходимой для ее использования при внедрении стандартов. Во-вторых, выполнение ряда требований СТО БР ИББС-1.0, перечисленных ниже.

• Персонал организации должен быть компетентным для выполнения своих функций в области обеспечения ИБ. Компетентность персонала следует обеспечивать с помощью процессов обучения в области ИБ, осведомленности персонала и периодической проверки уровня компетентности (п. 8.2.2.11).

• Процессы менеджмента ИБ организации должны быть «…стандартизованы, документированы и доведены до персонала посредством обучения» (из п. 11.4 при определении уровня зрелости организации).

• Краткие занятия с работниками организации по вопросам обеспечения ИБ, которые должны носить обязательный характер; аттестация персонала по вопросам обеспечения безопасности» (п. 11.6, при определении требований, которые должны выполняться для четвертого — рекомендуемого уровня зрелости).

Признавая важность процессов обучения при формировании у персонала Банка России необходимого уровня осознания ИБ, а также учитывая необходимость создания требуемых условий для успешного внедрения в Банке России Комплекса стандартов, было принято решение о проведении обучения определенных категорий специалистов подразделений Банка России. Такое обучение было проведено в 2006 и в 2007 годах на базе МИФИ. В данной статье рассматривается опыт, полученный при проведении обучения по программам, отражающим основные положения Комплекса стандартов. Кроме этого определяются перспективы, связанные с повышением эффективности процессов обучения в данном направлении.

1. Проведение обучения в 2006 году

В связи с утверждением второй версии стандарта СТО БР ИББС-1.0 и принятием решения о внедрении этого стандарта во всех территориальных учреждениях Банка России при разработке политик ИБ в 2006 году была поставлена задача проведения обучения: дать слушателям знания, необходимые для практического применения указанного выше стандарта, с целью повышения эффективности мероприятий по обеспечению и поддерживанию необходимого уровня ИБ Банка России и установления единых требований по обеспечению ИБ организаций банковской системы России. Кроме этого были определены категории специалистов, для которых предназначено обучение: руководители высшего и среднего звена подразделений Банка России и специалистов подразделений информатизации и защиты информации, непосредственно участвующие в процессах внедрения стандарта.

МИФИ разработал учебную программу «Вопросы внедрения Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», в состав которой вошли два модуля:

• Модуль СТ6-1: «Основы обеспечения информационной безопасности организаций банковской системы Российской Федерации» (для руководителей, 16 учебных часов);

• Модуль СТ6-2: «Обеспечение информационной безопасности подразделений Банка России» (для специалистов, 24 учебных часа).

Содержание программы прошло согласование в Главном управлении безопасности и защиты информации (ГУБЗИ) Банка России. Модули СТ6-1 и СТ6-2 имели одинаковый перечень разделов, который приводится ниже.

1. Введение:

1.1. Международный опыт по обеспечению ИБ организаций банковской системы;

1.2. Состояние и перспективы развития отечественной системы обеспечения ИБ в кредитно-финансовой сфере;

1.3. Цели, задачи и общая характеристика стандарта СТО БР ИББС-1.0.

2. Общие вопросы стандартизации:

2.1. Обзор международных стандартов и нормативных документов;

2.2. Обзор отечественных стандартов и нормативных документов;

2.3. Место стандарта СТО БР ИББС-1.0 в общей структуре отечественных стандартов и нормативных документов.

3. Концепция и принципы обеспечения ИБ организаций БС РФ:

3.1. Исходная концептуальная схема (парадигма) обеспечения ИБ организаций;

3.2. Общие принципы безопасного функционирования организаций;

3.3. Специальные принципы обеспечения ИБ организаций.

4. Модели угроз и нарушителей ИБ организаций БС РФ.

5. Политика ИБ организаций БС РФ:

5.1. Состав и назначение политики ИБ;

5.2. Требования по обеспечению ИБ, отображаемые в политиках ИБ организаций.

6. Управление ИБ в организациях БС РФ:

6.1. Общие подходы и модель зрелости процессов управления ИБ организаций;

6.2. Обзор методов аудита и мониторинга ИБ организаций БС РФ.

7. Внедрение и развитие Стандарта:

7.1. Основные подходы по внедрению и развитию Стандарта;

7.2. Специфика внедрения Стандарта в деятельность учреждений Банка России.

Различием явилось наполнение и направленность содержания модулей. При реализации программы учебные занятия проводили преподаватели МИФИ (рассмотрение основных положений стандарта) и специалисты ГУБЗИ Банка России (рассмотрение вопросов, связанных с практическим внедрением стандарта).

Для обеспечения требуемого уровня учебных занятий был подготовлен учебно-методический комплекс, в который вошли:

- учебно-методическое пособие, которое было издано в серии «Учебная книга факультета «Информационная безопасность» МИФИ», выпуск 16;
- презентации для всех учебных занятий;
- контрольные задания для проверки уровня знаний на входе и выходе обучения (комплект из 45 тестов);
- пакет раздаточного материала, который выдавался каждому слушателю.

Контингент специалистов, направленных на обучение, формировало Главное управление безопасности и защиты информации на основе заявок со стороны подразделений Банка России. В табл. 1 представлены количественные данные по контингенту специалистов, прошедших обучение по курсам СТ6-1 и СТ6-2.

Таблица 1.

Подразделения Банка России	Количество человек, прошедших обучение					
	СТ6-1	СТ6-2	Всего-6	СТ7-1	СТ7-2	Всего-7
Территориальные учреждения Банка России (ГУ, НБ)	89	86	175	115	90	206
Учреждения Банка России (Департаменты, Управления, Главные управления, Центры, Хранилища, Инспекции)	30	31	61	34	58	93
ВСЕГО	119	117	236	149	148	297

Анализ этих данных показывает, что обучение прошли представители почти всех территориальных учреждений и части учреждений Банка России. Среди территориальных учреждений, не приславших своих представителей, можно отметить ГУ по Калининградской области, ГУ по Ульяновской области и НБ Республики Саха (Якутия). Кроме того, десять Главных управлений и один Национальный банк направили своих специалистов только на один из курсов (или СТ6-1, или СТ6-2).

Контроль уровня знаний перед обучением и после обучения с использованием контрольных заданий показал результаты, которые проиллюстрированы диаграммами на рис. 1 и рис. 2 для курсов СТ6-1 и СТ6-2 соответственно.

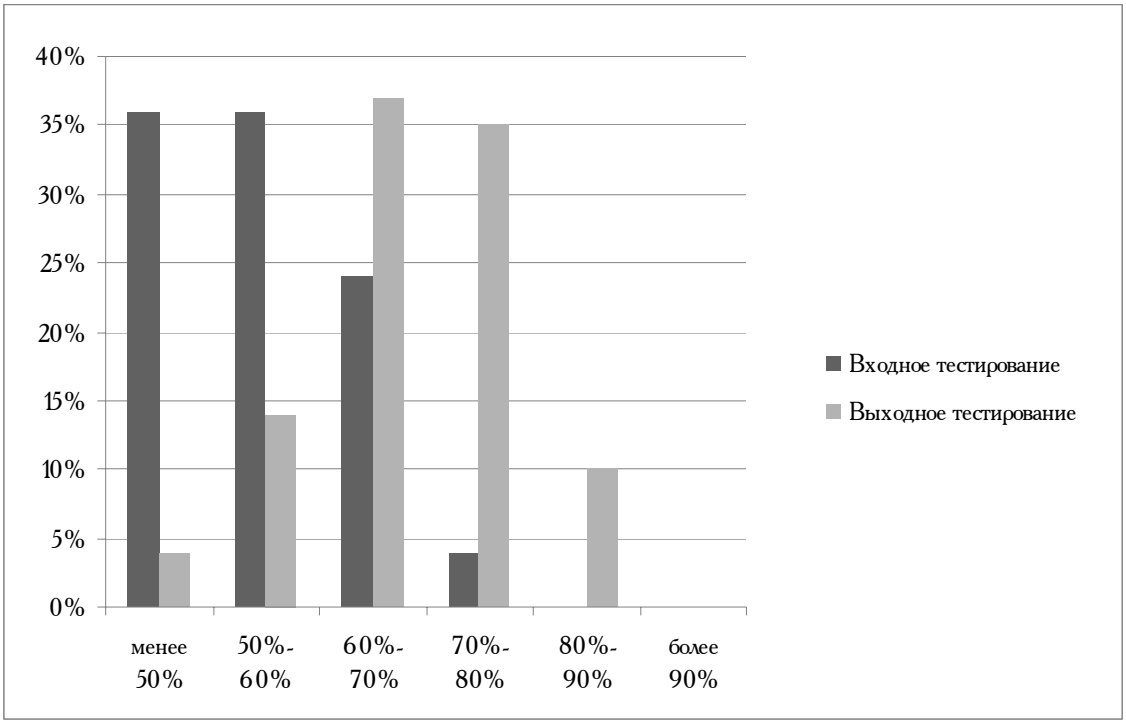

Рис. 1. Результаты контроля уровня знаний по курсу СТ6-1

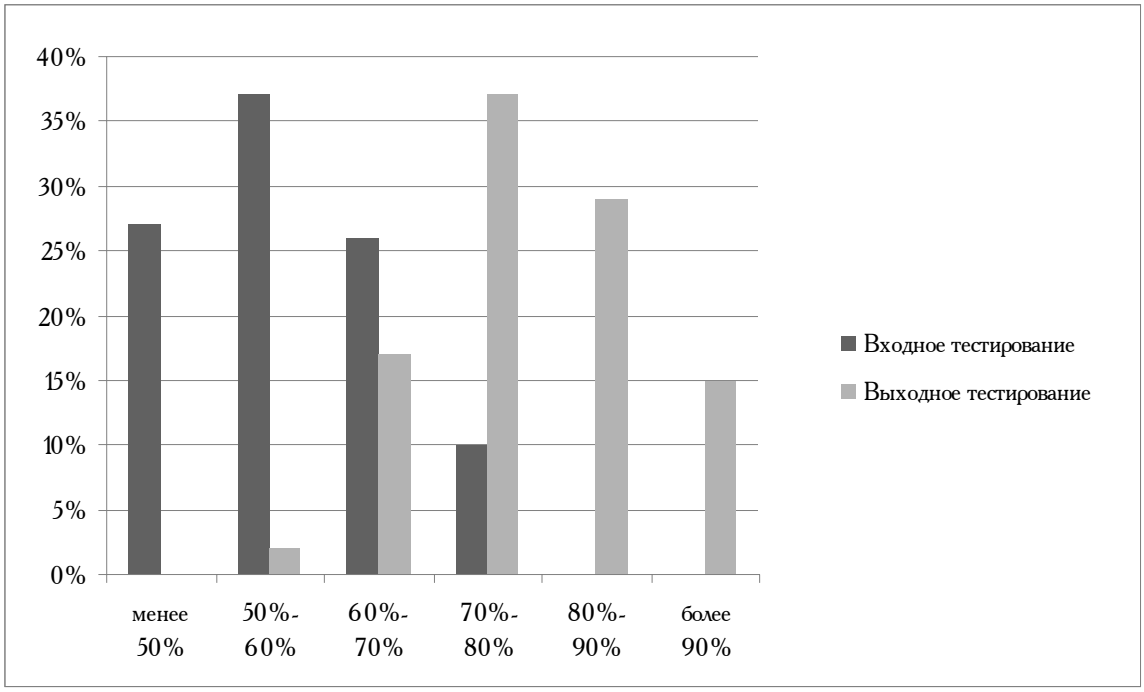

Рис. 2. Результаты контроля уровня знаний по курсу СТ6-2

Следует отметить, что результаты входного контроля оказались ниже у слушателей учебного курса СТ6-1, чем у слушателей учебного курса СТ6-2. Это можно объяснить тем, что параллельное с обучением внедрение стандартов в Территориальных учреждениях являлось побудительным фактором для специалистов, которые включились в процессы внедрения и самостоятельно работали над стандартом до приезда на обучение.

Этот факт частично объясняют и результаты контроля знаний после окончания обучения (Рис. 1 и 2): уровень знаний у специалистов на выходе обучения по курсу СТ6-2 заметно выше, чем по курсу СТ6-1. Был отмечен дополнительный фактор, повлиявший на этот результат: большая активность слушателей курса СТ6-2 во время учебных занятий, что объясняется наличием желания у специалистов получить как можно больше знаний, которые им необходимы при практической работе по внедрению стандарта.

При дополнительном анкетирование, которое проводилось в конце занятий, слушатели формулировали замечания и предложения, которые оперативно учитывались при организации и проведении занятий в последующих группах. Кроме этого у слушателей была возможность в анонимных анкетах оценить полезность учебных занятий, уровень преподавания и уровень организационного обеспечения. Анализ этих оценок показывает, что учебные занятия оказались полезными и были проведены на достаточно высоком уровне.

2. Проведение обучения в 2007 году

В связи с утверждением стандартов СТО БР ИББС-1.1, СТО БР ИББС-1.2, рекомендаций в области стандартизации Банка России РС БР ИББС-2.0, РС БР ИББС-2.1 и принятием решения о внедрении этих нормативных документов во всех территориальных учреждениях Банка России при проведении самооценки в 2007 году была поставлена задача проведения обучения специалистов подразделений Банка России: дать слушателям знания, необходимые для практического применения указанных выше документов. При этом был использован опыт, полученный при проведении учебных занятий в 2006 году в части определения категории специалистов, для которых организовано было обучение (руководители высшего и среднего звена подразделений Банка России и специалисты подразделений информатизации и защиты информации, непосредственно участвующие в процессах внедрения нормативных документов), определения номенклатуры курсов и длительности обучения, использования учебно-методического обеспечения, порядка проведения учебных занятий и контроля знаний.

МИФИ разработал учебную программу «Вопросы внедрения стандартов Банка России по информационной безопасности», в состав которой вошли два модуля:

- Модуль СТ7-1: «Базовые вопросы внедрения стандартов Банка России по информационной безопасности» (для руководителей, 16 учебных часов);
- Модуль СТ7-2: «Специальные вопросы внедрения стандартов Банка России по информационной безопасности» (для специалистов, 24 учебных часа).

Содержание программы прошло согласование в ГУБЗИ Банка России. Модули СТ7-1 и СТ7-2 имели одинаковый перечень разделов:

1. Общие вопросы стандартизации:

1.1. Обзор международных стандартов и нормативных документов;

1.2. Обзор отечественных нормативных документов и стандартов по обеспечению ИБ и применению информационных технологий;

1.3. Комплекс стандартов Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

1.4. Место стандартов Банка России в общей структуре отечественных стандартов и нормативных документов.

2. Документация в области обеспечения ИБ в соответствии с требованиями СТО БР ИББС-1.0»:

2.1. Общая характеристика документа Банка России РС БР ИББС 2.0;

2.2. Структура документов по обеспечению ИБ;

2.3. Состав внутренних документов по обеспечению ИБ (характеристики и примеры документов первого, второго, третьего и четвертого уровней);

2.4. Менеджмент документов по обеспечению ИБ.

3. Основы аудита ИБ:

3.1. Общая характеристика стандарта СТО БР ИББС-1.1;

3.2. Исходная концептуальная схема (парадигма) аудита ИБ организаций БС РФ;

3.3. Основные принципы проведения аудита ИБ организаций БС РФ;

3.4. Особенности менеджмента программы аудита ИБ;

3.5. Проведение аудита ИБ в контексте участия представителей проверяемой организации;

3.6. Проведение самооценки ИБ.

4. Оценка соответствия ИБ организации БС РФ:

4.1. Общая характеристика документа Банка России СТО БР ИББС-1.2;

4.2. Показатели ИБ. Способы оценивания показателей;

4.3. Оценка текущего уровня ИБ организации БС РФ;

4.4. Оценка менеджмента ИБ организации БС РФ;

4.5. Оценка осознания ИБ организации БС РФ;

4.6. Определение уровня соответствия ИБ организаций БС РФ требованиям Стандарта СТО БР ИББС-1.0-2006. Отображение оценок.

5. Самооценка соответствия ИБ организации БС РФ:

5.1. Общая характеристика документа Банка России РС БР ИББС-2.1;

5.2. Проведение самооценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.

6. Особенности внедрения стандартов в организациях БС РФ и в Банке России.

Различием в содержании курсов явилось наполнение и направленность содержания модулей. При реализации программы учебные занятия проводили преподаватели МИФИ (рассмотрение основных положений нормативных документов), специалисты организации, имеющей практический опыт по проведению внешнего аудита ИБ и оценки соответствия ИБ требованиям стандарта СТО БР ИББС-1.0 (ООО «Андэк»), и специалисты ГУБЗИ Банка России (рассмотрение вопросов, связанных с их практическим внедрением). Кроме этого, в программу курса СТ7-2 были включены практические занятия по проведению оценки соответствия, в том числе и с использованием автоматизированных методов (применение ЭВМ и прикладного программного обеспечения).

Для обеспечения требуемого уровня учебных занятий был подготовлен учебно-методический комплекс, в который вошли:

- учебно-методическое пособие, которое было издано в серии «Учебная книга факультета «Информационная безопасность» МИФИ», выпуск 17;
- презентации для всех учебных занятий;
- контрольные задания для проверки уровня знаний на входе и выходе обучения (комплект из 69 тестов);
- пакет раздаточного материала, который выдавался каждому слушателю.

Контингент специалистов, направленных на обучение, формировало Главное управление безопасности и защиты информации на основе заявок со стороны подразделений Банка России. В табл. 1 представлены количественные данные по контингенту специалистов, прошедших обучение по курсам СТ7-1 и СТ7-2.

Анализ этих данных показывает, что обучение прошли представители почти всех территориальных учреждений (не направил на обучение своих специалистов только НБ Карачаево-Черкесской Республики) и большей части учреждений Банка России. Кроме этого одиннадцать Главных управлений и пять Национальных банка направили своих специалистов только на один из курсов (или СТ7-1, или СТ7-2).

Контроль уровня знаний перед обучением и после обучения с использованием контрольных заданий показал результаты, которые проиллюстрированы диаграммами на рис. 3 и рис. 4 для курсов СТ7-1 и СТ7-2 соответственно.

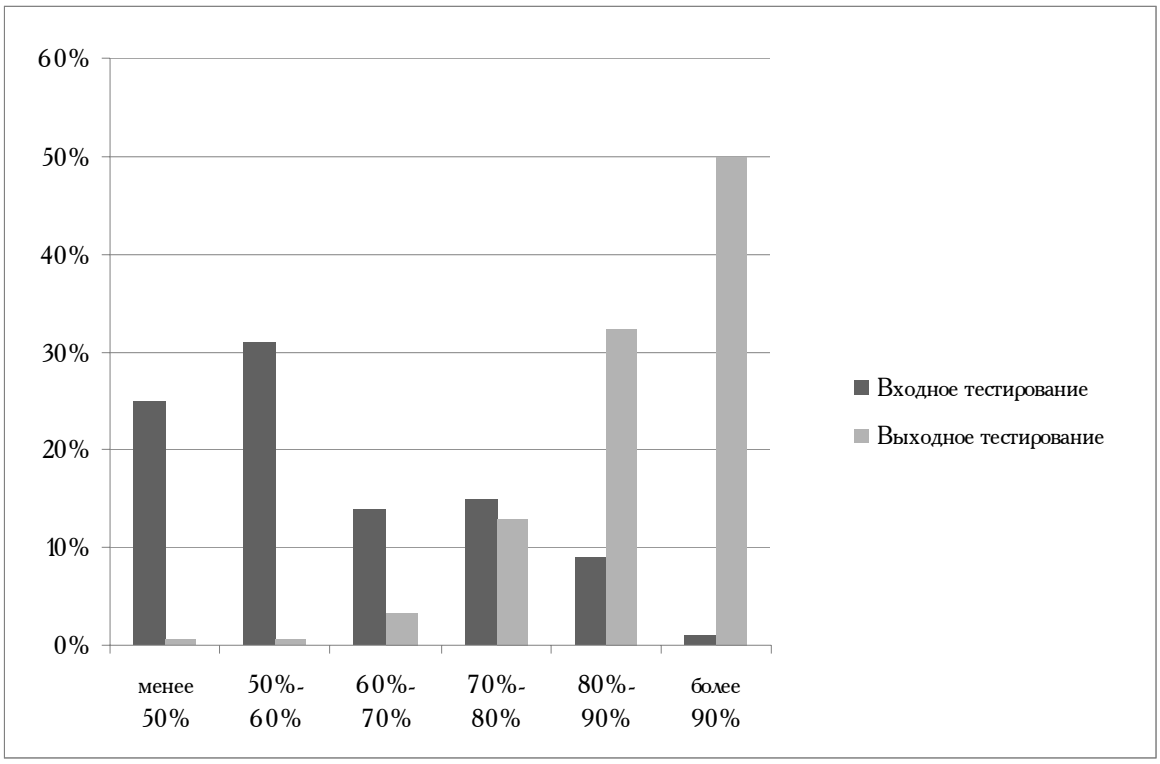

Рис. 3. Результаты контроля уровня знаний по курсу СТ7-1

Следует отметить, что результаты входного контроля уровня знаний у слушателей учебного курса СТ7-1 и у слушателей учебного курса СТ7-2 оказались близкими. Дополнительное анкетирование дало объяснение этого факта: примерно одинаковый процент слушателей по курсам СТ7-1 и СТ7-2 ознакомились с нормативными документами до начала обучения (45% и 42% соответственно).

Уровень знаний, показанный после окончания обучения (рис. 3 и рис. 4) также примерно одинаков для слушателей курсов СТ7-1 и СТ7-2 и достаточно высок. Последний факт говорит об эффективности проведенных учебных занятий.

При проведении учебных занятий было обнаружено не достаточное знание основных положений стандарта СТО БР ИББС-1.0. Поэтому преподаватели были вынуждены выделять определенное время на комментарии к стандарту СТО БР ИББС-1.0. Причину этого факта определило дополнительное анкетирование, которое показало, что большинство слушателей (98%) не проходили обучение в 2006 г.

При дополнительном анкетирование, которое проводилось в конце занятий, слушатели формулировали замечания и предложения, которые оперативно учитывались при организации и проведении занятий в последующих группах. Кроме этого у слушателей была возможность в анонимных анкетах оценить полезность учебных занятий, уровень преподавания и уровень организационного обеспечения. Анализ этих оценок показывает, что учебные занятия оказались полезными и были проведены на достаточно высоком уровне.

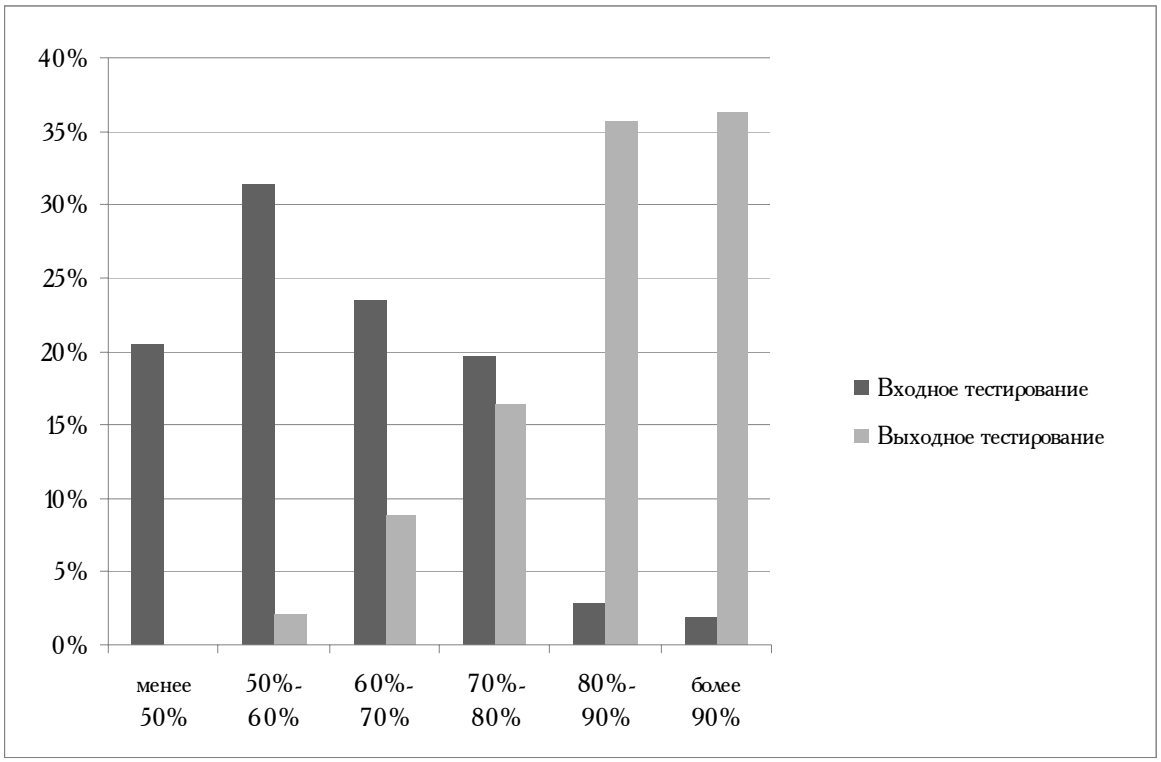

Рис. 4. Результаты контроля уровня знаний по курсу СТ7-1

Кроме реализации учебных программ, непосредственно связанных с внедрение Комплекса стандартов Банка России «Обеспечение ИБ организаций БС РФ», в 2007 г. при проведении учебных занятий по другим программам возникла потребность освещения отдельных положений стандартов.

Например, в цикле учебных программ «Администраторы информационной безопасности» (в 2007 г. прошло обучение 300 специалистов подразделений Банка России) при реализации модулей программы, отражающих вопросы устройства, установки, настройки и администрирования программно-аппаратных комплексов средств защиты информации от несанкционированного доступа семейств «Secret Net» и «Аккорд», были рассмотрены основные положения стандарта СТО БР ИББС-1.0, касающиеся ролей администраторов информационной безопасности и требований по обеспечению информационной безопасности при управлении доступом и регистрации.

Аналогичный подход был реализован в программе «Технология защиты информации от несанкционированного доступа в автоматизированных системах на основе Secret Net 5.0», предназначенной для специалистов подразделений информатизации (в 2007 г. прошло обучение 110 слушателей).

3. Направления развития учебной деятельности, связанные с внедрением Комплекса стандартов Банка России «Обеспечение ИБ организаций БС РФ»

При определении направлений развития учебной деятельности, связанной с внедрением Комплекса стандартов необходимо учитывать:

- опыт, накопленный при проведении обучения в данном направлении;
- тенденции и планы модернизации и расширения самого Комплекса стандартов;
- количественный и качественный состав контингента, для которого необходимо обучение;
- потребности в совершенствовании процессов обучения, направленного на повышение его эффективности.

Основываясь на отзывах, полученных от специалистов, прошедших обучение, можно подтвердить необходимость организации и проведения подобной работы. Основное внимание при этом следует обращать на оптимизации реализации теоретических частей программ (увеличение информативности,

совершенствование структурирования информации, расширение возможностей самостоятельной работы), на расширение практических разделов программ, включая в них рассмотрение практических вопросов, связанных с внедрением Комплекса стандартов, и знакомство с имеющимся опытом внедрения.

Содержание новых учебных программ должно включать комментарии к новым версиям стандартов (которые должны появляться не реже одного раза в два года), а также вопросы, связанные с новыми нормативными документами, включаемыми в Комплекс стандартов (например, готовится стандарт, относящийся к терминам в области ИБ, и будет подготовлен нормативный документ в форме рекомендаций по обеспечению ИБ при назначении и распределении ролей и обеспечении доверия к персоналу).

Контингент специалистов, которым будет рекомендовано пройти обучение по программам, относящимся к внедрению в Банке России Комплекса стандартов, должен определяться с учетом назначения и распределения ролей и уточнения квалификационных характеристик специалистов, участвующих в создании и сопровождении системы обеспечения ИБ и системы менеджмента ИБ.

Повышение эффективности учебной деятельности возможно по пути внедрения современных образовательных технологий, которые позволяют повысить информативность обучения, расширить возможности самостоятельного освоения учебного материала, увеличить эффективность получения практических навыков, совершенствовать процессы контроля знаний с переходом от сертификации знаний к аттестации специалистов и, наконец, оптимизировать затраты времени и средств на обучение.

К таким современным образовательным технологиям относится дистанционное обучение, дистанционное тестирование знаний и совмещение различных форм обучения, например, очного и заочного (дистанционного).

Представляется целесообразным освоение теоретического материала построить на работе слушателей с электронными учебниками без отрыва от основного места работы. Очное обучение сделать кратковременным и связать исключительно с практическими занятиями, направленными на закрепление теоретического материала и получения практических навыков, необходимых для выполнения своих должностных обязанностей, связанных с внедрением Комплекса стандартов. При этом особую роль должны играть формы контроля знаний, которые могут быть использованы на этапе подтверждения освоения теоретического материала, перед началом очного обучения и на этапе завершения этого обучения.

В настоящее время имеющийся в МИФИ опыт разработки электронных учебников и их использования при обучении и контроле знаний, а также наличие технологической базы дистанционного обучения и тестирования позволяет уже в 2008 г. перейти на новые формы обучения. Это даст возможность оперативно изменять содержание обучения и обеспечит необходимый уровень поддержки процессов внедрения в Банке России Комплекса стандартов, связанных с обеспечением ИБ.