УДК: 004.056

АВТОМАТИЗАЦИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ ОСНОВАННОГО НА СТАНДАРТАХ БАНКА РОССИИ

И. А. Будовских, Ю. Н. Загинайлов, Л. Д. Алферова

Алтайский государственный технический университет им. И.И. Ползунова, г. Барнаул

Статья посвящена обзору разработанного программного обеспечения, которое позволяет автоматизировать процесс проведения аудита информационной безопасности кредитных организаций на соответствие требований стандартов Банка России.

Ключевые слова: аудит информационной безопасности, защита информации, кредитные организации, стандарты Банка России.

Аудит информационной безопасности является одной из обязательных и стандартизированных процедур обеспечения информационной безопасности организации [1].

Для кредитных организаций в России разработан комплексе стандартов Банка России по обеспечению ИБ банковской системы РФ [2] (комплекс носит рекомендательный характер):

СТО БР ИББС – 1.0 – 2014. «Обеспечение ИБ организаций банковской системы РФ. Общие положения (5 редакция)».

СТО БР ИББС – 1.1 – 2007. «Аудит информационной безопасности».

СТО БР ИББС 1.2 – 2014. «Методика оценки соответствия ИБ организаций банковской системы РФ требованиям СТО БР ИББС – 1.0 - 2014».

Процесс аудита ИБ кредитных организаций включает три направления оценки, в рамках которых необходимо оценить около 500 частных показателей, в связи с чем, методика аудита является трудоёмкой и требует больших временных затрат. Для решения этой проблемы разработаны специализированные программные комплексы, однако введение в 2014 году новых стандартов ИББС, в том числе и методики аудита, делает эти комплексы сложно применимыми, что обусловливает актуальность разработки современных средств автоматизации.

Для обеспечения автоматизации аудита ИБ кредитных организаций была решена задача формализации процесса оценки ИБ основанного на методике СТО БР ИББС 1.2., сформирован алгоритм и разработано программное обеспечение «Аудит кредитных организаций».

Методика СТО БР ИББС 1.2 – 2014 учитывает специфику кредитных организаций РФ и позволяет объективно оценить следующие направления оценки: текущий уровень ИБ (10 групп – 250 частных показателей), менеджмент ИБ (17 групп – 160 частных показателей) и уровень осознания ИБ руководством организации (7 групп – 81 частный показатель)[4]. Итого: 3 направления, 34 группы, 491 частный показатель.

После определения уровня соответствия трех направлений, рассчитывается итоговый уровень R по формуле:

$$R = \min(EV1, EV2, EV3), \quad (1)$$

где EV1 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению «текущий уровень ИБ организации»;

EV2 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению «менеджмент ИБ организации»;

EV3 — оценка степени выполнения требований СТО БР ИББС-1.0 по направлению «уровень осознания ИБ организации».

Для оценки каждого направления нужно ответить на вопросы. Один вопрос – один частный показатель Mij. Частные показатели делятся на две группы: обязательные и рекомендуемые.

Обязательным показателям могут быть присвоены следующие значения:

1. «нет» - 0;
2. «частично» - 0.25, 0.5, 0.75;
3. «да» - 1;

4. «н/о» - нет оценки (вопрос не относится к деятельности организации).

Рекомендуемые показатели могут быть присвоены значения:

1. «нет» - 0;
2. «да» - 1;
3. «н/о» - нет оценки.

Частные показатели разбиты по группам. Всего 34 группы.

Оценка группового показателя EVmi вычисляется из оценок входящих в него частных показателей EVmij по формуле:

$$EVmi = \frac{\sum_j EV_{m_{ij}}}{j}, \quad (2)$$

где EVmi – групповой показатель;

EVm_{ij} – частный показатель i–ой группы.

Если в рамках группового показателя все входящие в него частные показатели определены как неоцениваемые, указанный групповой показатель также определяется как неоцениваемый и не учитывается в формировании дальнейших результатов оценки.

Текущий уровень ИБ организации вычисляется по формуле:

$$EV_1 = \min (EV_{БИТП}, EV_{БПТП}, EV^2_{ОЗПД}, EV_{ООПД}), \quad (3)$$

где $EV_{БИТП}$ — степень выполнения требований банковского информационного технологического процесса, которая рассчитывается по формуле:

$$EV_{БИТП} = k^1_{БИТП}\frac{\sum_j EV_{m_i}+EV_{m_8}}{7}, \; i = 1\div6. \quad (4)$$

$EV_{БПТП}$ — степень выполнения требований банковского платежного технологического процесса, которая рассчитывается по формуле:

$$EV_{БПТП} = k^1_{БПТП}\frac{\sum_j EV_{m_i}+EV_{m_7}}{7}, \; i = 1\div6. \quad (5)$$

$EV^2_{ОЗПД}$ — степень выполнения требований регламентирующих защиту ПД в ИСПД, с учетом оценки степени выполнения требований по обеспечению ИБ при использовании СКЗИ, которая рассчитывается по формуле:

$$EV^2_{ОЗПД} = k^1_{ОЗПД2}\frac{\sum_j EV_{m_i}+EV_{m_8}+EV_{m_{10}}}{8}, \; i = 1\div6. \quad (6)$$

$EV_{ООПД}$ — степень выполнения требований регламентирующих обработку ПД, которая рассчитывается по формуле:

$$EV_{ООПД} = k^1_{ООПД} * EVm_9 \quad (7)$$

Корректирующие коэффициенты $k^1_{БПТП}$, $k^1_{БИТП}$, $k^1_{ОЗПД2}$ и $k^1_{ООПД}$ определяются в соответствии с таблицей1.

Таблица 1 – корректирующие коэффициенты

Корректирующий коэффициент	Количество частных показателей, оценки которых равны нулю		
$k^1_{БПТП}$	0	1 – 20	Более 20
$k^1_{БИТП}$	0	1 – 20	Более 20
$k^1_{ОЗПД1}$	0	1 – 20	Более 20
$k^1_{ОЗПД2}$	0	1 – 20	Более 20
$k^1_{ООПД}$	0	1 – 8	Более 8
k_2	0	1 – 25	Более 25
k_3	0	1 – 10	Более 10
Значение корректирующего коэффициента	1	0,85	0,7

Оценка менеджмента ИБ рассчитывается по формуле:

$$EV_2 = k_2\frac{\sum_{i=11}^{27} EV_{m_i}}{17} \quad (8)$$

где EV2 – уровень менеджмента ИБ;

k_2 – корректирующий коэффициент, который определяется из таблицы 1;

EV_{Mi} – значения группового показателя i-ой группы.

Уровень осознания ИБ организации рассчитывается по формуле:

$$EV_3 = k3\frac{\sum_{i=28}^{34} EV_{m_i}}{7} \quad (9)$$

где EV3 – уровень осознания ИБ организации.

k_3 – корректирующий коэффициент, который определяется из таблицы 1.

EV_{Mi} – значения группового показателя i-ой группы.

В соответствии с рассмотренной методикой был сформирован алгоритм расчета уровня соответствия ИБ кредитных организаций стандарту Банка России, который представлен в [5].

На основе сформированного алгоритма было разработано ПО «Аудит кредитных организаций».

В качестве среды разработки была выбрана среда «MicrosoftVisualStudio 2010», язык реализации – C#.

На рисунке 1 представлена главная форма программы.

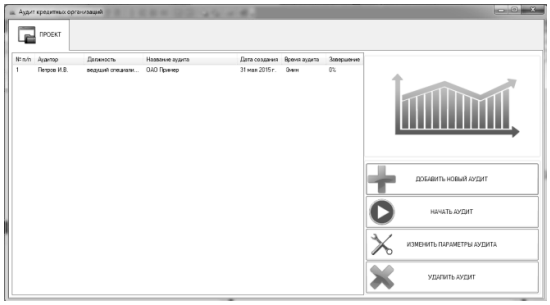

Рисунок 1 – Главная форма программы

Она включает 4 элемента управления:

1. «Добавить новый аудит» – активирует форму для создания нового проекта аудита.

2. «Начать аудит» – открывает проект аудита, который был выбран из списка проектов.

3. «Изменить параметры аудита» – открывает форму для изменения параметров аудита.

4. «Удалить аудит» – удаление выбранного проекта аудита и всех его данных.

На рисунке 2 представлена форма для создания проекта аудита.

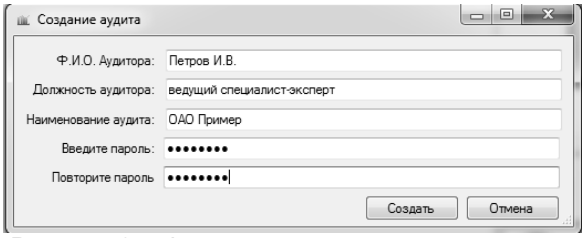

Рисунок 2 – Форма создания проекта аудита

Она содержит два элемента управления:

1. «Создать» - осуществляется проверка правильности заполнения полей. Если все поля заполнены, осуществляется запись информации о проекте в ресурсы программы.

2. «Отмена» - отмена создания аудита и закрытие формы.

На рисунке 3 представлена форма для изменения основных параметров аудита.

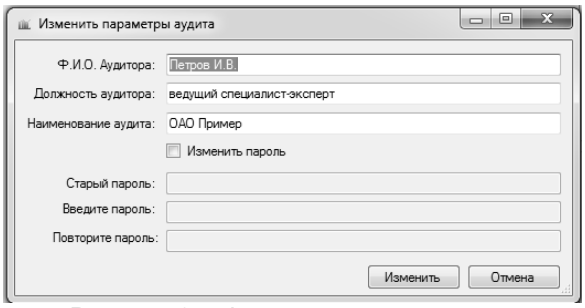

Рисунок 3 – Форма изменения параметров аудита

Форма содержит два элемента управления:

1. «Изменить» - осуществляется запись измененных данных в ресурсы программы.

2. «Отмена» - отмена внесения изменений и закрытие формы.

На рисунке 4 представлена вкладка «Аудит».

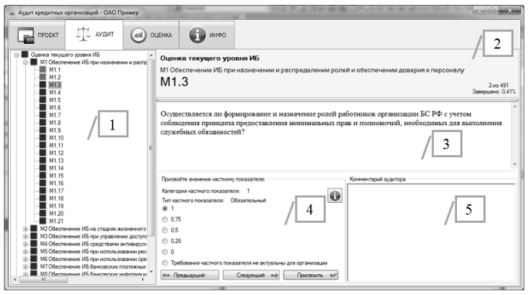

Рисунок 4 – Вкладка «Аудит»

На данной вкладке осуществляется процесс присвоения значений частным показателям. Описание областей вкладки.

Область 1 содержит частные показатели, которые разбиты по группам, а группы, разбиты по направлениям оценки.

В области 2 отображается номер текущего частного показателя, его группа, а так же направление оценки к которой принадлежит данная группа. Так же в этой области отображается статистика: скольким частным показателям присвоено значение, завершенность аудита в процентах.

Область 3 – это область отображения содержания частного показателя (вопроса).

Область 4 предназначена для выбора значения, которое следует присвоить частному показателю.

В области 5 аудитор может оставить комментарий к текущему частному показателю.

На рисунке 5 представлена вкладка «Оценка» на которой осуществляется расчет уровня соответствия ИБ.

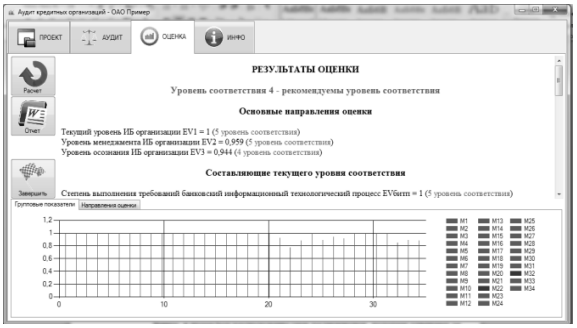

Рисунок 5 – Результаты оценки

Элементы управления:

1) «Расчет» - расчет уровня соответствия ИБ кредитной организации требованиям стандарта Банка России.

2) «Отчет» - автоматическое формирования отчета по проведенному аудиту в формате MS Word.

3)«Завершить» - автоматическое сохранение и закрытие проекта.

Вкладка содержит область, в которой отображаются результаты расчетов:

1. Итоговый уровень соответствия ИБ организации стандарту СТО БР ИББС 1.0.

2. Рассчитанные значения и уровни основных направлений оценки.

3. Степень выполнения $EV_{Битп}$, $EV_{Бптп}$, $EV^2_{озпд}$, $EV_{оопд.}$

4. Оценку групповых показателей.

Так же на данной вкладке отображаются графики значений групповых показателей и направлений оценки.

Представленное ПО прошло апробацию в Алтайском отделении Россельхозбанка России. Актом подтверждена способность автоматизировать процесс проведения аудита ИБ кредитных организаций на соответствие требованиям стандарта Банка России.

В таблице 2 приведены результаты замеров времени, затраченного на проведение аудита с использованием программы «Аудит кредитных организаций» и проведение аудита «Вручную».

Таблица 2 – Временные затраты

Время	ПО «Аудит кредитных организаций»	Вручную
освоение программы / методики	5 – 30 мин.	8 -16 ч.
затраты на ответы и вопросы.	3 – 7 час.	5 – 10 ч.
расчеты	2 – 5 сек.	5 – 10 ч.
составление отчета	1 – 2 мин.	3 – 5 ч
ИТОГ	3 ч. 6 мин – 7 ч. 32 мин.	21 – 41 ч.

Из таблицы 2 следует, что время на проведение аудита вручную затрачивается больше в шесть раз, чем с использованием ПО «Аудит кредитных организаций».

СПИСОК ЛИТЕРАТУРЫ

1. Милославская, Н.Г. Серия «Вопросы управления информационной безопасностью". Выпуск 5: учебное пособие / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон.дан. — М. : Горячая линия-Телеком, 2012.

2. Центральный банк Российской Федерации. Стандарты Банка России [Электронный ресурс] / Режим доступа: http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=Stnd— Загл. с экрана

3. Лукацкий, А. Аудит информационной безопасности: какой, кому, зачем? [Электронный ресурс] / А. Лукацкий. Режим доступа: http://bosfera.ru/bo/audit-informatsionnoj-bezopasnosti— Загл. с экрана

4. Стандарт СТО БР ИББС – 1.2 – 2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС 1.0 –2014. – М. Изд-во стандартов, 2014. – 101с.

5. Будовских И.А. Формирование алгоритма расчета уровня соответствия информационной безопасности кредитных организаций стандарту Банка России [Электронный ресурс] / И.А. Будовских, Л.Д. Алферова // Горизонты образования. – 2015. - №17. – Режим доступа: http://edu.secna.ru

Загинайлов Юрий Николаевич – к.в.н., доцент, тел.: (3852) 290-718, e-mail: zun25@ mail.ru;
Людмила Дмитриевна Алфёрова – старший преподаватель;
Будовских Иван Андреевич – магистрант.