РАЗДЕЛ IV

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 004.056

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ДЛЯ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О.Т. Данилова[1], З.В. Семенова[2], И.Р. Сафиюлин[1], С.А. Любич[2]
[1] ФГБОУ ВО «ОмГТУ», Россия, г. Омск
[2] ФГБОУ ВО «СибАДИ», Россия, г. Омск

Аннотация. *Одним из неотъемлемых этапов системы управления информационной безопасностью является проведение аудита информационной безопасности системы в соответствии с государственными и отраслевыми стандартами. Целью работы является автоматизация рабочего места сотрудника отдела ИБ банковской организации, с помощью разработки программного обеспечения для проведения оценки соответствия документов, содержащих свидетельство деятельности банка по информационной безопасности, в рамках стандарта и рекомендаций к стандарту Центрального Банка Российской Федерации СТО БР ИББС 1.0-2014 и РС БР ИББС 2.0 (2) - 2014. Подробно представлен один из модулей системы – автоматизированная библиотека документов в сфере информационной безопасности.*

Ключевые слова: *аудит, информационная безопасность, автоматизированная библиотека, стандарт, база данных, библиотека документов.*

Введение

При проведении аудита банковской организации, на соответствие стандарту Центрального Банка РФ (ЦБ РФ), руководство организации должно обеспечить документальное и, если это необходимо, техническое подтверждение того, что:

– политика информационной безопасности (ИБ) отражает требования бизнеса и цели организации;

– организационная структура управления ИБ создана;

– процессы выполнения требований ИБ исполняются и удовлетворяют поставленным целям;

– защитные меры настроены и используются правильно;

– остаточные риски оценены и остаются приемлемыми для организации;

– система управления ИБ соответствует определенному уровню зрелости управления ИБ;

– рекомендации предшествующих проверок документации реализованы [1].

Анализ систем защиты информации на соответствие стандарту проводится с целью повышения уровня информационной безопасности и минимизации рисков, связанных с информационными технологиями, а также получения максимальной отдачи от инвестиций в систему защиты информации. В задачу аудита входит составление экспертной оценки текущего состояния системы защиты информации, анализ информационных рисков (по определённым методикам на соответствие критериям, соответствующим российским и международным стандартам).

Постановка задачи

Алгоритм работы программного обеспечения строится, на основе четырёх уровней структуры внутренних документов организации Банковской Системы Российской Федерации (БС), рекомендованной стандартом ЦБ РФ [1].

При проведении самооценки, сотруднику отдела информационной безопасности банка предлагается ответить на вопросы анкеты, затем посредством экспертного оценивания формируется степень выполнения проверяемых требований.

По результатам проведения аудита сотруднику ИБ требуется составление отчета, содержащего:

– заполненные анкеты оценивания групповых показателей ИБ;

– документы, обосновывающие исключение частных показателей из области самооценки, по причине нахождения данных документов в сопутствующих частных показателях;

– документ, содержащий результат самооценки соответствия ИБ по направлениям, оценки и итоговый уровень соответствия ИБ организации БС РФ требованиям СТО БР ИББС 1.0, а также круговою диаграмму оценивания групповых показателей ИБ.

Для хранения форм требований стандартов, а также оценок степени выполнения этих требований в информационной системе была выбрана реляционная модель базы данных (БД) [2]. Как известно, запросы к таким базам данных возвращают таблицу, которая повторно может участвовать в следующем запросе. Кроме того, существует возможность свободного расширения объема базы данных.

Перед непосредственной разработкой программного обеспечения, целесообразно разработать информационно-логическую модель в каноническом виде (рис. 1). С ее помощью наглядно видны этапы работы приложения и связи между ними [3].

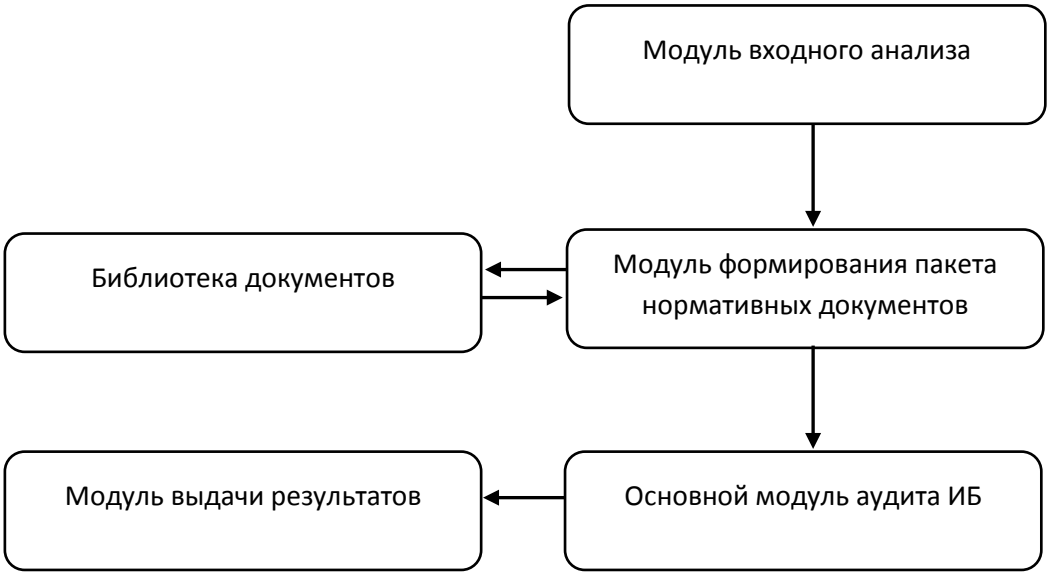

Рис. 1. Общая схема алгоритма программного обеспечения проведения аудита информационной безопасности

В процессе входного анализа происходит оценка процессов обработки защищаемой информации, всесторонний анализ объекта информатизации, анализ возможных угроз для защищаемой информации. Определяются требования по предотвращению утечки информации, анализируются возможные каналы утечки информации и несанкционированного доступа к объекту информатизации. Для получения полной и актуальной информации об исследуемой системе проводится анкетирование с помощью набора опросных листов, сформированных на основе специальных требований и рекомендаций по технической защите информации.

На основе полученных результатов предварительного исследования системы с помощью требований документов нормативно-правового поля устанавливается тип защищаемого объекта, его свойства, определяются необходимый тип и класс защиты информации. Руководствуясь государственным и отраслевыми стандартами, полученными данными об объекте, а также специальными требованиями и рекомендациями по защите конфиденциальной информации, производится определение перечня нормативно-правовых документов и документальных форм, необходимых для организации процесса защиты информации. Исходя из полученного перечня, производится запрос в

автоматизированную библиотеку документов на формирование полного пакета документов и документальных форм.

Библиотека документов

Библиотека документов представляет из себя централизованное, структурированное хранилище руководящих документов, технических требований, стандартов, нормативных документов, инструкций, анкетных и опросных форм, объединенных между собой иерархическими и логическими связями (рис. 2).

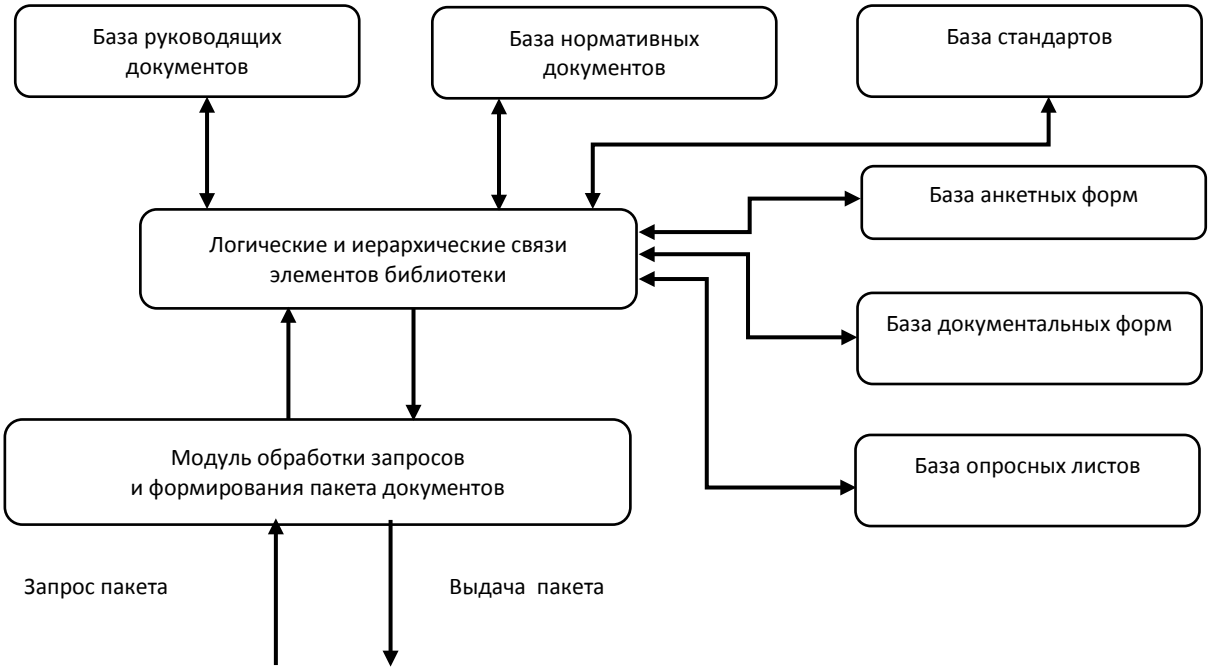

Рис. 2. Структурная схема библиотеки документов

При формировании библиотеки, каждый из документов проходит несколько этапов. На первом этапе определяется тип документа с целью отнесения его к уже существующей определенной группе документов. После установления типа документа, производится его анализ и определение объектов защиты, к которым допустимо применение данного документа, а также установка классов защищаемой информации, для которых возможно использование добавляемого документа при построении системы защиты информации. На основе данных, полученных на предыдущих этапах исследования документа, строятся логические и иерархические связи данного документа с другими объектами библиотеки, формируются правила и условия использования, вносятся исключения по сферам и ситуация применения документа. После выполнения всех вышеуказанных требований, документ проходит процесс нормализации, который заключается в приведении документа к определенной системной форме хранения для удобства последующего поиска и выбора документов. В завершении документ, его нормализованная форма и связи с другими объектами вносятся в библиотеку.

На основе данных, полученных в процессе входного анализа, формируется запрос на формирование пакета документов. Вначале выбирается руководящий документ, определяющий основные нормы и перечень необходимых сопутствующих документов. Далее, используя выбранный руководящий документ, его логические и иерархические связи, а также данные входного анализа, формируется пакет основных документов, стандартов, нормативно-правовых актов. Используя полученный перечень основных документов, дополнительно выбираются необходимые анкетные формы, опросные листы и формы заполнения документов.

Заключительным этапом процесса подбора документов является выдача сформированного пакета полных и актуальных документов.

Методика проведения самооценки

Текущий уровень ИБ организации БС РФ определяется с помощью групповых и частных показателей ИБ, позволяющих получить информацию о наличии или отсутствии документов по ИБ в соответствии со стандартами

СТО БР ИББС-1.0, РС БР ИББС-2.0 и РС БР ИББС-2.1 [4].

Групповые показатели ИБ образуют структуру направлений оценки, детализируя оценки текущего уровня ИБ, менеджмента и уровня осознания ИБ. Групповые показатели текущего уровня ИБ отражают совокупность требований ИБ к областям, определенным в соответствующих разделах СТО БР ИББС 1.0.

Оценки групповых показателей (EV_{Mi}) используются для получения оценки по направлениям ($EV1$, $EV2$ и $EV3$). Частные показатели ИБ входят в состав групповых показателей и представлены в виде вопросов, ответы на которые дают возможность определить оценки (EV_{Mij}), которые затем формируют оценки EV_{Mi} групповых показателей

Частные показатели текущего уровня ИБ отражают отдельные требования ИБ СТО БР ИББС 1.0, предъявляемые по каждой из затрагиваемых областей, действия документа.

Оценка частного показателя ИБ (EV_{Mij}) определяется посредством экспертного оценивания. Для принятия решения следует проводить анализ нормативных, распорядительных, программных и других документов организации БС РФ, имеющих отношение к проверяемым областям ИБ, и уточнять полученную информацию с помощью опросов сотрудников организации БС РФ и наблюдения за их деятельностью.

Устанавливается следующая шкала степени выполнения требований:

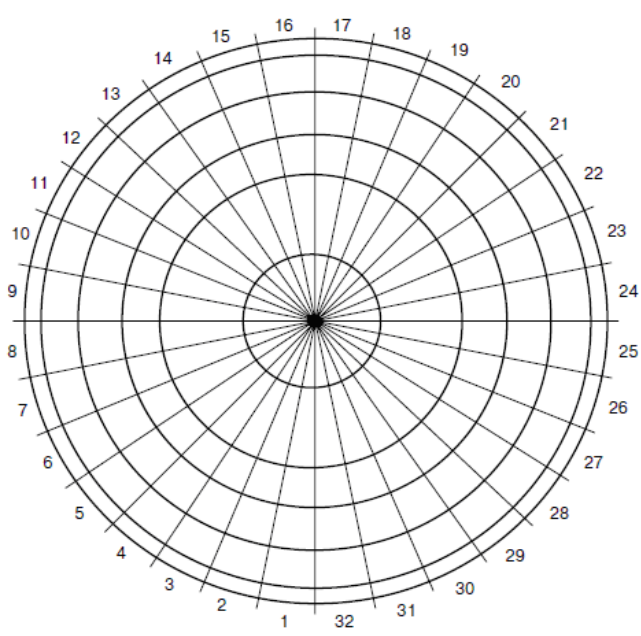

Рис. 3. Круговая диаграмма
для отображения результатов аудита

1) «нет» — оценке присваивается значение, равное нулю;

2) «частично» — оценке присваивается значение 0,25; 0,5 или 0,75;

3) «да» — оценке присваивается значение, равное единице.

Итоговая оценка EV1, отражающая текущий уровень ИБ организации БС РФ, определяется по наименьшему значению из оценок уровней ИБ банковского платежного технологического процесса и банковского информационного технологического процесса.

Значение уровня соответствия ИБ организации БС РФ требованиям СТО БР ИББС 1.0 R определяется по наименьшему значению из трех оценок по направлениям:

– оценки уровня осознания ИБ организации (EV3);

– оценки менеджмента ИБ организации (EV2);

– оценки текущего уровня ИБ организации (EV1).

На рис. 3 представлена круговая диаграмма для отображения результатов оценивания, где секторы 1 – 8 используются для отображения оценки текущего уровня ИБ организации БС РФ; секторы 9 – 27 используются для отображения оценки процессов менеджмента ИБ организации; секторы 28 – 32 предназначены для отображения оценки уровня осознания ИБ организацией БС РФ.

Описание программной реализации методики аудита

На основе представленных схем разработано программное обеспечение для расчета оценки соответствия документов по ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.2014. Исходным языком данной разработки является C#. Среда разработки – Microsoft Visual Studio. Используется система управления базами данных Microsoft SQL Server 2012.

В программе реализованы следующие функции:

- регистрация пользователей и даты проведения самооценки внутренней документации по ИБ;
- занесение в базу данных результатов проведения самооценки;
- расчет текущего уровня состояния внутренней документации по ИБ на основе групповых и частных показателей ИБ;
- построение гистограмм по каждому групповому показателю ИБ, а также вывод гистограмм внутри показателя по каждому вопросу анкеты стандарта;
- построение общей круговой диаграммы, отображения результатов оценивания;

• построения отчета, содержащего результат проведения самооценки, гистограммы и круговой диаграммы, определяющий уровень соответствия документов по ИБ требованиям стандарта СТО БР ИББС 1.0-2014.

Расчет уровня ИБ происходит в реальном времени. При создании нового периода проведения аудита в базе в таблице оценок требований появляются записи о невыполнении всех требований Стандарта в данном периоде. Далее пользователь оценивает степень выполнения предложенных Стандартом требований. При каждом изменении оценки идет обращение к БД. В базе данных сохраняются степени выполнения каждого требования (коэффициент значимости требования).

Затем формируется массив оценок требований Стандарта (считываем данные из БД). И в соответствии с тангенсом угла наклона построенных линий и значением групповых показателей, результаты аудита КСЗИ банка заносятся в соответствующие сектора окружности построенной круговой диаграммы.

Важной функцией системы является построение отчета, содержащего таблицы оценок групповых показателей, соответствующие гистограммы для частных показателей и круговой диаграммы отображения результатов оценивания информационной безопасности АС банка на соответствие требованиям СТО БР ИББС 1.0.

Для защиты от несанкционированного чтения данных аудита банковских систем РФ в программе предусмотрена авторизация (идентификация и аутентификация) пользователей.

Для контроля проведения оценки уровня ИБ ведется журнал регистрации, где фиксируется дата проведения аудита.

Пароли пользователей и журнал регистрации хранятся в базе данных. Для предотвращения нарушения конфиденциальности данных пароли пользователей сохраняются в БД в виде значения функции E = F(P, S), где F – хэш-функция MD5, P – пароль пользователя, S – случайный вектор, создаваемый при регистрации пользователя в системе (представлен структурой глобального уникального идентификатора – GUID [5]). Для обеспечения безопасности журнала регистрации используется симметричное шифрование AES с 256-разрядным ключом на стороне сервера БД (выбор данного алгоритма шифрования был обусловлен, в первую очередь, необходимостью обеспечения возможности дальнейшего перехода на БД более поздних версий).

Заключение

Преимуществами разработанной автоматизированной системы являются высокая гибкость и расширяемость, легкость дополнения новыми документами и актуализации существующих, быстрое создание и изменение как иерархических, так и логических связей между отдельными модулями, широкие возможности по наполнению различными дополнительными элементами, связанными с основными.

Библиографический список

1. Стандарт Банка России СТО БР ИББС 1.0–2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

2. Дейт, К. Дж. Введение в системы баз данных. − 8-е изд. / пер. с англ. – М. : Издательский дом «Вильямс», 2005. – 1328 с.

3. Соловьев, И.В. Проектирование информационных систем: Фундаментальный курс / И.В. Соловьев, А.А. Майоров. - М. : Академический проект, 2009 – 398 с.

4. Рекомендации в области стандартизации Банка России РС БР ИББС-2.1–2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» – Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.

5. Структура Guid. [Электронный ресурс]. – Режим доступа: https://msdn.microsoft.com/ru-ru/library/system.guid(v=vs.110).aspx

SOFTWARE DEVELOPMENT FOR AN AUTOMATED SYSTEM FOR CARRYING OUT INFORMATION SECURITY AUDIT

O.T. Danilova, Z.V.Semenova, I.R. Safiulin, S.A. Ljubich

Abstract. One of the essential stages of the system management information security is audit of information security systems in accordance with state and industry standards. The aim of this work is the automation of a workplace of the employee of the Department of information security of banking organizations, with software development for the assessment of conformity of documents containing evidence of the Bank's activities in IB, in the framework of the standard and recommendations to the standard Central Bank of the Russian Federation (RF) STO BR IBBS 1.0-2014 and RS BR IBBS-2.0 (2) -2014. Presented in detail one of the modules of the system – an automated document library in the sphere of information security.

Keywords: audit, information security, automated library, standard, database, library of documents.

References

1. Standard Bank of Russia STO BR IBBS 1.0–2014 «Ensuring information security of organizations of Bank system of the Russian Federation»

2. Date C.J., An Introduction to Database Systems. - M.: Williams, 2005. – 1328 с.

3. Soloviev, V. I. Design of information systems: the Foundation course / I. V. Solovyev, A. A. Mayorov. - M.: Academic project, 2009. – 398c.

4. Recommendations in standardization of the Bank of Russia RS BR IBBS-2.1–2007 "information security of organizations of Bank system of the Russian Federation" – the Guide to self-assessment of conformity of information security of organizations of Bank system of the Russian Federation with the requirements of STO BR IBBS-1.0.

5. Structure Guid. [Electronic resource]. - Access mode: https://msdn.microsoft.com/ru-ru/library/system.guid(v=vs.110).aspx

Данилова Ольга Тимофеевна (Омск, Россия) – канд. физ.-мат.наук, доцент кафедры Комплексная защита информации ФГБОУ ВО Омский государственный технический университет (644050, г.Омск, пр.Мира, 11, e-mail: olga.danlot@yandex.ru).

Семенова Зинаида Васильевна (Омск, Россия) – д-р пед. наук, профессор, заведующая кафедрой Информационная безопасность ФГБОУ ВО Сибирская государственная автомобильно-дорожная академия (644008, г. Омск, пр. Мира, 5, e-mail: semenova.z.v@gmail.com).

Сафиюлин Игорь Рашидович – аспирант кафедры Комплексная защита информации» ФГБОУ ВО Омский государственный технический университет (644050, г.Омск, пр.Мира, 11, e-mail: igorsafiulin@Gmail.com).

Любич Станислав Александрович (Омск, Россия) – старший преподаватель кафедры Информационная безопасность ФГБОУ ВО Сибирская государственная автомобильно-дорожная академия (644008, г. Омск, пр. Мира, 5, e-mail: ljubich.s.a@mail.ru).

УДК 621.879

РЕАЛИЗАЦИЯ ЭКСПЕРИМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ ЭНЕРГОЭФФЕКТИВНОСТИ ОДНОКОВШОВОГО ЭКСКАВАТОРА ЧЕРЕЗ ИНТЕГРАЦИЮ ВСПОМОГАТЕЛЬНЫХ ВИРТУАЛЬНЫХ КОМПЛЕКСОВ

В.В. Савинкин[1], В.Н. Кузнецова[2]

[1]Северо-Казахстанский государственный университет им. М. Козыбаева, Казахстан, г. Петропавловск

[2]Сибирская государственная автомобильно-дорожная академия, Россия, г. Омск

Аннотация. *Современный этап развития систем моделирования технологических процессов характеризуется повышением их функциональной насыщенности. Моделирование процессов работы гидропривода экскаватора является сложной иерархической задачей, так как при выполнении технологических операций экскаватора необходимо регистрировать и анализировать большое количество факторов и показателей, динамично изменяющихся во времени. В статье отражено описание разработанной комплексной системы реализации экспериментальных исследований энергоэффективности одноковшового экскаватора через интеграцию вспомогательных виртуальных комплексов, имеющей широкий спектр функциональных возможностей и позволяющей снизить трудоемкость проведения экспериментальных изысканий.*

Ключевые слова: энергоэффективность, следящая система, алгоритм, силы сопротивления, кинематическая пара.

Введение

Проблемы исследования энергоэффективности экскаватора с применением современного программного обеспечения, математического моделирования и автоматизированного проектирования рассмотрены в работах В.Г. Ананина, Н.С. Галдина, А.Г. Григорьева, Н.Н. Живейнова, Л.Б. Зарецкого, В. Г. Зедгенизова, Г.Н. Карасева, В.Я. Крикуна, Е.Ю. Малиновского, В.А. Мещерякова, В.В. Москвичева, В. П. Павлова, В.С. Щербакова [1]

Предшествующими исследователями установлено, что при моделировании виртуальных комплексов необходимо сформировать как можно больше значимых свойств для более полного приближения к реальной модели, а значит, и большими возможностями будет обладать система, использующая данную модель [2 - 4].

Результаты теоретических и практических исследований

В данном случае этапы виртуального моделирования включали: 1. разработку концептуальной модели, выявление основных элементов системы и элементарных связей взаимодействия; 2. выбор среды программного продукта и информационной площадки для реализации моделируемого эксперимента; 3. разработку математической модели; 4. соз-