Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.
ЧЕРНЫШЕВСКОГО»

Кафедра материаловедения, технологии
и управления качеством

ОСОБЕННОСТИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ В БАНКОВСКОЙ СФЕРЕ

ДИПЛОМНАЯ РАБОТА

студента 6 курса

по специальности 220501 «Управление качеством»

факультета нано- и биомедицинских технологий

Немова Алексея Андреевича

Научный руководитель

ст. преподаватель		А.В. Бурмистров
должность, уч. степень, уч. звание	подпись, дата	инициалы, фамилия

Зав. кафедрой

профессор, д.ф.-.м.н.		С.Б. Вениг
должность, уч. степень, уч. звание	подпись, дата	инициалы, фамилия

Саратов, 2016

ВВЕДЕНИЕ

Актуальность дипломной работы подтверждается тем, что при ее проведении была исследована действующая информационная система банка, а также использованы актуальные стандарты при проведении аудита.

Целью дипломной работы является определение особенностей управления качеством в банке, используя проведение аудита информационных систем как один из инструментов менеджмента.

В банковской сфере информация имеет особое значение, т.к. ее состояние напрямую влияет на качество оказываемых услуг.

Были поставлены задачи для достижения цели выпускной квалификационной работы :

1. Провести аудит информационных систем банка, а именно, в автоматизированной системе «Биллинг»
2. Сделать выводы о безопасности проведения операций через данную систему.
3. Предложить решение для обнаруженных проблем.
4. Определить взаимодействия аудита информационных систем и систем менеджмента.

Структуры дипломной работы содержит:

Введение

Глава 1 – Теоретические основы проведения аудита

Глава 2 – Проведение аудита

Заключение

Список использованных источников.

Основное содержание работы

Работа содержит в себе теоретическую и практическую части.

Теоретическая часть начинается с описания понятия аудита информационной системы и особенностей информационной безопасности. Также представлены стандарты, необходимые для построения оптимальной защиты информационной системы.

Аудит позволяет оценить текущую безопасность функционирования информационной системы, оценить и прогнозировать риски, управлять их влиянием на бизнес-процессы фирмы, корректно и обоснованно подойти к вопросу обеспечения безопасности ее информационных активов, стратегических планов развития, маркетинговых программ, финансовых и бухгалтерских ведомостей, содержимого корпоративных баз данных.

Далее идет описание стандарта ГОСТ Р ИСО 19011 – 2012 для правильности проведения аудита.

Стандарт рассчитан на широкий круг пользователей - аудиторов, организации, внедряющие системы менеджмента, и организации, которым необходимо проводить аудиты систем менеджмента в соответствии с контрактом или законодательством. Проведение аудита в соответствии со стандартом основано на менеджменте рисков и предполагает применение выборочных исследований на основе теории вероятностей и математической статистике.

В этом разделе также описаны все необходимые принципы и требования, содержащиеся в стандарте.

a) Целостность (integrity) - основа профессионализма.

b) Беспристрастность (fair presentation) - обязательство предоставлять правдивые и точные отчеты.

c) Профессиональная осмотрительность (due professional care) - прилежание и умение принимать правильные решения при проведении аудита.

d) Конфиденциальность (confidentiality) - сохранность информации.

e)Независимость (independence) - основа беспристрастности и объективности заключений по результатам аудита.

f) Подход, основанный на свидетельстве (evidence-based approach), - разумная основа для достижения надежных и воспроизводимых заключений аудита в процессе систематического аудита.

Данный стандарт был взят за основу при проведении аудита информационных систем. Сначала, для организации аудита, были использованы типовые действия его проведения, представленные на рисунке 1.

Рисунок 1- Типовые действия при проведении аудита.

Далее по структуре работы идет описание автоматизированной системы «Биллинг», при работе которой и необходимо будет проводить

проверки. В этом разделе полностью описана методика входа в программу – рисунок 2, а также алгоритмы выполнения операций – рисунок 3

Рисунок 2 – Блок-схема входа в программу АС «Биллинг»

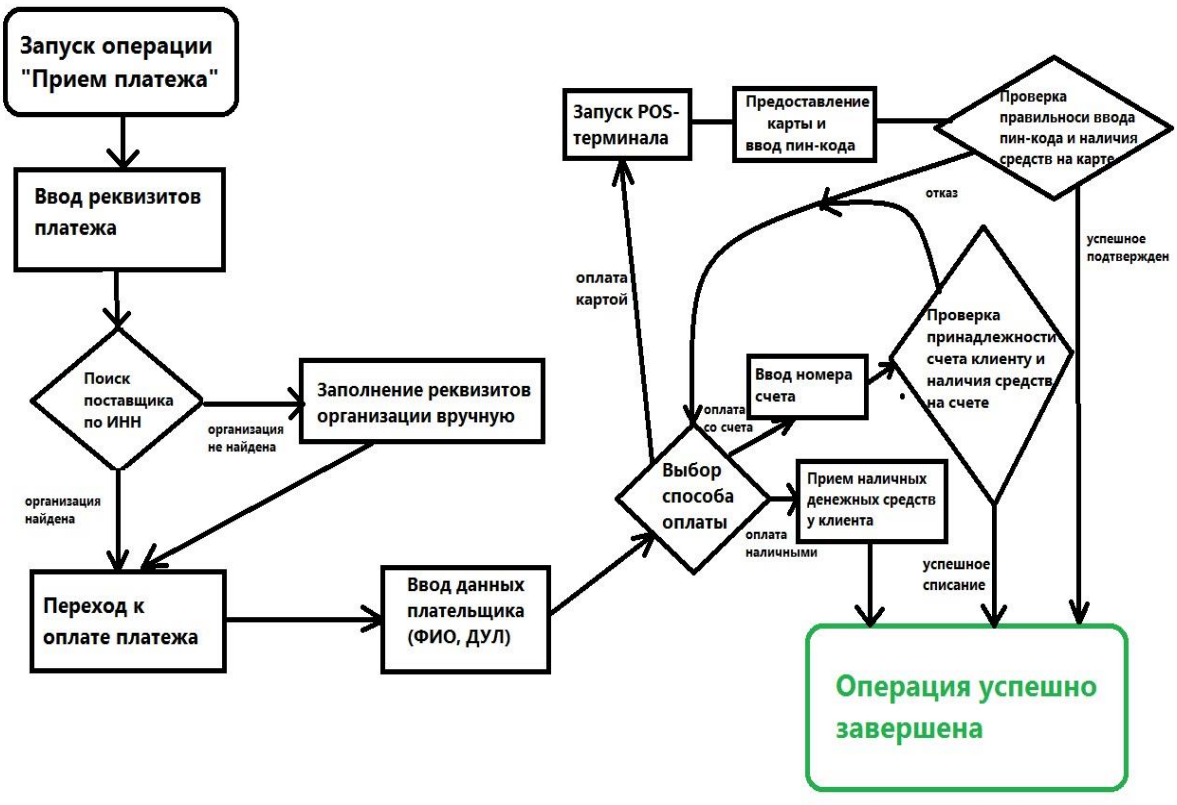

Рисунок 3 – Блок-схема процесса проведения платежа в АС «Биллинг»

Практическая часть – это непосредственно проведение аудита информационных систем. Сначала описывается установка первоначального контакта аудиторской группы и заказчика.

На первоначальном совещании был определен состав группы аудиторов и технических экспертов, обладающих необходимыми навыками и компетенциями. Также были установлены каналы передачи информации, контакты для связи и степень секретности полученной в ходе аудита информации.

Далее аудиторская группа приступает к ознакомлению документации, после чего составляет план проведения аудита.

План проведения аудита:

Обозначенная цель аудита - проверка информационных систем при работе в автоматизированной системе «Биллинг» (программа приема платежей у физических лиц).

Область аудита охватывает физический контроль доступа к оборудованию и серверам, обеспечивающим работоспособность АС Биллинг, аппаратное обеспечение безопасности, системное программное обеспечение, нормативную документацию, а также анализ защищенности соединения при передаче секретной информации из АС «Биллинг» в бэк-оффисные системы банке.

Также были оговорены критерии аудита по каждому из пунктов проверок. Оптимальная структура защиты информационных систем компании формируется на основании необходимых стандартов.

Руководитель группы распределяет обязанности в соответствии с компетенциями каждого из аудиторов.

Андрей Захарченко проводит проверку физического контроля доступа в серверное помещение, а также проверку аппаратных средств защиты информации.

Светлана Киселева будет проверять наличие необходимой документации, которая должна присутствовать в компании, желающей обеспечить информационную защиту своих ресурсов.

Андрей Усанов будет проводить аудит системного программного обеспечения на рабочих станция пользователей, работающих в автоматизированной системе «Биллинг».

Алексей Немов (т.е., я) согласно плану должен провести проверку защищенности во время работы в АС «Биллинг».

Далее проводится сам аудит, согласно которому составляется отчет.

В отчете представлены показания по текущему состоянию проверяемой зоны, обнаруженным нарушениям, а также описаны меры по исправлению ситуации.

Сначала была проверена нормативная документация, описывающая все требования и меры защиты информации в организации.

Далее проведены проверки физического контроля доступа в серверные помещения.

После этого проверялось аппаратное обеспечение безопасности информационной системы.

Далее отчет содержит проверку системного программного обеспечения.

И последним проверялась автоматизированная система «Биллинг» на предмет правильности выполнения алгоритма операции, а также защищенности передачи информации на сервера бэк-офисных систем банка.

В качестве метода проверки защищенности передачи данных был использован экспресс-тест, определяемый уязвимости сервера при подключении.

После прохождения всех этапов аудиторской проверки было проведено заключительно совещание группы, где анализировалась вся полученная

информации и сделаны выводы о степени защищенности информационной системы.

В пункте 2.4 Заключения по результатам аудита описаны сделанные выводы по каждой из проведенный проверок, а также предложены меры по устранению найденных замечаний.

В заключении работ сделаны выводы о том, что аудит, проведенный в данной работе, оказался важным инструментом для получения информации об АС «Биллинг», а его выводы послужили основанием для принятия правильного решения руководством банка о включении системы в промышленную зону.

После проверки серверов приложений были найдены уязвимые места, которые могли нанести ущерб банку – введении АС «Биллинг» в эксплуатацию было отложено на время, необходимое для исправления найденных проблем.

Эффективность применения аудита информационных систем как инструмента управления качеством была полностью подтверждена. И особенно высока, когда качество напрямую зависит от состояния информации в организации.

Такая ситуация наглядно показывает эффективность применения аудита информационных систем как инструмента управления качеством. Особенно, когда качество напрямую зависит от состояния информации в организации.

В банковской сфере информационная структура является основой для обеспечения конкурентоспособности организации на рынке. Это делает аудит информационных систем не только способом определения текущего состояния системы, но и необходимым механизмом для ее управления. А задавая новые векторы развития – механизмом управления всей организацией.

ВВЕДЕНИЕ

Актуальность дипломной работы подтверждается тем, что при ее проведении была исследована действующая информационная система банка, а также использованы актуальные стандарты при проведении аудита.

Целью дипломной работы является определение особенностей управления качеством в банке, используя проведение аудита информационных систем как один из инструментов менеджмента.

В банковской сфере информация имеет особое значение, т.к. ее состояние напрямую влияет на качество оказываемых услуг.

Были поставлены задачи для достижения цели выпускной квалификационной работы :

1. Провести аудит информационных систем банка, а именно, в автоматизированной системе «Биллинг»
2. Сделать выводы о безопасности проведения операций через данную систему.
3. Предложить решение для обнаруженных проблем.
4. Определить взаимодействия аудита информационных систем и систем менеджмента.

Структуры дипломной работы содержит:

Введение

Глава 1 – Теоретические основы проведения аудита

Глава 2 – Проведение аудита

Заключение

Список использованных источников.

Основное содержание работы

Работа содержит в себе теоретическую и практическую части.

Теоретическая часть начинается с описания понятия аудита информационной системы и особенностей информационной безопасности. Также представлены стандарты, необходимые для построения оптимальной защиты информационной системы.

Аудит позволяет оценить текущую безопасность функционирования информационной системы, оценить и прогнозировать риски, управлять их влиянием на бизнес-процессы фирмы, корректно и обоснованно подойти к вопросу обеспечения безопасности ее информационных активов, стратегических планов развития, маркетинговых программ, финансовых и бухгалтерских ведомостей, содержимого корпоративных баз данных.

Далее идет описание стандарта ГОСТ Р ИСО 19011 – 2012 для правильности проведения аудита.

Стандарт рассчитан на широкий круг пользователей - аудиторов, организации, внедряющие системы менеджмента, и организации, которым необходимо проводить аудиты систем менеджмента в соответствии с контрактом или законодательством. Проведение аудита в соответствии со стандартом основано на менеджменте рисков и предполагает применение выборочных исследований на основе теории вероятностей и математической статистике.

В этом разделе также описаны все необходимые принципы и требования, содержащиеся в стандарте.

a) Целостность (integrity) - основа профессионализма.

b) Беспристрастность (fair presentation) - обязательство предоставлять правдивые и точные отчеты.

c) Профессиональная осмотрительность (due professional care) - прилежание и умение принимать правильные решения при проведении аудита.

d) Конфиденциальность (confidentiality) - сохранность информации.

e)Независимость (independence) - основа беспристрастности и объективности заключений по результатам аудита.

f) Подход, основанный на свидетельстве (evidence-based approach), - разумная основа для достижения надежных и воспроизводимых заключений аудита в процессе систематического аудита.

Данный стандарт был взят за основу при проведении аудита информационных систем. Сначала, для организации аудита, были использованы типовые действия его проведения, представленные на рисунке 1.

Рисунок 1- Типовые действия при проведении аудита.

Далее по структуре работы идет описание автоматизированной системы «Биллинг», при работе которой и необходимо будет проводить

проверки. В этом разделе полностью описана методика входа в программу – рисунок 2, а также алгоритмы выполнения операций – рисунок 3

Рисунок 2 – Блок-схема входа в программу АС «Биллинг»

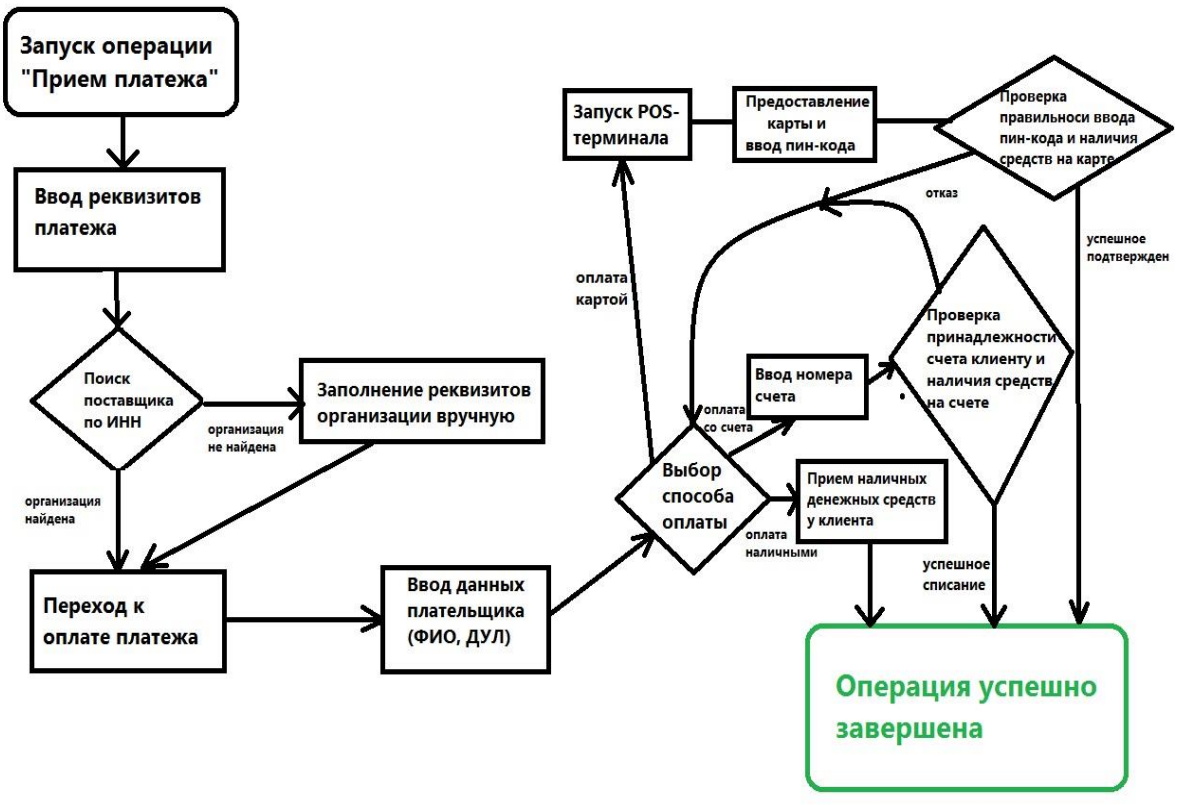

Рисунок 3 – Блок-схема процесса проведения платежа в АС «Биллинг»

Практическая часть – это непосредственно проведение аудита информационных систем. Сначала описывается установка первоначального контакта аудиторской группы и заказчика.

На первоначальном совещании был определен состав группы аудиторов и технических экспертов, обладающих необходимыми навыками и компетенциями. Также были установлены каналы передачи информации, контакты для связи и степень секретности полученной в ходе аудита информации.

Далее аудиторская группа приступает к ознакомлению документации, после чего составляет план проведения аудита.

План проведения аудита:

Обозначенная цель аудита - проверка информационных систем при работе в автоматизированной системе «Биллинг» (программа приема платежей у физических лиц).

Область аудита охватывает физический контроль доступа к оборудованию и серверам, обеспечивающим работоспособность АС Биллинг, аппаратное обеспечение безопасности, системное программное обеспечение, нормативную документацию, а также анализ защищенности соединения при передаче секретной информации из АС «Биллинг» в бэк-оффисные системы банке.

Также были оговорены критерии аудита по каждому из пунктов проверок. Оптимальная структура защиты информационных систем компании формируется на основании необходимых стандартов.

Руководитель группы распределяет обязанности в соответствии с компетенциями каждого из аудиторов.

Андрей Захарченко проводит проверку физического контроля доступа в серверное помещение, а также проверку аппаратных средств защиты информации.

Светлана Киселева будет проверять наличие необходимой документации, которая должна присутствовать в компании, желающей обеспечить информационную защиту своих ресурсов.

Андрей Усанов будет проводить аудит системного программного обеспечения на рабочих станция пользователей, работающих в автоматизированной системе «Биллинг».

Алексей Немов (т.е., я) согласно плану должен провести проверку защищенности во время работы в АС «Биллинг».

Далее проводится сам аудит, согласно которому составляется отчет.

В отчете представлены показания по текущему состоянию проверяемой зоны, обнаруженным нарушениям, а также описаны меры по исправлению ситуации.

Сначала была проверена нормативная документация, описывающая все требования и меры защиты информации в организации.

Далее проведены проверки физического контроля доступа в серверные помещения.

После этого проверялось аппаратное обеспечение безопасности информационной системы.

Далее отчет содержит проверку системного программного обеспечения.

И последним проверялась автоматизированная система «Биллинг» на предмет правильности выполнения алгоритма операции, а также защищенности передачи информации на сервера бэк-офисных систем банка.

В качестве метода проверки защищенности передачи данных был использован экспресс-тест, определяемый уязвимости сервера при подключении.

После прохождения всех этапов аудиторской проверки было проведено заключительно совещание группы, где анализировалась вся полученная

информации и сделаны выводы о степени защищенности информационной системы.

В пункте 2.4 Заключения по результатам аудита описаны сделанные выводы по каждой из проведенный проверок, а также предложены меры по устранению найденных замечаний.

В заключении работ сделаны выводы о том, что аудит, проведенный в данной работе, оказался важным инструментом для получения информации об АС «Биллинг», а его выводы послужили основанием для принятия правильного решения руководством банка о включении системы в промышленную зону.

После проверки серверов приложений были найдены уязвимые места, которые могли нанести ущерб банку – введении АС «Биллинг» в эксплуатацию было отложено на время, необходимое для исправления найденных проблем.

Эффективность применения аудита информационных систем как инструмента управления качеством была полностью подтверждена. И особенно высока, когда качество напрямую зависит от состояния информации в организации.

Такая ситуация наглядно показывает эффективность применения аудита информационных систем как инструмента управления качеством. Особенно, когда качество напрямую зависит от состояния информации в организации.

В банковской сфере информационная структура является основой для обеспечения конкурентоспособности организации на рынке. Это делает аудит информационных систем не только способом определения текущего состояния системы, но и необходимым механизмом для ее управления. А задавая новые векторы развития – механизмом управления всей организацией.