МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. И. РАЗЗАКОВА

ВЫСШАЯ ШКОЛА МАГИСТРАТУРЫ

Кафедра ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА

ОТЧЕТ
по научно-исследовательской практике

Выполнил:
магистрант гр. ПМм-1-21 Аскарова М.М.

Принял:
Руководитель практики от кафедры Осмонканов А.М.

БИШКЕК – 2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Научно-исследовательская практика (далее НИП) магистрантов предполагает выполнение исследовательской работы в рамках направления подготовки магистров по соответствующему профилю ООП ВПО. По итогам НИП магистрант должен завершить Выпускную квалификационную работу (магистерскую диссертацию) и публикацией ее результатов в научных изданиях в количестве не менее двух статей. Распределение исследовательских тем на НИП осуществляется на основе утверждённых тем Выпускных квалификационных работ студентов магистратуры.

Цель научно-исследовательской практики заключается в выработке у магистранта навыков и компетенций квалифицированно формулировать актуальные научные проблемы, проводить научные исследования по избранной теме магистерской диссертации, использовать научные методы при проведении исследований, анализировать, обобщать и использовать полученные результаты.

Основной задачей НИП является приобретение опыта в исследовании актуальной научной задачи, а также подбор необходимых материалов для подготовки доклада на научно-практических конференциях, для публикации статьи, выполнения выпускной квалификационной работы - магистерской диссертации.

Задачами научно-исследовательской практики магистрантов также являются:

- организация работы с эмпирической базой исследования в соответствии темой научного исследования (выпускной квалификационной работы - магистерской диссертации);

- рассмотрение вопросов по теме научного исследования (выпускной научно-квалификационной работы - магистерской диссертации);

- подготовка данных для составления обзоров, отчетов и научных публикаций;

- сбор, обработка, анализ и систематизация информации по теме исследования, выбор методов и средств решения задач исследования;

- изучение справочно-библиографических систем, способов поиска информации;

- работа с электронными базами данных отечественных и зарубежных библиотечных фондов;

- обобщение и подготовка результатов научно-исследовательской деятельности магистранта в виде научно-исследовательской работы (выпускной научно-квалификационной работы - магистерской диссертации);

- привитие навыков самообразования и самосовершенствования содействие активизации научно-исследовательской деятельности магистров.

В результате прохождения НИП магистрант должен овладеть навыками самостоятельной научно-исследовательской деятельности в профессиональной области на основе:

организации научного исследования магистрантов в соответствии с современной методологией науки;

соблюдение этапов и логики в проведении научного исследования (научность);

актуализации и стимулировании творческого подхода магистрантов к проведению научного исследования (креативность);

учета научных интересов магистрантов (практика предусматривает проведение научного исследования в соответствии с научно-исследовательскими интересами магистрантов).

Научно-исследовательская практика направлена на формирование следующих компетенций в соответствии с ГОС ВПО по данному направлению подготовки:

ИК-1. Способен вести профессиональные дискуссии на уровне профильных и смежных отраслей на одном из иностранных языков

ИК-2. Способен производить новые знания с использованием информационных технологий и больших данных для применения в инновационной и научной деятельности.

ПК-1. Способен проводить научные исследования и получать новые научные и прикладные результаты.

ПК-2. Может разрабатывать концептуальные и теоретические модели решаемых научных проблем и задач.

ПК-3. Готов углубленно анализировать проблемы, становить и обосновывать задачи научной и проектно-технологической деятельности;

ПК-10. Готов к разработке аналитических обзоров состояния области прикладной математики и информационных технологий по профильной направленности ООП магистратуры;

ПК-14. Готов к использованию основ защиты производственного персонала и населения от возможных последствий аварий, катастроф, стихийных бедствий и применения современных средств поражения, основных мер по ликвидации их последствий, способность к общей оценке условий безопасности жизнедеятельности.

1. ОсОО РК «АМАНБАНК»

1.1. Инфраструктура и деятельность организации ОАО РК «АМАНБАНК»

ОАО "РК Аманбанк" имеет следующую структуру:

Правление банка - высшее руководящее орган, ответственное за стратегическое управление банком.

Департамент по кредитованию - занимается выдачей кредитов клиентам банка.

Департамент по операциям с физическими лицами - осуществляет операции с физическими лицами, такие как открытие счетов, выдача кредитных и дебетовых карт и т.д.

Департамент по операциям с юридическими лицами - осуществляет операции с юридическими лицами, такие как выдача кредитов, организация расчетов и т.д.

Департамент по управлению рисками - занимается оценкой и управлением рисками, связанными с деятельностью банка.

Департамент по IT - занимается управлением информационными технологиями в банке.

Департамент по маркетингу и продажам - занимается разработкой маркетинговых стратегий и продажей банковских продуктов.

Департамент по финансовому учету и отчетности - отвечает за ведение бухгалтерского учета и формирование финансовой отчетности.

Отдел кадров - отвечает за управление персоналом банка.

Отдел юридического обеспечения - занимается юридическими вопросами, связанными с деятельностью банка.

Филиалы банка - являются подразделениями банка, расположенными в различных городах Кыргызстана. Каждый филиал имеет свою структуру и занимается обслуживанием клиентов банка в своем регионе.

1.2. Работы отдела Управления Автоматизации

Управление автоматизации в ОАО РК АМАНБАНК отвечает за разработку и поддержку информационных систем банка, а также за их эффективное использование в повседневной деятельности.

Ключевые задачи управления автоматизации в банке могут включать:

Разработка и внедрение информационных систем: управление автоматизации отвечает за разработку новых информационных систем и модулей, а также за их внедрение в банковскую инфраструктуру.

Поддержка информационных систем: управление автоматизации заботится о том, чтобы информационные системы банка были всегда доступны и работали без сбоев. Для этого необходимо проводить регулярное обновление и техническое обслуживание систем.

Обучение сотрудников: управление автоматизации занимается обучением сотрудников банка работе с информационными системами и программным обеспечением, а также разработкой методических материалов и инструкций по использованию систем.

Мониторинг и анализ: управление автоматизации отслеживает работу информационных систем банка, собирает статистику и анализирует ее, чтобы улучшить работу систем и повысить эффективность банковской деятельности.

Функции занимаемой должности

IT специалист- сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы компьютерной техники, сети и программного обеспечения, а также обеспечение информационной безопасности в банке. В круг типовых задач системного администратора обычно входит:

-подготовка и сохранение резервных копий данных, их периодическая проверка и уничтожение;

-установка и конфигурирование необходимых обновлений для операционной системы и используемых программ;

-установка и конфигурирование нового аппаратного и программного обеспечения;

-ответственность за информационную безопасность в банка;

-устранение неполадок в системе;

-планирование и проведение работ по расширению сетевой структуры банка;

-документирование всех произведенных действий.

В организациях с большим штатом сотрудников данные обязанности могут делиться между несколькими IT-специалистами.

-например, между IT-специалистами, учётных записей и резервного копирования. Также, в организациях с небольшим штатом сотрудников эти обязанности могут исполняться одним специалистом, занимающимся как консультированием пользователей, так и ремонтом аппаратной части персональных компьютеров и периферийных устройств. Среди плюсов профессии IT-специалиста можно выделить:

-Востребованность на рынке труда,

-Потребность в увеличении скорости.

Она может привести к обновлению оборудования, например, маршрутизаторов или самих каналов;

-Новые возможности администрирования. Упрощение обслуживания сети является веским основанием для приобретения административного инструментария, такого, как программное обеспечение для инвентаризации настольных систем;

-Необходимость стандартизации вычислительной среды для реализации планируемых приложений или сервисов.

В этой ситуации: стандартная среда позволит оптимизировать закупки, снизить затраты на обслуживание и обучение и упростить предоставление требуемых сервисов.

1.3. Профилактические работы на объектах сетевой инфраструктуры

Профилактические работы на объектах сетевой инфраструктуры Профилактические работы проводятся для того, чтобы обнаружить неисправные детали и отдельные элементы оборудования и сооружений, а также предупредить возникновение нарушений связи. Если своевременно не выявить и не устранить неполадки в работе компьютерной техники, то они могут привести к дорогостоящему ремонту, к потере корпоративной информации или к подрыву работы клиентских сервисов. По этим причинам были проделаны следующие профилактические работы для корректной работы сети:

-Периодическая чистка, как всей системы, так и отдельных её компонентов;

-Чистка и смазка всех основных элементов;

-Устранение последствий термических смещений микросхем;

-Замена термопасты на радиаторе;

-Оптимизация файла подкачки и дефрагментация жесткого диска;

-Своевременное обновление драйверов;

-Программный контроль температуры компонентов ПК;

-Обеспечение безопасности ОС;

-Очистка и дефрагментацию реестра;

-Резервное копирование данных;

-Очистка временных файлов.

Все эти работы позволили обеспечить надёжное функционирование сети предприятия. Описание управления и предложения по его улучшению

Практика проходила в непосредственном подчинении начальника Управлении Автоматизации. Обучение проходило посредством решения реальных задач, возникающих по мере функционирования предприятия. Я выполнял работу помощника начальника Управление автоматизации. Деятельность всего отдела подкреплена должностными инструкциями. По заданиям руководства мы устанавливали и настраивали программное обеспечение, операционные системы, базы данных, пользовательские приложение. Также мы следили за состоянием сервера, и за нагрузкой на сервер. На с возлагается максимальная ответственность в информационной работе предприятия. Перечислю следующие предложения по улучшению управления:

-Оказывать IT-специалисту нематериальную поддержку, многие руководители забывают, что, если все работает стабильно и ничего не происходит

-Необходимо минимизировать способы решения проблем, понятные только конкретному IT-специалисту т.к. в случае его увольнения преемник может потратить недели, разбираясь, почему в компании что-то работает или не работает;

2. Разработка метода обеспечения и проведение внутреннего аудита информационной безопасности автоматизированных банковских систем

2.1. Постановка задачи

Цели и задачи разработки метода обеспечения и проведения внутреннего аудита информационной безопасности автоматизированных банковских систем заключаются в обеспечении надежной защиты информации и минимизации рисков, связанных с использованием автоматизированных банковских систем. Это достигается путем определения уязвимостей и установления правил доступа к информации, а также разработки процедур контроля и мониторинга системы.

Актуальность темы обеспечения информационной безопасности автоматизированных банковских систем обусловлена тем, что банки являются объектами преступной деятельности, направленной на кражу денег и конфиденциальной информации. Также банки сталкиваются с риском взлома своих систем и получения несанкционированного доступа к данным своих клиентов.

Для разработки метода обеспечения и проведения внутреннего аудита информационной безопасности автоматизированных банковских систем используются различные научные методики. Одной из основных методик является анализ угроз и рисков, который позволяет определить наиболее вероятные и вредоносные сценарии атак. Также используются методы аудита, которые позволяют оценить эффективность существующих процедур безопасности и контроля.

Кроме того, для разработки метода обеспечения информационной безопасности автоматизированных банковских систем используются методы управления рисками, которые позволяют определить уровень риска и разработать меры по его уменьшению. Важным элементом также является методика управления доступом к информации, которая позволяет определить права доступа пользователей к конфиденциальным данным.

В целом, разработка метода обеспечения и проведение внутреннего аудита информационной безопасности автоматизированных банковских систем является сложным и ответственным процессом, который требует использования различных научных методик и подходов.

2.2. Анализ литературных источников

Анализ литературных источников по теме "Разработка метода обеспечения и проведение внутреннего аудита информационной безопасности автоматизированных банковских систем" позволяет выделить несколько основных направлений и подходов в данной области.

Во-первых, большое внимание уделяется анализу угроз и рисков, связанных с использованием автоматизированных банковских систем. Для этого используются различные методы, такие как метод анализа угроз и уязвимостей, метод проведения пенетрационного тестирования и др.

Во-вторых, для разработки метода обеспечения информационной безопасности автоматизированных банковских систем используются методы аудита, которые позволяют оценить эффективность существующих процедур безопасности и контроля. В рамках аудита проводятся проверки на соответствие нормативным требованиям, а также на оценку уровня рисков и эффективности мер по их уменьшению.

В-третьих, в литературных источниках выделяются методы управления рисками, которые позволяют определить уровень риска и разработать меры по его уменьшению. Они основываются на определении уязвимостей системы, вероятности возникновения инцидентов и степени их воздействия на банк.

В-четвертых, одним из ключевых элементов метода обеспечения информационной безопасности автоматизированных банковских систем является методика управления доступом к информации. Она позволяет определить права доступа пользователей к

конфиденциальным данным, управлять их уровнем и контролировать использование информации.
Таким образом, анализ литературных источников показывает, что разработка метода обеспечения и проведение внутреннего аудита информационной безопасности автоматизированных банковских систем требует использования различных научных методик и подходов, включая анализ угроз и рисков, методы аудита, управление рисками и управление доступом к информации.

2.3. Статья

ПОЛИТИКА АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ В БАНКОВСКОМ И ФИНАНСОВОМ СЕКТОРЕ

Начну с самого основного в последние годы деловые операции в банковском и финансовом секторе все больше зависят от компьютеризированных информационных систем. В настоящее время стало невозможно отделить информационные технологии (далее ИТ) от бизнеса банков и финансовых учреждений. Необходимо уделять особое внимание вопросам корпоративного управления информационными системами в компьютеризированной среде и мерам контроля за безопасностью в целях защиты информационных и информационных систем.

Применение информационных технологий привело к значительным изменениям в методах обработки и хранения данных учреждениями банковского и финансового секторов, и в настоящее время этот сектор готов к тому, чтобы одобрить различные изменения, такие, как банковские операции через Интернет, электронные деньги, электронные чеки и электронные чеки коммерция и др., как самые современные методы оказания услуг клиентам. Телекоммуникационные сети играют каталитическую роль в расширении и интеграции информационных систем (далее ИС) внутри учреждений и между ними, облегчая доступ к данным для различных пользователей. С учетом исключительно важного значения ИУ необходимо постоянно следить за безопасностью финансовых систем. Структурированные, четко определенные и задокументированные стратегии, стандарты и руководящие принципы безопасности закладывают основу для надежной безопасности ИС, и каждое учреждение обязано определять, документировать, передавать, осуществлять и проверять безопасность ИС для обеспечения конфиденциальности, целостность, достоверность и своевременное предоставление информации, которая имеет первостепенное значение для деловых операций.

Банки должны внедрить надежную систему внутреннего аудита. В целях укрепления доверия к инспекционной системе при выявлении случаев мошенничества/злоупотребления служебным положением необходимо принять необходимые меры для усиления инспекционно-ревизионного механизма и повышения квалификации должностных лиц инспекционного отдела. Инспекционный отдел в штаб-квартире должен возглавлять достаточно высокопоставленный офицер, подчиняющийся непосредственно президенту. Даже если у банка есть региональные офисы, должен быть механизм аудита под руководством высокопоставленного сотрудника в качестве главы регионального офиса для проведения периодических аудитов филиалов, находящихся под их юрисдикцией. Офицеры, размещенные в этом отделе, должны иметь достаточный опыт и знания.

Развитие информационных технологий оказывает огромное влияние на проведение ревизий. Информационная технология способствовала реорганизации

традиционных бизнес-процессов в целях обеспечения эффективного функционирования и улучшения связи внутри организации и между организациями и ее клиентами. Аудит в компьютеризованной и сетевой среде в Кыргызстане все еще находится в зачаточном состоянии, а установившаяся практика и процедуры эволюционируют. Хорошо спланированный и структурированный аудит необходим для управления рисками и мониторинга и контроля информационных систем в любой организации.

Аудит ИС представляет собой систематическое независимое изучение информационных систем и окружающей среды для определения того, достигнуты ли поставленные цели. Аудит также описывается как непрерывный поиск соответствия. Аудиторы могут не обязательно проверять всю систему. Они могут рассматривать только часть или части ее. Аудит охватывает прежде всего следующие широкие основные области деятельности :

а) сбор информации

Ь) сопоставление информации и

с) спрашивая, почему

Виды аудита: Для категоризации аудита применяются различные методы . Одним из таких методов классификации является разделение аудита на два типа, например, аудит адекватности (также называемый системным аудитом) и аудит соответствия. Другой метод позволяет классифицировать аудит по уровням - внутренний аудит, внешний аудит. Еще одним методом категоризации является ревизия сторонами - Первой стороной, Второй стороной и Третьей стороной. Наиболее распространенными видами ревизий являются финансовый аудит, аудит соблюдения требований, аудит информационных систем и аудит операций.

Факторы, которые следует учитывать для обеспечения информационной безопасности банков Кыргызской Республики:

Обеспечение информационной безопасности в банковской сфере Кыргызской Республики является критически важной задачей. Некоторые из факторов, которые следует учитывать для обеспечения информационной безопасности в банках Кыргызской Республики, включают в себя:

- Законодательные требования: Банки Кыргызской Республики должны соблюдать требования Положения об информационной безопасности и других соответствующих законов, например, Закон о банковской тайне.
- Угрозы безопасности: Банки должны учитывать различные угрозы информационной безопасности, такие как кибератаки, вредоносное ПО, фишинг, внутренние угрозы и другие.
- Риски и уязвимости: Банки должны регулярно оценивать свои системы и процессы на наличие рисков и уязвимостей, которые могут привести к утечке информации или другим нарушениям безопасности.
- Управление доступом: Банки должны иметь строгую политику управления доступом, которая ограничивает доступ к конфиденциальной информации только необходимым сотрудникам.
- Контроль и мониторинг: Банки должны контролировать и мониторить все свои системы и процессы, чтобы обнаружить любые нарушения безопасности.
- Культура безопасности: Банки должны создать культуру безопасности внутри организации, которая будет способствовать повышению осведомленности сотрудников о проблемах безопасности и снижению рисков.

- Обучение и подготовка: Банки должны обучать своих сотрудников и регулярно проводить учения и тренировки для того, чтобы быть готовыми к возможным инцидентам информационной безопасности.
- Сотрудничество с другими банками: Банки должны сотрудничать друг с другом и с органами государственного управления для обмена информацией об угрозах безопасности и разработки лучших практик в области информационной безопасности.

Учет этих факторов поможет банкам Кыргызской Республики обеспечить надежную информационную безопасность, защитить конфиденциальность и целостность своей информации, а также уменьшить риски утечки и нарушений безопасности. Это важно для сохранения доверия клиентов, защиты банковских средств и поддержания стабильности финансовой системы в целом.

Я могу назвать несколько примеров , связанных с политикой аудита информационных систем в банковском и финансовом секторе Кыргызстана:

1. Атака на системы банка "Айыл Банк": В 2020 году банк "Айыл Банк" подвергся кибератаке, в результате которой было украдено около 1,7 миллиона сомов. Это привело к необходимости проведения аудита информационных систем банка, чтобы убедиться в их безопасности и предотвратить подобные инциденты в будущем.
2. Нарушение безопасности в системе электронных платежей "Elsom": В 2019 году в системе электронных платежей "Elsom" произошла утечка данных, в результате которой были скомпрометированы личные данные более 1,5 миллиона пользователей. Это привело к необходимости проведения аудита безопасности и информационных систем компании, чтобы улучшить их защиту и предотвратить подобные инциденты в будущем.
3. Атака на системы Кыргызского национального банка: В 2016 году Кыргызский национальный банк был атакован хакерами, в результате которой были украдены личные данные более 1,5 миллиона граждан. Это привело к необходимости проведения аудита безопасности и информационных систем банка, чтобы улучшить их защиту и предотвратить подобные инциденты в будущем.
4. Нарушение безопасности в системе онлайн-банкинга "Optima Bank": В 2018 году в системе онлайн-банкинга "Optima Bank" произошла утечка данных, в результате которой были скомпрометированы личные данные клиентов банка. Это привело к необходимости проведения аудита безопасности и информационных систем банка, чтобы улучшить их защиту и предотвратить подобные инциденты в будущем.

Заключение

Из громких случаев нарушения политики аудита информационных систем в банковском и финансовом секторе Кыргызстана становится очевидно, что безопасность информационных систем является одной из наиболее важных задач в данной отрасли. Эти случаи подчеркивают необходимость регулярного аудита и мониторинга, а также строгих политик и процедур в области информационной безопасности.

В связи с этим, финансовые учреждения должны принимать все возможные меры для защиты конфиденциальных данных своих клиентов, включая обновление информационных систем, проведение тестирования на проникновение и обучение персонала. Кроме того, финансовые учреждения должны работать в тесном сотрудничестве с органами правопорядка и регуляторными органами, чтобы обеспечить максимальную безопасность и защиту данных.

В целом, существует необходимость в постоянном улучшении политики аудита информационных систем в банковском и финансовом секторе, чтобы защитить клиентов от потенциальных киберугроз и обеспечить надежность финансовых операций.

Список литературы

1. Аудит информационной безопасности. Авторы - Под общей редакцией А. П. Курило. Год издания – 2006г.
2. Аудит информационной безопасности. Автор - В. И. Аверченков Год издания – 2002г.
3. Издательство «Грамота» 2006-2023, научная статья на тему: Особенности информационной безопасности банковских систем и меры по ее обеспечению, Журавлева Валерия Вадимовна, Целых Александр Николаевич, Южный федеральный университет,
4. Международный научно-исследовательский журнал, научная статья на тему: Об аудите в информационной среде банка, Магистрант, Байкальский государственный университет экономики и права, Бухарова В.В. Выпуск: № 10 (17), 2013

ЗАКЛЮЧЕНИЕ

В современном мире информационная безопасность является одним из самых актуальных и важных вопросов, особенно в банковской сфере, где конфиденциальность и надежность хранения данных играют ключевую роль. Разработка метода обеспечения и проведение внутреннего аудита информационной безопасности автоматизированных банковских систем является необходимым условием для защиты от внутренних и внешних угроз, предотвращения потери данных, взломов и других видов нарушений безопасности.

В результате анализа литературных источников можно выделить ряд методов и подходов, которые могут быть использованы для разработки эффективного метода обеспечения информационной безопасности автоматизированных банковских систем. В частности, это методы анализа угроз и уязвимостей, аудита, управления рисками и управления доступом к информации.

Важно отметить, что разработка такого метода должна основываться на соблюдении всех нормативных требований и стандартов в области информационной безопасности, а также учитывать специфику банковской деятельности и особенности используемых автоматизированных систем.

В целом, разработка метода обеспечения и проведение внутреннего аудита информационной безопасности автоматизированных банковских систем является сложным, но необходимым процессом, который позволяет обеспечить надежность и защиту банковских данных, а также снизить риски возникновения инцидентов и ущерба для банка.