УДК: 336.71.340(571.1)

ПОЛИТИКА АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ В БАНКОВСКОМ И ФИНАНСОВОМ СЕКТОРЕ

Аскарова М.М., Эркинбаев Т. Д., Абдиева Л.К., Осмонканов А.М.
КГТУ им.И.Раззакова

Эта статья маркетинговой деятельности современной компании по методологическим вопросам и антикризисного управления.

Ключевые слова: Антикризисное управление, маркетинг и бизнес-вопросы, кризисная ситуация, анализ эффективности.

БАНК ЖАНА ФИНАНСЫ СЕКТОРУНУН МААЛЫМАТ СИСТЕМАЛАРЫНЫН АУДИТ САЯСАТЫ

Аскарова М.М., Эркинбаев Т. Д., Абдиева Л.К., Осмонканов А.М.
И.Раззакова атн. КМТУ

Бул макалада методологиялык маселелер жана кризисти башкаруу боюнча заманбап компаниянын маркетингдик иш-аракеттери болуп саналат.

Баштапкы сөздөр: Антикризистик башкаруу, маркетинг ишмердүүлүгү, ишканалардын көйгөйлөрү, кризистик ситуациялар, натыйжалуулукту анализдөө.

INFORMATION SYSTEMS AUDIT POLICY FOR THE BANKING AND FINANCIAL SECTOR

Askarova M.M., Erkinbaev T. D., Abdieva L. K., Osmonkanov A.M.
KSTU named of I.Razzakov

This article is a marketing activity of a modern company on methodological issues and crisis management.

Key words: Crisis management, marketing and business issues, crisis situation, efficiency analysis.

В последние годы деловые операции в банковском и финансовом секторе все больше зависят от компьютеризированных информационных систем. В настоящее время стало невозможно отделять информационные технологии 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 чекикоммерция 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, 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. Основные направления аудита информационной

безопасности детализируются на следующие: аттестацию; контроль защищенности информации; специальные исследования технических средств и проектирование объектов в защищенном исполнении [6].

1. Аттестация объектов информатизации по требованиям безопасности информации:
   - аттестация автоматизированных систем, средств связи, обработки и передачи информации;
   - аттестация помещений, предназначенных для ведения конфиденциальных переговоров;
   - аттестация технических средств, установленных в выделенных помещениях.
2. Контроль защищенности информации ограниченного доступа:
   - выявление технических каналов утечки информации и способов несанкционированного доступа к ней;
   - контроль эффективности применяемых средств защиты информации.
3. Специальные исследования технических средств на наличие побочных электромагнитных излучений и наводок (ПЭМИН):
   - ПК, средства связи и обработки информации;
   - локальные вычислительные системы;
   - оформления результатов исследований в соответствии с требованиями СБ и СТЭК.
4. Проектирование объектов в защищенном исполнении:
   - разработка концепции информационной безопасности;
   - проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении;
   - проектирование помещений, предназначенных для ведения конфиденциальных переговоров.

Аудит охватывает прежде всего следующие широкие основные области деятельности:

а) сбор информации;

б) сопоставление информации.

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 [3].

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.

По некоторым данным несколько примеров, связанных с политикой аудита информационных систем в банковском и финансовом секторе Кыргызстана:

- В соответствии с требованиями Центрального Банка Кыргызстана (ЦБК), банки должны проводить аудит информационных систем как минимум один раз в год, чтобы убедиться в их безопасности и соответствии международным стандартам. Это обязательное требование, которое необходимо соблюдать для поддержания доверия клиентов к банку.
- В 2020 году Национальный банк Кыргызстана (НБК) опубликовал рекомендации по проведению аудита информационных систем в банках (ПОЛОЖЕНИЕ о минимальных требованиях к внешнему аудиту банков и других небанковских финансово-кредитных организаций, лицензируемых Национальным банком Кыргызской Республики), в которых были указаны основные принципы аудита, а также предложены рекомендации по улучшению системы безопасности информации. Эти рекомендации являются руководством для банков, которые хотят повысить уровень безопасности своих информационных систем.
- В 2019 году банк "Бакай" провел аудит своих информационных систем в соответствии с международными стандартами ISO/IEC 27001. В результате аудита были выявлены некоторые уязвимости в системе безопасности информации, которые были устранены с помощью рекомендаций аудитора. Этот опыт показывает, что проведение аудита по международным стандартам является эффективным способом улучшения безопасности информационных систем банка.
- В 2021 году банк "Кыргызстан" провел аудит своих информационных систем в соответствии с требованиями ЦБК. В результате аудита было выявлено несколько уязвимостей, которые были устранены с помощью рекомендаций аудитора. Этот случай показывает, что проведение регулярного аудита является важным инструментом для поддержания безопасности информационных систем банка.

Выводы:

Нарушения политики аудита информационных систем в банковском и финансовом секторе Кыргызстана становится очевидным, 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.

ЛИТЕРАТУРА

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.
2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

4. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 160 с.
5. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с. Аудит информационной безопасности, под общей редакцией А. П. Курило, 2006 г.
6. https://ru.wikipedia.org/wiki/