Проведенное исследование показало, что несмотря на большую значимость прибыли предприятий в рыночной экономике, недостаточно внимания уделяется ее максимизации. Комплексное выполнение предложенных мероприятий позволит повысить прибыль предприятий, что положительно отразится на всех субъектах хозяйствования.

Список использованной литературы:

1. Акулич, В. В. Прибыль организации: оцениваем и управляем / В.В. Акулич // Планово–экономический отдел. – 2013. – № 1. – с. 103–107
2. Кириллова, Л. Н. Виды прибыли в системе управления прибылью / Л.Н. Кириллова // Экономический журнал. – 2009. – № 16. – с.57-76
3. Поздняков, В. Я. Экономика предприятия (организации). 4-е изд., перераб. и доп. / В. Я. Поздняков. – М.: ИНФРА-М, 2010 – 640с.
4. Шеремет, А. Д. Бухгалтерский учет и анализ: учебник / А.Д. Шеремет, Е.В. Старовойтова. - М.: ИНФРА-М, 2014. - 425 с.

© А.И. Коротков, Э.Э. Шамилева, 2015

УДК 336.71.078.3

М.Д. Костин, А.А. Удалов
студенты 2 курса кафедры «Финансы и кредит»
Научный руководитель: **А.В. Шляпкин**
к.т.н., доцент кафедры «Прикладная информатика в экономике»
Поволжский государственный университет сервиса
г. Тольятти, Российская Федерация

РАЗВИТИЕ IT В БАНКОВСКОМ СЕКТОРЕ: ПОТРЕБНОСТЬ В УСИЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ.

Аннотация:

Условия оказания банковских услуг в соответствии с необходимостью обеспечения информационной безопасности; рассмотрены возможные расходы на организацию финансовой безопасности в кредитных организациях, определены основные этапы организации и поддержки функционирования систем информационной безопасности.

Ключевые слова:

Функционирование кредитных учреждений, автоматизация банковских информационных технологий, информационная безопасность.

В наши дни технологические и технические элементы деятельности банков и других кредитных организаций невозможно представить без информационных технологий, позволяющих минимизировать банковские риски и максимально полно и оперативно удовлетворить потребности клиентов. Иными словами, оказание практически любой банковской услуги тесно связано как с техническими возможностями банка, так и с его временными и материальными затратами на их реализацию, т.е. с его информационной системой.

За всю историю возникновения и совершенствования информационные системы прошли длительный путь развития – начиная простейшими СУБД (системами управления базами данных), разработанными на персональных компьютерах, такими как dBase, Clipper, и заканчивая суперсовременными промышленными СУБД на базе клиент/серверных решений (Oracle, Sybase), которые позволяют автоматизировать практически все банковские бизнес-процессы – управление кадрами, ликвидностью, банковскими рисками и пр. [1]

Приходя в банк за тем или иным банковским продуктом, клиентов часто интересуют:

- техническая оснащенность предлагаемых сервисов,

- возможность настройки требуемых данных,
- платформа, являющаяся базой для реализации и поддержки,
- и, наконец, степень защищенности сервисных и информационных каналов.

В целом, сегодня этим требованиям удовлетворяет большая часть информационных систем для кредитных организаций, имеющихся на рынке программных продуктов. [1]

Во избежание рисков возникновения внешних и внутренних угроз для информационной безопасности банков и других организаций-представителей банковской системы РФ важно обеспечить и сохранить максимально высокий её уровень.

Именно для этого Банком России и был разработан Стандарт СТО БР ИББС . Его основными целями являются:

- повышение уровня доверия юридических и физических лиц к банковской системе РФ,
- повышение стабильности работы кредитных организаций в частности и всей банковской системы страны в целом,
- предотвращение и/или сведение к минимуму случаев нанесения ущерба в случаях нарушения информационной безопасности,
- достижение достаточных мер для защиты от возможных угроз информационной безопасности. [2]

На сегодняшний день прогресс в направлении внедрения вышеупомянутого стандарта очевиден: 41,7% российских банков уже применяют на практике некоторые положения стандарта, 40,8% кредитных организаций приняли решение о внедрении этого нормативного документа в ближайшем будущем. [3]

Также «Global Security Survey» было проведено исследование, в результате которого представителями компании Delloite были опрошены 169 международных финансовых институтов. Как оказалось, 44% компаний тратят на информационную безопасность 1-3% от IT-бюджета, а у 36% аналогичные расходы составляют 4-6%. По результатам исследования было выяснено, что кредитные организации готовы больше вкладывать в совершенствование системы информационной безопасности, а также говорить об этом вопросе публично.

Согласно исследованиям CNews Analytics в России банковский сектор, как и вертикальный рынок телекоммуникаций, занимают первое место по расходам на информационную безопасность. При этом в целом доля затрат на обеспечение информационной безопасности в единичных случаях превышает 1,5% совокупного объема IT-затрат, причем такая тенденция наблюдается во всех секторах экономики. [3]

В настоящее время представители банковской системы России ведут работы по организации единого центра обработки данных, неуклонному повышению уровня надежности IT-инфраструктуры, а также реализации актуальных сегодня проектов разработки единого информационного пространства банка с учетом имеющихся требований для перехода на единую централизованную обработку данных.

Развитие информационных систем для организаций-представителей банковской системы РФ включает создание и совершенствование центров обработки данных, коммуникационных каналов, наращивание серверных мощностей, причем как для распределенности бизнеса территориально, так и для обеспечения достаточных мощностей, соответствующих объемам производимых операций.

Совершенствование этих направлений поможет упростить и облегчить бизнес-процессы, унифицировать рабочие процессы внутри организации, позволит развить достаточно высокое качество специализации и распределения труда. Централизованное выполнение функций поддержки и основных процессов, которое обеспечивается за счет дистанционных систем обслуживания клиентов и достаточных мощностей, станет благоприятной почвой для эффективного развития банковского сектора и роста качества оказываемого сервиса вне зависимости от территориального расположения кредитной организации.

Всем перечисленным требованиям отвечает современная технология «прозрачной ЭП», обеспечивающая высокий уровень безопасности для организаций, являющихся клиентами банка, которые используют систему ПТК «Интернет-банк» для управления своими счетами. Высочайший уровень защиты обеспечивается благодаря многоуровневой аутентификации. Так, помимо стандартных логина и пароля клиент получает от банка eТокеп ГОСТ - уникальный защищенный носитель, позволяющий защитить хранящуюся на нем информацию как на физическом уровне, так и на программном.

Сегодня представители банковской системы РФ постоянно развивают свои системы информационной безопасности, повышая уровень защиты, и внедряют такие подсистемы, как:

- Автоматизированный контроль выдачи ссуд на основе модуля выдачи кредитных решений – необходим для исключения ошибок и возможных злоупотреблений, имеющих место при заключении кредитного договора.
- Подсистема, позволяющая корректировать открытую валютную позицию (ОВП) и обеспечивающая централизованную оценку с учетом валютных операций, проводимых другими подразделениями.
- Модуль «АРМ Руководителя 2.0», позволяющий руководящему составу получать текущие данные о работе подразделения с максимальной детализацией, включая первичные документы.
- Система контроля текущей деятельности в многофилиальной версии, способная самостоятельно анализировать работу различных информационных систем и на основе результатов анализа давать рекомендации по корректировке ситуации.

В целях повышения качества и уровня информационной безопасности в кредитных организациях были введены такие нормативные стандарты, как:

1. СТО БР ИББС – 1.0-2010 – Стандарт Банка России по информационной безопасности,
2. PCI DSS v. 2.0 – Стандарт международных платежных систем.

В целом работа кредитных организаций, связанная с повышением уровня информационной безопасности, должна соответствовать вышеуказанным стандартам.

Кроме того, банкам рекомендуется организовывать мероприятия по обучению персонала и повышению осведомленности в вопросах защиты информации, по рассмотрению инцидентов, связанных с нарушением информационной безопасности, а также повышать уровень информационной безопасности в филиалах.

Список использованной литературы:

1. Тютюн, А.В. Банковские информационные технологии // Информационный портал: Банки. Деньги, инвестиции, бизнес [Электронный ресурс]. URL: http://www.bankmib.ru/3204 (дата обращения 16.04.2015).
2. Обеспечение информационной безопасности организаций банковской системы Российской Федерации [Электронный ресурс]. URL: http://www.cbr.ru/credit/Gubzi_docs/ (дата обращения 18.04.2015).
3. Исследование: Информационная безопасность в банках. Общий взгляд // Research paper: Perimetrix [Электронный ресурс]. URL: http://perimetrix.ru/downloads/rp/PMX_Information_Security_in_Banks.pdf (дата обращения 19.04.2015).

© М.Д. Костин, А.А. Удалов, А.В. Шляпкин, 2015

УДК 613.83

М.Д. Костин, А.А. Удалов,
студенты 2 курса кафедры «Финансы и кредит»
Научный руководитель: **Е.А. Васильева**
к.э.н., доцент кафедры «Бухгалтерский учет, анализ и аудит»
Поволжский государственный университет сервиса
г. Тольятти, Российская Федерация

СТАТИСТИКА ПОТРЕБЛЕНИЯ «КУРИТЕЛЬНЫХ СМЕСЕЙ» НА ТЕРРИТОРИИ САМАРСКОЙ ОБЛАСТИ: ФАКТЫ И КОММЕНТАРИИ

Аннотация

Рассмотрена информация о первом появлении курительных смесей и статистики количества пострадавших от «спайсов» в Самарской области. А также представлены некоторые комментарии на сложившуюся ситуацию и реальные результаты препятствия распространению наркотических веществ.