DOI: 10.17117/na.2016.01.01.445

<http://ucom.ru/doc/na.2016.01.01.445.pdf>

Поступила (Received): 10.01.2016

Ксенофонтов А.С., Арванова С.М., Губжоков А.З. Актуальные механизмы безопасности банка

Ksenofontov A.S., Arvanova S.M., Gubzhokov A.Z.
Current mechanisms for bank security

В работе проводится анализ модели для обеспечения безопасности банка

Ключевые слова: политика информационной безопасности, коммерческая тайна, утечка информации, конфиденциальность

Ксенофонтов Александр Семенович

Кандидат физико-математических наук, заведующий кафедрой

Кабардино-Балкарский государственный университет им. Х.М. Бербокова
г. Нальчик, ул. Чернышевского, 173

Арванова Саният Мухамедовна

Ассистент

Кабардино-Балкарский государственный университет им. Х.М. Бербокова
г. Нальчик, ул. Чернышевского, 173

Губжоков Ахмед Замирович

Студент

Кабардино-Балкарский государственный университет им. Х.М. Бербокова
г. Нальчик, ул. Чернышевского, 173

The paper analyzes the model for bank security anies

Key words: information security policy, trade secret, information leakage, confidentiality

Ksenofontov Alexander Semenovich

Candidate of Physical and Mathematical Sciences, Head of Department

Kabardino-Balkarian state university named Kh.M. Berbokov
Nalchik, Chernyshevskogo st., 173

Arvanova Saniyat Mukhamedovna

Assistant

Kabardino-Balkarian state university named Kh.M. Berbokov
Nalchik, Chernyshevskogo st., 173

Gubzhokov Ahmed Zamirovich

Student

Kabardino-Balkarian state university named Kh.M. Berbokov
Nalchik, Chernyshevskogo st., 173

Политика информационной безопасности – важный стратегический инструмент защиты критического бизнес-ресурса любого банка, его конфиденциальной информации[1]. Для построения всеобъемлющей политики информационной безопасности, экономически эффективной и адекватной интересам банка необходим комплексный, системный подход. Политика информационной безопасности должна разрабатываться профессионалами из области информационной безопасности в тесном взаимодействии с ведущими аналитиками, IT-специалистами и руководством банка.

Безопасность банка, как и любого экономического хозяйствующего субъекта бизнеса складывается из многих составляющих, среди которых можно выделить: стратегию работы с клиентами, сохранение собственного персонала (уровень лояльности), работа с партнерами и конкурентами. Предотвращение

использования кредитных организаций в недобросовестной коммерческой практике является одной из приоритетных задач в развитии банковского сектора. Для выявления и пресечения деятельности отдельных экономических субъектов, вовлекающих банковскую систему в криминальную деятельность и использующих ее в целях отмывания преступных доходов необходимо взаимодействие банков с органами финансового надзора.

Для любого банка критически важным ресурсом ведения бизнеса является информация. Банковская информация сохраняется в корпоративных сетях банка, а также передается по внешним, неконтролируемым вычислительным сетям общего доступа (например, Интернет). Огромная доля коммерческой информации сосредотачивается в информационной вычислительной системе банка. Данные из информационной вычислительной системы используются операторами, менеджерами, а также партнерами и клиентами посредством веб-представительства банка в Интернете (Рис.1).

Рис. 1. Модель системы безопасности банка

Обеспечение информационной безопасности является важнейшей составляющей частью выполнения задачи обеспечения экономической безопасности бизнеса в целом. Экономически ценная информация используется при работе с клиентами, партнерами, внутри банка; к ней имеет непосредственный доступ персонал банка, а так же существует множество внешних злоумышленников, заинтересованных в организации несанкционированного доступа к интересующей их секретной информации.

Любые действия пользователей на компьютерах и в сетях приводят к перемещению или к обработке информации. Кроме того, информация находится в стадии хранения на информационных ресурсах. Любое финансовое учреждение занимается сбором и обработкой данных независимо от своих функций и целей. Кредитные организации учитывают важные аспекты обработки данных в своих операциях, включая различные учеты, автоматизацию производства, аналитическую и управленческую деятельность.

Руководство банка должно понимать важность обеспечения безопасности информационных ресурсов и иметь представление о том, какие правила информационной безопасности необходимы для эффективного баланса между защитой и оперативностью функционирования организации.

Относительно каждого банковского процесса информационное воздействие происходит с двух направлений: "сверху" и "снизу", с "внешней" и "внутренней" стороны. Например, законы государства, определяющие банковское регулирование, действуют на конкретный банковский процесс "сверху", оговаривая рамки свободной деятельности банка при проведении операций. В каждом банке своя структура подразделений, где действуют свои внутренние технологии и инструкции, задача которых направлять процессы к целевым потребностям. К внешнему сектору информации относятся данные о банковских процессах, которые созданы внешними регулируемыми органами (законы, нормативные акты и Банка России и т. п.). К внутреннему сектору информации относятся данные об организации и ведении процессов, созданные внутри самого банка.

Рис. 2. Схема информационного взаимодействия банка с внешним миром

На схеме (Рис.2) изображены наиболее значимые сущности экономического взаимодействия банка с внешним миром, каждая из которых осуществляет активный информационный обмен с банком. Безопасность этого обмена, в том числе и доступность каналов связи и скорость обмена данными, определяет экономический успех банковской деятельности.

Важной составляющей является и репутация банка, необходимо обеспечить ее защиту от внешних и внутренних посягательств[2]. Политика безопасности банка является приоритетным стратегическим документом, отражающий концепции банка в сфере обеспечения безопасности своей экономической деятельности.

Список используемых источников:

1. Мельников В.П., Клейменов С.А., Петраков А.В. Информационная безопасность. Академия, 2013. С. 336.
2. Арванова С.М. Криптографические механизмы безопасности // Научный альманах. 2015. №7(9). С. 578–580.

© 2016, Ксенофонов А.С., Арванова С.М.,
Губжиков А.З.
Актуальные механизмы безопасности банка

© 2016, Ksenofontov A.S., Arvanova S.M.,
Gubzhikov A.Z.
Current mechanisms for bank security