**УДК 343.335**

***Е. Ю. Долгих, С. П. Богунов***
*Кузбасский государственный технический университет им. Т.Ф. Горбачева, Кемерово, Россия*

# СОВРЕМЕННЫЕ МЕТОДЫ И СПОСОБЫ БОРЬБЫ С МОШЕННИЧЕСТВОМ В БАНКОВСКОЙ СФЕРЕ РОССИИ

научный руководитель: д.ф.н., профессор кафедры истории, философии и социальных наук Золотухин В.М.

В статье рассматриваются вопросы разработки и применения современных методов и способов борьбы с мошенничеством в российской действительности на примере деятельности Сбербанка России. Рассмотрены различные аспекты мониторинга и контроля банковской деятельности как на уровне самого банка, так и его сотрудников. Подчеркивается необходимость создания не только эффективных технологических механизмов по защите банковских вкладов от различных видов мошенничества, но и социокультурной среды, исключающей возможность совершения противоправных действий.

**Ключевые слова**: мошенничество, борьба, экономические риски, акции, банковская сфера

В современных социально-экономических условиях различные виды мошенничества, чаще всего связаны с банковской сферой. Одной из эффективных мер противодействия банковским мошенничествам является создание независимых органов для расследований экономических преступлений. Речь, прежде всего, идет о внешним аудите как органе, посредством которого возможен сбор легитимных доказательств противоправной деятельности. Службы внешних аудиторов позволяют снижать риски финансовых мошенничеств, а также эффективно проводить расследования противоправных деяний. Внешние аудиторы должны обладать достаточным багажом правовых, экономических и иных знаний, который позволят им оценить финансовую деятельность банковских структур не только с точки зрения осуществления технологических операций в банковской сфере, но и способны дать оценку степени влияния тех или иных операций на работников и клиентов баков. Немаловажным аспектом является оценка степени риска, понесенного банком из-за совершения мошенничества.

Работа внешних аудитов состоит из несколько этапов:

Первый этап включает диагностику, в рамки которой входит:

• Диагностика систем контроля банка и оценка других сфер функционирования;

• Анализ финансовой информации;

• Проведение интервью с сотрудниками банка;

• Анализ публичных источников информации о топ-менеджерах.

Следующим шагом специалистом извне, как правило, следует расследование потенциальных случаев мошенничества:

• Расследование случаев, выявленных на 1 этапе;

• Сбор данных о топ-менеджменте из непубличных источников;

• Оценка ущерба от мошенничества.

Заключительным этапом является составление отчета и формулирование рекомендаций, которые включают в себя:

• Рекомендации по возврату активов;

• Рекомендации по совершенствованию системы безопасности.

Заключительный этап проводится с целью оценки экономических рисков, репутации банка, поиск активов, проверка контрагентов, клиентов и сотрудников банка на их благонадежность, в то же время ведется поиск различных связей между сторонами. При корпоративной разведке специалисты используют внутреннюю информацию, а также иные открытые источники информации.

Количество осужденных лиц по статьям УК РФ [УК РФ, 1996], связанных с мошеннической деятельностью представлено в таблице 1 [Судебная статистика, 2019]. Как можно заметить, количество преступлений в РФ в банковской сфере уменьшается.

Для уменьшения противоправных действий в отношении к деятельности банка необходимо разрабатывать теоретические схемы их преодоления и применять на практике, в том числе это относится к проведению профилактических мер. В качестве примера, может является профилактическая деятельность банка по безопасному использованию клиентами банковских карт. Банковские структуры ведут активные теоретические исследования по противодействию мошенничеству в банковской сфере, которые обусловлены требованиями государства по максимальной защите банковских вкладов и карт в современной российской социокультурной реальности [Золотухин В.М., Степанцова, 2015].

Таблица 1

Данные о назначенном наказании по статьям УК за 2016-2018 г.г

| Год | 2016 | 2017 | 2018 |
|---|---|---|---|
| ст. 176 УК РФ Незаконное получение кредита | 75 | 73 | 55 |
| Ст. 183 УК РФ Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну | 46 | 35 | 22 |
| ст. 159, 159.1-159.6 УК РФ Мошенничество | 28776 | 30 464 | 24 195 |
| Ст. 172 УК РФ Незаконная банковская деятельность | 125 | 233 | 323 |

В последние годы в РФ наблюдаются несколько тенденций совершенствования внутренних мер по противодействию финансовым преступлениям в банковской сфере:

- постоянное увеличение инвестиции в инфраструктуру по противодействию финансовой преступности в банках;

- в определение «финансовые преступления» включены внутренние и внешние виды мошенничества, злоупотребления сотрудников банковской сферы, действия по легализации доходов, полученных преступным путем, случаи взяточничества и коррупции, а также кибер-преступления;

- созданы интегрированные подходы, охватывающие все уровни банка и использующие различные современные аналитические инструменты.

На примере публичного акционерного общества «Сбербанк» как одного из российских финансовых конгломератов и крупнейшего транснационального банка России, Центральной и Восточной Европы можно рассмотреть разрабатываемые меры и способы защиты от мошенничества в банковской сфере. Дан-

ный выбор обусловлен тем, что он контролируется Центральным банком Российской Федерации, которому принадлежит 50 % уставного капитала плюс одна голосующая акция [Банк России, 2020].

Одной из причин внимания к данному баку стала ситуация, когда база данных с подробной информацией о владельцах 60 млн. кредитных карт, как действующих, так и закрытых Сбербанка оказалась на черном рынке примерно в конце августа 2019 года. Эксперты, считают их подлинными и называют данную утечку самой крупной в российском банковском секторе. Сбербанк сообщил о проводимых мероприятиях в связи с утечкой информации и заверил своих клиентов в том, что денежная масса с их счетов и карт не будет потеряна.

Специалисты из центробанка также изучили «пробник» и выразили уверенность в том, что утечка информации могла произойти только из самого банка и, может быть связана с деятельностью самого банка и/или его сотрудников банка [Козырева, Криони, Морозов, 2019].

Газета «Коммерсант» сообщила, что на специализированном форуме, заблокированном Роскомнадзором, появилось объявление о продаже «свежей базы крупного банка» [Новость об утечки, 2019].

Продавец предлагал данные о более 60 млн. кредитных карт. Сбербанк заявил, что проверяет информацию о возможной утечке данных 60 млн. клиентов, но считает ее некорректной, так как банком всего было выпущено 40 млн. кредитных карт.

Аналитик и управляющий партнер BMS Group Алексей Матюхов считает, что Сбербанк — один из самых крупных операторов персональных данных, и информация об утечках должна повлиять на акции такой компании. В то же время Матюхов обратил внимание: Сбербанк — окологосударственная структура. Из-за этого репутационные потери окажутся не столь сильными. [Могут, 2019].

График динамики курса акций ПАО Сбербанк России представлен на рисунке 1 [Динамика, 2019]. На 3.10.19, в день, когда служба безопасности узнала про утечку, курс составлял 224.08 рубля, а на следующий день 222.76 рубля.

Как можно заметить, утечка данных не сильно повлияла на курс акций компании, а через небольшой промежуток времени показали уверенный рост, что может говорить нам о том, что инцидент не испортил репутацию Сбербанка в глазах акционеров.

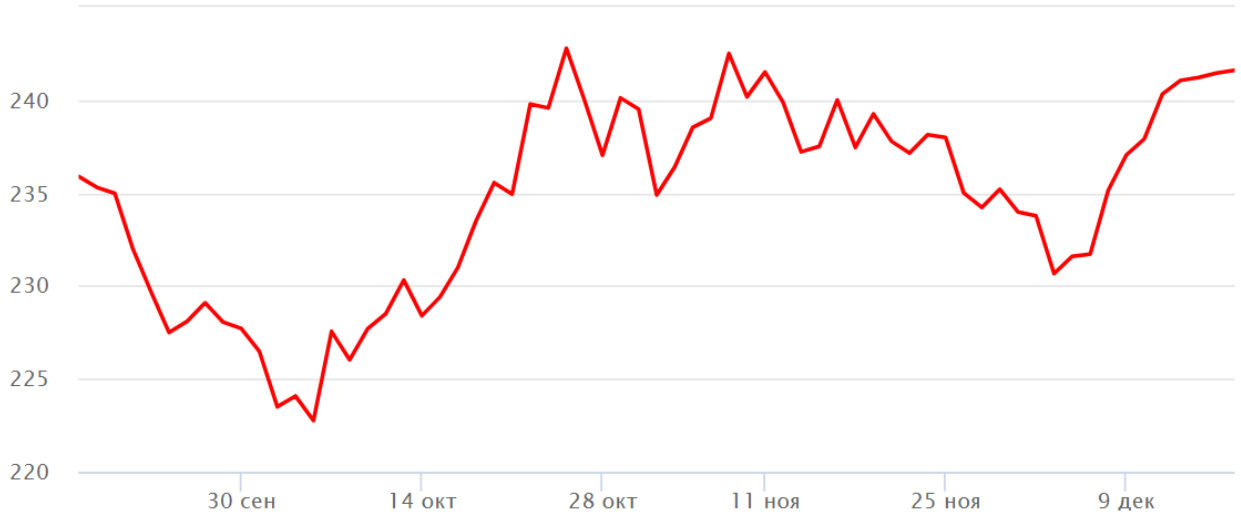


Рисунок 1 – График динамики курса акций ПАО Сбербанк России с 17.09.19 по 17.12.19 (руб., MOEX)

Утечка персональных данных очень опасна для граждан, информация о которых оказалась в публичном доступе. К сожалению, сейчас, как никогда, очень распространены мошеннические схемы с использованием ворованных паспортных данных. Это документ, по которому могут:

1) оформить на вас кредит;

2) повесить чужой долг или оформить фирму;

3) совершить незаконные действия с вашей недвижимостью;

4) распоряжаться средствами банковских карт;

5) открыть электронный кошелек;

6) использовать вашу личность для совершения мошеннических действий.

В данном случае была нарушена Статья 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну».

Сбор таких сведений любым незаконным путем может привести к штрафу до 500 тысяч рублей или наказанию до 2 лет тюремного заключения. Их разглашение третьим лицам или использование в своих целях увеличат меры финансовой ответственности до одного миллиона, свободу же можно будет потерять на срок до 3 лет. Если же злоумышленники причинили потерпевшему крупный ущерб или привели к тяжким последствиям, они могут повлечь за собой уже 5 или 7 лет тюремного заключения.

Сбербанк утверждает, что виновный – сотрудник кредитной организации, который руководил сектором в одном из бизнес–подразделений банка. Сбербанк совместно с правоохранительными органами установил виновного в утечке персональных данных клиентов. У виновного работника был доступ к базам данных клиентов в связи со своими должностными обязанностями. Данное действие было совершено «в корыстных целях» при отсутствии должно контроля за сохранностью банковской информации. Данный факт говорит о том, что в банке существовала низкая корпоративная культура, а российская социокультурная ментальность [Золотухин, Родионов, 2014], к сожалению, позволяет вариативно подходить к системам безопасности, в том числе, в банковской сфере.

По данным из Сбербанка сотрудник дал признательные показания, правоохранительные органы провели с ним процессуальные действия. В банке заверили, что больше утечек (чем о картах 200 клиентов) не будет, система безопасности банка усилила контроль за информационными ресурсами банка и будет усилена профилактическая работа среди сотрудников по формированию правовой и корпоративной культуры [Золотухин, Суслова, 2011], в том числе, через образовательные учреждения [Золотухин, Съедина, 2015]. «Мы сделали серьезные выводы и кардинально усиливаем контроль доступа к работе наших систем сотрудников банка, чтобы минимизировать влияние человеческого фактора», – приводятся в сообщении слова президента кредитной организации Германа Грефа. Он заявил, что преступление было раскрыто «в течение считанных часов» [Forbes, 2019].

**Библиографический список**

Банк России. Справочник по кредитным организациям. Открытое акционерное общество «Сбербанк России» [электронный ресурс] – Режим доступа – URL: http://www.cbr.ru/credit/coinfo.asp?id=350000004 – Дата обращения 10.12.2019.

Динамика курса акций ПАО СБЕРБАНК РОССИИ [электронный ресурс] – Режим доступа – URL: https://yandex.ru/news/quotes/60.html- (Дата обращения 11.12.2019)

Золотухин В.М., Родионов А.В. Социально-философский и социокультурный аспекты российской ментальности. // Вестник КемГУКИ, 2014. – № 4. – С. 17–24.

Золотухин В.М., Степанцова Е.В. Российская ментальность в рамках правовой нормативности. // Вестник Кемеровского государственного университета, 2015. – № 1-2 (41). – С 207–210.

Золотухин В. М., Суслова С. В. Правовая культура и образование // Вестник Кемеровского государственного университета, 2011. – № 2. – С. 178–181.

Золотухин В. М., Съедина Н. В. Готовность студентов к самоконтролю как процесс педагогического взаимодействия субъектов воспитательно-образовательного процесса // Профессиональное образование в России и за рубежом, 2015. – № 3. – С. 48–54.

Могут ли утечки клиентских данных повлиять на акции Сбербанка сайт РБК [электронный ресурс] – Режим доступа – URL: https://quote.rbc.ru/news/forecast_idea /5db1c2af9a794752c1b7a401 (Дата обращения 11.12.2019).

Новость об утечки данных клиентов Сбербанка на сайте газеты Коммерсант [электронный ресурс] – Режим доступа – URL: https://www.kommersant.ru/doc/4111863 (Дата обращения 10.12.2019)

Козырева М. В., Криони А. Е., Морозов Н. В. Социокультурный и правовой аспекты социальной деятельности субъектов в банковской сфере. // Вестник Кемеровского государственного университета. Серия Гуманитарные и общественные науки, 2019. – Т 3 № 2 (10). – С. 159–164.

Судебная статистика РФ [электронный ресурс] – Режим доступа – URL: http://stat.xn--7sbqk8achja.xn--p1ai/stats/ug/t/14/s/17 (Дата обращения 10.12.2019)

Уголовный кодекс Российской Федерации от 13.06.1996 г. №63-ФЗ (ред. от 12.11.2018 г.) // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891 (дата обращения 03.11.2019).

Forbes Герман Греф сделал «серьезные выводы» после утечки в Сбербанке [электронный ресурс] – Режим доступа – URL: https://www.forbes.ru/biznes/384915-german-gref-sdela- Дата обращения 11.12.2019 (Дата обращения 10.12.2019).

***E. Y. Dolgikh, S. P. Bogunov***
*T.F. Gorbachev Kuzbass State Technical University, Kemerovo, Russia*

## MODERN METHODS AND METHODS OF COMBATING FRAUD IN THE BANKING SECTOR OF THE RUSSIAN

supervisor: D. F. N., Professor of history, philosophy and social Sciences Zolotukhin V. M.

The article investigates modern methods and methods of combating fraud in Russian reality. On the example of the activities of Sberbank of Russia. Consideration of various aspects of monitoring banking activities of both the bank and its employees. The necessity of creating effective mechanisms to protect bank deposits from various types of fraud is emphasized.

**Keywords:** fraud, fighting, economic risks, stocks, banking**.**