Хасанова Зарина Ильшатовна
магистр экон. наук, менеджер
ПАО «Быстробанк»
г. Чебоксары, Чувашская Республика

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ КОММЕРЧЕСКОГО БАНКА

***Аннотация**: статья посвящена методам и инструментам определения финансовой безопасности коммерческих банков. Инструменты финансового обеспечения коммерческих банков включают финансовое планирование, финансовый анализ, финансовое регулирование и финансовый контроль. Особое внимание уделено внутренним и внешним методам обеспечения финансовой устойчивости коммерческих банков.*

***Ключевые слова**: коммерческий банк, финансовая безопасность, финансовая устойчивость, внешние методы, внутренние методы, инструменты.*

В современной экономической литературе проблемы методов и инструментов обеспечения финансовой безопасности недостаточно изучены. То есть в настоящее время не существует единого перечня внешних и внутренних методов и инструментов финансового обеспечения коммерческих банков. Существующая работа рассматривает только отдельные вопросы финансовой безопасности.

Безопасность коммерческого банка – это состояние защищенности интересов владельцев, руководства и клиентов, а также материальных ценностей и информационных ресурсов от внутренних и внешних угроз.

Руководит отделом безопасности всем подразделением вице-президент по безопасности, каковой имеет отношение к высшему руководству банка. В обязанности его входит вырабатывание стратегии предоставления безопасности банка, заключение проходящих вопросов с начальниками структурных подразделений и высшим руководством, взаимодействие с правоохранительными органами, контроль над выполнением поставленных перед всеми подразделения-

ми задач, решение всех ее внутренних проблем и непосредственное руководство службами собственной безопасности и экспертов-консультантов.

При рассмотрении кредитной заявки важная часть работы ложится на сотрудника службы безопасности банка. Он проверяет все предоставленные заемщиком документы. По коду ОГРН производится проверка баз данных, из которых видно местоположение предприятия, контактная информация, финансовое положение компании-работодателя и отсутствие задолженностей.

Еще необходимо проверить не является ли предприятие банкротом, не находится ли его имущество под арестом, а также делаются ли отчисления в пенсионный фонд и фонд социального страхования, соответствует ли заявленная зарплата в справке действительности. Как один из методов используются звонки на предприятие для уточнения статуса сотрудника.

Подвергаются проверке и личные данные заемщика: отсутствие судимости, психических заболеваний и наркозависимости у него и у членов семьи. После этого надо проверить наличие невыплаченных кредитных обязательств и качество кредитной истории. Учитывается поведение клиента в качестве поручителя или залогодателя по кредитам третьих лиц.

Возможно обращение в Бюро кредитных историй для получения информации обо всех кредитах клиента. При кредитовании недвижимости информация о наличии обременений отражается в выписке из Единого государственного реестра сделок с недвижимым имуществом. Данные, предоставленные заемщиком, тоже проверяет сотрудник службы безопасности.

Часто специалисты службы безопасности разных банков неофициально делятся информацией. Так могут быть получены сведения об аресте счетов предприятия или о неоплаченной картотеке к расчетному счету работодателя. Крупные банки, например Сбербанк, Альфа-Банк, имеют неформальные связи в правоохранительных органах, налоговой инспекции, что также позволяет получать необходимую информацию.

Для заемщиков-юридических лиц добавляется проверка данных основных контрагентов компании и выявление конечных собственников бизнеса. А если

находятся предприятия-партнеры, влияющие на компанию-заемщика, то они привлекаются в поручители. Это снижает риски по кредиту.

Окончательное решение по заявке кредитный комитет выносит только после получения положительного решения от службы безопасности банка.

Банковский бизнес развивается в условиях, которые носят неопределённый характер. Финансовые организации должны выстраивать целостную систему управления всеми выявляемыми банковскими рисками.

Таблица 1

Число персональных компьютеров в организациях. Данные Росстата

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Число персональных компьютеров в обследованных организациях – всего, тыс. шт.	4150,5	4558,3	5709,6	6684	7528,4	8267,3	8743,7	9288,1	9972,2	10807,5	11438,0	11740,8	11992,3	12422,1
из них:														
имевшие доступ к глобальным информационным сетям	1204,0	1513,4	2032,0	2606,3	3267,5	3873,5	4313,5	4997,1	5663,2	6508,1	7220,8	8157,5	8362,0	8782,2
в том числе к сети Интернет	986,0	1218,8	1686,1	2232,0	2888,4	3411,5	3866,4	4553,3	5198,3	6066,5	6764,4	7277,6	7561,5	8117,9
Поступило персональных компьютеров в отчётном году, тыс. шт.	656,2	743,8	984,2	1170,9	1257,9	1159,2	890,6	999,9	1251,6	1454,1	1351,5	1177,7	952,2	986,7
Число персональных компьютеров на 100 работников – всего, шт.	18	20	23	26	29	32	35	36	39	43	44	47	49	49
в том числе с доступом к сети Интернет	4	5	7	9	11	13	15	18	21	24	26	29	31	32

Таблица 2

Потери в финансовой системе России в 2016 году, млрд руб.

	Похищено	Сохранено	Всего	Эффективность хищений, %
Физ. лица	1,23	1,24	2,48	50
Юр. лица	0,38	1,12	1,51	26
АРМ КБР*	1,20	1,67	2,87	42
Итого:	2,82	4,04	6,86	41

**Автоматизированное рабочее место клиента Банка России.*

Согласно статистике, предоставленной Росстатом (табл. 1), за 13 лет произошёл прирост количества информационно-коммуникационных технологий (ИКТ) в организациях в раза, что подтверждает темпы прогресса.

Интерес представляет процент количества персональных компьютеров, имевших доступ к сети «Интернет» в общем числе персональных компьютеров в обследованных организациях, возросший с в 2003 году до в 2016 году.

По подсчётам[3] Банка России из финансовой системы России в 2016 году киберпреступниками было похищено почти 6,7 млрд руб. (табл. 2). Для сравнения: минимальный размер оплаты труда с 1 июля 2016 года составлял 7500 рублей в месяц.

Дистанционное взаимодействие всех систем и участников денежной банковско-финансовой системы – возможность цивилизации. Предоставление ссуд по сети «Интернет» и открытие депозитных счетов без визита в офис, интернет-трейдинг (онлайн-торговля), дистанционные объединённые счета (Omnibus Account), индивидуальные финансовые порталы и др.

На рис. 2 перечислены основные причины, заставляющие человека нарушить систему защиты информации организации кредитно-финансовой сферы (ОКФС).

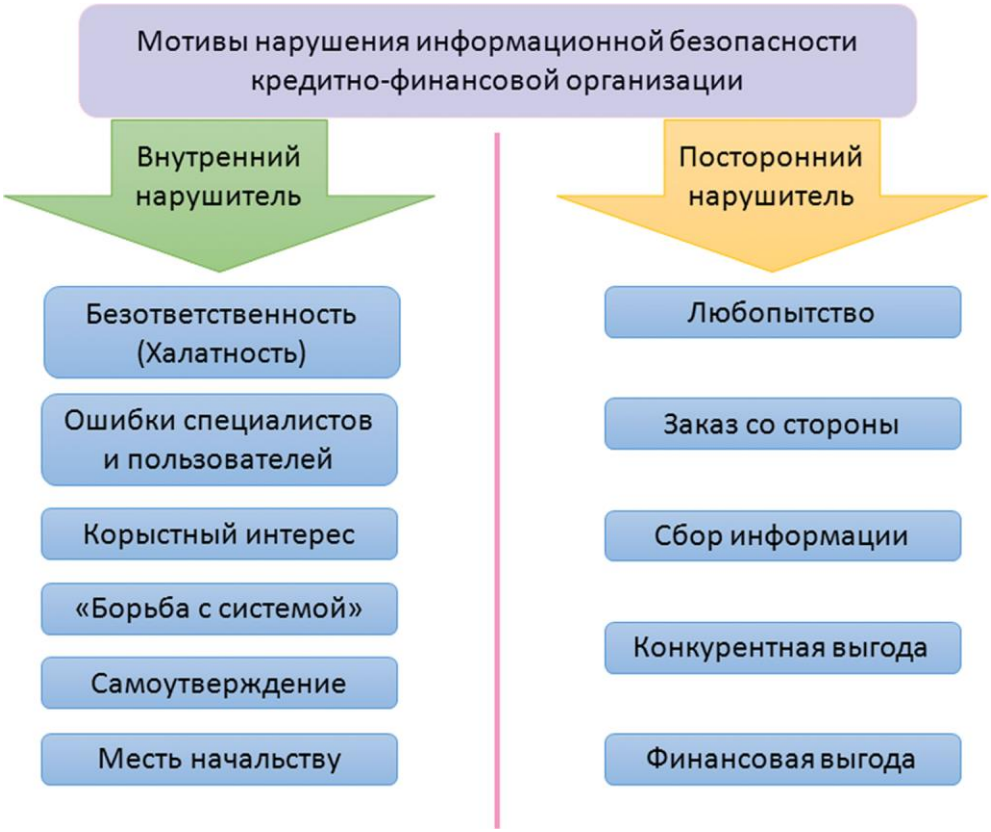

Рис. 1. Мотивы, движущие нарушителем информационной безопасности банка

Доступность информации показывает возможность реализации пользователями информации своих прав доступа. Целостность данных показывает их неизменность при выполнении операций с ними, будь то передача, использование или хранение информации. Конфиденциальность информации представляет собой запрет на её разглашение неуполномоченным лицам без предварительного согласия сторон.

Список литературы

1. Бухгалтерский учет в коммерческих банках. – М.: Юрайт; Юрайт-Издат, 2017. – 480 с.

2. Малахов А. Влияние монетарной политики Банка России на национальную экономику. – М.: LAP Lambert Academic Publishing, 2015. – 144 с.

3. Международная практика резервных аккредитивов ISP98. Типовые формы резервных аккредитивов по ISP98 / International Standby Practices ISP98: Model ISP98 Forms. – М.: Инфотропик Медиа, 2014. – 180 с.

4. Исторический очерк / Н. Смирнова. – М.: Машиностроение, 2017. – 102 с.

5. Филина С. Деловые ожидания и монетарная политика. – М.: LAP Lambert Academic Publishing, 2013. – 894 с.

6. Ахматов Х. Эффективность деятельности многофилиального банка: анализ и оценка / Х. Ахматов, С. Дубова. – М.: LAP Lambert Academic Publishing, 2013. – 148 с.