Секция «6. Экономическая и информационная безопасность: проблемы»

Девиантное экономическое поведение руководящего персонала как угроза информационной безопасности банка

***Зарубин Ю.С.*[1], *Воробьёв А.А.*[2]**

1 - Балтийский федеральный университет имени И. Канта, Институт соцально-гуманитарных технологий и коммуникации, 2 - Балтийский федеральный университет имени И. Канта, Институт прикладной математики и информатики, Калининград, Россия

E-mail: Felis.zh@gmail.com

Научный руководитель

к. п. н. Шахторина Екатерина Валентиновна

Современная реальность предъявляет высокие требования к руководящему персоналу предприятия. Особенно предприятия, постоянно работающего с финансовыми потоками и большим объемом конфиденциальной информации, персональными данными сотрудников и клиентов компании. Кредитные учреждения соответствуют всем вышеперечисленным критериям. Именно по этой причине мы посчитали весьма актуальной и интересной проблему поведения топ-менеджмента банков в ситуации постоянной угрозы экономической и информационной безопасности организации.

Под экономическим поведением субъекта авторы понимают, экономическое поведение по Г.Н. Соколовой, согласно которой экономическое поведение - поведение, связанное с перебором альтернатив с целью относительно рационального выбора. Выбора, в котором минимизируются все издержки, а чистая выгода стремится к максимуму. Выбора, обусловленного состоянием экономического сознания в обществе, экономическим мышлением, экономическими интересами и социальными стереотипами индивидов и групп.

Под девиантным экономическим поведением мы будем понимать поведение субъектов, нарушающее существующие установленные отраслевые нормы и правила поведения. Можно выделить различные причины, которые могут привести к отклонениям от ожидаемой модели поведения: ограниченность способностей к принятому поведению, банальная неосведомленность, социально-сравнительные мотивы, демонстративные формы поведения и неучастие (незаинтересованность) в управлении (Соколова, 1998).

Согласно анонимному исследованию агентства «Zecurion» и Ассоциации Российских Банков от 2013 года (Zecurion, 2013) лишь примерно две трети учреждений данного сектора (63,5%) имеют в своей структуре выделенные подразделения, обеспечивающие информационную безопасность организации. При этом отдельно стоит отметить, что собственный, отдельный бюджет на информационную безопасность существует только у половины банковских организаций, имеющих такой штат (31,3%). Широкую практику имеет смешение бюджетов ИТ и ИБ подразделений (23,1%). Это решение может быть очевидно и приемлемо в тех случаях, когда на ИТ-службу банка возложено обеспечение информационной безопасности и является грубейшим нарушением политики обеспечения информационной безопасности при наличии выделенной службы ИБ (Zecurion,

2013).

В целом, такая финансовая политика в области финансирования подразделений, обеспечивающих информационную безопасность, прямо противоречит рекомендациям стандарта Банка России по информационной безопасности СТО БР ИББС, где прямо указано на необходимость выделения отдельной службы, обеспечивающей информационную безопасность организации, обладающую независимым от департамента ИТ бюджетом (Банк России, 2010). В таких попытках сэкономить и объединить несколько ролей в одном отделе, руководство кредитной организации превышает допустимые информационные риски. Не менее важным критерием обеспечения информационной безопасности является анализ, прогнозирование и снижение информационных рисков. Можно говорить о том, что оценка и управление рисками лежат в основе системы управления информационной безопасностью организации. Однако на практике оценкой рисков в области ИБ занимаются лишь в каждом четвертом (26,1%) российском банке, где она имеет более-менее регулярную основу. Большая часть (35,1%) банков в процессе своей деятельности риски не оценивала и определяет приоритеты ИБ, исходя из субъективных представлений. Еще 9,7% опрошенных специалистов заявили, что на оценку рисков у них просто нет времени (Zecurion, 2013).

Показателем незаинтересованности принимающего решения персонала в обеспечении информационной безопасности может выступать тот факт, что несмотря на то, что приглашения к участию в исследованиях рассылаются непосредственно топ-менеджменту и руководству кредитных организаций, доля их участия в исследовании составила наименьший показатель (3,7%) от общего числа принявших в исследовании специалистов кредитных организаций, связанных с обеспечением информационной безопасности (Zecurion, 2013).

С другой стороны имеет место значительное и противоречивое нормативное давление на игроков кредитного рынка. Об этом заявляют большинство (76,9%) участников (Zecurion, 2013). Неудивительно, ведь банковские подразделения ИБ должны учитывать требования пяти регуляторов: ФСБ, ФСТЭК, Роскомнадзора, ЦБ и Росфинмониторинга. Каждый из этих органов ведет работу в рамках своих компетенций и обусловленного ими подхода. Однако для игроков столь значительное количество и регуляторов, и несогласованных требований, и норм представляет значительную проблему. Логичным итогом такого нормативного регулирования является то, что обеспечение ИБ банка исчерпывается выполнением нормативных требования регулятора в подавляющем большинстве (91,2%) кредитных организаций. Про экономические и конкурентные преимущества задумывается лишь треть (33,6%) руководителей. Соответственно оставшиеся две трети руководителей рассматриваю обеспечение ИБ лишь с точки зрения затрат. Не менее интересным является то, что несмотря на вступление в действие ФЗ №152 “О защите персональных данных” и увеличение в 2012 году штрафов для юридических лиц, только 7% руководителей считают необходимость обеспечивать конфиденциальность персональных данных сотрудников и клиентов своей организации (Zecurion, 2013).

Человеческий фактор является определяющей и важнейшей проблемой в области информационной безопасности. Согласно аналитическим отчетам Cisco Security Systems за 2012 год более 80% всех успешных атак на информационные системы имели характер именно человеческого фактора. Согласно данным опроса Harris Interactive от 2010 года

конфиденциальную информацию сознательно крадет каждый пятый офисный сотрудник. В случае же увольнения информационные риски увеличиваются в 2,5 раза - почти половина опрошенных уносит с места работы конфиденциальные данные.

Человеческий фактор проявляется не только в сознательном злонамеренном поведении. Например, лишь треть офисных сотрудников никогда не работает с корпоративной информацией вне офиса. При этом 23% персонала, напротив, делают это постоянно, несколько раз в неделю. Кроме того, топ-менеджмент кредитных организаций требует возможности открытого доступа к любой информации предприятия в любом месте и из любой точки мира, при том, что четверть (25,4%) руководства банков полностью не поддерживают существующую в их организации политику информационной безопасности (Zecurion, 2013).

Риски утечки в случае руководства высокого ранга чрезвычайно высоки, поскольку речь идет об информации критического уровня и с точки зрения обеспечения информационной безопасности регламент доступа именно к этой информации должен быть максимально жестким. Однако исключительные правила для топ-менеджмента, удобство доступа и удобство использования информации приводит к систематическому пренебрежению вопросами безопасности.

Кроме того не стоит забывать о консерватизме как одном из основных сдерживающих факторов сопротивления изменениям в любой организации. В подавляющем большинстве случаев ни рядовые сотрудники, ни топ-менеджмент не видят никакой выгоды от принятия мер для контроля доступа к информации, справедливо опасаясь, что реформы могут изменить устоявшийся уклад работы и вынудить, к примеру, уменьшить использование корпоративных каналов коммуникации в личных целях.

Можно сделать предварительный вывод, что экономическое поведение руководящего персонала кредитных организаций соответствует, скорее, девиантной модели экономического поведения. Наблюдается отклонение в большей части составляющих экономического поведения. Мы считаем, что причины этого явления требуют более подробного и внимательного изучения в дальнейшем.

Литература

1. Соколова Г. Н. Экономическая социология. Мн.: «Высшая школа», 1998;
2. Информационная безопасность в российских банках. Аналитический отчет Zecurion, Москва, 2013;
3. Офинсная небезопасность. Почему сотрудники офисов безнаказанно сливают информацию, Москва, 2013;
4. Отчет SECURIT Analytics об утечках информации за 2010 год, Москва 2010;
5. Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации, Москва, 2010.

Слова благодарности

Выражаем особую благодарность нашему научному руководителю - кандидату педагогических наук Шахториной Екатерине Валентиновне.