УДК 336.1115
DOI: 10.17223/22229388/20/2

А.А. Земцов

КОНЦЕПЦИЯ ПРОБЛЕМ КАК ВЫРАЖЕНИЕ СПЕЦИФИЧЕСКИХ ОПАСНОСТЕЙ ДОМОХОЗЯЙСТВА

> Ведь у нас, к сожалению, периодически проявляется некий синдром жареного петуха – люди превентивно мало думают о возможных рисках. А когда начинают думать, то, скорее всего, петух уже клюнул.
>
> *Касперская Н., 2014*

Особенность статьи – проблемная направленность, причем рассматриваются в основном финансовые проблемы домашнего хозяйства в описательном плане.

Ключевые слова: *домохозяйства, специфические опасности, финансовые проблемы.*

Это – очередная [36, 38] статья об опасностях, окружающих и практически составляющих домашнее хозяйство. Её особенность – проблемная направленность, исходя из подхода Р. Фарсона, так как проблем существует невообразимое множество и не меньше их разновидностей. Мы коснемся некоторых из них, преимущественно финансового профиля, связанных и с компетентностью, и с праводействием. Существуют общие финансовые проблемы для всех классов, частные для низшего, среднего и высшего, единичные, относящиеся к отдельному домохозяину. Кроме того, способы жизни, нами ранее рассмотренные, созвучны различным группам проблем. Да и позиция домохозяйства, элемент жизненного пути личности, о чем хорошо сказано у М. Вартофского, в общем виде: пациент – пассивное лицо, на которое направлено действие. Клиент, очевидно, может что-то сказать о своих желаниях и нуждах, пациент же нет. Из этого примера следует существование альтернативных моделей как способов действия [15. С. 131–132].

Если говорить о конкретной цели самоменеджмента жизни, механизм которого в аспекте несчастных случаев описан в доходно-расходных позициях – возможность перехода в «необычную сферу», можно применить структуру общества по Т. Малевой: 10-70-20, где 10 % – низший класс; 20 % – средний, 70 % – ниже среднего, т.е. задача домохозяйства – попадание в 20 и удержание там. «Сила среднего класса и сейчас будет проверяться не количеством денег, а гибкостью и способностью в адаптации в новых обстоятельствах» [54. С. 26].

«Вес» опасностей и их значение для домохозяина зависят от способа жизни «и от сочетания позиций», допустим: «мать-студентка», мать-«аспирантка», «мать-докторантка»»

Очень важный момент: разница между безопасностью как реальностью и ощущением. «По мере роста требований к безопасности полетов в гражданской авиации, которые год от года становились все более и более изощренными и достигли апогея в 2006-м с введением ограничений перевозки жидкостей в ручной клади на европейских направлениях, их критики настойчиво повторяли, что логика, лежащая в их основе, имеет существенные изъяны. У террориста, сознательно идущего на самоубийство, всегда будет преимущество перед обычными людьми, не готовыми к смерти», – Брюс Шнайер (Bruce Schneier), один из наиболее яростных противников кампании по закручиванию гаек, начавшейся после 11 сентября [9. С. 126].

По его мнению, невозможно сделать воздушные путешествия существенно безопаснее, запрещая все новые предметы, которые могут использовать террористы или которые потенциально могли бы быть им полезны. Для чего правительства продолжают навязывать эти дорогостоящие и трудоемкие ограничения? На этот вопрос есть много вариантов ответов, которые связаны с желанием политиков и служб безопасности показать активность и оправдать своё существование и зарплату в глазах избирателей и нанимателей. Но главная причина, по мнению Шнайера, – базовая человеческая потребность чувствовать себя уверенно и защищенно, даже если это чувство имеет очень отдаленное отношение к состоянию уверенности и защищенности. Для мер, которые изобретаются и воплощаются большей частью для того, чтобы заставить людей чувствовать себя в безопасности, а в действительности никак не способствуют повышению её уровня, Шнайер изобрел термин «Театр безопасности» (Security Theater – книга Beyond Fear (2003). Psychology of Security www.schneier.com/essays 155,ntml (С. 127).

Он считал, что этот театр на самом деле делает нас беззащитнее, и в какой-то степени его мнение недалеко от истины. «Театральная» обстановка поглощает средства, которые с большим толком можно было бы использовать в борьбе с терроризмом (С. 128). Не все стратегии, направленные на укрепление чувства безопасности, действительно обеспечивают нашу безопасность. Они могут оказывать и прямо противоположное действие. По славам Шнайера, «безопасность означает и ощущения, и реальность, а это не всегда одно и то же». Часто упоминаемые в последние годы когнитивные искажения, т.е. то, каким

именно образом наши представления о действительности отличаются от нее, во многом объясняют типичные заблуждения относительно безопасности. Неподконтрольных ситуаций (например, положение пассажира в самолете) мы страшимся больше, чем тех, которые, как нам кажется, контролируем (например, вождение автомобиля) (С. 131).

Один из подходов к анализу проблем домохозяйства, вытекает из сути технологии комплаенс [85]. Комплаенс – обеспечение уверенности в том, что организация соответствует всем относящимся к ней нормам и правилам, а управление бизнесом осуществляется на высоком уровне этики и добропорядочности (Международная комплаенс-ассоциация). Базельский комитет по банковскому надзору – комплаенс – набор конкретных технических функций, реализация которых позволяет управлять правовым, репутационным и некоторыми операционными рисками, которые в совокупности называются комплаенс-рисками [Там же. С. 47, 50]. Применительно к домохозяйствам: рассмотрение процесса функционирования домохозяйства в плане его соответствия многочисленным нормативным требованиям: гражданским, уголовным и др., причем сами группы требований могут противоречить друг другу, ставя роленосца в двусмысленное положение, чреватое нарушением группы норм: валютные правила до сих пор остаются крайне жесткими для современных экономических реалий. Правила налогового и валютного резидентства и практика их применения влекут за собой существенные валютные риски для миллионов проживающих за рубежом граждан РФ – налоговых нерезидентов РФ. Они не обязаны уплачивать российские налоги, но считаются валютными резидентами при каждом приезде в Россию и подпадают под риск штрафа в 75–100 % от суммы операций. Очевидно, что исторически сложившиеся правила валютного регулирования в части режима зарубежного счета являются атавизмом. Без кардинального изменения этих правил перевернуть офшорную страницу истории и осуществить успешную декларационную кампанию крайне сложно [23].

Другой аспект комплаенса ДХ – отсутствие реальной защиты путем применения многочисленных оговорок, которые съедают её: страховки для туристов, без которых нельзя получать визу во многие страны мира, на практике часто не защищают выезжающих за рубеж. Все дело в многочисленных оговорках и исключениях, число которых может варьировать в зависимости от страховой фирмы от 50 до 120. Туристы редко обращаются в суд в случае отказа в выплате, и зря. На практике более 98 % разбирательств по страховым случаям выигрывают граждане [88].

Одну из групп опасностей мы уже рассматривали [36] – нахождение в зоне высокого уровня риска – смертельного уровня риска (ВУР ↔СУР). Собственно человек (домохозяин) может случайно оказаться в этой зоне, допустим, авиапассажир. Эту ситуацию и рассматривает Рипли. Но можно и специально, осознанно входить в неё, допустим, экстремальные виды спорта. Существуют некоторые абсолютные характеристики, показывающие, сколько времени отделяют ВУР от СУР – так называемая абсолютная информация: человек может находиться под снегом (лавина и т.п.) всего 25 мин. Следовательно, катание в «дикой» местности в одиночестве смертельно опасно. Есть такие показатели для нахождения в холодной воде; без воды и без воздуха.

В работе С. Баррера [5] рассматривается спорт: «…весь мой личный опыт, а также более тринадцати лет медицинской практики убеждают меня в том, что любой спорт – это травмы (С. 13). Мы, врачи, прописываем лекарства в строго определенной дозировке, которая тщательно рассчитывается для обеспечения максимальной эффективности и безопасности. И превышать дозировку даже самого полезного лекарства чрезвычайно опасно. Точно так же злоупотребление физической активности может иметь пагубные последствия для здоровья человека и даже быть опасным для его жизни (С. 19). Благотворное влияние физической активности на сердце, а также на здоровье и общее благополучие человека считается абсолютно доказанным фактом, который подтверждается массивом всевозможных исследований, особенно осуществленных на протяжении последних десятилетий. Но… есть и обратная сторона медали. Я утверждаю, что занятия спортом могут причинить вред вашему здоровью в нескольких отношениях. Травмы можно получить в результате даже самых простых и легких физических упражнений. Кроме того, серьезную опасность таит в себе кумулятивный эффект, который могут давать самые тривиальные травмы или же просто длительная чрезмерная нагрузка на наши суставы и мышцы даже при отсутствии травм. Злоупотреблять спортом опасно… Убеждение, что спорт – это необходимое зло (ударение на слово «зло»). Я хотел объяснить, почему ныне существует культ спорта, несмотря на то, что занятия им чреваты потенциальными опасностями, как несомненными, так и не вполне очевидными (С. 21–23). Как хирург перед проведением любой операции я этически и юридически обязан получать от пациента информированное согласие на это вмешательство, которое требует, чтобы пациент знал от меня в мельчайших деталях, что может пойти не так. Если пациент не в состоянии понять, что я ему говорю, я должен объяснить это опекуну. Кроме того, я должен рассказать обо всех рисках, присущих хирургическим вмешательствам…, а также об индивидуальных рисках. К сожалению, в индустрии физической культуры и розничной торговле спортивными товарами не существует доктрины «информированного согла-

сия» (С. 25). Эта книга предлагает любителям спорта основу для информированного согласия. В книге я подробно обсуждаю некоторые из наиболее распространенных опасностей, возникающих при занятии спортом и способы, как их избежать. В конце концов физическая активность действительно полезна. Я надеюсь убедить вас в том, что в нашем отношении к спорту должно быть место умеренности и здравому смыслу, поскольку спорт может причинить вред (С. 27). Главная моя цель – помочь вам понять, что вы должны внимательно относиться к своему телу и его потребностям. Мне хотелось бы думать, что большинство людей обладают здравым смыслом. Именно к нему и обращается эта книга» (С. 28).

В сфере автомобильного транспорта статистика свидетельствует: в странах, где 50 км/ч – предельная «городская» скорость, на дорогах гибнет меньше людей. После того, как в Великобритании ограничили скорость внутри жилых районов до 30 км/ч, количество аварий с участием детей – пешеходов и велосипедистов снизилась на 67 %. Состояние дорог и автомобильного парка существенно влияет на безопасность движения. Но не меньший вклад вносят различные ограничения и ужесточения, касающиеся автомобилистов. 1,24 млн человек гибнут в результате ДТП каждый год во всем мире (таблица). В списке причин смертей во всем мире ДТП занимают 8-е место для людей возраста 15–29 лет. 77 % погибших в ДТП – мужчины. 60 % погибших в ДТП – люди в возрасте 15–44 лет. В 2,5 раза возрастает риск ДТП для молодых и неопытных водителей (по сравнению с более опытными) при содержании алкоголя в крови около 0,05 г/ л [6. С. 26]. До 75 % снижается смертность для пассажиров на задних сиденьях автомобилей при использовании ремней безопасности. 8 % ДТП со смертельным исходом в России происходит по вине водителей, находящихся в состоянии алкогольного опьянения [Там же. С. 27].

Смертность ДТП по видам участников дорожного движения, %

Регион	Участники				
	Водители автомобилей и пассажиры	Мотоциклисты	Велосипедисты	Пешеходы	Прочие
Мир	31	23	5	22	19
Европа	50	12	4	27	7
Россия	57	7	2	33	1

Во многом безопасность водителей зависит от их поведения в конфликтных дорожных ситуациях, которые описываются в статье с точным названием: не стройте из себя героя [29].

Количество и разнообразие зависимостей поражает, одна из новейших – использование электронных устройств и технологий. В работе Сиберга (Цифровая диета. М., 2015) предлагается 4-шаговая стратегия, помогающая свести использование электронных устройств и технологий к разумным и комфортным для каждого пределам: 1-й шаг: Задумайтесь. 2-й: Перезагрузитесь. 3-й: Подсоединитесь. 4-й: Оживите.

За последнее десятилетие мы превратились из общества, пользующегося технологиями, в общество, полностью поглощенное ими. Этот огромный объем начал подминать нас, а растущие ряды гаджетов, веб-сайтов и устройств стали превращаться в силу, заполняющую нашу жизнь. Эта сила действует не как атомный взрыв, она подобна нашествию колонии муравьев. Настало время более внимательно присматриваться к нашим действиям, ненадолго вернуться назад и затем пересмотреть отношения к технологиям, чтобы заставить их работать на нас, вместо того чтобы нам работать на них. Мы должны принять эту мысль. Думайте об этом как о необходимости питаться, но только лучшими продуктами и в правильное время, регулярно выполняя физические упражнения, чтобы быть в отличной форме. Цифровая диета поможет вам повысить свою эффективность при общении. Используя постепенный подход в стиле диетического питания, цифровая диета поможет вам укрепить связь с окружающим миром и любимыми людьми. Её смысл в том, чтобы вы жили здесь и сейчас и владели инструментами, которые поддерживали бы в вас этот образ мыслей всю жизнь. Вы узнаете, как переизбыток устройств и услуг вредит нашему физическому, психическому и эмоциональному здоровью (С. 14). Десять правил цифровой диеты:

1. Ведите себя вежливо. Не бросайте смартфон на стол в ресторане или дома. Пусть он лежит в кармане или сумке за исключением случаев крайней необходимости. Если вам необходимо доставать его, предупредите об этом ваших спутников и объясните, что будете смотреть в него только в крайнем случае. Вы оцените, если другие будут вести себя так же.

2. Живите в реальном мире. Если вы хотите обновить статус, написать твит или опубликовать в блоге что-то о своей жизни, подумайте, готовы ли вы объявить об этом любому при личной встрече.

3. Спросите себя, действительно ли вам нужен этот гаджет (С. 197).

4. Пользуйтесь технической поддержкой. Просите о помощи и используйте технологии для «передачи третьей стороне функций самоконтроля», когда вам это нужно. Пробуйте разные программы, которые могут помочь в распределении вашего времени за компьютером.

5. Регулярно устраивайте детоксикацию. После завершения диеты возвращайтесь к этой фазе раз в месяц на один день. Используйте этот день, чтобы не забывать, какой может быть жизнь без технологий.

6. Уберите устройства на время сна.

7. Или человек, или устройство. Старайтесь пользоваться устройствами в личное время, а не когда вы общаетесь с другими.

8. Помните о принципе «если – то». Выбор, который вы делаете в виртуальном мире, может влиять на реальный мир. Например, если вы не находите времени, чтобы иногда откладывать гаджеты, то можете потерять возможность оценить прекрасные моменты жизни.

9. Структурируйте свой электронный день. Работайте над тем, чтобы четко определить начало и конец времени, когда вы доступны.

10. Доверяйте своим инстинктам. Внутренний голос подскажет вам, когда стоит остановиться. Прислушивайтесь к нему. Помните о цели поддерживать равновесие и делать осознанный выбор (С. 197–199).

В классической Энциклопедии о риске менеджмента говорится, что причинами неопределенности являются три основных группы факторов: незнание, случайность и противодействие (цит. по [38]). Третий фактор очень важное значение играет в конкурентных сферах, поэтому его действие прогнозируемо: необходимо знать его проявления и способы противодействия противодействию. Системообразующим является понятие «доверие», без учета которого невозможно выстроить грамотную стратегию защиты от противодействия [38], существует явление «недоверенная среда» [42].

Следующее явление в аспекте опасности многомерно:

1. Потеря денег из-за неадекватности предлагаемых инструментов.

2. Потеря здоровья (а то и жизни) из-за применения нетрадиционного лечения, в ходе которого поздно будет применять действенное традиционное лечение.

Речь идет о псевдонауке и паранормальных явлениях. В работе Д. Смит «Псевдонаука и паранормальные явления» (М., 2015) говорится: …Я искренне верю, что заявления астрологов, экстрасенсов, спиритуалистов, телепатов, сгибателей ложек, специалистов по комплементарной и альтернативной медицине, иглоукалывателей, целителей и креационистов надо воспринимать всерьез. Не потому, что их заявления могут быть истинными или ложными. Дело не в этом. Я верю, что экстраординарные заявления могут вызвать экстраординарные последствия. Одноединственное достоверно продемонстрированное паранормальное явление может заставить человечество переписать едва ли не все учебники. Как известно, 73 % американцев верят в паранормальное, и доля верующих постоянно растет (С. 13). Я написал эту книгу для студентов. Она могла бы стать основой для нескольких курсов: профессионалов сферы здравоохранения. Сиделки, социальные работники, консультанты, психологи и врачи сталкиваются с паранормальными явлениями на различных курсах и практикумах по комплементарной и альтернативной медицине; журналистов. Паранормальное – вечная тема, представляющая громадный интерес для СМИ; чиновников; религиозных искателей и педагогов; исследователей паранормального (С. 14–15). Общая цель книги – рассмотреть и применить систематический подход сверки с реальностью к сообщениям о паранормальных явлениях – инструментарий здравомыслящего критика (С. 16). Моя цель – принимать факты, но не выдумки, даже если они неудобны (С. 18).

В работе [71] приводится пример: экстрасенс N. в 2008 г. стала финалисткой проекта «Битва экстрасенсов», сейчас ее любая консультация стоит 25 тыс. руб., «безвестный» экстрасенс или гадалка обойдутся примерно в пять раз дешевле (С. 35). Попытки запретить или ограничить деятельность магов предпринимаются постоянно на протяжении многих веков, и ни в одной стране не найдено идеальное решение (С. 37).

В 1991 г. народные целители объединились в организацию, которая сейчас называется Российская ассоциация народной медицины (РАНМ). Из тысячи ее членов только 300 прошли профессиональную экспертизу. Чтобы стать «законным» экстрасенсом, нужно зарегистрировать ИП, ЧП или компанию, получить Код общероссийского классификатора видов экономической деятельности «психологи, парапсихологи, экстрасенсы, астрологи» номер 85.32 или 43.05, встать на учет в налоговой инспекции. Далее можно дать объявление в газете и ждать клиентов (С. 38).

И «экстрасенсы» – лишь малая часть мошенников, посягающих на деньги, здоровье и жизнь домохозяев. В работе О. Логинова сказано: «Это скорее просто подборка публиковавшейся ранее информации о многообразии форм мошенничества и обмана, об известных аферистах и малоизвестных борцах с ними. Это – энциклопедия мошенничества во всех его видах и проявлениях. Она рассказывает обо всех существующих на сегодняшний день способах обмана… Читайте, делайте выводы и не попадайтесь в загребущие лапы мошенников и аферистов. Дураков не сеют, а жнут» [50. С. 11].

К сожалению (некоторые говорят – к счастью [9]), течение жизненного пути редко бывает плавным, чаще оно прерывается различными кризисами, природа которых очень разнообразна. Советы Л. Бершидского относятся к финансово-экономическим кризисам:

1. Составьте внятную картину того, что собственно произошло. Не доверяйте никому, одному источнику. Как только вы со всем разберетесь сами, сразу станет ясно, каких последствий надо ждать и к чему готовиться.

2. Проведите ревизию вашей личной бухгалтерии. Нарисуйте ваш баланс, посмотрите на него, подумайте о его сильных и слабых сторонах.

3. Принимайте на себя валютные риски, только если ваши житейские и потребительские планы связаны с иностранными валютами.

4. Прикиньте, какова ваша личная инфляция. Это полезно знать, принимая решения об инвестициях.

5. Попытайтесь обыграть рынок, только если хорошо понимаете, что это очень рискованно и скорее всего бесперспективно (С. 246). Есть только три разумные рыночные стратегии: 1) «покупка рынка» через индексный фонд; 2) инвестиции только в то, что вы очень хорошо знаете (метод Баффета), и 3) скальпинг (работа на рынке как компьютерная игра).

6. Если у вас большие долги и нет возможности их выплачивать, спокойно расстаньтесь с купленной в долг собственностью.

7. Решая, что покупать или продавать, гасить кредиты или объявлять по ним дефолт, никого не слушайте. Считайте сами, как бы ни был велик соблазн разделить с кем-то ответственность.

8. Задумайтесь о том, что вы могли бы делать, если бы не сидели на нынешней работе. Кризис – отличный момент для того, чтобы сменить профессию или начать свое дело.

9. Приведите в порядок свои социальные сети – и те, что в Интернете, и те, что вне его.

Они пригодятся, чтобы в случае чего искать работу и бизнес-возможности – а то и для строительства деловых цепочек.

10. Начните анализировать свое потребительское поведение: скоро импульсы, которые заставляют вас тратить деньги, покажутся вам нелепыми и смешными, и вы станете тратить меньше.

11. Перечитайте любую книгу, какая бы она не была, в кризис это работает как душ после потного дня (С. 247).

12. Нарисуйте таблицу «Добро и зло», как Робинзон Крузо. Перечитайте стоиков – они все знали про кризисы (Бершидский Л. Кризис в ж.***. М., 2009. С. 248).

Интернет – неуничтожимая информация, один из аспектов информационной открытости-закрытости. Существует множество публикаций, описывающих это свойство Интернета с разной степенью эмоциональности. «В рецензируемой книге показывается, что легкость поиска и хранения данных в цифровой среде – не только достижение, но и проклятие компьютерной эры. Человеческая память творчески перерабатывает свои представления о произошедшем с нами. У компьютерной памяти такой способности нет. Сколь бы случайными и нерелевантными ни были попавшие туда сведения, они будут храниться в неизменном виде, там, куда мы их положим, оставаясь доступными для окружающих. Ими сможет воспользоваться кто угодно и в любых целях – разумеется, если нет специальной защиты. Как же можно оградить себя от желающих вторгнуться в нашу жизнь и злоупотребляющих нашей беспечностью? Один из способов – абстиненция; другой – усовершенствовать законодательство, защищающее личные данные. Третий – обязать владельцев сайтов стирать все данные о людях по истечении определенного срока… (Чернозатонская Е. // HBR. 2010. № 6–7. С. 112–113).

В работе Д.В. Гундорина [27] говорится: чтобы правильно выстроить информационную защиту в организации (и в ДХ тоже. – *А.З.*), нужно четко представить, какими приемами пользуются злоумышленники для кражи информации. Одним из наиболее популярных и одновременно самых простых методов сбора информации является социальная инженерия – методы воздействия на человека с целью получения неавторизированного доступа и кражи информации (С. 70). Всплеск киберпреступности поддерживается тем, что люди, не задумываясь, составляют в Интернете множество информации о себе: контакты, фотографии, информацию о месте работы, друзьях, увлечениях и даже планах. Все эти сведения представляют угрозу, обеспечивают злоумышленников необходимыми данными для атаки (рис. 1). Часто поступки людей и их реакции на то или иное внешнее воздействие во многих случаях предсказуемы и потому легко моделируются социальными инженерами (С. 71).

.

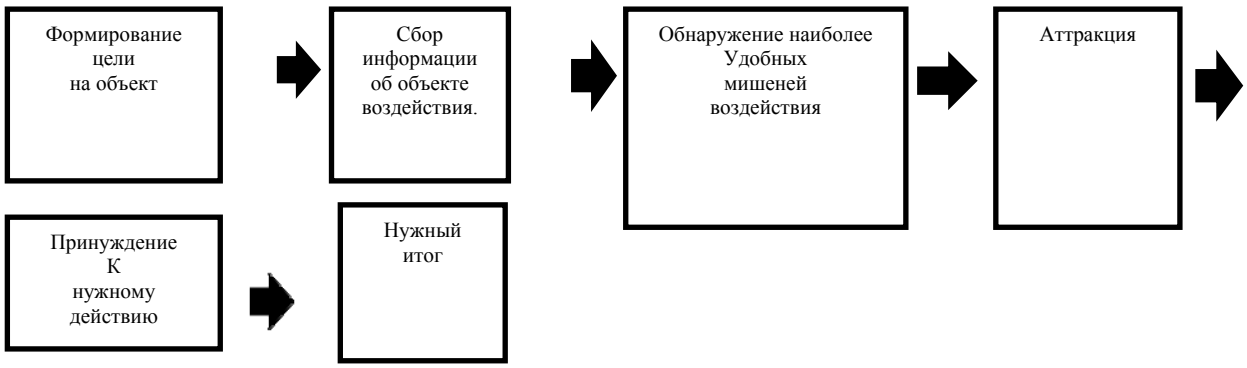

Рис. 1. Обобщенная схема действий злоумышленников [27]

Аттракция – состояние, к которому подводят жертву, чтобы она выполняла нужные злоумышленнику действия. Необходимо построить процесс повышения осведомленности сотрудников, включающий регулярные тренинги и контроль уровня знаний. Помимо этого, совершать так называемые внутренние диверсии (тестирование на проникновение с использованием социальной инженерии), позволяющие выявить реальный уровень подготовки сотрудников к защите от атак. Защиту от человеческого фактора нужно постоянно поддерживать и актуализировать. Главный девиз людей, занимающихся информационной безопасностью, – безопасность это процесс, а не результат (С. 71).

В РФ создан Центр мониторинга и реагирования на компьютерные атаки в финансовой сфере, действует в ЦБ с 1.6.15. Количество электронных платежей в России ежегодно растет в среднем на 10 %, при этом ежегодно число атак на банки с целью хищения средств увеличивается на 20 %. Карточные мошенники в РФ за год украли 1,58 млрд руб. Для этого злоумышлинники использовали данные более 70 тыс. платежных карт, 70 % из которых – дебетовые. Самый популярный вид мошенничества – скимминг – кража данных карты при помощи считывающего устройства, тайно установленного на банкоматах и других платежных устройствах общего пользования [90. С. 45].

88 % компаний по миру становятся жертвами мошенников. Новый тренд: информацию стали красть чаще, чем осязаемые активы, особенно от такого воровства страдает финансовый сектор (подчеркнуто нами. – *А.З.*) [Финанс. 2010. № 39]. 65 % всех украденных данных в РФ похищают не сторонние хакеры, а сами сотрудники компаний, заявила Н. Касперская.

Почти 90% – персональные данные, 5 % – коммерческая тайна, 3 % – государственная тайна [РБК. 2015. № 11. С. 26].

По мнению А.И. Бычкова, мобильный банк – удобный SMS-сервис, позволяющий получать информацию обо всех операциях по пластиковым картам, а также совершать платежи, переводы и другие операции с помощью мобильного телефона в любое время и в любом месте. Данный сервис имеет и ряд недостатков, связанных с возможными несанкционированными списаниями денег со счета гражданина. При утрате мобильного телефона необходимо срочно обратиться к оператору сотовой связи для его блокировки и в контактный центр банка для приостановления или отключения сервиса «Мобильный банк». Важно обратить внимание на правильность оформления документов и точность содержащихся в них данных [11. С. 107]. Если гражданин решил отказаться от номера мобильного телефона, к которому был прикреплен «Мобильный банк», ему немедленно следует информировать об этом банк. Банк не вправе определять и контролировать направления использования денежных средств клиента и устанавливать другие, не предусмотренные законом или договором банковского счета ограничения его права располагать денежными средствами по своему усмотрению.

Если никаких конкретных доказательств необоснованного описания денежных средств банком со своего счета клиент не представит, …суд откажет в удовлетворении его иска к банку о признании незаконным списания денежных средств. Суд учитывает все заслуживающие внимания обстоятельства [Там же. С. 108] .

В настоящее время мобильные платежи (МП) становятся привычной операцией для многих клиентов крупных и средних банков. Эксперты в области банковского дела признают, что у сферы беспроводных денежных трансакций отличные перспективы. К основным услугам с использованием МП относятся: переводы, осуществляемые посредством SMS-сообщений; платежи в торговых автоматах за счет аванса средств, внесенных оператору связи; платежи с использованием банковских карт; платежи через системы мобильного банкинга.

Главные преимущества МП: доступная стоимость; высокая скорость передачи данных; простой доступ к передовым технологиям [73. С. 56].

В то же время использование мобильных телефонов для оплаты товаров и услуг и осуществления денежных переводов без обладания банковскими счетами в условиях анонимности и слабого надзора создает благоприятные возможности для отмывания денег и совершения иных противозаконных действий. МП значительно облегчают использование «денежных мулов» – финансовых посредников, которые открывают и используют банковские счета для перевода денежных средств со счетов обманутых на счета преступников. Как правило, люди выступающие «денежными мулами», не догадываются о своей роли в этих аферах. Учитывая, что вся «антиотмывочная» система как в России, так и в мировом пространстве ныне выстроена на идентификации клиентов, МП значительно усложняют выполнение всех принятых ранее процедур [Там же. С. 57]. Физическое лицо может осуществлять платежи электронными денежными средствами либо после идентификации, либо инкогнито. В случае с МП задача идентификации усложняется во много раз [Там же. С. 58].

Количество российских интернет-пользователей на апрель 2015 г. составляло 82 млн чел., за последние 20 лет сформировалось так называемое информационное общество.

Стремительное развитие информационных технологий имеет главное воздействие на платежную индустрию. Развитие виртуальных взаимоотношений между людьми и различными организациями создало и новый класс преступников,

специализирующихся на преступлениях в области высоких технологий, – киберпреступников. Для борьбы с ними возникли киберполицейские и такое понятие, как кибербезопасность. Она направлена на защиту компьютеров, сетей, программы и данных от случайного или преднамеренного несанкционированного доступа, изменения и уничтожения информации [72. С. 66].

В целом кибербезопасность – состояние защищенности в новой виртуальной сфере, которая достигается благодаря набору средств, стратегий, принципов обеспечения безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты виртуальной среды, ресурсов организаций и пользователей сервисов от целенаправленного деструктивного воздействия. Наряду с очевидными преимуществами технологии ДБО принесли в банковский сектор дополнительные риски, связанные с особенностями функционирования аппаратно-программного обеспечения системы ДБО и надежностью каналов связи. Особенностью информационного контура банковской деятельности в условиях ДБО является возникновение новых участников: для интернет-банкинга – интернет-провайдеров, для мобильного – операторов сотовой связи. Провайдеры в настоящее время находятся вне зоны контроля и правового регулирования со стороны Банка России или иного органа, проводящего согласованно с ним политику, что повышает риски, связанные с ДБО. Информационное общество меняет значение привычного выражения «банковское дело».

Виртуализация банковской деятельности и широкое распространение технологий ДБО стали притягивать к себе киберпреступников, основной целью которых становится воровство денег со счетов кредитных организаций и их клиентов. Усложняют задачу обеспечения кибербезопасности ряд неблагоприятных факторов развития информационной инфраструктуры: стремительное устаревание техники; безграничность Интернета и неадекватность нормативно-правовой базы, регулирующей информационные потоки; чрезвычайная сложность (в ряде случаев и невозможность) идентификации киберпреступников; ограниченные ресурсы обеспечения кибербезопасности (С. 67).

Основная угроза для организаций кредитно-финансовой сферы, которая непосредственно связана с распространением компьютерных мошенничеств, заключается в потере контролируемости и как следствие управляемости внедренных компьютерных технологий и реализующих их банковских автоматизированных систем (включая систему ДБО), что влечёт потерю доверия обслуживаемого данными организациями населения, что практически всегда приводит к катастрафическим последствиям для банка. Обналичивание чаще всего осуществляется с помощью «белого пластика». Снятие наличных осуществляют «дропперы» (мулы), которые за определенную плату обналичивают «белый пластик» через банкоматы (С. 68). Основной сдерживающий фактор на пути более динамичного развития технологий ДБО как на Западе, так и в России – опасения клиентов по поводу безопасности (С. 69).

Можно выделить три основных направления совершенствования кибербезопасности в организациях кредитно-финансовой сферы в условиях ДБО:

1. Нормативно-правовое регулирование в области кибербезопасности.

2. Надежность аппаратно-промышленного обеспечения систем ДБО.

3. Финансовая грамотность населения и уровень профессиональной подготовки персонала ОКФС.

В перспективе необходимо стремиться создать не только систему надзора в виртуальном пространстве, но и поднять культуру поведения в нем всех участников информационного обмена. За рекламой различных систем ДБО должна стоять ответственность банка за качество предоставляемых услуг (С. 70–71).

При умелом обращении кредитная карта необязательно сделает из вас раба финансовых услуг, отдающего всю зарплату банку. Но пользоваться ею, как и другими кредитными продуктами, стоит с осторожностью. Мы лишь напоминаем, как выжать из кредитки максимум дополнительных услуг, если уж вы решились платить от 300 до 30 000 руб. в год (1-й кв. 2011. – *А.З.*) за возможность иметь под рукой дополнительный кошелек [91. С. 16].

Предоплаченная карта не привязана к банковскому счету, и это делает её уникальным продуктом для тех, у кого этого счета нет [45. С. 66]. Эксперты называют 3 ниши, где предоплаченные карты смогут завоевать кошельки потребителей:

1. Подарочные карты.

2. Оплата товаров и услуг через Интернет и мобильную связь. Виртуальная карта, как правило, дебетовая, т.е. привязанная к счету. И опытный хакер может добраться до ваших денег. В прошлом году интернет-преступники похитили 12,5 млрд долл., причем 4,5 млрд долл. пришлось на российских или русскоговорящих хакеров (Group-IB). Предоплаченная карта не привязана к банковскому счету, абсолютно автономна, даже самый опытный хакер может поживиться разве что остатком на ней.

3. Различные бонусные программы [Там же. С. 67].

Еще одно преимущество карты, которое европейцы оценили уже после кризиса, – это планирование семейного бюджета [Там же. С. 68].

Безопасности при применении банковских карт посвящена огромная литература, см. [2, 8, 14, 16, 43]. Общие итоги – в «Памятке ЦБ» [68].

«Лукавство операторов сотовой связи и невнимательность самих абонентов стоят последним миллионы долларов. Оставайтесь начеку; незаметно подключаемые платные услуги, входящие SMS с короткого номера, или откровенное мошенничество. На помощь операторам приходят некоторые профессиональные хитрости и невнимательность абонентов. Сотовики не заинтересованы в досконального разъяснении клиентам деталей тарифных планов при заключении договоров. Роуминг – не единственный подводный камень для клиентов сотовых компаний. Недобросовестные контент-операторы наловчились цеплять абонентов на свои удочки. Как не угодить в капкан мошенников и не пасть жертвой собственного доверия:

• Проверить, сколько Sim-карт зарегистрировано на ваш паспорт.

• Внимательно изучить расценки на всевозможные услуги связи.

• Не стоит открывать сообщения с незнакомых коротких номеров.

• Обращение в суд [80. С. 74].

В последнее время операторы начали борьбу с SMS-спамом и несанкционированными подписками. На смену SMS-мошенничеству идут мобильные вирусы, крадущие деньги со счета абонента. В России ими заражены сотни тысяч смартфонов, а ущерб достигает сотен миллионов рублей в год [39].

2 лица маркетинга:

А) Маркетинг ДХ, т.е. дозирование информации о нем. Создание и пользование позитивным имиджем ДХ. Направлено на внешний мир.

Б) Защита от маркетинга, рекламных воздействий, окружающего мира (предприятия, государственные органы и прочие «мошенники»). То есть сортировка, «обогащение» информации, отделение «хвостиков» от содержания. О «втором» лице прекрасно сказано в книге М. Линдстром «Вынос мозга…» [48].

Эта книга с очень красноречивым подзаголовком «Как маркетологи манипулируют нами и убеждают покупать их товары» очерчивает целую страну опасностей, которые покушаются на бюджет каждого человека, вмешиваясь в процесс принятия решения о покупках, речь конечно же идет о всех приобретаемых товарах и услугах. Эта сторона весьма обширна и специфична, требуя от нас постоянного внимания, подкрепленного реальными знаниями. Начнем с оглавления: Введение. Брендовая детоксикация. Гл. I. Покупай, покупай, детка! Как компании начинают продавать нам в утробе матери. Гл. II. Лучшие продавцы – паника и паранойя. Почему страх поднимает продажи. Гл. III. Не могу сказать прощай. Брендозависимость, шопоголики и – почему мы не можем жить без смартфонов. Гл. IV. Купи и будет тебе секс. Сексуальный подтекст в рекламе. Гл. V. Смотри на меня, делай как я. Сила социального давления. Гл. VI. Эти сладкие воспоминания. Новое (оно же старое) лицо рыночной ностальгии. Гл. VII. Короли маркетинга. Тайная власть популярности и славы. Гл. VIII. Надежда во флаконах. Сколько стоит здоровье, счастье и духовное просветление. Гл. IX. Они слышат каждый наш вздох. Лишние права на неприкосновенность личной жизни. Заключение. Мне то же самое, что у миссис Моргенсон. Самый мощный тайный манипулятор – мы сами.

Одна из впечатляющих глав, особенно в нашем исследовательском аспекте, гл. 9, материал которой налагается на тему «Кибербезопасность»: «Благодаря сложным технологиям, которыми располагают современные компании, где вы делаете покупки, знают о ваших желаниях, потребностях, мечтах и привычках, вероятно даже больше, чем вы сами. И используют эту информацию, чтобы заработать на вас такими способами, которых вы даже представить себе не можете. Добро пожаловать в мир добычи данных – бизнес стоимостью в 100 миллиардов долларов [48. С. 222]. Благодаря техническому процессу каждое наше действие производит сегодня больше данных, чем в прошлом (С. 223). И поверьте, компании используют эти данные, чтобы отобрать у нас деньги таким образом, о каком мы даже не подозреваем (С. 224).

Аналогичные выводы высказывает Н. Касперская: «Простой обыватель нужен как источник сбора информации о массовых перемещениях граждан, их предпочтениях, о том, с кем он дружит, чем пользуется, куда ездит. Большие данные (big data) – технологии в области аналитики для сбора таких данных со всех электронных устройств, поступающих в некий центр» [42].

На английском языке аферы называют unregulated investments chemes – неконтролируемые инвестиционные схемы. Они представлены двумя модификациями: схемой Понци (Ponzi`s cheme) и финансовой пирамидой (pyramids cheme), которые, в российском понимании, часто путают между собой [59. С. 42].

Финансовая пирамида основана на принципе многоуровневого маркетинга, когда каждый участник обязан привлечь в схему нескольких новых участников, взносы от которых идут в карман основателей и более ранних участников. Крах пирамиды связан с естественными ограничениями аудитории участников махинации.

Устойчивость схемы Понци определяется непрерывностью потока платежей инвесторов. К. Понци – итальянский аферист, устроивший в 1919–1920 гг. в США вымышленную спекуляцию на почтовых купонах (С. 45). Экономическое содержание любых схем в духе Понци заключается в том, что привлеченные средства от инвесторов

образуют фонд, за счет которого поддерживается привлекательность вложений, например через растущие выплаты от фиктивной деятельности. Схемы Понци заканчивают свою жизнь, когда объем изъятий из фонда перекрывает платежи новых инвесторов (С. 42).

У любой финансовой аферы есть закономерный цикл жизни, который неизбежно заканчивается крахом и попыткой ее основателя скрыться с остатками денег. Объем средств, аккумулируемых схемами, растет по экспоненте, а срок жизни зависит от величины обещанных доходов и размера целевого рынка или аудитории. Пирамида рушится, когда число ее участников уже не может расширяться. Схема Понци теоретически может держаться сколь угодно долго, если инвесторы полностью реинвестируют в нее свой доход. Однако и она не вечна, так как рушится из-за смены настроений участников или когда требуемые новые инвестиции превышают размер целевого рынка. Игра похожа на велосипед, который падает, как только прекращает движение. Учредители, как правило, прибегают к психологическим уловкам, чтобы создать впечатление или снискать к себе расположение потенциальных «клиентов» (С. 45).

Интервьюирование потерпевших показывает, что их вовлечению в мошенничество способствуют или сопутствуют несколько обстоятельств:

1) жертвами становятся преимущественно пожилые, однако образованные граждане;

2) информация об «успехах» устно распространяется среди круга лиц, хорошо знающих друг друга;

3) первые участники схем публично демонстрируют сверхдоходы (что подтверждает работоспособность схемы);

4) отсутствует психологическое давление, побуждающее вкладывать в схему;

5) учредители схемы имеют хорошую репутацию, например, «благотворителя» или «опытного», «профессионального» инвестора (С. 45).

Последствия краха финансовых схем включают в себя, прежде всего, общественные потрясения, макроэкономические эффекты… (С. 43).

Для России финансовые мошенничества на заре рыночной экономики были в диковинку. За рубежом они столь же стары, как и сам капитализм. Разнообразие схем ограничено только воображением преступников и легковерием инвесторов. Опыт борьбы со схемами за рубежом показывает, насколько важно уделять внимание регулированию финансовых рынков. Во-первых, во многих случаях инициаторы схем и их компании не лицензировались и не регулировались, в результате чего они находились вне сферы внимания властей. Во-вторых, насколько быстрой оказывается реакция регуляторов на сомнительные финансовые продукты, настолько меньшими будут потери.

Очевидно, что пока людьми движет жажда легких денег, схемы будут процветать. Надо вести информационную борьбу против схем, дискредитируя их в глазах потенциальной целевой аудитории (С. 44).

«Финансовая пирамида – схема организации инвестиционного бизнеса, в которой доход по привлеченным денежным средствам выплачивается не за счет их вложения в прибыльные активы, а за счет привлечения все новых инвесторов и денежных средств. Потенциальных инвесторов побуждают вкладывать денежные средства обещанием и выплатой первым из них больших доходов за счет последующих клиентов» [13. С. 56].

Финансовые пирамиды могут быть организованы на основе различных инструментов. Это могут быть договоры займа, траста, селенга, страхования, договоры на продажу товаров народного потребления и жилья по низким ценам, условием которых является предоплата с отсрочкой получения, а также ценные бумаги и суррогаты ценных бумаг. Одним из важнейших принципов деятельности финансовых пирамид, использующих в качестве финансового инструмента ценные бумаги и их суррогаты, является принцип самокотировки, создающий иллюзию ликвидности. Самокотировка ценных бумаг сочетается с пирамидальной системой выплат. Понятия «финансовая пирамида» и «мошенничество» не всегда тождественны. Так, по принципу пирамиды действуют многоуровневые маркетинговые конструкции, предлагающие своим участникам неплохие комиссионные, если они продадут товар следующим покупателям и убедят их продвигать его дальше. Принцип пирамиды лежит в основе любой схемы пенсионного обеспечения, основанной на распределительном механизме, – пенсионеры получают пенсии за счет ныне работающих граждан. Наибольшую известность получила финансовая пирамида Карло Понти (С. 57). Всего же в России начиная с 1991 г. сотрудниками МВД выявлено 518 пирамид, похитивших более чем у 400 тыс. граждан свыше 40 млрд руб. Всех жертв финансовых пирамид можно разделить на три категории: Первая – это люди, отдающие себе отчет в том, что инвестируют в финансовую пирамиду, но надеющиеся получить обещанную прибыль и вовремя выйти из нее. Вторая – люди, не имеющие ни малейшего понятия о том, откуда берутся деньги. Для инвестирования в финансовую пирамиду они берут кредит в банках, рассчитывая погасить его за счет полученных доходов. Третья, самая беззащитная и самая доверчивая, – пенсионеры, инвалиды, ветераны ВОВ, которые несут последние деньги в надежде их преумножить (С. 59). Выделим несколько наиболее существенных пунктов, которые позволят неквалифицированным инвесторам из большого числа финансовых структур, действующих на финансо-

вом рынке, выделить те из них, которые имеют признаки финансовых пирамид:

- обещание в рекламе и объявлениях гарантированных процентных выплат по привлеченным средствам по ставке, превышающей среднерыночный уровень (свыше 20 % годовых), сопровождающееся декларированием минимальных рисков;
- мимикрия под законно действующие финансовые структуры (указание номера чужой лицензии, использование в рекламе и объявлениях названий и фирменной символики известных компаний), спекуляция терминами и чужим авторитетом;
- отсутствие специальных лицензий. Форма привлечения средств – договор займа, с которым клиент может ознакомиться только в офисе компании или при личной встрече;
- отсутствие организации в числе членов СРО участников финансового рынка;
- неспособность компании подтвердить свою деятельность – куда размещаются средства и где можно проверить информацию об их размещении;
- приглашение к сотрудничеству агентов, выплаты которым осуществляются в зависимости от объемов привлеченного инвестирования;
- подведение духовно-ценностной базы под материальные интересы инвесторов, создание сообществ единомышленников;
- использование в качестве средства приема платежей в инвестиционные проекты систем интернет-платежей, а также системы почтовых переводов;
- прием денежных средств без выдачи квитанций или каких-либо других бухгалтерских документов, подтверждающих их внесение;
- распространение рекламы в основном в газетах бесплатных объявлений и на интернет-сайтах, а также использование спама для привлечения клиентов;
- отсутствие собственного сайта компании в сети Интернет или же размещение сайта компании на бесплатном хостинге, а также безграмотное содержание сайта…

…финансовые пирамиды представляют собой одну из наиболее распространенных и опасных моделей криминального поведения в сфере финансовых инвестиций (С. 61).

5 признаков современных финансовых пирамид:

1) Обещание гарантированной доходности свыше 20% годовых.

2) Отсутствие специальных лицензий, форма привлечения средств – договор займа.

3) Мимикрия, спекуляция терминами и чужим авторитетом.

4) Приглашение к сотрудничеству агентов, выплаты в зависимости от объемов привлеченного инвестирования.

5) Опиум для народа – ряд компаний не просто собирают деньги, но подводят духовно-ценностную базу под бренные материальные интересы, создавая некое сообщество единомышленников [69].

«10 поводов насторожиться, список черт, которые не обязательно свидетельствуют о противозаконности схем, однако свойственны многим сегодняшним пирамидам:

1. Средства привлекаются по договорам займа, в рекламе их называют вкладами.
2. Основное внимание акцентируется на процентных ставках и графике выплат, о способе приумножения капитала рассказывается в общих словах.
3. Вам предлагают инвестировать в некие уникальные, высокодоходные проекты, ноу-хау.
4. Не упоминается о рисках частичной или полной потери вложений.
5. По договорам доверительного управления гарантируется доходность.
6. В рекламе фигурируют лицензии, не относящиеся к основной деятельности.
7. Организация зарегистрирована в форме кредитного кооператива или потребительского общества и работает по принципу сетевого маркетинга.
8. Договор заключается не с тем юридическим лицом, которое упоминается в рекламе.
9. Вам перечисляют «известных» партнеров, например зарубежных, о существовании которых вы никогда не слышали.
10. Обещанная доходность заметно превышает ставки по банковским вкладам» [55].

Современный итог российского пирамидоведения: россияне не могут распознать признаки финансовой пирамиды – правильный ответ дали 27 % респондентов. По данным НАФИ, эта цифра почти не меняется на протяжении 7 лет. Россияне не могут распознать признаки пирамиды из-за невысокой финансовой грамотности и плохой осведомленности о различных продуктах и услугах кредитно-финансовых и инвестиционных компаний. В 2014 г. граждане РФ лишились свыше 2 млрд руб. по вине финансовых пирамид. В 2014 г. была пресечена деятельность 250 пирамид [77].

Одна из разновидностей мошенничества – таймшер – особая форма собственности, предусматривающая, что одним и тем же зданием или квартирой, как правило, на знаменитых европейских курортах поочередно владеют несколько людей определенное число дней в году. По данным пресс-службы Европола, многолетняя практика таймшера показывает, что в большинстве случаев эта форма собственности является чистым мошенничеством [86. С. 5]. Я понял одно, что люди так созданы и пороки есть почти у всех. Только пороки разные. Жадность – это один из пороков, которому подвержены многие. Пока есть

люди, ведомые жадностью, будут существовать люди, которые строят свой бизнес на этом. Все одинаковые: и клиенты, которые хотят получить на пустом месте тысячи, и те, которые на этом живут [Там же. С. 95]. Клиенты никак не хотели признаться в том, что они сами отдали эти проклятые деньги, потому что сами непомерно жадные и гнались за сверхприбылями, готовы были зарабатывать деньги из воздуха, не думая, откуда и как [Там же. С. 172–173]. Человек, который купил свой таймшер за тысячу долларов, приходит к вам продать за десять–двадцать тысяч долларов?! И верит, что это возможно! И готов платить столько, сколько вы попросите. Он давно знает, что у него на руках простая бумажка, воздух, потому и хочет от неё избавиться. То есть хочет, чтобы кто-нибудь другой за сумасшедшие деньги купил у него этот воздух. Вот что движет клиентами: желание погреть руки на глупости другого [Там же. С. 312].

Одиночное проживание, отягощенное алкоголизмом: черные риэлторы.

Мой дом – моя крепость, фортификация в сфере охраны жилищ: «большинство новых клиентов к нам приходят уже после того, как произошли неприятности – ограбили квартиру или дом, взломали дверь у соседей. Но с течением времени люди все чаще начинают задумываться о превентивных мерах по защите жилья – своего и своих близких [78. С. 96]. Что касается частных лиц…: если человек привык каждый день ставить квартиру на охрану и чувствовать себя спокойно, он будет делать это независимо ни от чего. Постепенно меняется менталитет: все чаще люди стали задумываться о профилактике в сфере личной безопасности. Мировой опыт показывает, что охраняемые квартиры подвергаются нападению реже на 87 %. Преступник ведь боится не сигнализации, а оперативного реагирования» [Там же. С. 97]. Среднее время реагирования по Москве – 8 минут, в области – чуть больше. В Москве в день вскрывается от 100 до 200 квартир, а в области такое «посещение» дач – вообще национальный вид спорта. В Европе и США услуги охраны очень тесно связаны со страхованием имущества, а у нас этот рынок находится в зачаточном состоянии. Мы не зарабатываем на установке оборудования, основной оборот для нас составляет абонентская плата – 1 590 руб. ежемесячно (мониторинг, сервисное обслуживание, услуги реагирования). Монтаж охранной системы стоит около 30 тыс. руб., на оборудование действует пожизненная гарантия. Постепенно люди приходят к пониманию необходимости обращения к специалистам, если речь идет об обеспечении собственной безопасности [Там же. С. 98].

Может быть, явление для РФ пока не очень привычное: престижный адрес как прикрытие сомнительных контор. Престижный офис – «виртуальный», им могут пользоваться десятки клиентов, платя за аренду по 100 долл. в месяц. «Виртуальный» офис – тот же добрый а/я, только в более изощренной форме. Снимая помещение, можно пользоваться службой ответов на звонки, ресепшн и переговорными комнатами, почтовым адресом. Это почти обычный офис, арендуемый несколькими фирмами или бизнесменами. Только большинство съемщиков редко там появляются. В мире насчитывается 8 тыс. операторов «виртуальных» офисов. В массе своей пользующиеся ими бизнесы абсолютно легитимны. Но плевые расценки привлекают и аферистов [21].

«УК устанавливает ответственность и за получение взятки, и за дачу взятки должностному лицу. Такое преступление, как дача взятки, подразумевает выполнение каких-либо действий. В российском законодательстве за дачу взятки должностному лицу предусмотрена уголовная ответственность. Юридические лица не могут быть привлечены к уголовной ответственности, поэтому за дачу взятки по всей строгости закона придется отвечать физическим лицам – взяткодателям» [33. С. 80]. Дарение госслужащим подарков за совершение или действие (бездействие) в пользу дарителя уголовный закон рассматривает в качестве взятки независимо от стоимости передаваемой вещи. Чтобы признать подарок инспектору взяткой, необходимо доказать причинно-следственную связь между подарком и совершением должностным лицом определенных действий в пользу дарителя. Существующая грань между дарением и взяткой во многом носит оценочный характер, поэтому любое вручение подарка налоговому инспектору может быть связано для главного бухгалтера с риском привлечения к уголовной ответственности за дачу взятки [Там же. С. 81].

Существует и гражданско-правовая ответственность директора, членов коллегиальных органов [61], а также административная ответственность. Выделено 12 составов. Уголовная – 10 составов [66]. КОАП РФИ УКРФ содержит ряд статей со сходными названиями. Разница в том, какие статьи применяются, состоит в масштабе допущенных нарушений и размере причинённого вреда (потенциальной возможности его причинения). Действует алгоритм: если налицо факт нарушений, руководитель компании подлежит уголовной ответственности. Невозможна «двойная ответственность» директора за один и тот же поступок. Уголовную ответственность можно рассматривать как крайнюю меру в отношении руководителей. В отличие от гражданско-правовой и административной, к уголовной ответственности могут быть привлечены только руководители организаций, но не юридические лица [Там же].

Еще один аспект: фальшивые деньги, за хранение и сбыт которых предусмотрено наказание – лишение свободы до 8 лет со штрафом или без такового (ст. 186, ч. 1. УК РФ).

Личная безопасность. Здесь мы исходим из положения Бека: любой человек для любого человека представляет большую или меньшую степень риска.

Из книги Л. Замперини [34]. Бесплатные советы: 1. Осведомленность – залог спасения. Будьте всегда начеку – и это спасет вам жизнь. Я всегда учу детей обращать внимание на то, что происходит вокруг… и оценивать обстановку, думая о последствиях. Это единственное, чему не учат в школах; между тем это залог выживания в этом мире. Доктор Роберт называл это бдительностью, но вы можете называть «простой мудростью» (С. 189). 2. Если у парня пистолет – и вы не на поле боя, ведите себя тише воды ниже травы. 3. Мы с Синтией всегда давали друг другу право на частную жизнь. Когда наступают непростые времена [в браке], нужно постараться не допустить того, чтобы стороны начали бросаться друг на друга. Я всегда разговаривал отдельно с мужем и отдельно с женой. Я повторял им то, что мне однажды сказал брат: Если ты не прав, признай это. Если прав, держи рот на замке. Большинство этих пар прожили вместе еще много счастливых лет» (С. 190).

«Если уже возникла необходимость в охране, агентство следует выбирать очень тщательно. Мнение профессионалов однозначно: любой бизнесмен или банкир может избежать покушения на свою жизнь; опасные ситуации возникают в большинстве случаев из-за неправильности поведения самого предпринимателя. Предотвратить убийство, когда киллер уже «в работе», очень трудно. Профессиональные охранные предприятия стремятся к профилактике покушений еще на ранних стадиях криминального «наезда». Они дают не только физическую защиту, но и разъясняют клиенту те ошибки в его поведении, которые вызвали у его конкурентов желание его убить.

… телохранители делят всех бизнесменов на три группы:

• Лавочники, которых бандиты долго-долго предупреждают и долго-долго пугают, прежде чем перейти к серьезным криминальным мерам.

• Мелкие и средние бизнесмены. Их тоже предупреждают заранее, угрожая смертью.

• Уровень крупных бизнесменов. Люди должны понять, что их могут убрать [92].

Ю. Конева (2008). Как вести себя при встрече с милицией [44]. Гл. I. Предупрежден – значит вооружен. Гл. II. Предъявите документы. Гл. III. Административное задержание. Гл. IV. Уголовное задержание. Гл. V. Кто идет работать в милицию. Гл. VI. Применение силы. Гл. VII. Как обжаловать действия сотрудников милиции. Гл. VIII. Способы психологической защиты. Гл. IX. Если к вам в офис пришла милиция. (Ю. Конева, к.ю.н., ректор Института правовой и экономической безопасности). Ценность подхода заключается как минимум в следующих аспектах:

Господство, доминирование личного интереса домохозяина.

Грамотная ролевая аранжировка – законопослушный гражданин, он же налогоплательщик, а с другой стороны, госслужащий, защитник гражданина, представитель налогополучателя.

Не стоит сбрасывать со счетов и возможность силового предпринимательства, его влияние на специфику ролеприменения [19], опасности от людей: матрицу наказаний осужденным (облсуды и проч.).

Очень важный вопрос – документы, которыми обладает домохозяин в промежутке от самого первого – «свидетельство о рождении» до самого последнего, их может быть мало или много, что зависит от активности домохозяина в ролевой сфере. Вот перечень, может быть, немножко выше среднего обычного домохозяина:

1. Паспорт гражданина РФ. 2. Свидетельство о регистрации транспортного средства. 3. Водительское удостоверение. 4. Заграничный паспорт. 5. Свидетельство о браке. 6. Свидетельство о среднем образовании. 7. Документ о высшем образовании. 8. Диплом кандидата наук. 9. Диплом доктора наук. 10. Аттестат доцента. 11. Аттестат профессора. 12. Служебное удостоверение. 13. Трудовая книжка. 14. Пенсионное свидетельство. 15. Полис ОМС. 16. Полис ОСАГО (год). 17. Полис КАСКО (год). 18. Полис страхования имущества. 19. Полис страхования жизни. 20. Банковские карты. 21. Свидетельство о собственности жилища и т.д. Самый распространенный и универсальный – паспорт гражданина РФ, без которого нечего делать во многих учреждениях, оказывающих услуги, особенно государственные и финансовые. Утрата паспорта может привести к негативным последствиям для его хозяина, если он не отреагирует быстро и правильно. Документы – тема отдельной публикации: получение, срок годности, хранение, безопасность и т.п.

Огромный раздел – обязательства: А) понятия в аспектах: экономическом, финансовом, домохозяйственном, правовом. Б) Классификация. В) Последствия: коллекторы, суды, личное банкротство, перемещение. Коллекторство – очень противоречивое явление, о котором много пишут. Интересный подход см. в [17]. Г) Служба судебных приставов; разные, сферы деятельности. «Служба приставов разработала типовое соглашение с банками, которое позволяет отправлять запросы о списании средств в электронном виде. Теперь банки и приставы могут обмениваться информацией через выделенный интернет-канал с использованием специального криптошлюза – устройства для защиты данных, которое соответствует требованиям ФСБ – и электронной подписи.

Есть схема взаимодействия: 1) судебное решение; 2) запрос ССП; 3) ответ КБ; 4) постановление о списании средств.

Исключение: невозможно удержать средства с кредитной карты; не могут быть списаны различные пособия; запрещается изымать более 50 % ежемесячного дохода [4].

Банк впервые списывает денежные средства со счета клиента по общему правилу только с его согласия – акцепта, который означает, что плательщик признает платежное требование кредитора (своего контрагента по сделке) правильным и подлежащим оплате и тем самым поручает банку списать сумму платежного требования со своего счета. Исключение, которое позволяет банку списывать деньги со счета клиента и без его согласия, т.е. в без акцентном порядке. Выделено 5 случаев [10. С. 82].

«Когда человек ручается за другого, он должен хорошо осознавать, что идет на риск, нужно здраво оценивать уровень платежеспособности заемщика, для которого вы хотите стать гарантом» [40. С. 42]. Некоторые граждане готовы не только полностью принять на себя риски по неуплате долга заемщиком, но и поручаться за совершенно незнакомого человека. Законных способов «отвертеться» от выплат по чужому кредиту фактически нет.

Можно попытаться в судебном порядке признать договор поручительства недействительным. Поручитель, погасивший долг, согласно ГК имеет право требовать от заемщика возмещения суммы, которая была выплачена кредитору. Зачастую люди искренне убеждены, что поручительство – это всего лишь жест вежливости [Там же. С. 43].

«Чтобы возник долг, не обязательно брать его самому, достаточно принять наследство, которое переходит к другим лицам в порядке универсального правопреемства – в неизменном виде как единое целое и в один и тот же момент. В состав наследства входят принадлежавшие наследодателю на день открытия наследства (его смерти) вещи, иное имущество, в том числе имущественные права и, что важно, обязанности. Это означает, что принять в наследство ценное имущество, отказавшись от долгов наследодателя, нельзя. Не входят в состав наследства права и обязанности, неразрывно связанные с личностью наследодателя.

Под долгами наследователя следует понимать все имевшиеся у наследодателя к моменту открытия наследства обязательства, не прекращающиеся смертью должника, независимо от наступления срока их исполнения, а равно от времени их выявления и осведомленности о них наследников при принятии наследства. Лица, принявшие наследство, становятся должниками кредитора наследодателя» [57. С. 65].

В любом случае целесообразно просчитать возможность уплаты долгов и налогов еще до принятия наследства. Возможно, окажется, что проще отказаться от него вовсе [Там же. С. 68]. Приняв наследство, можно стать не просто должником, но и примерить на себя роль банкрота. В наше время у каждого есть возможность стать субъектом кредитной истории, даже у тех, кто избегает брать долг. Кредитная история – это информация, характеризующая исполнение заемщиком принятых на себя обязательств по договорам займа (кредита) и хранящаяся в бюро кредитных историй (БКИ).

После 1.03.15 в перечень субъектов кредитных историй входят не только заемщики по договору займа (кредита), но и поручители, принципалы, в отношении которых выдана банковская гарантия. Источником формирования кредитной истории может стать организация, в пользу которой вынесено вступившее в силу и не исполненное в течение 10 дней решение суда о взыскании денежных сумм в связи с неисполнением обязательств по внесению платы за жилое помещение, коммунальные и иные услуги. Запись в информационной части кредитной истории заемщика формируется в БКИ заимодавцем или кредитором (банком, микрофинансовой организацией, кредитным кооперативом и др.) по каждому поданному ими заявлению о предоставлении займа (кредита). Аналогично собирается информация о поручителях. Даже если заемщику в займе (кредита) отказано, данные о его заявлении и причинах отказа попадут в кредитную историю [Там же. С. 70].

Полная материальная ответственность означает возмещение работником причинного ущерба в размере его фактической стоимости исходя из рыночных цен на день причинения ущерба. Она наступает, когда на работника в соответствии с трудовым Кодексом РФ или иными федеральными законами возложена материальная ответственность в полном размере за ущерб, причиненный работодателю при исполнении работником трудовых обязанностей. Необходимо соблюдение ряда условий… [46. С. 108]. Разновидности полной материальной ответственности – индивидуальная и бригадная (коллективная).

Приведем структуру одного из немногих учебных пособий по домохозяйственному менеджменту [74]. 3 части: I. Организация домашнего хозяйства. II. Управление финансами семьи. III. Семейный менеджмент.

В I части есть глава V. Безопасность дома. 5.1. Ваш дом – ваша крепость. 5.2. Советы по безопасности в доме. 5.3. Технические средства безопасности. 5.4. Средства индивидуальной защиты. 5.5. Защита от нападений на улице и дома. 5.6. Безопасные покупки. Гл. VI. Экология дома. 6.1. Экология жилища. 6.2. Вода. 6.3. Бытовая химия. 6.4. Радиационный фон. Гл. VIII. Гараж и автомобиль. 8.2. Защита автомобиля. 8.4. Охрана гаража. Во II части. – гл. II. Страхование семьи. 2.1. Личное. 2.2. Имущества. 2.3. Ответственность. Гл. XII. Финансовый портфель ДХ. 12.4. Финансовая безопасность: недвижимость, антиквариат. В III части гл. 18. Здоровье семьи…

Здесь избран распределенный метод описания опасностей для домашнего хозяйства, другой метод, требующий хорошей теоретическо-практической проработки – объектной, когда все вопросы сосредоточены в одном месте.

Итак, весьма сжато мною рассмотрены проблемы безопасности домохозяйства, по преимуществу в описательном виде, единственно возможном в условиях становления целостной теории домохозяйства и окружающих его сред.

Литература

1. *Акимов К.* Долгостройка // Бизнес- журнал. 2011. № 10. С. 68–70.
2. *Александров П.* Карточный разбор // РБК. 2010. № 5. С. 108–111.
3. *Алексеевских А.* Реальные банки не пускают на виртуальные барахолки // Финанс. 2008. № 19. С. 38–39.
4. Банки начнут массово списывать деньги с должников судебным решением // Банковское дело. 2015. № 9. С. 9.
5. *Баррер С.* Осторожно, спорт. М., 2015. 230 с.
6. *Бахвалова М., Сорокина А.* Тише едем // РБК. 2014. № 8, С. 26–27.
7. *Белоусов А.Л.* Становление института банкротства физических лиц в аспекте развития потребительского кредитования // Финансы и кредит. 2014. № 25. С. 32–37.
8. *Богданова О.* Не прячьте ваши денежки // РБК. 2013. Дек. С. 32–34.
9. *Буркеман О.* Антидот. Противоядие от несчастливой жизни. М., 2014. 240 с. (особенно гл. 6. «Ловушка безопасности»).
10. *Бычков А.И.* О безакцептном списании денег со счета // Банковское дело. 2015. № 3. С. 70–75.
11. *Бычков А.И.* Риски использования мобильного банка// Бухгалтерский учет. 2015. № 5. С. 107–110.
12. В России используется только каждая пятая кредитная карта // Банковское дело. 2015. № 6. С. 35.
13. *Вавулин Д.А., Федотов В.Н.* Финансовые пирамиды: понятие, механизм функционирования, примеры из мировой практики // Финансы и кредит. 2009. № 29. С. 56–61.
14. *Вакильев Ф.* Борьба с карточным мошенничеством // Аналитический банковский журнал. 2008. № 2. С. 70–74.
15. *Вартофский М.* Модели. Репрезентация и научное понимание. М., 1988.
16. *Вахламова А.* Чип не могущий // РБК. 2011. № 1–2. С. 46–49.
17. *Великжанин Т.Г.* Как вести себя с коллектором? // Деньги и кредит. 2009. № 10. С. 57–60.
18. *Волков В.* За что убивают бизнесменов // Forbs. 2009. № 4.
19. *Волков В.* Силовое предпринимательство. XXI век. Экономико-социологический анализ. СПб., 2012.
20. *Глазов А.А.* Банковская верификация: планирование, верификационные ситуации и версии // Банковское дело. 2016. № 1. С. 75–79.
21. *Голдстейн М.* Шик и блеск // Buisnes week Россия. 2008. № 14. С. 035–039.
22. *Голенищев А.А.* Банкоматное мошенничество: как уберечь себя и своих клиентов // Банковское дело. 2009. № 1. С. 74–76.
23. *Гольцблат А., Торопов А.* Валютный риск // Ведомости. 2015. 21 апр.
24. *Гостева Е.* Плакали ваши денежки // РБК. 2008. № 2. С. 52–55.
25. *Гринберг Э.* Стартап 007 // Forbs. 2013. № 10. С. 212–217.
26. *Гудман М.* Чему можно научиться у преступного сообщества // Harvard Business Review. 2011. № 12. С. 17–20.
27. *Гундорин Д.В.* Социальная инженерия – альтернативный способ совершения преступлений // Банковское дело. 2011. № 11. С. 70–71.
28. *Гуркина Е.* Как защищался пластик // Финанс. 2009. № 41. С. 36–41.
29. *Диденко М.* Не стройте из себя героя // Комсомольская правда. 2015. 1–8 июля.
30. *Достов В.Л., Шуст П.М.* Меры по надлежащей проверке клиента: новые подходы к повышению эффективности // Банковское дело. 2012. № 5. С. 60–64.
31. *Евдокимов Д.А.* Безопасность мобильного банкинга: защита от «краж по воздуху» // Банковское дело. 2014. № 8. С. 70–73.
32. *Жеглова Ю.* Крутой уокер для сети // Компания. 2010. № 36. С. 46–49.
33. *Жильцов А.* Подарок или взятка: юридические аспекты // Главный бухгалтер. 2008. № 1. С. 77–81.
34. *Замперини Л., Ренсин Д.* Не отступать и не сдаваться. Моя невероятная история. М., 2016.
35. *Зарщиков А.* Алло, мы ищем криминальные таланты // Финанс. 2010. № 34. С. 30–32.
36. *Земцов А.А.* Введение в самоменеджмент здоровья и жизни домохозяина // Проблемы учета и финансов. 2013. № 2. С. 3–15.
37. *Земцов А.А.* Версия VI. Содержание и структура направления «Финансы домохозяйств» // Проблемы учета и финансов. 2015. № 1. С. 3–8.
38. *Земцов А.А.* Концепция трудностей как выражение неспецифических опасностей домохозяина и его домохозяйства // Проблемы учета и финансов. 2015. № 3. С. 16–30.
39. *Кадачигов В.* Отмычка для смартфонов // Ведомости. 2015. 6 июня. № 3846.
40. *Калинникова Т.* Кредит в «наследство» // Финанс. 2007. № 42. С. 42–43.
41. *Кантышев П.* Киберпреступники в списках не значатся // Ведомости. 2015. 6 февр. № 3766.
42. *Касперская Н.* Мы все – большие данные // Вестник Науфор. 2014. № 12. С. 15–24.
43. *Керценбаум К.* Кредитные карты по выгодным ценам: все, что вы хотели узнать о подпольной экономике, но боялись спросить // Аналитический банковский журнал. 2008. № 11–12. С. 75–78.
44. *Конева Ю.* Как вести себя при встрече с милицией. М., 2008.
45. *Крюков Д., Бахвалова М.* Оплата вперед. Российский рынок предоплаченных карт // РБК. 2012. № 6. С. 66–68.
46. *Ларина Л.Л.* Полная материальная ответственность работника // Бухгалтерский учет. 2013. № 6. С. 108–113.
47. *Легуенко М., Трофинова Е.* Граница на замке // РБК. 2011. Итоговый. С. 125–127.
48. *Линдстром М.* Вынос мозга! Как маркетологи манипулируют нами и убеждают покупать их товары. М., 2013. 296 с.
49. *Линдстром М.* Идеальная манипуляция // Forbes. 2012. № 10. С. 258–263.
50. *Логинов О.* Энциклопедия мошенничества. М., 2007.
51. *Лотфуллин Р.К.* Что дает банкам институт банкротства граждан? // Банковское дело. 2015. № 11. С. 82–86.
52. *Лямин Я.В.* Проблемы управления рисками, связанными с электронными банкингом // Банковское дело. 2010. № 10. С. 74–78.
53. *Максуров А.А.* Правовая основа деятельности коллектора // Банковское дело. 2008. № 12. С. 88–90.
54. *Малева Т.* Устойчивая неподвижность // Вестник Науфор. 2015. № 3. С. 21–26.
55. *Мальцев О.* Вечное обаяние пирамид // Финанс. 2008. № 20. С. 42–47.
56. *Маркополос Г.* Финансовая пирамида Бернарда Мэддоффа. М., 2012.
57. *Мацкявичене Е.В.* Долговые обязательства граждан // Бухгалтерский учет. 2015. № 5. С. 65–68.
58. Между должником и президентом Медведевым // Банковское обозрение. 2010. № 1. С. 94–97.
59. *Моисеев С.* Долой аферы // Банковское обозрение. 2012. № 12.

60. *Молохов А.В., Андрусяк А.В*. Коллектор и пристав банку не товарищи? // Банковское дело. 2012. № 6. С. 80–82.

61. *Молохов А.В.* О гражданско-правовой ответственности топ-менеджеров кредитных организаций // Банковское дело. 2013. № 3. С. 87–89.

62. *Молохов А.В., Порубиновская В.В.* Когда клиент прав // Банковское дело. 2015. № 3. С. 79–81.

63. *Молохов А.В., Порубиновская В.В.* Когда вклад все-таки клад // Банковское дело. 2014. № 7. С. 84–86.

64. *Молохов А.В., Порубиновкая В.В*. Защита вкладов – теперь на конституционном уровне! // Банковское дело. 2015. №12. С. 79–81.

65. *Молохов А.В., Порубиновская В.В.* Дважды проверь поручителя // Банковское дело. 2015. № 6. С. 89–91.

66. *Никитина В.Ю*. За что могут наказать руководителя компании // Бухгалтерский учет. 2015. № 2. С. 99–102.

67. *Новикова В.* Как защищаться от кибервторжения // Аналитический банковский журнал. 2012. № 5. С. 50–54.

68. Памятка ЦБ РФ «О мерах безопасного использования банковских карт»// Деньги и кредит. 2009. № 11. С. 69–70.

69. Пять признаков современных финансовых пирамид // Наши деньги. 2007. № 6. С. 6–11.

70. *Разин С.А.* Большой потенциал и быстрое развитие // Финансовый бизнес. 2006. № 11–12. С. 10–17.

71. *Ракшенко Л*. Магический бизнес // Harvard Business Review. 2012. № 6–7. С. 34–40.

72. *Ревенков П.В., Бердюгин А.А*. Основные направления обеспечения кибербезопасности в условиях ДБО // Банковское дело. 2015. № 7. С. 66–71.

73. *Ревенков П.В., Тимкова А.А*. Мобильные платежи: риски использования в сомнительных операциях // Финансы и кредит. 2012. № 2. С. 56–61.

74. *Резник С.Д., Бобров В.А., Егорова Н.Ю*. Менеджмент в домашнем хозяйстве: учеб. пособие. 3-е изд. М., 2010.

75. Рейтинг мошенничеств // Финанс. 2010. № 39.

76. *Рипли А*. Кризисы и катастрофы: кто и почему выживает. М.: Эксмо, 2009.

77. Россияне не могут распознать признаки финансовой пирамиды // Банковское дело. 2015. № 8. С. 59.

78. *Рябов С.* Стражи порядка // РБК. 2010. Май. С. 95–98.

79. *Савкин А.* Заслуженный строитель (О.С. Мавроди) // Forbes. 2012. Март. С. 132–137.

80. *Саруханова О.* Золотой роуминг // РБК. 2010. № 12. С. 78–83.

81. *Сачков И*. DDOSатаки. Технологии. Тенденции. Реагирование и оформление доказательств // Аналитический банковский журнал. 2010. № 9. С. 82–85.

82. *Седаков П.* Криминалисты в сети // Forbes. 2014. № 1. С. 110–115.

83. Сплошной возврат // Персональные финансы. 2007. № 5. С. 13–17.

84. *Талеб Н., Гольдстайн Д., Шпицнагель М.* Черные лебеди и риск- менеджмент // Harvard Business Review. 2009. № 12. С. 60–65.

85. Технология комплаенс. Тема номера // Банковское обозрение. 2012. № 12. С. 45–69.

86. Точка А. Таймшер. Сертификат в страну дураков. М., 2006. 320 с.

87. *Тысячникова Н.А*. Риски Интернет-банкинга: принципы и организация надзора // Банковское дело. 2010. № 10. С. 79.

88. *Хачатуров А*. Исключения в поиске // РБК. 2015. 21 авг.

89. *Хемп П*. Смерть от передозировки информации // Harvard Business Review. 2009. № 12. С. 73–80.

90. Центр мониторинга компьютерных атак начал работу // Банковское дело. 2015. № 8. С. 45.

91. *Чайкина Ю.* Безопасная карта. Как выбрать кредитку, чтобы она работала на вас, а не вы на нее // Forbes. 2012. № 4. С. 106–109.

92. *Швырков Г., Клин Б.* Спасение бизнесмена – дело рук самого бизнесмена // Коммерсантъ. 1995. № 10. С. 42–46.

93. *Шикин В.В*. Профилактика дефолта заемщика: определение стратегии взыскания на ранних этапах нарушения графика обслуживания долга // Банковское дело. 2015. № 11. С. 63–65.

94. *Эзрох Ю.С*. Достоверность отчетности российских банков по депозитам физических лиц // Банковское дело. 2014. № 7. С. 54–59.

95. Экономическая безопасность. Производство–финансы–банки. М., 1998.