кадровая безопасность в банках

в марте 2018 года состоялся круглый стол «Кадровая безопасность в банках». В мероприятии приняли участие более 70 человек, среди которых были руководители департаментов безопасности, начальники отделов по работе с персоналом, руководители HR-служб, руководители управлений рисками российских банков, а также представители компаний, работающих в сфере ИБ и кадровой безопасности

Среди активных участников Круглого стола были: вице-президент ООО КБ «Международный расчетный банк» **Валерий ГОЛЕВ**; вице-президент по работе с персоналом АО АКБ «Алеф-Банк» **Екатерина СУХОБАЕВСКАЯ**; директор департамента безопасности ПАО «АК БАРС» БАНКА **Евгений ИВАНОВ**; руководитель кадровой службы ООО «Банк БЦК-Москва» **Елена ЖАРОВА**; начальник группы сопровождения трудовых отношений отдела сопровождения административных дел и исковой работы ООО «Хоум Кредит энд Финанс Банк» **Ольга ЧЕРЕМУХИНА**; директор департамента организационного развития и управления персоналом АКБ «РосЕвроБанк» **Оксана ЛЫНДИНА**; руководитель перспективных разработок АО «ИнфоВотч» **Андрей АРЕФЬЕВ**; заместитель генерального директора INFOSECURITY **Михаил ЛЕВАШОВ**; управляющий партнер юридической фирмы «Делио» **Елена КИСЛОВА**; начальник отдела по работе с персоналом департамента кадровой политики АО «НС-Банк» **Вера КИСЕЛЕВА**; доцент кафедры прикладной информатики и информационной безопасности, РЭУ им. Г.В. Плеханова **Владимир КРЕОПАЛОВ**; независимый эксперт **АЛЕКСАНДР ТУРКИН**; начальник отдела департамента комплаенс-контроля АО АКБ «РосЕвроБанк» **Сергей БАБУШКИН**; начальник отдела кадров ПАО АКБ «Держава» **Юлия БУЛАНОВА**; начальник управления информационной безопасности АО КБ «ЗЛАТКОМБАНК» **Александр ВИНОГРАДОВ**; Head of Security, Russia & CIS Digital Finance International **Игорь ХОБТА**; эксперт по информационной безопасности и судебной экспертизе **Евгений ЦАРЕВ** и др.

Организатор: **Национальный Банковский Журнал (NBJ)** при содействии Ассоциации российских банков.
Модератор: заместитель генерального директора Академии информационных систем (АИС) **Игорь ЕЛИСЕЕВ**.

Игорь ЕЛИСЕЕВ,
заместитель генерального директора Академии информационных систем (АИС)

NBJ: В первую очередь, хочется обсудить один из самых актуальных вопросов, который возникает, когда речь заходит о кадровой политике банков, – моделировании угроз, как исходящих от персонала финансово-кредитных организаций, так и нацеленных на персонал. Наверное, не откроем ни для кого секрет, сказав, что человеческий фактор – уязвимое звено в любой коммерческой организации, но особенно это справедливо для банков, поскольку в них люди оказываются максимально близки к деньгам.

Второй вопрос, непосредственно связанный с тем, о чем говорилось выше, – защита персональных данных сотрудников, принимающих ключевые для банков решения. Это напрямую относится к безопасности финансово-кредитных организаций. И тема, которая особенно интересна, – применение полиграфа и психофизиологических инструментов при проведении внутренних служебных расследований; противодействие социальной инженерии. И наконец, мы считаем важным затронуть и такой момент, как регулирование кадровой политики банков. Мы знаем, что разрабатываются профессиональные стандарты, повышаются требования к репутации и опыту ключевых сотрудников кредитных организаций. Всем хорошо известно, что уже давно применяется и такой инструмент, как профессиональная дисквалификация для людей, попавших в «черные списки» в результате банкротств банков или из-за введения в банки временных администраций. При этом круг лиц, которые теоретически могут оказаться «отлученными от профессии», постоянно расширяется. И это весьма настораживающая тенденция, поскольку отзывы лицензии происходят постоянно. Соответственно, все больше становится тех, кто не сможет на протяжении ряда лет занимать ведущие позиции в финансовых организациях.

Все эти и другие вопросы организаторы круглого стола и предлагают нам обсудить. Очевидно, что для этого потребовался бы, наверное, целый день, а не несколько часов, которыми мы располагаем, но надеемся, что нам удастся все же рассмотреть наиболее интересные аспекты заявленных проблем.

В. КРЕОПАЛОВ (РЭУ им. Г.В. Плеханова): Я представляю РЭУ им. Плеханова и одновременно являюсь экспертом Академии информационных систем в области экономической безопасности и конкурентной разведки. Мне хотелось бы начать нашу дискуссию с вопроса, непосредственно относящегося как к кадровой безопасности, так и к безопасности кадров. Очень часто мы с вами говорим об угрозах, которые исходят только от персонала, и не обращаем или обращаем очень мало внимания на угрозы, направленные на персонал. То есть эти два понятия или явления «разрываются», а ведь они непосредственно связаны между собой. Мы концентрируем внимание в основном на безопасности руководителей организаций. Но занимаемся ли мы в достаточной мере обеспечением безопасности рядовых сотрудников? Давайте говорить честно: мы живем в такое время, когда злоумышленники действуют очень осмысленно и целенаправленно. Они собирают информацию о сотрудниках, выявляют слабые места каждого из них. А потом используют эту информацию для шантажа или запугивания и т.д. Главный метод противодействия тут один – ликбез, который необходимо периодически проводить среди персонала. Сотрудникам надо рассказывать о том, какие угрозы существуют, как они могут реализовываться. И второй момент – надо собирать информацию о персонале и выявлять внутри него группы риска, которые могут заинтересовать злоумышленника. Такой подход позволит, к примеру, отслеживать изменения привычного поведения людей, их отношение к своим должностным обязанностям и т.д. Это даст нам возможность на начальном этапе выявлять угрозы, направленные на наших сотрудников.

Резюмирую вышесказанное: основой кадровой безопасности должна быть постоянная информационно-аналитическая работа, непрерывный сбор сведений о жизни и деятельности наших сотрудников. Для всего этого необходимо, в том числе, выстроить доверительные отношения с людьми.

NBJ: Это действительно очень важный момент. Расхожая реакция людей на попытки сбора о них

Владимир КРЕОПАЛОВ,
доцент кафедры прикладной информатики и информационной безопасности,
РЭУ им. Г.В. Плеханова

информации – это вмешательство в личную жизнь. Тут же на первый план выходят правовые и морально-этические вопросы.

А. ТУРКИН (независимый эксперт): Я хотел бы задать вопрос и модератору, и первому нашему спикеру. Какое, на ваш взгляд, подразделение в банке должно заниматься кадровой безопасностью – HR, СБ или какое-либо иное? Существует ли в высшей школе профессиональный стандарт для данных должностей, какие-то специальные требования регулирующих органов к таким сотрудникам? Готовят ли где-то специалистов по кадровой безопасности?

В. КРЕОПАЛОВ (РЭУ им. Г.В. Плеханова): Если в банке существует подразделение кадровой безопасности, то непосредственно оно и должно этим заниматься. Если его нет, то над выстраиванием доверительных отношений должно работать подразделение по обеспечению экономической безопасности. Мне кажется, что стандарт работы этого отдела уже разработан. И это правильно, потому что одна из основных угроз в сфере кадровой безопасности – это утечка информации, а в этом чаще всего бывают задействованы наши сотрудники, причем далеко не всегда персонал в таких случаях действует из дурных побуждений. Есть такой инструмент, как выведывание информации, при его применении объект не осознает, что он делится с собеседником теми данными, которые он не должен выдавать. И тут мы переходим уже к социальной инженерии, которая позволяет масштабировать этот процесс выведывания.

А. ТУРКИН (независимый эксперт): Мы знаем, что разработаны и известны модели угроз в сфере ИБ, а есть ли что-то аналогичное, когда речь идет об обеспечении кадровой безопасности? Существует ли законодательная база, рекомендации и инструкции ЦБ, других регуляторов, на которые можно было бы опираться при выработке такой модели и методов предотвращения и устранения таких угроз. Мне они не известны, кроме отдельных требований Банка России. При этом не прописаны методы их выполнения. Как многие коллеги знают, большинство сотрудников этой категории, к сожалению, вынуждены работать вне рамок правового поля. Если и есть внутренние банковские инструкции и технологические карты, то написаны они с опорой на экспертное мнение. А все потому, что нет утвержденных единых требований и стандартов.

В. КРЕОПАЛОВ (РЭУ им. Г.В. Плеханова): Угрозы в кадровой безопасности есть, общепринятых моделей нет, все зависит от человеческого фактора.

М. ЛЕВАШОВ (INFOSECURITY): Очень хорошо, что мы затронули тему угроз, связанных с работой сотрудников. Часто используются инструменты, которые позволяют увидеть, чем

Александр Туркин,
независимый эксперт

сотрудник занимается на своем служебном компьютере. Можно, к примеру, записывать работу сотрудника с клавиатурой, можно делать скриншоты (видеозаписи) экрана монитора. Но при этом все аутентификационные данные, которыми пользуется сотрудник, будут известны работникам службы безопасности, которые мониторят этого работника. Это уже нарушение правил работы с такими данными. В дальнейшем при проведении расследовании сотрудник может сослаться на то, что его конфиденциальные данные были доступны другим лицам. Кроме того, собираются и анализируются и другие сведения из жизни и работы сотрудников. В связи с этим возникают два вопроса. Что делать в случаях фиксации указанных выше аутентификационных данных – это первый вопрос. А второй заключается в следующем: не является ли сбор и анализ сведений о сотрудниках вмешательством в их частную жизнь? Хотелось бы получить ответы юриста.

О. ЧЕРЕМУХИНА (Хоум Кредит энд Финанс Банк): Мы в таких случаях подключаем руководителей подразделений, чтобы доверительные отношения, о

Михаил ЛЕВАШОВ,
заместитель генерального директора INFOSECURITY

необходимости которых здесь совершенно справедливо говорилось, выстраивались именно на уровне руководителей и их непосредственных подчиненных. Это делается для того, чтобы подключать службу безопасности только в исключительных случаях, избегать ситуаций, когда сотрудников пугают расследованиями по любому поводу. Мое мнение таково: в принципе, здесь очень востребованы человеческие отношения, не стандарты, не какие-то нормативные вещи, а то, чтобы между людьми были контакт и взаимопонимание. Такой подход дает хорошую отдачу.

А. ТУРКИН (независимый эксперт): Кто виноват и кто должен быть наказан за то, что банку был нанесен финансовый или репутационный ущерб или, если брать крайние случаи, остановка деятельности банка? Мы все были свидетелями известных прецедентов, возникающих после банкротства банков, когда выяснялось, что финансово-кредитная организация, по сути, разграблена его руководством или собственниками. Практика показывает, что банки «падают», как правило, не в результате вреда, нанесенного менеджерами среднего звена, хотя и такие случаи известны. В списке дисквалифицированных лиц банков я не встречал уборщиц и кассиров. Думаю, что, инициировав принятие 281-ФЗ от 29 июля 2017 г. «О совершенствовании обязательных требований к учредителям (участникам), органам управления и должностным лицам финансовых организаций», законодатели четко дали понять, кто из персонала представляет наибольшую угрозу для деятельности банков.

В этой связи еще один вопрос: должно ли данное подразделение, отвечающее за кадровую безопасность, быть «карманным» или же подчиняться в первую очередь действующему законодательству государства, в котором существует? Должны ли сотрудники в случае хищений денежных средств руководством «помогать грузить мешки в машину» или же вправе отказаться? Любая кредитная организация не существует изолированно, это часть банковской системы страны, и угроза одному банку должна восприниматься как угроза банковской системе в целом. В таком случае, когда речь идет о вопросе выживания банка как организации, вопросы о лояльности конкретным руководителям (тем более если они превышают свои полномочия) не должны быть приоритетными. Очень не хотелось бы, чтобы сотрудник безопасности сталкивался с таким выбором. А трудовой договор и должностные обязанности содержат, как правило, пункт № 2: «Если начальник неправ, читай пункт первый». В противном случае все заканчивается так – ответственный за кадровую безопасность ищет работу, а руководство отдыхает за границей, находясь в международном розыске.

Но это про нестандартные случаи. Просто в последнее неспокойное время их все больше. А в целом я, конечно, не утверждаю, что не надо проводить мероприятий в рамках

Елена КИСЛОВА,
управляющий партнер юридической фирмы «Делио»

стандартных процедур в отношении рядового персонала.

Да, а к вопросу, кто виноват. Виновата как всегда безопасность. Как вы там проверяли?

Е. КИСЛОВА (юридическая фирма «Делио»): Я, с вашего позволения, буду давать короткие ремарки по тем вопросам, которые уже были здесь подняты. Судебная практика и Гражданский Кодекс, а также профессиональные стандарты говорят нам о том, что в случае возникновения у организации финансовых и/или репутационных проблем надо защищать юридическое лицо. Ни его собственников, ни его руководителей, ни рядовых сотрудников, работающих в банке, а именно юридическое лицо, поскольку, когда вы вступаете в трудовые отношения с юрлицом, то обязанности у вас наступают именно перед ним, а не перед его собственником или менеджером, занимающим более высокую должностную позицию, чем вы. Собственник получает дивиденды, и только у него есть возможность принимать решения, но у нет при этом права

Валерий ГОЛЕВ,
вице-президент
ООО КБ «Международный расчетный банк»

отдавать вам указания, каким образом спасать банк от угроз. Вы отвечаете за исполнение обязанностей, которые, в том числе, должны быть направлены на сохранение активов, на продолжение стабильной работы банков и т.д. Именно так и никак иначе распределяются обязанности и возможности.

В. ГОЛЕВ: (Международный расчетный банк): Я хотел выступить по поводу безопасности кадров, но разговор зашел о «мешках с деньгами», и я, увлеченный ею, решил внести некоторые коррективы в свое выступление. Проблема решается очень просто: есть инструкции, которыми должен руководствоваться отдел экономической безопасности. Банк – образчик бюрократии, организация, все действия которой должны быть прописаны, регламентированы. Деньги любят порядок и тишину. Если каждый сотрудник будет смотреть, кто и как грузит мешки с деньгами, то ни порядка, ни тишины не будет. Если вывозятся большие суммы денег и при этом это делают не инкассаторы, которые приезжают регулярно; если мешки грузит председатель правления, значит, либо председатель правления и его подчиненные своими действиями нарушают инструкции, либо виновата служба безопасности, которая не удосужилась соответствующие инструкции разработать и прописать.

Отсюда вытекает и следующий вопрос – о безопасности кадров. У сотрудника выведывают информацию, на каком основании он беседует с представителем внешней организации или с посторонним физическим лицом. В банках есть инструкции, в соответствии с которыми сотрудникам должно даваться специальное разрешение на беседы с третьими лицами и в которых должно четко прописываться, что их они должны вести исключительно в рамках своих полномочий. Если менеджер по работе с клиентами, например, начинает объяснять клиенту специфику стратегии банка, то это явно выход за пределы своей компетенции.

О. ЛЫНДИНА (РосЕвроБанк): У нас все такие вещи прописываются в документах банка, и они являются обязательными для ознакомления и подписания всеми сотрудниками. Что касается систем слежения за действиями сотрудников, то мы знаем, что в некоторых банках они используются. Насколько это законно? Вот как раз по этому вопросу пока нет ясности, а он, с моей точки зрения, относится к числу важнейших.

Е. КИСЛОВА (юридическая фирма «Делио»): Опираясь на свой профессиональный опыт, я могу сказать следующее: это является законным только в том случае, когда получено письменное согласие от сотрудника на использование данных слежения, прослушивания телефонов, просмотр почты и т.д. И оно должно быть получено до официального трудоустройства сотрудника. Вы должны при приеме на работу поставить его в известность о том, что вы, как

Оксана ЛЫНДИНА,
директор департамента организационного развития и управления персоналом АКБ «РосЕвроБанк»

работодатель, имеете право проверять его корпоративную почту и личный телефон и это не будет вмешательством в его личную жизнь.

NBJ: Что подразумевается под термином «личный» в данном контексте? Персональный корпоративный телефон сотрудника или его собственный гаджет, принадлежащий лично ему?

Е. КИСЛОВА (юридическая фирма «Делио»): Я имела в виду второй вариант. Если работник использует личный телефон в рабочее время, находясь на рабочем месте, то он должен быть готов, что результаты его разговоров по личному телефону могут быть собраны, проанализированы и использованы в качестве доказательства. Понятно, что судебная практика по данному вопросу различается. Но здесь надо понимать, что чем больше у вас будет юридически грамотно собранных данных, тем более высокой будет вероятность того, что суд в итоге встанет на вашу сторону.

Ольга ЧЕРЕМУХИНА,
начальник группы сопровождения трудовых отношений отдела сопровождения административных дел и исковой работы ООО «Хоум Кредит энд Финанс Банк»

М. ЛЕВАШОВ (INFOSECURITY): Ваша рекомендация является совершенно правильной и ценной, но только не в том случае, который я уже привел выше. Предположим, все необходимые документы сотрудником подписаны до его приема на работу. Но что делать, если он уже после возникновения какого-либо прецедента отрицает факт своей причастности к нему? И у него при этом есть следующий аргумент: его учетные данные в системе были известны тому или тем сотрудникам, которые по долгу службы осуществляли наблюдение за ним. И второй момент – как все же быть с личной жизнью сотрудников: не с тем, чем они занимаются в интернете в рабочее время, находясь на рабочем месте, а с тем, что они делают, например, в социальных сетях в свободное от работы время? Можно ли будет предъявлять данные, собранные в результате наблюдения за интернет-активностью людей?

О. ЧЕРЕМУХИНА (Хоум Кредит энд Финанс Банк): А я бы, со своей стороны, отметила бы еще один момент: отказ от своих прав является юридически ничтожным. Даже если вы будете иметь предварительное согласие сотрудника на использование данных, полученных с его личного телефона, то это вам никак не поможет в суде. Сотрудник может отказаться от этого согласия на любой стадии судебного процесса.

Е. КИСЛОВА (юридическая фирма «Делио»): Я говорила не об отказе сотрудника от прав, а о получении работодателем права вести наблюдение за сотрудником. Но я согласна: в этих вопросах всегда есть тонкая грань. Например, она возникает в случаях, когда сотрудник использует и для работы, и для личной жизни телефон, данный ему работодателем. Естественно, работодатель имеет право проверять этот гаджет в любое время, которое он сочтет нужным, а не только в рабочее.

Е. ЦАРЕВ (АИС): Если мы говорим о судебной практике, то надо понимать следующее: там, где речь идет об использовании данных, полученных с помощью технических средств, всегда должна проводиться компьютерно-техническая экспертиза. Если мы говорим о гражданских спорах, то суду будет очень интересно узнать, что по этому поводу думают эксперты. Приведу простой пример: у меня был кейс, который длился полтора года. Одна из судебных инстанций вернула дело на новое рассмотрение, поскольку суд не назначил экспертизу по вопросу об обязательности или необязательности выполнения стандарта СТО БР ИББС. Мы с вами все знаем, что это рекомендательный стандарт, и именно это и стало камнем преткновения.

Хочу еще поделиться своим опытом. Обычно, когда речь идет о служебных расследованиях, то формулировка бывает следующей – мы очень хотим уволить этого сотрудника.

Евгений ЦАРЕВ,
эксперт по информационной безопасности и судебной экспертизе

Это сразу начинает нас напрягать, поскольку мы понимаем, что речь явно идет о некоей внутрикорпоративной войне. Дело обычное, но для нас, как экспертов, это совершенно неважно: мы не делаем никаких правовых выводов, мы можем только установить, что в конкретное время с определенного устройства были совершены действия, которые впоследствии оказали некое влияние на работу информационной системы. Дальше пусть выводы делают сотрудники банка, суд, следствие и т.д.

Здесь было сказано, что сотрудников нужно обучать. Я согласен с этим тезисом и считаю, что принципиально важно доносить до людей следующий пункт: когда вы делаете что-то, выходящее за рамки ваших служебных инструкций, то это автоматически создает для вас риски. По поводу того, что возможны угрозы сотрудникам со стороны третьих лиц, то в моей практике такого не было. А вот прецедентов, связанных с использованием сотрудников «в темную», было более чем достаточно.

О. ЛЫНДИНА (РосЕвроБанк): Я хочу еще раз уточнить ответ на вопрос, насколько законным является изучение информации о сотруднике, собранной в соцсетях.

Е. КИСЛОВА (юридическая фирма «Делио»): Соцсети – это публичная, а не личная площадка, и, если вы приглашаете в друзья кого-то или вы делаете какую-то информацию публичной, то и она, и ваши беседы с друзьями могут быть использованы в суде в качестве доказательств, как и фотографии, которые вы размещаете в соцсетях. Тут можно дать только один совет: прежде чем войти на страницу в соцсети и начать там социальную активность, читайте служебные инструкции.

Еще один момент, который я хотела бы отметить. Нигде в законе не сказано, что императивно запрещено иным лицам прослушивать, проглядывать либо иным образом вмешиваться в личную жизнь, если публичное лицо кого-то пригласило в свою личную жизнь. Тут реализуется договорная функция: физлицо приглашает кого-то на свою страничку в соцсети, соглашается с его присутствием на ней, то есть фактически заключает с ним договор о дальнейшем общении. После этого ссылки на то, что приглашенное лицо вмешивается в личную жизнь, несостоятельны.

А. ВИНОГРАДОВ: Мы все время забываем о том, что банки бывают разными, в том числе и по численности персонала. Вы планируете, например, сделать стандарт по кадровой безопасности. Очень интересно, как вы собираетесь это делать? Как будете определять группы риска – по внешним признакам? Что вы будете прослушивать и отслеживать? Личные телефоны и мессенджеры после 18:00? И в чем смысл этого? Никто не будет компрометирующую себя информацию отправлять до конца рабочего дня, прекрасно понимая, что есть системы DLP, видеонаблюдения и т.д. Это во-первых. А во-вторых, есть банки, в которых

Александр ВИНОГРАДОВ,
начальник управления информационной безопасности АО КБ «ЗЛАТКОМБАНК»

работает по 100 человек, и в них люди просто так, с улицы не приходят. Уровень доверия там между сотрудниками беспрецедентный, и никто никого там не проверяет. Наконец, представим себе такую ситуацию: поставили мы DLP, собрали информацию обо всех, но как мы будем из этого огромного массива информации вычленять то, что нам нужно? У нас нет ни нужного для этого штата безопасников, ни штатных экстрасенсов. Мы работаем по факту – когда где-то на стороне всплывает критичная для банка информация или «уходят» деньги.

А.ТУРКИН (независимый эксперт): Совершенству, как известно, нет предела. В том числе и вопросах кадровой безопасности. Поэтому и должен быть определен список мер разумных и достаточных. Не надо забывать, что все проверочные мероприятия весьма затратны и если применять их в отношении всех сотрудников в полном объеме, то не хватит ни денег, ни времени. Я сталкивался с ситуацией, когда в подразделение внутренней безопасности численностью три сотрудника поступало на проверку до 50 анкет кандидатов в день. Что там можно было проверить при такой загрузке? Трудоемкость, нормы загрузки, методики, наконец, бюджет подразделения – все это можно обсуждать, только если будут сформулированы единые требования к кадровой безопасности, опирающиеся на модель угроз, требования регуляторов и действующее законодательство.

Этого мы на сегодняшний день не видим, в то же время хорошо, что приняли 281-ФЗ от 29 июля 2017 года «О совершенствовании обязательных требований к учредителям». Хотелось бы еще, чтобы был описан механизм его реализации, чтобы институты, владеющие информацией о квалификации персонала, обязаны были отвечать банкам на их запросы, а органы, владеющие информацией о «деловой репутации» граждан, охотнее ей делились.

В. КРЕОПАЛОВ (РЭУ им. Г.В. Плеханова): Вы говорите о расследовании уже состоявшихся инцидентов, а давайте вспомним выводы, к которым пришел за свой 40-летний опыт практических исследований на полиграфе Валерий Алексеевич Варламов, создатель первого в СССР чернильно-пишущего детектора лжи, первого компьютерного детектора лжи, серии полиграфов «Барьер», «Крис», «Риф», не имеющих аналогов в мире. Так вот, выводы, к которым он пришел, таковы: 10% сотрудников направлены на совершение противоправных действий, 10% их никогда не совершат, а 80% могут осуществить противоправные действия, если для этого возникнут благоприятные условия. Мне кажется, что основная работа служб безопасности в банках должна быть направлена как раз на эти 80%, чтобы не создавать этих благоприятных условий, а расследования уже мы будем проводить по фактам, опираясь на сведения, которые будут нам поставлять 10% сотрудников-«патриотов».

NBJ: Интересно то, что у нас всегда вне подозрений остаются сотрудники и руководители служб экономической, информационной и кадровой безопасности. Но при этом бывают же прецеденты, когда и они попадают в «черные списки», например, когда по указанию топ-менеджеров банков совершают действия, ведущие к банкротству финансово-кредитной организации. Получается конфликт интересов: по долгу службы они должны работать на руководство банка, и оно же понуждает их делать то, что наносит банку вред.

М. ЛЕВАШОВ (INFOSECURITY): А откуда они знают, что действия, к которым их принуждают, ведут к банкротству банков? Они не могут так глубоко разбираться в структуре бизнеса и в стратегических вопросах. То же самое можно сказать и о риск-контролерах, и об аудиторах.

NBJ: Тем не менее и на них возлагается ответственность, и они отвечают своей репутацией и карьерой в случае, если все заканчивается для банка печально. Но давайте мы теперь перейдем к следующей, не менее животрепещущей теме – прием и увольнение персонала. Мы предлагаем Андрею Арефьеву поделиться с нами наработками его компании по данному вопросу.

А. АРЕФЬЕВ (компания «ИнфоВотч»): Скорее, я хотел бы поговорить немного о другом – не о том, как следует увольнять сотрудников, а о том, как на ранней стадии и по каким признакам можно обнаружить то, что сотрудник собирается уйти. Вопрос не только в том, что при увольнении сотрудника возникает «пустота», которую надо заполнить. В результате этого могут возникнуть и существенные дополнительные финансовые расходы, особенно если речь идет о высокооплачиваемом специалисте, и информационные издержки, если уходит известный на рынке человек. Поэтому к таким

Андрей АРЕФЬЕВ,
главный разработчик руководитель перспективных разработок АО «ИнфоВотч»

событиям следует готовиться заранее.

Принятие нового сотрудника на работу – тоже не такая простая задача, как это может показаться на первый взгляд. Есть сферы экономики, где «текучка» считается совершенно нормальным и неизбежным процессом, но банковский бизнес – это совсем другое дело. Поэтому всегда интересно, как банки оценивают для себя экономический эффект прихода и ухода сотрудников.

О. ЛЫНДИНА (РосЕвроБанк): То, что вы описали, – абсолютно стандартные ситуации, которыми должны заниматься кадровые службы в банках. Если говорить о раннем предупреждении увольнения, то обычно первичная информация по этому вопросу исходит от непосредственного руководителя сотрудника. По ряду признаков он приходит к выводу, что человек стал не так ревностно выполнять свои должностные обязанности, как раньше, чаще отвлекаться и т.д. После получения такого сигнала начинается мониторинг, то есть информация о данном человеке собирается системно. Если наши подозрения подтверждаются, то дальше начинается планомерная и очень аккуратная работа по удержанию этого специалиста: надо выяснить, чем он недоволен, в чем видит преимущества новой работы, если она уже им найдена. С учетом полученной информации выстраивается и новая мотивационная система для этого человека. Нести расходы на подбор нового специалиста мало кому хочется. Конечно, оптимальный вариант – это сохранить того, кто уже «приработался» в нашей организации.

Е. ЖАРОВА (Банк БЦК-Москва): Я хотела бы заметить, что мы, как банкиры, часто в негативном контексте упоминали в рамках нашей дискуссии социальную инженерию. Именно с ее помощью злоумышленники выведывают у сотрудников информацию, именно в соцсетях люди могут сболтнуть лишнее. Но надо понимать, что мы и сами не можем обойтись без социальной инженерии. Я думаю, что у всех банков есть такие замечательные ресурсы, как закрытые порталы, на которых сотрудники могут обмениваться информацией, достижениями, наблюдениями и т.д. То есть создается своего рода специализированная виртуальная реальность, потому что совсем «отлучить» людей от соцсетей в современном мире невозможно. Значит, надо создать для них максимально безопасную и комфортную интернет-среду – со своими модераторами, кругом участников и т.д.

NBJ: Давайте теперь поговорим о самой грустной теме – увольнении персонала. Понятно, что банки пытаются предупредить уход ключевых сотрудников на ранней стадии, ясно, что они пытаются предложить специалистам, которых они ценят, «конфеты» в виде повышения зарплаты или продвижения по службе и т.д. Но все мы хорошо знаем, что бывает так, что ничего не действует и сотрудник все равно уходит. Как сделать так, чтобы

Елена ЖАРОВА,
руководитель кадровой службы
ООО «Банк БЦК-Москва»

минимизировать для банка все сопутствующие этому издержки – репутационные, финансовые и организационные, а также снизить риски в сфере ИБ, которые могут возникнуть, если сотрудник являлся носителем критично важной для банка информации?

И. ХОБТА (компания Digital Finance International): Знаете, самые большие сложности в данном контексте возникают у компаний и банков, работающих не в Москве, а в отдаленных от столицы регионах. Там априори меньше возможностей подобрать замену ушедшему ключевому сотруднику, и поэтому там цена кадровой ошибки существенно возрастает.

М. ЛЕВАШОВ (INFOSECURITY): Честно говоря, я с этой оценкой не согласен. Мне иногда приходится плотно работать с регионами. На мой взгляд, там достаточно много профессиональных кадров.

И. ХОБТА (компания Digital Finance International): Мы говорим о подборе персонала в небольших населенных пунктах. И при этом очевидно, что замена там ключевых сотрудников требует, как и в столице, и в крупных городах, предварительного тестирования и собеседования. Сложно ожидать, что руководитель головного офиса будет «бегать» по городам и весям, собеседуя претендентов. В связи с этим мне хотелось бы узнать, насколько у банков автоматизированы эти процессы. Используют ли они специализированные программы для проведения дистанционного психологического тестирования?

Е. СУХОБАЕВСКАЯ (Алеф-Банк): Во-первых, когда речь идет о регионах, то я рекомендую использовать тех кандидатов, которые там есть, других не будет. А во-вторых, вам нужна определенная социальная активность. О вашей компании должны получать позитивную информацию, что она предлагает хорошие зарплаты, интересный социальный пакет, обучение и т.д. В конце концов, должно быть имя, авторитет. Но все же главную роль, конечно же, играют деньги.

NBJ: И все-таки, коллеги, вы явно уходите от предложенной нами печальной темы – как уволить сотрудника, избежав при этом массы неприятных последствий. А ведь этот вопрос так или иначе – из серии тех, с которыми сталкивается руководитель любой компании.

М. ЛЕВАШОВ (INFOSECURITY): На мой взгляд, правильным способом будет являться следующий. Чтобы минимизировать риски для компании, уволить любого сотрудника, в том числе сообщить ему эту новость и решить вопрос о компенсациях, должен руководитель, который его приглашал. Если речь идет о ключевом сотруднике, обладающем критически важной для банка информацией, то это представитель высшего менеджмента. Одновременно с обсуждением условий увольнения работники ИБ должны заблокировать все его учетные записи.

Е. КИСЛОВА (юридическая фирма «Делио»): Если говорить о юридических аспектах, то мы в любом случае «не перепрыгнем» через три главных основания, которые есть при расставании с сотрудником, – увольнение по инициативе сотрудника, то есть по собственному желанию, по инициативе работодателя и по соглашению сторон. Мы обсудили вопрос, что делать, когда речь идет о первом варианте. Но есть и иная сторона – инициатива работодателя. Есть 14 пунктов, по которым это возможно сделать, и за рамки них вы не зайдете, каким бы большим ни было бы ваше желание расстаться с конкретным человеком. В том числе есть и такие специфические основания, как принятие руководителем, его заместителем и/или бухгалтером решений, которые приводят к убыткам для компании; разглашение коммерческой тайны; совершение однократных грубых действий по нарушению трудовой дисциплины – сюда могут входить и разговоры по соцсетям, представляющие угрозы для компании.

Вопрос заключается в следующем: если вы будете расставаться по статье, то это большой ущерб для сотрудника, и, конечно же, он будет пытаться в ответ нанести репутационный ущерб работодателю. Соответственно, можно ожидать распространения сведений, приводящих к имиджевым или финансовым потерям, можно ожидать и воровства, если называть вещи своими именами. Какую технологию следует использовать, чтобы этого избежать? Конечно же, для сохранения денег, репутации и времени лучше всего выбирать увольнение по соглашению сторон. Если же вы все же выбрали первое, то вы должны иметь на руках все доказательства, подтверждающие обоснованность вашего решения. Потому что есть вероятность, что этот трудовой спор вам придется решать с уже бывшим сотрудником в суде. Если вы чувствуете, что ваша позиция уязвима, доказательств его вины недостаточно, то, повторюсь,

лучше всего идти на соглашение сторон. Сотрудник в этом случае, с одной стороны, получает компенсацию, а с другой стороны, лишается возможности причинить вам убыток.

В. ГОЛЕВ (Международный расчетный банк): А почему бы нам не действовать по римской пословице «хочешь мира – готовься к войне»? Иными словами, почему бы не класть перед кандидатом договор со списком требований, а не формулировать их, когда наступает миг расставания?

О. ЧЕРЕМУХИНА (Хоум Кредит энд Финанс Банк): Именно так во многих банках уже делают. Что же касается того, о чем мы говорили, то я знаю, что есть прецеденты, когда происходит расторжение трудового контракта по соглашению сторон, и в нем сначала прописывается выплата увольняемому сотруднику достаточно высокой компенсации, а потом она ему не выплачивается. На моей памяти был случай, когда человек подал в суд на своего бывшего работодателя, дошел до Верховного суда, но суд отклонил его иск, мотивируя свое решение тем, что в трудовом контракте не было ничего о повышенных выплатах при увольнении. Так что, в конечном счете, процедура увольнения по соглашению сторон тоже небезупречна.

Е. КИСЛОВА (юридическая фирма «Делио»): Надо понимать, что в таких случаях речь обычно идет о выплате «золотых парашютов». Они обычно выходят по своим размерам за пределы разумной суммы, а ей считаются три ежемесячных оклада. Это как флаг, на который надо равняться. Если же вы назначаете сотруднику, который «не в топах», а в среднем звене, выплату в десять окладов, то вы должны ожидать того, что этот пункт может быть оспорен в суде, поскольку такую выплату суд не будет трактовать как разумную.

Евгений ИВАНОВ,
директор департамента безопасности ПАО «АК БАРС»

Общий вывод, который можно сделать и из многочисленных прецедентов, и из судебной практики: нужно правильно оформлять трудовые договоры, чтобы сотрудник потом не мог ссылаться на то, что он не знал о каком-то пункте, потому что тот был не прописан в документе. И в этом договоре должны быть очень кропотливо обозначены и обязанности сотрудников, и основания для его увольнения, и, конечно же, все финансовые аспекты. И еще принципиально важно помнить, что каждый случай увольнения по своему особенный. Тут можно только сослаться на знаменитую цитату из произведений Льва Толстого о том, что все счастливые семьи счастливы одинаково, каждая несчастная семья несчастлива по-своему. Если процедура приема на работу более или менее отработана и ясна, то к процедуре увольнения надо относиться очень аккуратно и вдумчиво в том числе и потому, что этот процесс всегда на 80% психология и лишь на 20% бюрократия.

NBJ: Под «занавес» заседания нашего круглого стола мы хотели бы еще раз вернуться к теме социальной инженерии. Мы уже поднимали ее, но все же хотелось бы еще раз заслушать представителей банковских организаций – как вы обучаете своих сотрудников моделям рисков в этой сфере?

Е. ИВАНОВ (АК БАРС БАНК): Я согласен с тем, что мои коллеги уже отметили, отвечая ранее на этот вопрос, поэтому я могу только дополнить их. Мы при приеме сотрудников собираем группы, состоящие из 30-40 человек, и достаточно подробно освещаем поднятую вами тему. Сразу скажу, что с шантажом с помощью социальных сетей мы сталкиваемся реже, а вот с попытками подкупа, влияния на людей – достаточно часто. И опять-таки правильно говорят коллеги, что очень важно доверие между сотрудниками. В том числе оно должно быть между специалистами, работающими в различных департаментах, и сотрудниками служб безопасности. Потому что именно к нам, по идее, должны в первую очередь бежать люди, когда они сталкиваются с чем-то – с шантажом ли, с угрозами, с каким-то с виду невинным общением, которое тем не менее вызывает у них беспокойство.

NBJ: Мы хотим выразить большую признательность всем, кто принял участие в заседании нашего круглого стола. Очевидно, что нам удалось лишь вкратце обсудить различные вопросы, связанные с кадровой безопасностью в банках, ведь спектр актуальных тем гораздо больший. И это, на наш взгляд, указывает, с одной стороны, на то, что Национальный банковский журнал выбрал правильную тему для своего круглого стола, а с другой стороны, на то, что есть смысл провести аналогичное мероприятие еще не раз. NBJ