Министерство образования Российской Федерации

Международный образовательный консорциум «Открытое образование»

Московский государственный университет экономики, статистики и информатики

АНО «Евразийский открытый институт»

А.Р. Алавердов

Организация и управление безопасностью в кредитно-финансовых организациях

Учебное пособие

Москва 2004

УДК 336.71
ББК 65.262.1
А 45

Алавердов А.Р. **ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ В КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ**: Учебное пособие Московский государственный университет экономики, статистики и информатики.– М., 2004. – 82 с.

Содержание

Введение

Предмет и актуальность курса

Предметом настоящего курса является управление одним из направлений деятельности финансово-кредитной организации, призванного обеспечить защиту от различных внешних и внутренних угроз ее безопасности.

В условиях рыночной экономики функционирование любого хозяйствующего субъекта связано с разнообразными рисками. Часть из них определяется объективными факторами – внезапными изменениями конъюнктуры спроса и предложения, недостаточной квалификацией собственного персонала, форс-мажорными обстоятельствами и т.п. Однако имущественные и неимущественные потери фирмы могут быть следствием целенаправленной деятельности заинтересованных в них субъектов – конкурентов, криминальных структур, иногда – собственных сотрудников. Специфические условия трансформации отечественной экономики, а также отраслевая специфика функционирования кредитно-финансовых организаций значительно увеличивают вероятность негативной реализации подобных рисков.

Для профилактики и отражения указанных выше угроз любая кредитно-финансовая организация, от гигантской транснациональной корпорации до небольшого специализированного банка, вынуждена постоянно заниматься проблемой обеспечения собственной безопасности. В соответствии с требованиями современного менеджмента такая работа должна осуществляться на профессиональной основе, в рамках специальной системы управления. Следует учитывать, что ее конечная эффективность не может быть обеспечена силами исключительно специализированного подразделения – службы безопасности, какими бы широкими возможностями она не располагала. Полноценная защита от угроз безопасности банка достигается лишь при условии активного участия в соответствующих мероприятиях всего персонала. Поэтому настоящая дисциплина выступает в качестве необходимого элемента подготовки банковских менеджеров любой специализации.

Цель и задачи изучения дисциплины

Изучение настоящей дисциплины направлено на формирование у обучаемых понимания необходимости управления процессом обеспечения безопасности банка на системной основе.

В процессе изучения учебного курса, обучаемые должны ознакомиться со следующими основными вопросами:

- общим понятием и основами методологии менеджмента в области безопасности, его современной отечественной спецификой;
- требованиями к процессам формирования и последующей корректировки соответствующей стратегии банка;
- основами организации деятельности службы безопасности банка, ее функциональными обязанностями и полномочиями;
- основными прикладными методами защиты информации, имущества, персонала банка от внешних и внутренних угроз их безопасности.

Взаимосвязь курса с другими дисциплинами учебной программы

Для успешного освоения настоящего курса необходимо предварительно завершить изучение следующих дисциплин: основы бизнеса, основы менеджмента, основы маркетинга, экономическая безопасность, банковское дело, стратегический менеджмент в банке, персональный менеджмент в банке, информационные технологии в банковском деле.

Раздел 1. Безопасность кредитно-финансовых организаций как объект управления

1.1. Общее понятие безопасности банка и ее компоненты

Термин «безопасность» может применяться по отношению к самым различным субъектам, например, международная безопасность, государственная безопасность, безопасность предприятия, безопасность граждан. Обычно под ней понимается ***текущая и перспективная защищенность субъекта от разнообразных угроз имущественного и неимущественного характера***. Кроме того, рассматриваемое понятие включает в себя разнообразные функциональные направления, например, политическая безопасность, военная безопасность, экологическая безопасность и т.п. Возможна дифференциация безопасности субъекта в зависимости от причин ее нарушения. В частности, выделяются угрозы внешнего характера – со стороны иностранных государств, изменения экономической политики собственного государства, неблагоприятной динамики конъюнктуры рынка и т.п. Угрозу безопасности субъекта могут определить и внутренние факторы, например, низкая квалификация собственного персонала или недостаток финансовых ресурсов. Поэтому изучение проблемы обеспечения безопасности осуществляется в рамках многих учебных дисциплин, ориентированных на подготовку специалистов и менеджеров для различных работодателей (государства, предприятий, общественных организаций) и разнообразных специализаций (информационная, экологическая безопасность, безопасность персонала и т.п.).

В настоящем курсе рассматривается один из аспектов обеспечения безопасности кредитно-финансовой организации. ***Он связан с защитой лишь от тех угроз, которые определены деятельностью юридических и физических лиц, специально направленной на нанесение конкретному банку имущественного или неимущественного ущерба***. С учетом этого ограничения, изучению процесса управления обеспечением безопасности должна предшествовать классификация подобных угроз.

Предметная классификация угроз безопасности банка.

а. По признаку целевой направленности угрозы выделяются:

- *угроза разглашения конфиденциальной информации*, которое может нанести банку ущерб в форме ухудшения его конкурентных позиций, имиджа, отношений с клиентами или вызвать санкции со стороны государства;
- *угроза имуществу* банка в форме его хищения или умышленного повреждения, а также сознательного провоцирования к осуществлению или непосредственного осуществления заведомо убыточных финансовых операций;
- *угроза персоналу* банка, реализация которой способна ухудшить состояние кадрового направления деятельности, например, в форме потери ценного специалиста или возникновения трудовых конфликтов.

б. По признаку источника угрозы (субъекта агрессии) выделяются:

- *угрозы со стороны конкурентов*, т.е. отечественных и зарубежных банков, стремящихся к усилению собственных позиций на соответствующем рынке путем использования методов недобросовестной конкуренции, например, экономического шпионажа, переманивания высококвалифицированных сотрудников, дискредитации соперника в глазах партнеров и государства;
- *угрозы со стороны криминальных структур и отдельных злоумышленников*, стремящихся к достижению собственных целей, находящихся в противоречии с интересами

конкретного банка, например, захвату контроля над ним, хищению имущества, нанесению иного ущерба;

- *угрозы со стороны нелояльных сотрудников банка*, осознанно наносящих ущерб его безопасности ради достижения личных целей, например, улучшения материального положения, карьерного роста, мщения работодателю за реальные или мнимые обиды и т.п.

в. По экономическому характеру угрозы выделяются:

- *угрозы имущественного характера*, наносящие банку прямой финансовый ущерб, например, похищенные денежные средства и товарно-материальные ценности, сорванный контракт, примененные штрафные санкции;
- *угрозы неимущественного характера*, точный размер ущерба от реализации которых обычно невозможно точно определить, например, сокращение обслуживаемого рынка, ухудшение имиджа банка в глазах его клиентов и деловых партнеров, утеря ценного специалиста.

г. По вероятности практической реализации угрозы выделяются:

- *потенциальные угрозы*, практическая реализация которых на конкретный момент имеет лишь вероятностный характер (соответственно, у субъекта управления есть время на их профилактику или подготовку к отражению);
- *реализуемые угрозы*, негативное воздействие которых на деятельность субъекта управления находится в конкретный момент в различных стадиях развития (соответственно, у субъекта имеются шансы на их оперативное отражение в целях недопущения или минимизации конечного ущерба);
- *реализованные угрозы*, негативное воздействие которых уже закончилось и ущерб фактически нанесен (соответственно, субъект управления имеет возможность лишь оценить ущерб, выявить виновников и подготовиться к отражению подобных угроз в дальнейшем).

Проведенная классификация позволяет сформулировать **три основных компонента безопасности современной кредитно-финансовой организации**:

- *информационная безопасность банка*, предполагающая его защищенность от любых угроз разглашения или утери информации, имеющей коммерческую или иную ценность;
- *безопасность персонала банка*, предполагающая его защищенность от любых угроз персоналу, прежде всего, высококвалифицированной его части;
- *имущественная безопасность банка*, предполагающая его защищенность от любых угроз денежным средствам, ценным бумагам, товарно-материальным ценностям и другим элементам активов.

Более детальная классификация будет проведена в соответствующих разделах курса. Общая же направленность мероприятий по защите банка от рассмотренных выше угроз иллюстрируется с использованием следующей принципиальной схемы:

СХЕМА 1.

Принципиальная схема обеспечения безопасности банка

Факторы, определяющие отраслевую специфику управления обеспечением безопасности банка. Первым и наиболее важным фактором является ***автоматическое перенесение возможных потерь от реализованных угроз на клиентов и партнеров банка***. В зарубежных условиях на один доллар его собственного капитала приходится не менее десяти долларов привлеченных средств. Соответственно любые имущественные потери кредитно-финансовой организации уменьшают ее возможности выполнить свои обязательства перед клиентами.

Второй особенностью является ***большая степень уязвимости банка как хозяйствующего субъекта в случае возможной утечки конфиденциальных сведений***. Наряду с характерной для любых отраслей необходимостью защиты *коммерческой тайны (т.е. информации, разглашение которой наносит ущерб самому банку)*, обеспечение информационной безопасности кредитно-финансовой организации имеет еще один аспект. Он связан с сохранением *банковской тайны – части конфиденциальной информации, находящейся в распоряжении кредитной организации, разглашение которой наносит ущерб интересам ее клиентов*. К ней относятся любые сведения о размерах и движении денежных средств на открытых в банке счетах, о финансовом состоянии заемщиков, переданных ему в трастовое управление имуществе или сохраняемых ценностях. Разглашение подобной информации имеет своим основным негативным последствием утерю кредитно-финансовой организацией имиджа доверенного лица в глазах не только имеющихся, но и потенциальных клиентов. Допустивший подобную «утечку информации» банк в короткие сроки лишается наиболее привлекательной клиентуры из числа корпоративных структур и крупных частных вкладчиков. Поэтому в системе управления безопасностью защита банковской тайны всегда имеет приоритет перед защитой тайны коммерческой.

В заключение можно отметить ***более обширный в сравнении с другими сферами деятельности перечень потенциальных угроз банковской безопасности и, соответственно, объектов защиты***. Это связано со спецификой уставной деятельностью кредитно-финансовой организации, в частности, постоянной работой ее с высоколиквидными средствами – денежными средствами, валютой, драгоценными металлами, ценными бумагами и т.п.

Дополнительные особенности организации банковской безопасности в современных отечественных условиях:

- общий уровень криминагенности экономики переходного периода;
- высокая степень криминагенности банковской деятельности, например, участие отдельных банков в противоправных финансовых операциях, связи с "теневой" экономикой и преступными группировками;
- более высокий уровень распространенности угроз банковской безопасности насильственного характера (ограбления, покушения на персонал);
- недостаточная лояльность банковских служащих к своему работодателю;
- не всегда достаточная квалификация сотрудников службы безопасности в области защиты компьютерной информации;
- недостаток у многих банков финансовых ресурсов для внедрения высокоэффективных систем защиты информации и имущества;
- непонимание многими руководителями службы безопасности необходимости системного подхода к решению этой проблемы из-за общей ориентации на односторонние по своей направленности методы – защита персонала, защита имущества, защита информации.

1.2. Система управления безопасностью банка

Обеспечение собственной безопасности является одним из постоянно действующих направлений деятельности любой кредитно-финансовой организации. Соответственно, **управление безопасностью** выступает в качестве одного из необходимых элементов внутрибанковского менеджмента. Оно определяется как формализованный (т.е. закрепленный в соответствующих нормативных документах) **процесс, направленный на решение установленного перечня управленческих задач по соответствующему направлению деятельности.**

Для обеспечения необходимой эффективности управление безопасностью должно осуществляться в рамках целостной системы управления, структура которой иллюстрируется следующей схемой:

СХЕМА 2.

Стратегия обеспечения безопасности – совокупность долгосрочных целей и управленческих подходов, реализация которых обеспечивает защиту кредитно-финансовой организации от потенциальных угроз разглашения коммерческой и банковской тайны, а также нанесения ей любых других форм ущерба имущественного и неимущественного характера.

В своей основе стратегия обеспечения безопасности банка может иметь одну из трех рассмотренных ниже концепций:

Вариант 1. Концепция «упреждающего противодействия».

Данная концепция является логическим следствием ранее избранной банком стратегии роста[1] и вытекающей из нее агрессивной конкурентной стратегии. Она предполагает возможность использования службой безопасности наиболее активных методов профилактики и противодействия возможным угрозам. Основным критерием выбора служит максимальная эффективность того или иного метода, при этом вопросы этичности его применения отходят на второй план. При реализации рассматриваемой концепции допускаются, в частности, банковский шпионаж, не всегда легитимные методы контроля над лояльностью собственного персонала и т.п.

[1] см. УПП «Стратегический менеджмент в банке».

Преимущества концепции:

- возможность эффективного решения возникающих у банка проблем, связанных с обеспечением собственной безопасности, практически без участия государства;
- обеспечение приоритета методов профилактического противодействия потенциальным угрозам;
- возможность обеспечения эффективной поддержки других направлений внутрибанковского менеджмента, в первую очередь, маркетинга и управления персоналом.

Недостатки концепции:

- высокая вероятность адекватного ответа со стороны пострадавших от подобной политики конкурентов;
- неизбежные противоречия с действующим законодательством, следовательно, потенциальные проблемы с правоохранительными, судебными и надзорными органами;
- необходимость более высокого уровня ресурсной поддержки – финансовой, кадровой, материально-технической.

Рекомендации по применению: для крупных банков, ориентированных на обслуживание высокорентабельных предприятий (отраслей) или работающих в условиях жесткого прессинга со стороны конкурентов либо криминальных структур.

Вариант 2: Концепция «пассивной защиты».

Данная концепция является логическим следствием ранее избранной банком стратегии сокращения и вытекающей из нее пассивной конкурентной стратегии. Она предполагает приоритетную ориентацию банка на защиту со стороны государства в лице правоохранительных и судебных органов. Это позволяет резко ограничить функции собственной службы безопасности, сохранив в ее инструментарии лишь минимально необходимую номенклатуру методов профилактики и отражения потенциальных угроз.

Преимущества концепции:

- минимальные затраты на ее практическую реализацию;
- отсутствие угроз применения к банку соответствующих санкций со стороны государства в силу его полной законопослушности как хозяйствующего субъекта по рассматриваемому направлению деятельности.

Недостатки концепции:

- полная зависимость безопасности банка от эффективности деятельности правоохранительных органов государства;
- ориентация на методы противодействия уже реализованным угрозам, которые являются менее эффективными по сравнению с профилактическими и пресекающими.

Рекомендации по применению: для небольших банков, работающих либо на наименее конкурентных рынках, либо под непосредственным патронажем органов государственного управления.

Вариант 3. Концепция «адекватного ответа».

Данная концепция является логическим следствием ранее избранной банком стратегии ограниченного роста и вытекающей из нее наступательной конкурентной стратегии. Она предполагает возможность использования службой безопасности всего комплекса легитимных методов профилактики и отражения потенциальных угроз. В порядке исключения допускается использование и не полностью легитимных методов, но лишь в отношении тех конкурентов или иных источников угроз, которые первыми применили подобные методы против конкретного банка.

Вариант является компромиссом между первой и второй концепциями, смягчая их радикальные недостатки (однако, не позволяя в полной мере использовать и достоинства). В современных условиях применяется большинством кредитно-финансовых организаций.

Факторы, определяющие выбор базовой концепции обеспечения безопасности банка:

- общая стратегия развития (“миссия”) банка, например, ориентация на обслуживание высокорентабельных отраслей или теневой экономики;
- степень агрессивности конкурентной стратегии банка;
- степень “криминагенности” региона размещения банка;
- финансовые возможности банка по обеспечению собственной безопасности;
- квалификация персонала службы безопасности банка;
- наличие поддержки со стороны местных органов государственной власти.

Общая последовательность реализации избранной стратегии:

- определение общего перечня реальных и потенциальных угроз безопасности банка, а также их возможных источников;
- формирование ранжированного перечня объектов защиты;
- определение ресурсов, необходимых для реализации стратегии;
- определение рациональных форм защиты по конкретным объектам;
- определение функций, прав и ответственности службы безопасности банка;
- определение задач других структурных подразделений и управленческих инстанций банка в рамках реализации стратегии;
- разработка оперативного плана мероприятий и целевых программ.

Операционные подсистемы – это самостоятельные элементы системы управления, каждый из которых направлен на решение формализованного перечня однотипных задач по обеспечению безопасности. Отражая установленные стратегией управления цели и приоритеты, операционные подсистемы имеют своими объектами:

- информационную безопасность;
- безопасность персонала;
- имущественную безопасность.

В соответствии с методологией менеджмента, при формировании операционных подсистем необходимо соблюдать следующие общие требования:

- подсистемы не могут содержать элементов (методов, процедур и т.п.), практическое функционирование которых может объективно затруднить эксплуатацию смежных подсистем;
- общая структура каждой из подсистем должна соответствовать следующей типовой схеме: “определение целей процесса – планирование и организация процесса – оперативное управление процессом – оценка результатов процесса путем сопоставления их с ранее запланированными целями”;
- формализованное закрепление функций, связанных с эксплуатацией подсистем, за соответствующими руководителями и специалистами как штабных, так и коммерческих подразделений фирмы, включая и механизм личной ответственности за их выполнение.

Блок обеспечения является необходимой частью любой управляющей системы. Формируя исходные условия для эффективного управления, он включает в себя несколько направлений.

а. Информационное обеспечение системы управления безопасностью включает в себя три компонента:

- используемые в рамках системы методы и конкретные процедуры получения субъектами управления необходимой первичной информации;
- формализованные каналы прохождения информации в рамках системы, которые определяют маршрут движения ранее собранной информации по инстанциям (принципиальная схема: «от кого – кому – в какой форме – в какие сроки»);
- базы данных, связанных с любыми проблемами внутренней и внешней безопасности, которые накапливаются и обновляются в течение всего периода функционирования на рынке и используются при формировании управленческих решений любого уровня.

б. Нормативно-методическое обеспечение включает в себя комплект внешних и внутренних регламентов, используемых в процессе управления рассматриваемым направлением деятельности, а также документов рекомендательного, т.е. не директивного характера. К внешним регламентам относятся законодательные (например, Закон РФ «О частной детективной и охранной деятельности в РФ») и подзаконные (например, Постановление Правительства РФ «О перечне сведений, которые не могут составлять коммерческую тайну») акты. К внутренним регламентам и рекомендациям относятся любые постоянно действующие документы, разработанные в рамках конкретного банка и введенные в соответствии с действующим в нем порядком – инструкции, приказы, распоряжения и т.п. Единственным ограничением при разработке внутренних регламентов является их хотя бы формальное соответствие (непротиворечивость) действующему законодательству.

в. Технологическое обеспечение определяется как совокупность формализованных технологий обеспечения безопасности банка от различных видов угроз. Их наличие является основной предпосылкой эффективности управления, поскольку позволяет четко определить:

- непосредственных участников (инстанции и рабочие места, принимающие участие в описываемой операции по защите от конкретной угрозы);
- управленческие процедуры (мероприятия, осуществляемые в рамках операции);
- типовые сроки по операции в целом и каждой управленческой процедуре в отдельности;
- ответственность участников за нарушение описываемой технологии.

г. Инструментальное обеспечение определяется как совокупность прикладных методов управления, используемых в рамках системы. Применительно к управлению безопасностью их можно дифференцировать на три группы:

- *методы профилактического характера*, позволяющие не допустить практической реализации потенциальной угрозы;
- *методы пресекающего характера*, позволяющие отразить уже реализуемую угрозу, не допустив или минимизировав возможный ущерб;
- *методы карающего характера*, позволяющие наказать непосредственных виновников реализованной угрозы.

д. Трудовое обеспечение определяется как полностью укомплектованный штат службы безопасности, включающей в себя три квалификационные категории работников:

- *менеджеры*, т.е. руководители различного уровня – от возглавляющего рассматриваемое направление вице-президента банка до бригадира смены охранников;

- *эксперты*, т.е. высококвалифицированные сотрудники службы безопасности, специализирующиеся на определенных направлениях ее обеспечения (аналитики, разработчики специальных программных средств и т.п.), но не выполняющие при этом прямых управленческих функций;
- *исполнители* (охранники, ремонтники спецоборудования и др.).

е. Финансовое обеспечение определяется как совокупность финансовых ресурсов, выделяемых на поддержание и развитие рассматриваемого направления (приобретение спецоборудования, зарплата персонала, оплата информации и т.п.).

При формировании, эксплуатации и развитии системы управления безопасностью банка необходимо соблюдать некоторые **общие методические требования**. Главным из них выступает ***системный подход к проблеме обеспечения безопасности***. Под этим понимается недопустимость акцентирования усилий службы безопасности на отражении какого-либо одного или нескольких видов потенциальных угроз в ущерб остальным. Нарушение данного требования до настоящего времени характерно для многих отечественных коммерческих фирм и определяется, чаще всего, прежней областью профессиональной деятельности руководителя рассматриваемого направления. Так, бывшие сотрудники Второго Главного управления КГБ СССР основное внимание уделяют противодействию банковскому шпионажу, сотрудники ФАПСИ – защите информации, сотрудники МВД – защите имущества и т.п. В результате, в системе защиты безопасности возникают уязвимые места, которые и могут использоваться злоумышленниками. Очевидно, что указанное здесь требование не должно вступать в противоречие с принципом рационального ранжирования потенциальных угроз, который рассматривается ниже.

Вторым требованием определяется ***приоритет мероприятий по предотвращению потенциальных угроз (т.е. методов профилактического характера)***. Оно не требует дополнительных обоснований уже в силу обеспечиваемой возможности не допустить ущерба в принципе, тогда как прочие методы в лучшем случае позволяют его сократить или наказать виновников.

Третьим требованием выступает ориентированность системы на ***обеспечение приоритетной защиты конфиденциальной информации*** и лишь затем иных объектов потенциальных угроз. Роль информации и информационных технологий в функционировании современной цивилизации, государства, отдельных фирм последовательно увеличивается. Все для большего числа хозяйствующих субъектов утеря или разглашение информации становится более значимой потерей, нежели хищение денежных средств и материальных ценностей. Появление и развитие глобальных компьютерных сетей определило появление еще одного источника постоянных угроз информационной безопасности – несанкционированное проникновение в базы данных. Хакерство из экзотической формы интеллектуальной деятельности ограниченного контингента специалистов по разработке программных средств уже в конце 70-х годов превратилась в новую профессиональную специализацию для работников не только государственных спецслужб, но и частного, в том числе и криминального, бизнеса. Наблюдаемый в последние десятилетия резкий рост как общей номенклатуры угроз информационной безопасности банков, так и масштаба потерь от них, определяет необходимость реализации данного требования.

Четвертым требованием является ***непосредственное участие в обеспечении безопасности банка всех ее структурных подразделений и сотрудников*** в рамках установленной им компетенции и ответственности. Структура возможных угроз, среди которых не последнее место занимают и угрозы со стороны собственного персонала, исключают

возможность эффективного противодействия им силами исключительно сотрудников службы безопасности. Поэтому в заключительном разделе пособия специально рассматривается комплекс мероприятий по воспитанию в трудовом коллективе соответствующей идеологии и обучению его членов методам профилактики и пресечения наиболее вероятных угроз.

Пятым требованием выступает ***обеспечение взаимодействия системы управления безопасностью с другими направлениями менеджмента***. Указанное требование реализуется как на стратегическом, так и на оперативном уровне системы управления. В следующем разделе специально рассматривается зависимость стратегии обеспечения безопасности от общей миссии банка и его конкурентной стратегии. В отечественных условиях в режиме оперативного управления наиболее тесная взаимосвязь должна обеспечиваться между рассматриваемой системой и персональным менеджментом. Нарушение требования о координации управления различными направлениями деятельности может привести к крайне негативным последствиям. В случае, когда при разработке смежных систем управления (например, финансового менеджмента или маркетинга) будут нарушены требования со стороны рассматриваемой системы, резко увеличивается вероятность негативной реализации соответствующих угроз. В свою очередь, нормальное функционирование смежных систем управления будет постоянно нарушаться, если управление безопасности будет организовано по принципу самодостаточности – «безопасность ради самой безопасности». Таким образом, комплексная система управления должна формироваться с учетом обеспечения относительного паритета или баланса интересов каждого из направлений деятельности кредитно-финансовой организации.

Шестым требованием является ***соразмерность затрат на обеспечение безопасности банка реальному уровню угроз.*** Оно связано с реализацией принципа «разумной достаточности». С позиции конечной эффективности системы в равной степени недопустимо экономить на рассматриваемом направлении деятельности, ослабляя собственную безопасность, и преувеличивать возможные угрозы, осуществляя излишние, т.е. не окупаемые расходы. Учитывая, что руководство службы безопасности по очевидным причинам склонно именно к завышению уровня потенциальных угроз, для соблюдения данного требования желательно привлечение независимых экспертов в лице сотрудников государственных правоохранительных органов или частных охранных структур.

Заключительным требованием является ***формализованное закрепление не только функциональных обязанностей, но и полномочий (предела компетенции) службы безопасности***. В отличие от других направлений деятельности банка работа большинства сотрудников этого подразделения всегда связана с угрозой превышения служебных полномочий. В результате велика вероятность возбуждения против кредитно-финансовой организации уголовных дел и гражданских исков по обвинению в нарушении действующего законодательства или гражданских прав.

Оценка эффективности управления безопасностью является необходимым элементом системы. Она позволяет решить несколько прикладных задач, в частности, осуществлять статистический анализ вероятности негативной реализации тех или иных угроз, а также объективно оценивать результативность деятельности службы безопасности. В отличие от большинства других направлений менеджмента здесь не всегда можно точно подсчитать обеспеченный экономический эффект. В частности, затруднительно определить возможные потери от своевременно пресеченных угроз. По некоторым видам угроз, например, в адрес сотрудников банка прямой эффект невозможно рассчитать в принципе. Поэтому приходится опираться на результаты не только прямой, но и косвенной оценки.

Ниже приводится перечень критериев, которые целесообразно использовать для решения этой задачи:

- общее количество выявленных угроз, с дифференциацией на угрозы, пресеченные в полном объеме, пресеченные лишь частично, негативно реализованные в полном объеме (в динамике в сравнении с предыдущими периодами);
- прямой финансовый ущерб, нанесенный банку в результате частично и полностью реализованных угроз;
- потенциальный ущерб, который могли бы нанести банку полностью или частично пресеченные угрозы;
- результаты реализации плановых профилактических мероприятий;
- отсутствие обоснованных претензий к службе безопасности со стороны правоохранительных органов, собственных подразделений и отдельных сотрудников.

Раздел 2. Служба безопасности кредитно-финансовых организаций

2.1. Служба безопасности в системе управления банком и возможные подходы к ее организации

В организационной структуре управления банком **служба безопасности выступает в качестве одного из штабных**, т.е. наделенных распорядительными полномочиями, **подразделений**. Она несет основную ответственность за эффективную защиту имущественных и неимущественных интересов кредитно-финансовой организации от рассматриваемого в настоящем курсе перечня угроз, получая для этого необходимые ресурсы и полномочия.

Особое место рассматриваемой здесь службы среди других структурных подразделений банка определено самим характером ее деятельности. Она включает в себя исполнение сотрудниками службы безопасности по отношению к другим работникам фирмы многочисленных контрольных, ограничивающих и пресекающих функций. Это вызывает подсознательную негативную реакцию даже у той части персонала, которая в силу своего должностного уровня не может не понимать вынужденную необходимость подобных действий. Ощущая такое отношение, сотрудники службы безопасности часто «идут на принцип», т.е. намеренно демонстрируют свои полномочия, ведут себя откровенно агрессивно – недружелюбно по отношению к работникам других подразделений банка (так называемый «милицейский синдром») и, тем самым, лишь усугубляют ситуацию. Поэтому отношения между службой безопасности и остальной частью трудового коллектива банка всегда имеют потенциально конфликтный характер. Это определяет необходимость регулярных профилактических мероприятий, направленных, с одной стороны, на основную часть персонала, а с другой – на сотрудников самой службы безопасности. В противном случае становится невозможным обеспечить практическую реализацию одного из базовых методических требований к организации управления безопасностью, а именно вовлечения в этот процесс всех сотрудников и инстанций.

Выбор принципиального подхода к организации службы безопасности в конкретном банке определяется многими факторами. ***Главным из них является избранная ее руководством стратегия по рассматриваемому направлению деятельности***, а именно – степень ее активности (агрессивности). Чем более активна эта стратегия, тем большие требования предъявляются к службе безопасности, соответственно, сложнее ее внутренняя структура, больше численность персонала. Например, при ориентации руководства кредитной организации на проведение стратегии пассивной защиты от возможных угроз, явно нецелесообразно создание в составе службы специального аналитического подразделения, занимающегося экономической разведкой.

Вторым фактором является ***ориентация руководства на возможное использование услуг специализированных структур*** в лице частных охранных агентств или службы вневедомственной охраны Министерства внутренних дел. Ниже проводится сравнительный анализ трех возможных подходов.

Первый из них предполагает полный отказ от их услуг и характерен, обычно, для крупных банков, ориентированных на проведение стратегии «упреждающего противодействия». В этом случае кредитная организация вынуждена формировать собственную службу безопасности «по полной программе», комплектуя ее всеми необходимыми специалистами и обеспечивая соответствующими ресурсами.

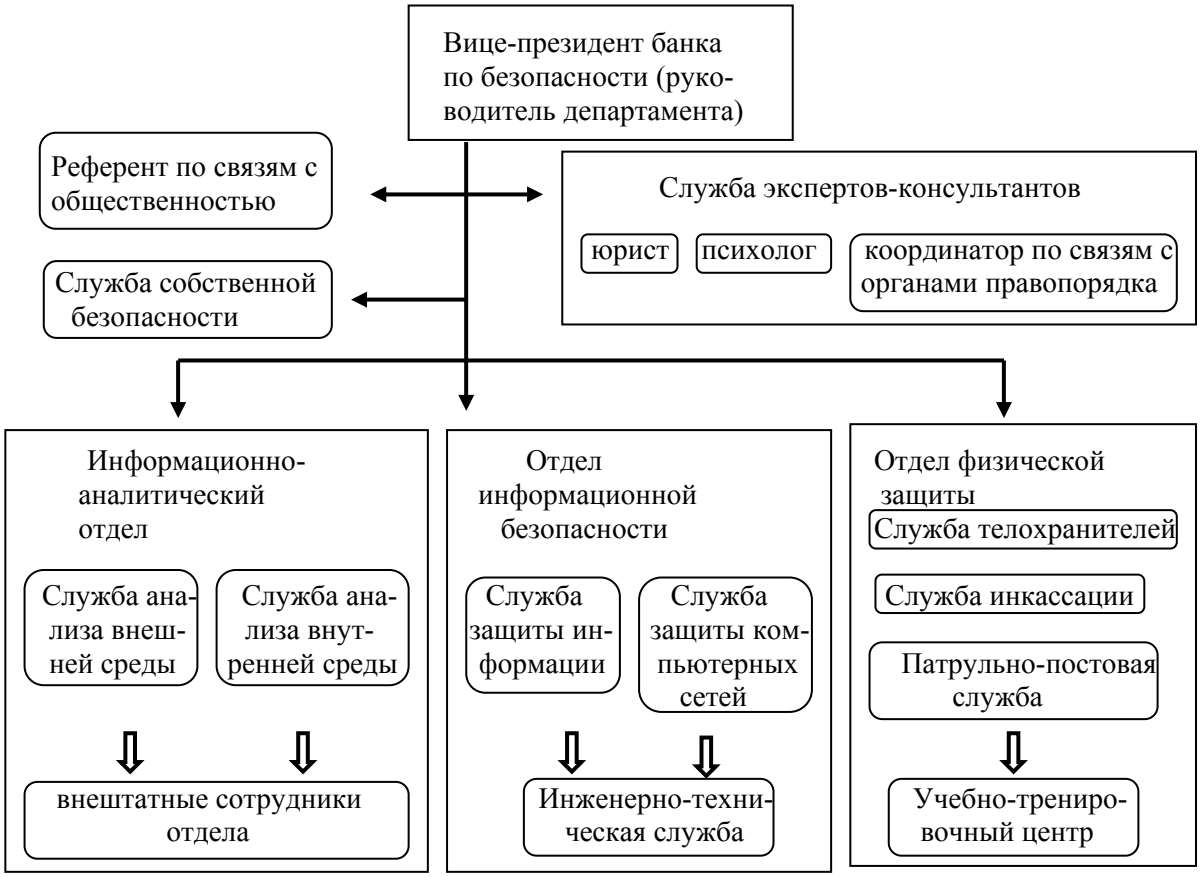
Основным преимуществом данного варианта является большая степень доверия со стороны руководства банка к собственным сотрудникам, входящим в постоянный штат организации. При правильной организации управления деятельностью службы и, прежде всего, ее персоналом, появляется возможность воспитания у него так называемого «корпоративного духа». Этот термин, пришедший в Россию из зарубежной теории персонального менеджмента, предполагает наличие у сотрудника не только лояльности (которая может быть обеспечена и иными средствами), но и личной преданности интересам работодателя. Это может скомпенсировать изложенные ниже недостатки рассматриваемого варианта, за исключением, естественно, полной профессиональной некомпетентности.

Недостатками данного варианта выступают высокий уровень затрат на содержание подобной службы, а для периферийных банков – объективные сложности с комплектацией ее высококвалифицированными сотрудниками всех необходимых специальностей.

Принципиальная организационная структура управления службы безопасности, созданной по такому варианту, представлена на схеме 3.

СХЕМА 3.

Типовая структура департамента безопасности банка



Второй, прямо противоположнный, *подход предполагает минимизацию штатных сотрудников службы безопасности банка, с возложением основных ее функций на сторонние специализированные структуры*, привлекаемые на контрактной основе.

Привлекательность данного подхода обеспечивается многими факторами, среди которых можно выделить:

- меньшую капиталоемкость;

- гарантированный контрактом профессионализм привлеченных из специализированных структур сотрудников;
- в отечественных условиях – отсутствие многих ограничений, связанных с частной охранной деятельностью.

Однако в отличие от предприятий в других отраслях экономики, российские и зарубежные банки используют данный подход крайне редко. Это определяется, в первую очередь, низким доверием к любым сторонним для конкретного банка структурам.

Рекомендации по применению: для государственных и небольших банков, реализующих пассивную конкурентную стратегию.

Принципиальная организационная структура управления службы безопасности, созданной по такому варианту, представлена схемой 4.

СХЕМА 4.

Третий, компромиссный, подход предполагает возможность частичного использования услуг специализированных частных структур для выполнения локальных задач. Он ориентирован на кредитные организации, реализующие стратегию «адекватного ответа» и при этом относительно редко сталкивающиеся со сложными задачами обеспечения собственной безопасности, например, утечкой конфиденциальной информации, хищением денежных средств с использованием компьютерных технологий, шантажом и угрозами в адрес сотрудников. В соответствии с изложенными выше требованиями к организации системы, для таких банков целесообразно ориентироваться на принцип «разумной достаточности» и не включать в постоянный штат службы безопасности сотрудников, чей опыт и квалификация будет востребована от случая к случаю.

2.2. Основные аспекты управления деятельностью службы безопасности банка

Нормативно-правовая база деятельности службы включает в себя:

- законы и подзаконные акты, действующие на территории Российской Федерации (см. перечень рекомендуемой литературы), а также иностранных государств, в которых размещены филиалы, отделения и деловые партнеры банка;

- Положение о службе безопасности банка, утвержденное его президентом и содержащее информацию об организационной структуре управления этой службы, ее основных функциях, полномочиях и ответственности (основной документ, используемый в процессе оперативного управления деятельностью службы);
- должностные инструкции по всей номенклатуре рабочих мест, содержащие информацию о подчиненности, должностных обязанностях, правах и ответственности занимающих их сотрудников.

Планирование деятельности службы осуществляется на основании специальных заданий руководства и утвержденных в установленном порядке плановых документов. К последним относятся:

- целевые программы по автономно выделенным в системе направлениям деятельности службы безопасности, рассчитанные на продолжительный (более одного квартала) срок;
- план-графики регулярных проверок соблюдения установленных правил внутренней безопасности структурными подразделениями и сотрудниками банка;
- индивидуальные плановые задания конкретным специалистам службы безопасности (режим оперативного планирования).

Ресурсное обеспечение службы безопасности осуществляется на основе регулярно (год, квартал) представляемых ею заявок в рамках установленных финансовой службой банка лимитов. Помимо постоянных расходов на оплату труда штатных сотрудников и финансирования договоров на оказание соответствующих услуг сторонними организациями, основными направлениями ресурсного обеспечения, выступают:

- финансовые ресурсы, необходимые для выполнения функций, предусмотренных Положением о службе безопасности банка (включая средства специального фонда оперативных мероприятий);
- информационные ресурсы (профильные периодические издания, связь, компьютерные коммуникации);
- материально-технические ресурсы (оргтехника, транспортные средства, средства технической защиты, оружие и спецсредства и т.п.).

Управление персоналом службы осуществляется в соответствие с общей методологией персонального менеджмента, скорректированной с учетом специфики деятельности рассматриваемого подразделения. Основной задачей является правильный (т.е. наиболее рациональный для конкретного банка) выбор стратегических приоритетов. К ним относятся:

- в части привлечения персонала – выбор приоритетного источника трудовых ресурсов (например, найм сотрудников может осуществляться из числа бывших работников спецслужб, милиции, выпускников профильных образовательных учреждений и т.п.);
- в части организации найма – выбор формы и критериев отбора (найм на основании либо доверия к рекомендациям, представленным кандидатами от известных руководству банка учреждений и лиц, либо отбора и проверки этих кандидатов с использованием специальных методик);
- в части обучения и дальнейшей подготовки персонала – выбор между организацией данного процесса в собственном учебном центре или в сторонних для банка структурах;

- в части оплаты труда персонала – выбор между фиксированными должностными окладами и гибкой формой оплаты труда, предусматривающей прямую зависимость фактических выплат от оценки эффективности выполнения установленных функций.

Контроль над деятельностью службы безопасности осуществляется по трем направлениям:

- со стороны правоохранительных органов (отсутствие нарушений законодательства при исполнении службой безопасности своих функций);
- со стороны дирекции банка (эффективность исполнения установленных ей функций и отсутствие фактов превышения установленных полномочий);
- в режиме внутреннего контроля в рамках самой службы (по аналогу с деятельностью службы собственной безопасности в государственных правоохранительных органах).

ПРИМЕЧАНИЕ: при организации управления целесообразно учитывать невозможность отражения в положении о деятельности службы и должностных инструкциях ряда ее сотрудников всего перечня фактически установленных функций, следовательно, использования строго формализованных методов планирования и контроля.

2.3. Функции руководителя и основных подразделений службы безопасности

Основные функции вице-президента банка по безопасности

Вице-президент по безопасности является руководителем рассматриваемого направления деятельности в целом. Вне зависимости от избранных стратегии обеспечения безопасности и самого подхода к организации службы, он, в силу занимаемой должности, относится к числу высших руководителей банка. Для эффективной реализации своих функций ***вице-президент по безопасности должен обладать необходимыми полномочиями, в частности, правом***:

- доступа к любой конфиденциальной информации;
- участия в совещаниях и переговорах любого уровня, где затрагиваются вопросы, представляющие потенциальную угрозу для безопасности банка (при невозможности личного участия – полный отчет или магнитофонная запись переговоров);
- свободного доступа к Президенту банка, а в экстренной ситуации – Председателю Совета директоров;
- функционального руководства и контроля деятельности других должностных лиц в рамках установленной компетенции.

Основные функциональные обязанности этого руководителя:

- формирование общей стратегии обеспечения безопасности банка и ее оперативная корректировка при изменении внешних или внутренних условий;
- решение текущих проблем с высшим руководством и начальниками структурных подразделений банка;
- организация взаимодействия с местными правоохранительными органами;
- формирование и контроль над исполнением целевых программ и текущих планов структурных подразделений службы безопасности, решение всех ее внутренних административных вопросов, организация ресурсного обеспечения;

- непосредственное руководство службами собственной безопасности и экспертов–консультантов.

Основные функции информационно-аналитического отдела

В системе управления деятельностью службы безопасности данное подразделение обычно выполняет функции «мозгового центра», в который стекается и анализируется вся информация об ее деятельности, а также формируются рекомендации для руководства и других подразделений банка. Особенностью работы данного подразделения в крупных банках, нацеленных на реализацию стратегии упреждающего противодействия, является наличие у него определенного (иногда значительного по численности) контингента внештатных сотрудников как вне, так и внутри организации.

Как правило, деятельность информационно-аналитического отдела организуется параллельно по нескольким направлениям.

Первое направление связано со сбором и анализом чисто коммерческой информации, которая отсутствует в открытых источниках и, соответственно, недоступна специалистам маркетинговой службы банка. К ней относятся сведения:

- о конкурентах в части изменений их рыночной стратегии, имеющихся ресурсов, деловых связей, используемых технологий и, естественно, прямых угрозах безопасности банка с их стороны;
- о клиентах и деловых партнерах в части, прежде всего, их коммерческой добропорядочности, финансовой надежности, планов дальнейшего сотрудничества с банком;
- о динамике государственной экономической политики на федеральном уровне, а также на отраслевых и региональных рынках.

Результатами такого анализа являются специальные аналитические обзоры и докладные записки строго конфиденциального характера, предназначенные для дирекции и руководства заинтересованных подразделений банка.

Второе направление связано со сбором и анализом информации о потенциальных угрозах со стороны криминальных структур. К ней относятся сведения:

- об общей криминогенной ситуации в регионе размещения банка;
- о деятельности преступных группировок, представляющих потенциальную или реальную угрозу для безопасности банка;
- о наиболее известных хакерах, специализирующихся в области проникновения в компьютерные сети финансовых институтов;
- о подготовке конкретных покушений на безопасность банка, а также иных, враждебных ему, акций в режиме внешних угроз.

В отличие от предыдущего направления, результаты этой работы используются, прежде всего, самой службой безопасности при подготовке к отражению соответствующих угроз. Кроме того, референтом по связям с общественностью на основе проанализированной и обобщенной информации должны периодически готовиться информационно-обзорные бюллетени. Их можно эффективно используемые в процессе специального обучения персонала (см. раздел 4 настоящего Пособия).

Третье направление связано со сбором и анализом информации о потенциальных угрозах со стороны собственного персонала банка. К ней относятся сведения:

- о соблюдении в трудовых коллективах банка правил обеспечения безопасности, которые невозможно получить в ходе плановых и внезапных проверок режима;
- о сотрудниках, лояльность которых стала вызывать сомнения у непосредственного руководителя или психолога банка;

- о сотрудниках, занимающих ключевые рабочие места, служебные возможности которых делают необходимым постоянный контроль;
- об общем психологическом настрое в трудовых коллективах банка, дополняющие информацию от психолога службы персонала.

Результаты этой работы могут использоваться самой службой безопасности для отражения угроз со стороны нелояльных сотрудников, службой персонала для внесения соответствующих изменений в систему управления им, а также руководителями структурных подразделений банка для формирования персонифицированных управленческих решений.

Основные функции отдела информационной безопасности

Деятельность данного подразделения направлена на защиту любой конфиденциальной информации банка. Поэтому в его работе наиболее целесообразно выделить следующие три направления:

- защита компьютерных сетей и баз данных от несанкционированного проникновения с целью копирования и повреждения;
- защита информации на бумажных носителях, что связано, в основном с разработкой специальных правил работы с документацией и ее хранения;
- защита устной информации от перехвата с использованием специальных технических средств.

В соответствии с поставленными задачами необходимым структурным элементом данного подразделения является инженерно-техническая служба, в обязанности которой входит:

- приобретение и поддержание эксплуатационной готовности технических средств защиты (см. раздел 3 настоящего Пособия), обучение сотрудников банка их правильному использованию;
- совместно с компьютерной службой банка обеспечение необходимого уровня защиты его компьютерных сетей и баз данных, безопасности системы обмена электронными данными.

Основные функции отдела физической защиты

Деятельность данного подразделения направлена на защиту имущества и персонала банка. По аналогу с отделом информационной безопасности в его деятельности выделяются три направления:

- обеспечение личной безопасности сотрудников банка ***(служба телохранителей)***;
- обеспечение безопасности перевозок денежных средств ***(служба инкассации)***;
- обеспечение физической охраны здания банка, отдельных его помещений – депозитария, кладовой, офисов режимных подразделений, непосредственно прилегающей к нему территории ***(патрульно-постовая служба)***.

В данном отделе числится большинство штатных сотрудников банка, специализация которых (охранники и, особенно, телохранители) требует постоянного поддержания профессиональной квалификации. Поэтому для крупных банков целесообразно создание в этом отделе специального учебно-тренировочного центра, которым смогут пользоваться другие сотрудники службы безопасности и даже желающие руководители организации.

Основные функции отдела собственной безопасности

Данное подразделение находится в прямом подчинении вице-президента банка и обеспечивает защиту от угроз со стороны некомпетентных или нелояльных работников самой службы безопасности. Необходимость существования такого подразделения в крупных банках подтверждается многолетним опытом работы государственных правоохранительных органов и спецслужб, а также негативными фактами из практики российских банков. Основными функциями подразделения выступают:

- участие в разработке внутренних регламентов службы безопасности, определяющих правила поведения ее сотрудников при исполнении служебных обязанностей и в быту;
- профилактический контроль над деятельностью всех сотрудников службы безопасности банка в части исполнения указанных выше правил;
- проведение служебных расследований в отношении сотрудников, допустивших нарушения при исполнении своих обязанностей или поставивших под сомнение свою лояльность работодателю.

Сотрудники рассматриваемого подразделения должны проходить особо тщательную процедуру отбора на стадии найма, либо перевода из других отделов службы безопасности. Рекомендуется также поддерживать предельно высокий уровень их оплаты и социальной поддержки.

2.4. Основные направления взаимодействия службы безопасности с другими подразделениями банка

а. Взаимодействие с маркетинговой службой:

- совместное изучение и анализ конкурентов, подготовка аналитических обзоров и рекомендаций для руководства банка и коммерческих отделов;
- выполнение специальных поручений по сбору дополнительной информации об отдельных клиентах и партнерах банка (в том числе и потенциальных).

б. Взаимодействие со службой персонала:

- проведение специальных проверок при найме новых сотрудников по заявке со стороны службы персонала;
- участие в первичном обучении вновь нанятых сотрудников банка;
- координация действий по контролю над лояльностью персонала и соблюдением им правил обеспечения безопасности банка–работодателя.

в. Взаимодействие с финансовой службой:

- передача и обоснование заявок на финансовые ресурсы, необходимые для подразделения, отчеты об использовании выделенных средств;
- совместное расследование фактов нарушений внутрибанковской финансовой дисциплины (в случае прямых хищений и растрат).

г. Взаимодействие со службой компьютерного обеспечения:

- совместные действия по защите компьютерных сетей банка от несанкционированного проникновения и повреждения;
- при разработке службой компьютерного обеспечения новых программных продуктов – проверка их защищенности от соответствующих угроз.

Раздел 3. Обеспечение информационной безопасности кредитно-финансовых организаций

3.1. Конфиденциальная информация банка как объект защиты.

К конфиденциальной информации относятся любые сведения, разглашение которых способно нанести ущерб их владельцу, пользователю или связанным с ними лицам. Отличительной особенностью банковского сектора экономики является статус кредитно-финансовой организации как доверенного лица своих клиентов, располагающего конфиденциальными сведениями об их финансовой и коммерческой деятельности. Эти сведения составляют ***банковскую тайну***, являющуюся приоритетным объектом защиты в системе безопасности любого банка.

Конфиденциальная информация формируется кредитно-финансовой организацией в процессе всего периода ее функционирования на рынке. Она касается деятельности самого банка, его клиентов, деловых партнеров, конкурентов, контактных аудиторий. Порядок сбора, накопления и хранения информации о собственной деятельности определяется требованиями внутрибанковского менеджмента и должен быть зафиксирован в соответствующих внутренних регламентах (инструкциях, положениях и т.п.). Объем и порядок сбора информации о сторонних организациях зависит от избранной банком стратегии развития, в том числе по направлениям коммерческой деятельности и обеспечения безопасности. Так, ***сбор внешней информации может осуществляться***:

- исключительно легитимными методами, силами службы маркетинга, других штабных служб и коммерческих отделов банка;
- в том числе и нелегитимными методами, осуществляемыми силами специального подразделения в составе службы безопасности (см. раздел 2 УПП).

Классификация конфиденциальной информации осуществляется по нескольким признакам:

По характеру информации она разделяется на:

- информацию, содержащую банковскую тайну (см. выше);
- информацию, содержащую коммерческую тайну, т.е. сведения, разглашение которых способно нанести ущерб интересам самого банка.

По содержанию информации она разделяется на:

- политическую информацию, например, отсутствующие в открытых источниках сведения об ожидаемых изменениях политической ситуации, законодательства, других политических факторах, способных повлиять на рыночное положение банка или связанных с ним хозяйствующих субъектов;
- экономическую информацию, например, отсутствующие в открытых источниках сведения об экономической ситуации в конкретных регионах и отраслях;
- финансовую информацию, например, отсутствующие в открытых источниках сведения о финансовом состоянии клиентов и других партнерах банка;
- коммерческую информацию, например, результаты проведенного специалистами банка анализа соответствующих рынков или его планы их освоения;
- технологическую информацию, например, сведения о разработанных, но еще не внедренных банком новых технологий обслуживания клиентов;
- управленческую информацию, например, сведения об используемых банком методах управления по конкретным направлениям собственной деятельности.

По используемому носителю информации она разделятся на:

- информацию в устном виде, например, сведения, обсуждаемые в процессе делового совещания;
- информацию на бумажных носителях, т.е. традиционная форма документов, используемых кредитно-финансовой организацией;
- информацию в электронном виде, т.е. компьютерные базы данных, а также сведения, передаваемые по компьютерным коммуникациям или телефонным сетям (приоритетный объект защиты в современных условиях).

По степени секретности информации она разделятся на:

- абсолютно конфиденциальную, содержащую секретные сведения, разглашение которых способно нанести ущерб стратегического характера;
- строго конфиденциальную, содержащую совершенно секретные сведения;
- конфиденциальную, содержащую секретные сведения;
- для служебного пользования, содержащую наименее секретные сведения, не предназначенные лишь для открытой печати.

Нормативные ограничения в этой области определены требованиями Постановления Правительства РФ от 05.12.1991г. № 35 «Перечень сведений, которые не могут составлять коммерческую тайну». К ним относятся:

- учредительные документы, а также документы, дающие право заниматься предпринимательской деятельностью (лицензии, сертификаты и т.п.);
- сведения, касающиеся деятельности предприятия как налогоплательщика;
- документы о платежеспособности (что, по нашему мнению, является очень расширительной трактовкой соответствующей финансовой информации);
- сведения о деятельности предприятия как работодателя;
- сведения об имеющихся нарушениях действующего законодательства (экологического, трудового и т.п.).

Кредитно-финансовые организации дополнительно руководствуются в своей деятельности требованиями Закона РФ «О банках и банковской деятельности», определяющими необходимость сохранения банковской тайны.

3.2. Угрозы информационной безопасности банка

Отраслевая специфика банка как посредника на финансовых рынках и доверенного лица своей клиентуры определяет более обширный, чем в других отраслях, перечень возможных угроз его информационной безопасности. Их ***объектом могут выступать любые конфиденциальные сведения***, рассмотренные в п. 1.3.1 настоящего УПП. Однако приоритетным объектом всегда являются сведения, составляющие банковскую тайну, что и определяет главное направление защиты конфиденциальной информации кредитно-финансовых организаций.

Субъектами угроз информационной безопасности банка могут выступать:

- *конкуренты* как самого банка, так и его клиентов, пытающиеся улучшить собственные рыночные позиции путем либо опережения, либо компрометации своих противников;
- *криминальные структуры*, пытающиеся получить сведения о самом банке или его клиентах для решения разнообразных задач (от подготовки примитивного ограбления, до определения размеров «неформальных пошлин» с рэкетируемых ими предприятий – клиентов банка);

- *индивидуальные злоумышленники (в современных условиях – чаще всего наемные хакеры)*, выполняющие либо заказ соответствующего нанимателя (например, конкурента), либо действующие в собственных целях;
- *собственные нелояльные сотрудники банка,* пытающиеся получить конфиденциальные сведения для их последующей передачи (по различным мотивам) сторонним структурам или шантажа своего работодателя;
- *государство в лице фискальных или правоохранительных органов*, использующих специальные методы сбора информации для выполнения установленных им контрольных или оперативных функций.

Угрозы информационной безопасности банка могут проявляться в следующих ***формах***:

- *перехват конфиденциальной информации*, в результате которого у субъекта угрозы оказывается ее дубликат (особая опасность этой формы угрозы для пострадавшего банка заключается в том, что о самом факте утечки он, чаще всего, узнает лишь после того, когда конечная цель перехвата уже достигнута);
- *хищение конфиденциальной информации*, в результате которого субъект угрозы одновременно решает две задачи – приобретает соответствующие сведения и лишает их пострадавший банк;
- *повреждение или уничтожение информации*, в результате которого субъектом угрозы достигается лишь задача нанесения ущерба атакуемому банку.

Методы реализации угроз информационной безопасности банка дифференцируются в зависимости:

- от вида данных, являющихся объектом угрозы;
- от субъекта угрозы.

При использовании классификации по первому признаку можно отметить, что основной угрозой является несанкционируемый доступ к *информации в электронном виде*. В отличие от информации, существующей на других носителях, здесь могут быть реализованы все формы угроз (перехват, хищение, уничтожение). Другим отличием является то, что для достижения поставленных целей субъект угрозы вынужден использовать наиболее сложные с технологической точки зрения, следовательно, дорогостоящие методы. Сторонние для банка структуры и индивидуальные злоумышленники используют специальные компьютерные программы, позволяющие преодолеть существующие у любого банка системы защиты баз данных, локальных сетей и иных компьютерных коммуникаций (см. 1.3.3 настоящего УПП). Другим методом является использование специальных сканеров, позволяющих со значительно расстояния перехватывать («снимать») информацию с работающих компьютеров, факсов, модемов. Возможности субъектов угроз по достижению поставленных целей резко возрастают при использовании услуг сотрудников самого банка, особенно из числа лиц, имеющих доступ к защищаемой информации или компьютерным системам защиты.

Для реализации угроз в отношении *информации на бумажных носителях* субъекты используют такие методы, как копирование (фотографирование), прямое хищение, а при необходимости уничтожения сведений – включение систем самоуничтожения содержимого соответствующих сейфов. Учитывая, что проникновение посторонних лиц в банк всегда достаточно затруднительно, сторонние для него субъекты угроз также стремятся использовать в этих целях собственный персонал кредитно-финансовых организаций.

Наконец, для перехвата *информации в устном виде* используют разнообразные технические устройства – скрытые магнитофоны, видеокамеры, специальные дальнодей-

ствующие сканеры и направленные микрофоны. Они позволяют со значительного расстояния прослушивать устные и телефонные разговоры (включая аппараты сотовой связи), в том числе – в изолированных, но не оборудованных дополнительными средствами защиты помещениях. Основным ограничением выступают здесь финансовые возможности субъекта угрозы и атакуемого банка в части приобретения необходимых технических средств перехвата информации и защиты от него (по некоторым видам устройств цена может достигать нескольких сотен тысяч долларов США).

Классификация по второму признаку позволяет выделить следующие наиболее распространенные методы. Наиболее широкую их номенклатуру потенциально могут использовать *конкуренты как самого банка, так и его клиентов*. Чаще всего ими применяются:

- вербовка сотрудников территориальных налоговых органов и учреждений Центрального банка, по долгу службы располагающих конфиденциальными для конкурентов, но не для государства сведениями (что доступно любому конкурирующему банку и особенно распространено в современных отечественных условиях);
- внедрение своих агентов в атакуемый банк, что доступно лишь для наиболее крупных конкурирующих банков и корпораций, располагающих мощными службами безопасности и специально подготовленными сотрудниками;
- вербовка сотрудников атакуемого банка с использованием методов подкупа и реже шантажа (см. раздел 1.4 настоящего УПП);
- использование услуг собственных (в составе специального подразделения службы безопасности) или наемных хакеров;
- использование разнообразных технических средств перехвата конфиденциальной информации в разовом, регулярном или постоянном режимах.

Криминальные структуры для обеспечения доступа к конфиденциальной информации обычно используют сотрудников атакуемого банка, применяя для этого прямые угрозы, шантаж и, реже, подкуп. Наиболее крупные преступные группировки могут использовать и более сложные методы.

Индивидуальные злоумышленники (в современных условиях – чаще всего наемные хакеры) применяют специальные компьютерные программы собственной или чужой разработки.

Нелояльные сотрудники банка могут действовать в собственных целях (месть, корыстные интересы) или по поручению сторонних для банка структур. Чаще всего, при реализации рассматриваемых угроз они используют собственное служебное положение, обеспечивающее им доступ к соответствующим конфиденциальным данным. В отдельных случаях они могут выполнять роль резидентов нанявших их сторонних для банка структур. В этом случае, сотрудники могут использовать самые разнообразные методы агентурной работы, например, вербовка информаторов из числа своих коллег, выведывание нужных сведений, установку технических средств перехвата информации, прямое хищение или уничтожение конфиденциальных данных.

Фискальные или правоохранительные органы государства в отличие от конкурентов, чаще используют метод внедрения в контролируемый ими банк собственных сотрудников. Уровень их подготовки обычно очень высок, поскольку осуществляется силами специализированных учебных структур государственных спецслужб. В отношении небольших банков функции этих агентов обычно ограничиваются выполнением конкретного задания (например, получение документальных подтверждений факта сокрытия доходов от налогообложения или сведений о конкретном клиенте из числа представителей теневой

экономики). В крупнейшие банки агенты государственных органов могут внедряться на длительный срок, выполняя функции резидентов.

3.3. Обеспечение информационной безопасности банка

Организация работы по рассматриваемому направлению осуществляется в следующей общей последовательности.

Первым этапом является формирование ранжированного перечня конфиденциальных сведений банка как объекта защиты и присвоение им соответствующего грифа секретности. Можно рекомендовать следующий типовой укрупненный перечень (исходя из условий конкретного банка нуждающийся в последующей конкретизации и детализации).

Абсолютно конфиденциальные сведения (гриф XXX[2]) включают в себя:

- информацию, составляющую банковскую тайну, разглашение которой способно нанести стратегический ущерб интересам клиентов банка (стратегия маркетинга, новые научные и технологические разработки, финансовые резервы и места их хранения, используемые схемы налогового планирования и т.п.);
- закрытую информацию о собственниках, принадлежащих им активах, механизмах коммерческого партнерства с банком, формах участия в прибылях;
- информацию о стратегических планах банка по коммерческому и финансовому направлениям деятельности, вопросам перспективного регионального развития, слияния с другими кредитно-финансовыми организациями или поглощения их, о дружественных банках и иных финансовых институтах (особый характер отношений с которыми необходимо на время скрыть);
- любую информацию о деятельности службы безопасности, реализуемой в рамках стратегий «упреждающего противодействия» и, частично, «адекватного ответа»;
- прикладные методы защиты информации банка (коды, пароли, программы).

Строго конфиденциальные сведения (гриф XX) включают в себя:

- все прочие конфиденциальные сведения о клиентах банка;
- информацию маркетингового, финансового и технологического характера, составляющую коммерческую тайну;
- информацию о сотрудниках банка, содержащуюся в индивидуальных досье.

Конфиденциальные сведения (гриф X) включают в себя:

- базы данных по направлениям деятельности кредитно-финансовой организации, созданные и поддерживаемые в качестве элементов обеспечения соответствующих систем управления;
- сведения о заработной плате и индивидуальных «социальных пакетах» сотрудников банка, а также составе «резерва на выдвижение»;
- внутренние регламенты (положения, инструкции, приказы и т.п.) используемые в системе внутрибанковского менеджмента.

[2] Коммерческим структурам не рекомендуется использовать традиционную систему грифов «Секретно», «Совершенно секретно», «Для служебного пользования», «ООО» и т.п., поскольку это облегчает поиск наиболее ценной информации для хищения. Более целесообразно применять собственную систему грифов.

Наконец, к *информации для служебного пользования* относятся любые другие сведения, не подлежащие публикации в открытых источниках.

Результатом этой работы является внутренний (строго конфиденциальный) документ – «Перечень сведений, составляющих банковскую и коммерческую тайну». Наряду с определением общего состава защищаемой информации он должен содержать порядок понижения уровня ее секретности и последующего полного рассекречивания. Это является отражением процессов естественного устаревания любых конфиденциальных сведений. По прошествие определенного времени или при изменении ситуации (например, ликвидации фирмы – клиента банка) они перестают нести угрозу информационной безопасности банка, поэтому дальнейшая их защита становится нецелесообразной.

Вторым этапом является оценка возможных каналов утечки (перехвата) конфиденциальной информации банка. При этом выделяются следующие группы каналов:

Каналы утечки через внешние и локальные компьютерные сети банка, целью определения которых является выявление (для последующей организации их особой защиты) терминалов:

- объединенных в закрытые локальные сети;
- используемых работниками банка – носителями особо секретных сведений;
- подключенных к локальным сетям и доступных для использования клиентами банка, а также другими лицами, не являющимися его сотрудниками.

Каналы утечки с использованием технических средств перехвата информации, целью определения которых является выявление помещений, нуждающихся в особой защите:

- зал заседания Правления и Совета директоров;
- кабинеты высших руководителей и ведущих экспертов;
- хранилище банка;
- офисы службы программного обеспечения;
- офисы службы безопасности;
- помещения, в которых обычно осуществляется неформальное общение сотрудников банка (туалетные и курительные комнаты, буфеты, столовая);
- комнаты для переговоров и т.п.

Каналы утечки по вине нелояльных или безответственных сотрудников банка, целью определения которых является составление перечня рабочих мест (должностей), ранжированных по принципу доступа к различным группам защищаемой информации и нуждающихся в специальном обучении, защите или особом контроле:

- носители абсолютно конфиденциальной информации (допуск «А»);
- носители строго конфиденциальной информации (допуск «В»);
- носители конфиденциальной информации (допуск «С»);
- группа повышенного риска (молодые специалисты и недавно нанятые сотрудники).

Основной целью работы по второму этапу выступает выявление наиболее вероятных угроз в отношении каждой из позиций указанного выше «Перечня», следовательно – обеспечение возможности выбора наиболее целесообразных методов и форм защиты.

Третьим этапом является определение перечня прикладных методов защиты информации. Они делятся на следующие группы:

К методам программно-математического характера относятся:

- программы, ограничивающие доступ в компьютерные сети и отдельные компьютеры банка;

- программы, защищающие информацию от повреждения умышленно или случайно занесенными вирусами (автоматическое тестирование при включении компьютера, при использовании СД – дисков или дискет);
- программы, автоматически кодирующие (шифрующие) информацию;
- программы, препятствующие перезаписи информации, находящейся в памяти компьютера, на внешние носители или через сеть;
- программы, автоматически стирающие определенные данные с ограниченным для конкретного пользователя временем доступа.

К методам технического характера относятся*:*

- использование экранированных помещений для проведения конфиденциальных переговоров;
- использование специальных хранилищ и сейфов для хранения информации на бумажных носителях (при необходимости с устройствами автоматического уничтожения ее при попытке несанкционированного проникновения);
- использование детекторов и иной аппаратуры для выявления устройств перехвата информации;
- использование защищенных каналов телефонной связи;
- использование средств подавления устройств перехвата информации;
- использование средств автоматического кодирования (шифровки) устной и письменной информации.

К методам организационного характера относятся:

- мероприятия по ограничению доступа к конфиденциальной информации (общережимные мероприятия, системы индивидуальных допусков, запрет на вынос документов из соответствующих помещений, возможность работы с соответствующей компьютерной информацией лишь с определенных терминалов и т.п.);
- мероприятия по снижению возможности случайного или умышленного разглашения информации или других форм ее утечки (правила работы с конфиденциальными документами и закрытыми базами компьютерных данных, проведения переговоров, поведения сотрудников банка на службе и вне ее);
- мероприятия по дроблению конфиденциальной информации, не позволяющие сосредоточить в одном источнике (у сотрудника, в документе, файле и т.п.) все сведения по вопросу, интересующему потенциального субъекта угроз;
- мероприятия по контролю над соблюдением установленных правил информационной безопасности;
- мероприятия при выявлении фактов утечки той или иной конфиденциальной информации.

Четвертым этапом является непосредственное формирование и внедрение подсистемы информационной безопасности банка, предполагающее:

Разработку общей концепции информационной безопасности как элемента общей стратегии безопасности банка, определяющей:

- принципы ранжирования конфиденциальной информации по степени ее важности для банка, следовательно, по требованиям к эффективности защиты;
- подходы к обеспечению специальными программными продуктами (самостоятельная разработка или заказ у специализированных подрядчиков);

- подходы к распределению ответственности за обеспечение информационной безопасности между уполномоченными штабными службами (безопасности, персонала, маркетинга, информационных технологий) и линейными подразделениями;
- подходы к выбору методов пресечения выявленных угроз;
- подходы к выделению ресурсов, необходимых для профилактики и пресечения возможных угроз (фиксированный процент от общей суммы собственных расходов банка, выделение средств под представленные сметы и целевые программы и т.п.);
- критерии оценки эффективности защиты конфиденциальной информации;

Разработку внутренней нормативной базы в составе:

- общих для всего банка регламентов (например, «Положение о правилах обеспечения информационной безопасности», «Правила проведения конфиденциальных переговоров», «Правила работы с закрытыми базами данных», «Перечень сведений, составляющих банковскую и коммерческую тайну» и т.п.),
- внутренних регламентов службы безопасности банка, включая должностные инструкции ее сотрудников, специализирующихся в этой области;
- правил обеспечения информационной безопасности, фиксируемых в регламентах конкретных структурных подразделений банка и должностных инструкциях его сотрудников.

Расчет и выделение финансовых ресурсов необходимых:

- для приобретения (самостоятельной разработки), эксплуатации и обновления программных средств и средств инженерно-технической защиты;
- для проведения соответствующих организационных мероприятий;
- службе безопасности для осуществления специальных профилактических и контрольных мероприятий.

Обучение персонала банка и специалистов самой службы безопасности правилам обеспечения информационной безопасности (см. подраздел 1.4).

Формирование и последующее развитие формализованных процедур контроля над соблюдением установленных в рамках данной подсистемы правил силами:

- службы безопасности банка;
- руководства структурных подразделений.

Раздел 4. Обеспечение безопасности персонала кредитно-финансовых организаций

4.1. Персонал банка как объект потенциальных угроз

В современных условиях персонал предприятия необходимо рассматривать как самостоятельный объект защиты от различных угроз. Это определяется рядом факторов, отражающих имущественные и неимущественные интересы работодателя. Так, часть сотрудников предприятия в силу занимаемой должности является носителями конфиденциальной информации, опасность разглашения которой подробно рассматривалась в предыдущем разделе Пособия. Не меньшую угрозу представляет для работодателя утеря ценных для него кадров из числа руководителей и ведущих специалистов.

Дополнительная актуальность защиты собственного персонала в банковском секторе экономики связана с действием следующих факторов:

- больший удельный вес сотрудников, выступающих как носителей информации, составляющей банковскую и коммерческую тайну;
- более высокая степень профессиональной специализации и технологической обособленности труда банковских служащих, что создает дополнительные проблемы при необходимости оперативного замещения внезапно освободившихся рабочих мест.

Типовой перечень потенциальных угроз персоналу:

- прямое переманивание конкурентами ведущих руководителей и специалистов банка;
- вербовка сотрудников банка конкурирующими и криминальными структурами, а в отдельных случаях – правоохранительными органами;
- шантаж или прямые угрозы в адрес конкретных сотрудников с целью склонения их к нарушению доверия со стороны работодателя (т.е. к совершению различных должностных нарушений);
- покушения на сотрудников (прежде всего, высших руководителей банка) и членов их семей.

Перечень категорий сотрудников банка как объектов защиты (ранжированный по степени приоритетности):

- высшее руководство банка (президент и его первые заместители);
- главные специалисты и эксперты банка по конкретным направлениям деятельности (финансы, маркетинг, компьютерные технологии и т.п.);
- сотрудники, занимающие рабочие места, предполагающие доступ к особо конфиденциальным сведениям (стратегические планы развития, обслуживание элитных клиентов, организация систем безопасности и т.п.);
- прочие сотрудники банка.

Защита первых трех категорий сотрудников осуществляется службой безопасности в постоянном режиме (естественно, с различной степенью интенсивности), последней категории – лишь при возникновении в их адрес реальных угроз. Непосредственная организация защиты банковских служащих, как и других объектов, предполагает использование двух групп методов – профилактических и пресекающих.

4.2. Организация защиты персонала от возможных угроз

а. Защита от переманивания сотрудников конкурентами реально может быть обеспечена лишь путем справедливого отношения к ним со стороны работодателя. Эта проблема является предметом изучения в рамках специального курса «Персональный менеджмент в банке» (см. соответствующее УПП). Здесь констатируется лишь ***главное методическое требование к ее решению*** – удовлетворенность сотрудника своим работодателем определяется не только уровнем оплаты труда, но и тремя сопутствующими факторами:

- удовлетворенностью текущим служебным положением и уверенностью в возможности дальнейшего карьерного роста;
- наличием эффективной социальной и психологической поддержки;
- корректным отношением со стороны руководства.

б. Защита от вербовки сотрудников осуществляется службой безопасности по двум направлениям. Первым из них является целевое обучение, организация которого далее специально рассматривается. Второе направление предполагает необходимость решения нескольких прикладных задач.

Прежде всего, ***служба безопасности должна определить перечень рабочих мест, в отношении которых вербовка наиболее вероятна***. В данном случае целесообразно «отталкиваться» от перечня потенциальных субъектов данной угрозы. В частности, *объектами вербовки со стороны фискальных и правоохранительных органов государства* будут являться сотрудники бухгалтерии, через которых проходят расчеты налоговых платежей и сведения по движению финансовых потоков банка. В отделе расчетно-кассовых операций подобная угроза возникает по рабочим местам, через которые проходит обслуживание клиентов, потенциально интересных для указанных выше государственных органов. *Объектами вербовки со стороны конкурентов* с высокой степенью вероятности будут являться специалисты отдела маркетинга, отвечающие за перспективные программы развития на рынке и внедрение новых технологий обслуживания клиентов, а также помощники первых руководителей (референты, личные секретари). Наконец, *объектами вербовки со стороны криминальных структур* приоритетно могут выступать сотрудники, имеющие доступ к информации, составляющей банковскую тайну (финансовое состояние клиентов из числа юридических и физических лиц), а также связанные с транспортировкой, хранением и охраной наличных денежных средств.

Следующей задачей службы безопасности является ***организация специальной проверки сотрудников, занимающих указанные выше рабочие места***. Подобная проверка осуществляется силами службы безопасности и службы персонала. В ее процессе специалистами этих служб изучаются индивидуальные досье сотрудников, проводятся личные беседы (в том числе с участием психолога), при необходимости собираются дополнительные сведения. Объектами изучения являются имущественное положение сотрудников, их личностные качества, отношения с руководством и коллегами по работе. По результатам проверки проводится группировка объектов потенциальной угрозы на три условных категории. *К первой категории риска относят банковских служащих, которые очевидно уязвимы по отношению к возможной вербовке*. Подобную оценку могут определить, например, следующие факторы:

- наличие постоянных связей (контактов) с работниками структур, представляющих соответствующую угрозу для банка;
- неудовлетворенность отношениями с руководителем, коллегами по работе;
- открытое недовольство должностным и материальным положением;

- личностные качества, определяющие потенциальную нелояльность работодателю (тщеславие, меркантилизм, зависть, доверчивость и т.п.).

В отношении данной категории наиболее эффективными методами профилактики являются увольнение или перевод на должность, не представляющую интереса для субъекта вербовки.

Ко второй категории риска относят сотрудников, чьи личностные качества, имущественное положение или зависимость от работодателя делают их практически неуязвимыми для вербовки. Следует признать, что это самая немногочисленная категория персонала, особенно для России, где еще не сформировались ни династии банковских служащих, ни определенный трудовой менталитет. В отношении данной группы единственным методом профилактики является короткая беседа о гипотетической возможности вербовки. При этом проводящий беседу сотрудник обязан неоднократно подчеркнуть, что единственной ее целью является разъяснение правил поведения в такой ситуации, обеспечивающее личную безопасность исключительно ценного для банка служащего (лояльность которого работодателю естественно сомнений не вызывает). В дальнейшем служба безопасности проводит лишь периодический контроль над сохранением данными сотрудниками качеств, позволивших отнести их к рассматриваемой категории.

Наиболее многочисленной группой являются все оставшиеся сотрудники, информация о которых не позволяет отнести их к первым двум категориям. В отношении их служба безопасности использует такой профилактический метод как специальное обучение, входящее в общую программу подготовки персонала, а также контролирует их лояльность специальными методами.

в. Защита от шантажа и угроз в адрес сотрудников банка по методике своей организации во многом совпадает с предыдущим направлением. Начиная с XIX века, когда в большинстве стран окончательно сформировалась система специальных служб, профессионалам известно общее правило: «шантажировать можно того, кто сам напрашивается на шантаж». На практике это означает, что жертвами шантажа за редким исключением становятся те сотрудники банка, которые своим поведением уже скомпрометировали себя перед работодателем и вынуждены любым путем скрывать это. Поэтому субъекты потенциальных угроз, при их подготовке концентрируют свои усилия на поиске сотрудников, которые либо уже допустили соответствующие нарушения, либо теоретически способны на это. В первом случае первым этапом шантажа становится получение компрометирующих материалов о том или ином сотруднике. Во втором – искусственное создание компрометирующей ситуации, которая в дальнейшем станет предметом шантажа.

В современных условиях *основными предметами шантажа в адрес сотрудников банка* являются (в ранжированном виде):

- уже допущенные сотрудниками нарушения доверия работодателя (хищения, коррупция, разглашение конфиденциальной информации и т.п.);
- факты и обстоятельства, способные скомпрометировать в глазах работодателя личностные или профессиональные качества сотрудника (образ жизни, хронические заболевания, постоянные контакты и т.п.);
- факты и обстоятельства, способные стать причиной претензий к сотруднику со стороны правоохранительных органов (административные или уголовные правонарушения) или налоговых служб;
- факты и обстоятельства, способные стать причиной угроз благополучию личной жизни сотрудника (с учетом изменившихся морально-этических норм поведения – в современных условиях наименее вероятно).

Наряду с традиционными методами служб безопасности и персонала банка по контролю над общей лояльностью сотрудников, *основным методом профилактики* подобных угроз является разъяснение им:

- техники шантажа как одного из инструментов угроз безопасности банка;
- типовых ситуаций, при которых шантаж может стать возможным;
- правил поведения в случае шантажа (при этом четко излагается основной тезис: «если объект шантажа, ранее действительно нарушивший доверие работодателя, немедленно ставит об этом в известность службу безопасности, то он либо полностью освобождается от ответственности, либо несет ее в минимально возможном объеме»).

После того, как факт шантажа установлен, служба безопасности банка может в зависимости от общей стратегии своей деятельности использовать различные *методы пресечения*:

- самостоятельно или через шантажируемого сотрудника довести до субъекта угрозы информацию об ее выявлении (наиболее простой метод, рекомендуемый для банков, проводящих стратегию пассивной защиты);
- в случае выявления факта шантажа без участия его объекта либо сразу уволить шантажируемого сотрудника, либо «втемную» использовать его как источник дезинформации субъекта угрозы (вариант, рекомендуемый для банков, проводящих стратегию адекватного ответа);
- использовать добровольно признавшегося сотрудника в качестве источника дезинформации субъекта угрозы (вариант, требующий дополнительных гарантий личной безопасности участвующему в операции сотруднику).

В отличие от шантажа, **прямые угрозы в адрес сотрудников банка** чаще всего не связаны с негативными моментами в их профессиональной деятельности или личной жизни. *Основным критерием выбора объекта угроз является должностное положение сотрудника* и возможности, которые из него вытекают. Лишь в случае, когда целям субъекта угрозы могут способствовать одновременно несколько банковских служащих, на его выбор могут повлиять их личные качества, например, нерешительность, боязнь любых открытых конфликтов, любовь к семье и т.п.

Субъектами подобных угроз чаще всего выступают:

- криминальные структуры (в основном из категории «молодых группировок», обычно не представляющие серьезной опасности для банка из-за ограниченных возможностей);
- собственные сотрудники банка, заинтересованные в сокрытии информации о допущенных нарушениях (обычно либо прямые руководители объекта угрозы, либо начальники инспектируемых им подразделений).

Основным методом профилактики является разъяснение сотрудникам банка необходимости немедленного информирования службы безопасности о факте угрозы, высказанной в любой форме. При этом до сведения обучаемого доводятся:

- полная бесперспективность для субъекта практической реализации угрозы, если о ней уже стало известно работодателю;
- возможности службы безопасности по защите от подобных угроз;
- возможность получения объектом угроз, оперативно оповестившим службу безопасности, специальных компенсационных выплат или социальных льгот (естественно, при подтверждении реальности такой угрозы).

Для подтверждения факта угроз служба безопасности может использовать разнообразные технические средства и оперативные мероприятия, в рамках, регламентированных действующим законодательством.

Пресечение дальнейших угроз осуществляется различными методами, в зависимости от избранной стратегии обеспечения собственной безопасности:

- увольнение или иные санкции к своему сотруднику, допустившему угрозы в адрес подчиненного или ревизора;
- оповещение правоохранительных органов;
- решение проблемы с внешним для банка субъектом угрозы иными, не противоречащими закону методами.

г. Защита от покушений на сотрудников банка и членов их семей является традиционной функцией службы безопасности любого российского банка. В современных отечественных условиях вероятность реализации подобных угроз существенно выше, нежели в большинстве зарубежных стран. С начала 90-х годов жертвами покушений стали более полутора тысяч высших должностных лиц самых различных по размерам и территориальному расположению банков. Это объясняется не только общей криминагенностью российской экономики и характерной для отечественных преступных группировок ориентацией на «силовые» методы. По мнению специалистов как правоохранительных органов, так и экспертов в области безопасности предпринимательской деятельности, основными (в порядке убывающей вероятности) причинами физического устранения банкиров являются:

- участие банка в борьбе за раздел или последующий передел государственной собственности (например, за контрольный пакет акций нефтяной компании, горно-обогатительного комбината, крупного отеля), осуществляемой с использованием нелегитимных методов;
- невыполнение обязательств, принятых на себя в рамках прямого сотрудничества банка с «теневой» экономикой и организованной преступностью («отмывание» денег и перевод их за рубеж, операции с «черным налом»);
- борьба за контроль над конкретным банком между двумя преступными группировками, если его высшее руководство занимает сторону одной из них;
- невыполнение принятых на себя обязательств в отношении крупных клиентов и партнеров (было характерно лишь в первой половине 90-годов).

Дополнительной отраслевой спецификой организации защиты от рассматриваемых здесь угроз, является повышенные требования к профессионализму соответствующих сотрудников службы безопасности. Им следует учитывать, что к организации покушений против руководителей банков «заказчики» привлекают исключительно профессиональных киллеров, в нашей стране часто подготовленных еще государственными спецслужбами. Практика показывает, что чаще всего службе безопасности не удается пресечь покушение. Поэтому, ***главным требованием к организации защиты от рассматриваемых угроз является их профилактика***, т.е. создание ситуации, при которой заказ на покушение не поступит вообще или будет отозван самим заказчиком.

Работа по защите персонала банка от покушений осуществляется службой безопасности по нескольким направлениям и, соответственно, включает большое количество организационно-технических процедур и мероприятий. С учетом изложенного выше требования, *основным направлением является профилактика угроз в режиме «раннего предупреждения»*. Этой работой занимаются сотрудники информационно-аналитического отдела, чьей обязанностью является выявление потенциальных заказчиков покушения, конкретных объектов угроз и, по возможности технических деталей (формы покушения, сроков, исполнителя). При успешном решении этой задачи у банка появится возможность выбора между несколькими вариантами поведения:

- решение проблемы путем ликвидации самой причины готовящегося покушения (урегулирование конфликтной ситуации в процессе переговоров, реализация принятых обязательств и т.п.);
- решение проблемы путем использования угроз адекватного воздействия на самого заказчика;
- усиление защиты объекта покушения до уровня, делающего угрозу практически нереализуемой (трудно осуществимо с технической точки зрения);
- обращение за помощью к правоохранительным органам (наименее эффективное решение, целесообразное лишь для банков, реализующих стратегию «пассивной защиты»).

Другим методом профилактического характера является *изучение службой безопасности статистики подобных угроз с последующей подготовкой специального аналитического доклада для высшего руководства банка*. В докладе, наряду с обобщенным фактологическим материалом, должны быть в ранжированном виде перечислены действия банка, которые могут стать причинами покушений на его руководство. Эта рекомендация особенно актуальна для вновь создаваемых кредитно-финансовых организаций, руководство которых может не до конца представлять возможные последствия тех или иных действий. В рамках использования данного метода целесообразно также привлечение руководителя службы безопасности к экспертизе крупных контрактов или коммерческих программ, намеченных к реализации. От него требуется выявить вероятность сопутствующих ей угроз и доложить о них руководству.

Наконец, традиционным методам профилактики является *обучение объектов потенциальных угроз в лице высших руководителей и членов их семей основным правилам личной безопасности*. Оно осуществляется по двум направлениям. Первое связано с поведением объектов защиты во время сопровождения их сотрудниками службы безопасности (т.е. личными телохранителями). Главная цель обучения – формирование у объекта рефлекса моментального и безоговорочного подчинения любому требованию телохранителя. Следует учитывать, что в случае реальной угрозы покушения, у его объекта есть в лучшем случае несколько секунд для эффективного реагирования (например, уход с линии огня, выход из помещения и т.п.). Поэтому любые пререкания с сотрудником личной охраны, выяснение причин поступившей от него команды или промедление с ее исполнением может стоить объекту жизни. Второе направление имеет своей целью обучение объектов потенциальных покушений правилам поведения в отсутствие личной охраны. В настоящем Пособии они не рассматриваются, поскольку уже сформулированы в специальных инструкциях и методиках, хорошо знакомых профессионалам служб безопасности.

Непосредственная организация защиты объектов угроз от покушений реализуется специальным подразделением отдела физической защиты. В зависимости от избранного стратегического приоритета комплектации службы, оно может формироваться как из ее штатных сотрудников, так и из специалистов частных охранных агентств. Профессиональная подготовка и дальнейшее поддержание квалификационного уровня телохранителей является предметом специальных учебных курсов и в настоящем Пособии не рассматривается. Ниже формулируются лишь наиболее важные рекомендации к организации деятельности группы личной защиты:

- при комплектации группы штатными сотрудниками банка предпочтение следует отдавать профессиональным телохранителям, получившим специальную подготовку в государственных или частных структурах (но не бывшим спортсменам или офицерам

специальных войск, поскольку методика их обучения имела принципиально иные задачи);

- в составе группы целесообразно выделять контингент постоянных личных телохранителей ограниченного числа высших руководителей банка и дежурных телохранителей для разовой охраны других его специалистов (например, на время их служебной командировки);
- в процессе периодического мониторинга уровня профессиональной подготовки телохранителя необходимо обращать внимание на его психологическое состояние, при необходимости обеспечивая соответствующую коррекцию;
- штатные телохранители банка подлежат обязательному личному страхованию за счет работодателя (для сотрудников частных агентств это входит в стоимость контракта), при этом экономия недопустима.

4.3. Обучение персонала правилам обеспечения безопасности банка-работодателя

Изучение рассмотренных в предыдущих разделах угроз безопасности кредитно-финансовой организации показывает, что необходимым участником процесса защиты от них является собственный персонал. Это определяет актуальность специальной подготовки банковских служащих, которая может рассматриваться в системе управления безопасностью в качестве одного из важнейших профилактических методов. Следует учитывать, что в силу действия психологических факторов в глазах сотрудников эта подготовка, в отличие от профессионального обучения и повышения квалификации, всегда будет носить вторичный по значимости характер. Для большинства же высококвалифицированных специалистов, особенно руководителей среднего и высшего звена, она чаще всего будет вызывать плохо скрываемое раздражение (по крайней мере, до момента первого серьезного столкновения с реальными угрозами).

Общими методическими требованиями к организации подготовки:

- распространение подготовки на все категории персонала банка, с дифференциацией ее форм и методов по должностным категориям обучаемых;
- непрерывность подготовки, что обеспечивается регулярным проведением специальных профилактических бесед или разбором уже состоявшихся угроз в адрес банка;
- привлечение к подготовке не только специалистов службы безопасности, но и руководителей структурных подразделений банка, обычно имеющих в глазах своих подчиненных больший авторитет;
- использование в процессе обучения наряду с теоретическими материалами практических примеров из деятельности своего и иных банков;
- использование методов обучения, способных вызвать интерес обучаемых к самому процессу подготовки, например, ролевые игры, видеозаписи, демонстрация некоторых технических средств защиты и т.п.

Организация подготовки вновь нанятых сотрудников банка

Это подготовка является необходимым элементом первичного обучения и адаптации зачисленного в штат персонала (см. УПП «Персональный менеджмент в банке»). *Она дифференцирована по двум категориям сотрудников – молодых специалистов и банковских служащих, уже имеющих опыт практической работы* в других кредитно-финансовых организациях.

Для первой категории рассматриваемая подготовка особенно актуальна, поскольку они в лучшем случае имеют лишь чисто теоретическое представление о безопасности банковской деятельности[3]. Кроме того, в силу своего возраста они более легкомысленны, амбициозны, следовательно, особо уязвимы к различным методам воздействия со стороны потенциальных субъектов угроз. Обучение данной категории сотрудников осуществляется в несколько последовательных этапов. На первом этапе занятия проводятся со всеми нанятыми молодыми специалистами в форме беседы – инструктажа[4]. Практическая их организация возлагается на службу безопасности банка, специалист которой должен разъяснить обучаемым:

- общие понятия и направления обеспечения безопасности предпринимательской деятельности;
- отраслевую специфику обеспечения безопасности в банковском секторе;
- дополнительные требования в этой области, действующие в конкретной кредитно-финансовой организации.

Здесь следует выделить две связанные друг с другом цели. Во-первых, обучаемые должны осознать необходимость строгого соблюдения установленных правил обеспечения безопасности работодателя. Во-вторых, и это является более сложной задачей, обучаемых необходимо убедить в целесообразности ***сотрудничества со службой безопасности как залога их собственного благополучия.*** Практика показывает, что большинство сотрудников любой российской организации крайне неохотно идут на подобное сотрудничество, считая аморальным информирование службы безопасности о соответствующих нарушениях со стороны коллег по работе. Именно поэтому молодым работникам банка следует в предельно доходчивой форме объяснить возможные последствия этих нарушений для них лично.

Например, сотрудником службы безопасности может быть рассмотрена ситуация по следующей упрощенной схеме. Нелояльный сотрудник передает конкуренту конфиденциальную информацию. Его коллега случайно узнает об этом, но из соображений ложной солидарности скрывает данный факт. Через какое то время виновный сотрудник увольняется из банка и переходит на работу к конкуренту, улучшая при этом свое должностное и финансовое положение. Разглашение информации приводит к ухудшению конкурентных позиций работодателя на соответствующем рынке, следствием которого является вынужденное сокращение штата профильного подразделения. Традиционной группой попадающих под сокращение сотрудников в современных условиях являются именно молодые специалисты. В результате, проявивший «солидарность» сотрудник теряет работу со всеми вытекающими для него последствиями.

На этом этапе новому сотруднику вручают специальную «памятку», которая, выступая элементом внутреннего нормативно-методического обеспечения системы, содержит:

- общие правила обеспечения безопасности банка;
- ответственность сотрудника за соблюдение установленных правил;
- перечень полномочий службы безопасности по контролю и прямому функциональному руководству соответствующим направлением деятельности банковского персонала;

[3] До настоящего времени в программах даже ведущих финансовых вузов проблемам обеспечения банковской безопасности уделяется недостаточное внимание

[4] Найм которых обычно осуществляется работодателями в рамках ежегодной «компании» в течение ограниченного периода после завершения очередного учебного года (июнь – август)

- рекомендации по предотвращению ситуаций, способных сделать работника банка объектом вербовки и шантажа;
- рекомендации по поведению в случае попытки вербовки и шантажа.

На втором этапе первичного обучения занятия с молодыми специалистами проводят их непосредственные руководители в структурных подразделениях банка. Их задачей является доведение до обучаемых конкретных правил обеспечения безопасности на конкретных рабочих местах. Прежде всего, обучение касается правил работы с конфиденциальной информацией, включая закрытые базы данных. По некоторым рабочим местам оно может включать изучение особых правил работы с соответствующими клиентами банка, дополнительных элементов технологий проведения финансовых операций.

Первичная подготовка сотрудников, уже имеющих опыт работы в банковском секторе экономики, проводится по сокращенной программе. Она осуществляется на рабочих местах и включает изучение лишь специфических правил обеспечения безопасности в рамках исполняемых служебных обязанностей. Для работников категорий «руководители» и «эксперты» подготовку завершает оформление допуска к конфиденциальной информации различной степени секретности (см. раздел 3 настоящего Пособия).

Организация последующей подготовки сотрудников банка

В соответствии с методическим требованием непрерывности обучения, подготовка сотрудников банка по рассматриваемому направлению деятельности осуществляется службой безопасности в двух формах.

Регулярная профилактическая работа с персоналом банка проводится дифференцированно по категориям персонала. Для высшего руководства она имеет форму специального обзора, ежемесячно представляемого за подписью вице-президента по безопасности. Обзор освещает динамику ситуации по рассматриваемому направлению в конкретном банке и включает в себя:

- фактологический материал – состоявшиеся и предотвращенные угрозы безопасности банка, потери от них, непосредственные виновники или причины, принятые меры и т.п.;
- ранжированный перечень реальных угроз безопасности банка в текущий момент и рекомендации по их профилактике;
- обзор ситуации по анализируемому направлению на региональном или общенациональном рынке банковских услуг (с особым выделением ситуации у главных конкурентов).

Для руководителей самостоятельных структурных подразделений банка ежеквартально проводятся специальные встречи с вице-президентом по безопасности. Для остального персонала служба безопасности проводит специальный инструктаж непосредственно в соответствующих структурных подразделениях (также ежеквартально). При этом рекомендуется основное внимание уделять не уже известным сотрудникам правилам безопасности, а разбору выявленных нарушений. В этих же целях служба безопасности может готовить и размещать на общедоступном сайте локальной сети банка регулярно обновляемый бюллетень с соответствующей информацией. Наконец, при выявлении серьезных нарушений правил обеспечения безопасности (разглашение информации, коррупция, саботаж) в конкретном подразделении, обязателен разбор его на общем собрании сотрудников.

4.4. Организация контроля над соблюдением персоналом правил обеспечения безопасности и его лояльностью.

Контроль по рассматриваемому направлению осуществляется службой безопасности банка. В зависимости от ее организационной структуры, им могут заниматься либо уполномоченные сотрудники специализированных подразделений (отдела информационной безопасности, физической защиты и т.п.), либо инспектора специального подразделения контроля внутреннего режима. Основными задачами проведения данной работы выступают:

- оценка общей эффективности управления обеспечением безопасности в конкретных структурных подразделениях банка;
- контроль над лояльностью конкретных сотрудников;
- выявление конкретных нарушений и их виновников.

Исходя из этого, организация данной работы осуществляется службой безопасности одновременно по нескольким направлениям.

Профилактический контроль над соблюдением правил обеспечения безопасности в трудовых коллективах банка проводится с использованием различных методов и процедур, в частности:

- ***плановых и внезапных проверок***, в процессе которых служба безопасности проверяет соблюдения в структурных подразделениях правил работы с конфиденциальной информацией, хранения денежных и иных ценностей, а также работоспособность технических средств защиты;
- ***мониторинга ситуации с использованием специальных технических средств наблюдения*** (например, видеокамер, первоначально установленных в качестве технических средств защиты имущества и персонала);
- ***мониторинга ситуации силами нештатных информаторов службы безопасности из числа сотрудников соответствующих подразделений банка*** (подобная практика широко используется службами безопасности предприятий и органов государственного управления, хотя обычно и не рекомендуется в открытых учебных материалах).

По результатам оперативного контроля служба безопасности готовит специальные отчеты для президента банка, информационные записки на имя руководителей его структурных подразделений. При необходимости она организует проведение специальных совещаний у руководства, собраний в трудовых коллективах подразделений, готовит проекты приказов о поощрениях или взысканиях.

Контроль личной лояльности персонала осуществляется службой безопасности ***в отношении сотрудников***:

- занимающих ключевые рабочие места (кроме должности президента), обеспечивающие доступ к особо конфиденциальной информации или возможность принимать решения стратегического характера;
- привлекших внимание службы безопасности своим поведением или иными фактами, ставящими под сомнение их лояльность.

Обязательным условием организации такого контроля является соблюдение требований действующего законодательства, прежде всего, Закона РФ «О частной детективной и охранной деятельности в РФ», а также конституционных гарантий неприкосновенности прав граждан.

В зависимости от цели и используемых методов контроля могут быть выявлены ***прямые нарушения в деятельности сотрудника***, являющиеся основанием для передачи соответствующего иска в судебные или заявления в правоохранительные органы, увольн-

нения, иных форм дисциплинарных взысканий. К числу подобных нарушений относятся подтвержденные соответствующими документами или иными материалами факты:

- проникновения в закрытые компьютерные базы данных и операционные системы с целью их копирования или проведения несанкционированных операций по счетам;
- любых попыток хищения денежных средств или материальных ценностей;
- коррупции в форме получения взяток от клиентов или партнеров банка;
- успешной вербовки сотрудника субъектами потенциальных угроз;
- склонения подчиненных к нарушению доверия работодателя;
- нарушений правил внутренней безопасности банка, в том числе и не приведших к реализации соответствующих угроз.

Кроме того, по результатам персонифицированного контроля служба безопасности может выявить ***факторы, определяющие сомнения в потенциальной лояльности сотрудника***, например:

- необъяснимое объективными причинами внезапное улучшение материального положения сотрудника или контактирующих с ним родственников;
- не вызванные служебной необходимостью контакты с представителями субъектов потенциальных угроз (конкурирующих банков, криминальных структур, налоговой полиции и т.п.);
- изменение образа жизни сотрудника или появление привычек и личностных качеств, делающих его уязвимым для вербовки и шантажа;
- зафиксированные регулярные высказывания недовольства работодателем, служебным положением, доходами и т.п.

В этом случае, в зависимости от занимаемого сотрудником служебного положения, профессиональных качеств, отзывов руководителя, к нему могут быть применены разнообразные методы воздействия. По отношению к малоценным для банка работникам рекомендуется невозобновление трудового контракта после истечения его срока, а до этого момента постоянный контроль над их поведением. В остальных случаях с сотрудником должна быть проведена индивидуальная профилактическая работа силами непосредственного руководителя, психолога службы персонала или специалиста службы безопасности.

Результаты персонифицированного контроля должны отражаться в системе специального учета самой службы безопасности и в индивидуальном досье сотрудника (см. УПП «Персональный менеджмент в банке»).

Выявление уже реализованных угроз безопасности банка с участием его собственного персонала может осуществляться силами штатных специалистов службы безопасности, приглашенных сотрудников частных охранных структур, государственных правоохранительных органов. При этом используются разнообразные оперативно-следственные мероприятия, не являющиеся предметом изучения в рамках настоящего Пособия. Ниже формулируются лишь общие методические правила и ограничения, которые необходимо соблюдать при проведении этой работы:

- при проведении расследования без привлечения государственных правоохранительных органов, обязательным условием является соблюдение требований действующего законодательства, прежде всего, Закона РФ «О частной детективной и охранной деятельности в РФ»;
- главной организационной предпосылкой эффективной работы по расследованию фактов нелояльности собственного персонала является наличие механизма персонифицированного контроля и учета;
- при наличии такой возможности – использование материалов и результатов подобных расследований для последующего обучения сотрудников.

Раздел 5. Обеспечение имущественной безопасности кредитно-финансовых организаций

5.1. Имущество банка как объект защиты

С позиции вероятных угроз имущественной безопасности банки оказались в «зоне повышенного риска» с момента своего появления на рынке в качестве самостоятельной категории хозяйствующих субъектов. Очевидной ***причиной такой ситуации является структура их имущества, основную часть которых составляют высоколиквидные активы*** – наличные деньги, ценные бумаги, золото. Это всегда привлекало к кредитно-финансовым организациям особое внимание злоумышленников. Зарубежная статистика показывает, что объектом реализованных угроз имущественной безопасности банки оказываются в 4,5 раза чаще, чем представители других отраслей экономики. Можно выделить три исторических этапа развития рассматриваемых угроз.

Первый этап начался с появлением первых кредитно-финансовых организаций в XIV – XV веках и продолжался почти до конца XIX века. Основными объектами угроз выступали наличность банка и, значительно реже, ценные бумаги на предъявителя. Соответственно субъектами угроз были индивидуальные и совместно действующие злоумышленники (взломщики сейфов и грабители), а также нелояльные сотрудники банка, по долгу службы имевшие доступ к его активам. Примеры практической реализации таких угроз широко отражены не только в специальной, но и в художественной литературе, в кинематографе. Отражать подобные угрозы для крупных банков было относительно просто. Для этого был необходим лишь достаточный штат охраны, надежные сейфы и кладовые, а также механизм контроля над ограниченным числом собственных служащих. Небольшие банки предпочитали пользоваться услугами крупных частных и государственных кредитно-финансовых организаций, в которых хранилась основная часть активов. Более сложных методов защиты требовали такие угрозы имущественной безопасности, как подделка ценных бумаг и мошенничества при получении кредитных ресурсов. Со всеми перечисленными угрозами банки сталкиваются до настоящего времени.

Переход ко ***второму этапу*** связан с появлением безналичного денежного оборота. Основной угрозой имущественной безопасности банков стали мошенники, подделывающие соответствующие финансовые документы для получения наличных денег или перевода средств. Защититься от подобных угроз можно было только путем принципиального усложнения системы внутрибанковского финансового учета и контроля, а также активизации сотрудничества между кредитно-финансовыми организациями в этой области. В современных условиях рассматриваемое направление защиты имущественной безопасности не потеряло своей актуальности. Примером наиболее масштабной реализации подобных угроз является общеизвестное мошенничество с «чеченскими авизовками», осуществленное в середине 90-х годов прошлого века и нанесшее российской банковской системе ущерб в десятки миллионов долларов.

Третий этап развития угроз имущественной безопасности кредитно-финансовых организаций связан с появлением компьютерных технологий обслуживания клиентов и межбанковских коммуникаций. Уже в 60-х годах США столкнулись с первыми успешными попытками использования компьютерных программ для хищения денежных средств. При этом масштаб угроз возрастал в геометрической пропорции. В 1962 году одним из

первых примеров хищения с использованием программных средств стала потеря Городским банком г. Детройта 7,1 тыс. долларов (программист изменил методику начисления компьютером процентов по депозитным счетам). В конце же 90-х годов ФБР с трудом предотвратила попытку хищения 700 млн. долларов в Первом национальном банке г. Чикаго. Развитие глобальных сетей компьютерных коммуникаций позволяет сегодня злоумышленнику совершить кражу, находясь за тысячи километров от атакуемого банка. Общеизвестным в России примером стало хищение жителем г. С.-Петербург В. Левиным с помощью своего офисного компьютера 2,8 млн. долларов у одного из лондонских банков. Принципиально важным является и тот факт, что очень часто угрозы имущественной безопасности банка сопряжены с угрозами безопасности информационной (в том числе – государственной). Так, в 1999 году объектом атаки стали компьютерные данные о секретных счетах Английского Банка. Отразить ее удалось лишь путем изменения кодов всех его корреспондентских счетов, на что ушло несколько недель. Возможные финансовые потери, исчисляемые десятками миллионов фунтов стерлингов, в этом случае были бы несопоставимы с ущербом, нанесенным государственной безопасности Великобритании. Таким образом, в современных условиях защита имущества банка требует от его руководства постоянного внимания и масштабных затрат.

Классификация угроз имущественной безопасности банка (в ранжированном по важности виде):

- хищение денежных средств путем несанкционированного проникновения в компьютерные сети банка и перехвата управления финансовыми операциями;
- хищение денежных средств с использованием поддельных банковских карточек;
- хищение денежных средств с использованием поддельных платежных документов (поручений, сертификатов, чеков, векселей и т.п.);
- мошенничество при получении кредитов;
- хищение высоколиквидных активов банка (наличных денег, ценных бумаг, золота и т.п.) с использованием насильственных методов (ограбление);
- хищение высоколиквидных активов банка с использованием ненасильственных методов (кража);
- хищение или умышленная порча материальных активов банка.

Возможными субъектами угроз имущественной безопасности банка в современных условиях чаще всего являются индивидуально действующие злоумышленники (хакеры, мошенники, взломщики), нелояльные собственные служащие и, реже, преступные группировки. Распространенным и наиболее опасным явлением выступает преступный сговор между сотрудником банка и сторонними злоумышленниками. Показательно, что в совремнных условиях общий уровень подготовки субъектов угроз в рассматриваемой области несколько ниже, чем по другим направлениям обеспечения безопасности. Причиной этого является отсутствие здесь угроз со стороны государства и конкурентов (в отличие от угроз безопасности информации и персонала). Последние сегодня пользуются услугами исключительно профессионалов, подготовленных в специальных учебных заведениях и чаще всего более компетентных в своей области, чем сотрудники службы безопасности большинства банков.

Отечественная специфика угроз имущественной безопасности:

- меньшая вероятность хищения денежных средств с использованием компьютерных сетей, в силу причин технологического характера (наличие подобных сетей лишь в ограниченном количестве крупных городов России);

- худшие возможности противодействия возможным угрозам из-за ограниченных финансовых возможностей большинства отечественных банков;
- большая степень вероятности угроз имущественной безопасности банка со стороны собственного персонала;
- большее распространение насильственных методов реализации угроз.

5.2. Защита от угроз с использованием сетей межбанковских компьютерных коммуникаций

Основные угрозы имущественной безопасности банка по данному направлению прямо или косвенно связаны с электронными платежами и расчетами в рамках общей системы обмена электронными данными. Суть концепции электронных платежей заключается в том, что должным образом оформленные и переданные сообщения по системе SWIFT[5] или другим сетям являются основанием для совершения одной или нескольких банковских операций. При этом расчеты могут осуществляться непосредственно между двумя банками (с использованием счетов лоро – ностро), либо с помощью специализированного клирингового банка. Сегодня в странах с развитой и технологически продвинутой банковской системой используется множество разнообразных технологий электронных платежей и расчетов, подробно рассматриваемых в специальных учебных курсах.

Несомненные преимущества использования информационных технологий в банковском деле определили их широкое распространение. Но, одновременно с этим, они вызвали к жизни новую форму угроз имущественной безопасности кредитно-финансовых организаций. Для защиты от этих угроз банк – участник системы обмена электронными данными обязан использовать специальные ***системы шифрования (или криптосистемы)***, представляющей собою совокупность алгоритмов шифрования и методов распространения ключей к этим шифрам. Правильный выбор криптосистемы позволяет:

- скрыть содержание сообщения от посторонних лиц, потенциально способных проникнуть в сеть и перехватить его;
- обеспечить возможность совместного использования сети группой пользователей системы обмена электронными данными путем криптографического разделения информации и соответствующего протокола распределения ключей (каждый из пользователей может иметь доступ только к своим сообщениям);
- своевременно обнаружить искажение или прямую подделку документа путем введения криптографического контрольного признака (имитовставки);
- удостовериться в том, что абонент действительно тот, за кого он себя выдает (аутентификация источника / получателя).

Главным элементом криптосистемы традиционно считается ***метод распространения ключей***, направленный на предотвращения доступа в сеть посторонних лиц. Сегодня используются несколько таких методов:

- *метод базовых ключей*, предполагающий наличие иерархии их распределения между пользователями системы (главный ключ, ключ шифрования ключей, ключ шифрования данных);
- *метод открытых ключей*, при котором часть ключа остается открытой и может быть передана по обычным линиям;

[5] The Society for Worldwide Inter-banc Financial Telecommunication – бесприбыльное кооперативное международное сообщество, целью которого является организация межбанковских расчетов по глобальным компьютерным сетям.

- *метод выведенного ключа*, при котором ключ для шифрования каждой последующей транзакции вычисляется путем одностороннего преобразования предыдущего ключа и параметров транзакции (применяется при расчетах клиентов банка с использованием электронных карточек);
- *метод ключа транзакции* отличается от предыдущего метода тем, что при вычислении ключа для следующей транзакции не используются ее параметры.

Выбор между различными по степени защищенности методами зависит от конкретной кредитно-финансовой организации, которая должна решить вопрос приоритета – большие затраты при меньшем риске или наоборот.

5.3. Защита от угроз, связанных с использованием электронных банковских карточек.

В современных условиях электронные банковские карточки получили широкое распространение (на начало XXI века их выпущено уже более миллиарда), резко сократив в экономически развитых странах наличный денежный оборот. Эти карточки классифицируются по многим признакам (эмитенту, наличия собственного микропроцессора, принципу поступления средств и т.п.), механизм работы с ними является предметом изучения в рамках специальных учебных курсов. В настоящем Пособии рассматриваются только проблема защиты банка от возможных угроз, связанных с их использованием.

По различным оценкам суммарные потери эмитентов, связанные с банковскими карточками, составляют не менее 1,5 млрд. долларов в год. Наиболее распространенными причинами потерь (в ранжированном виде) выступают:

- мошенничество продавца, снимающего с карточки большую сумму, чем требуется для оплаты товара или услуги;
- кража карточки с последующим ее использованием похитителем;
- подделка карточек;
- искажение данных, содержащихся в интеллектуальной карточке.

Следует также учитывать, что возможные прямые потери кредитно-финансовой организации в случае многократных случаев реализованных угроз по данному направлению (например, в случае недостаточной степени защиты выпускаемых ею карточек) дополняются ущербом ее имиджу в глазах имеющихся и потенциальных клиентов.

Основными требованиями к банковским карточкам являются их уникальность и необратимость. Первое требование предполагает, что среди всех выпущенных банком карточек не должно быть ни одной с одинаковыми характеристиками. В этом случае, создание подобной карточки будет полностью исключено для потенциального злоумышленника. Согласно второму требованию, первоначальная информация (например, прежняя сумма на платежной карточке) не может быть восстановлена после уже проведенных пользователем операций.

Имущественная безопасность банка по данному направлению ***обеспечивается несколькими методами:***

- специальные методы защиты обычных карточек (например, магнитные водяные знаки или сэндвич);
- переход от обычных к интеллектуальным карточкам, уровень защищенности которых принципиально выше;

- защита банкоматов (в части обеспечение безопасного места их расположения и уровня индивидуальной защиты);
- защита кассовых аппаратов, работающих с карточками, от угрозы вмешательства в их работу со стороны недобросовестных продавцов.

5.4. Защита банка от мошенничества при получении кредита

Имущественные потери банка в процессе управления его ссудным портфелем могут быть связаны с различными причинами. Большинство кредитных рисков определяются недостаточной эффективностью менеджмента по данному направлению деятельности, что является предметом изучения в рамках специальных учебных курсов[6]. В настоящем Пособии рассматривается только одна из разновидностей кредитных рисков, причиной которых является сознательный обман заемщиком своего кредитора. В современных отечественных условиях защита от подобных угроз особенно актуальна вследствие низкой деловой этики российского бизнеса, общей информационной непрозрачности рынков, меньшей степени лояльности собственного персонала.

Наиболее распространенными ***формами реализации рассматриваемых угроз*** выступают:

- получение кредита на основании фальсифицированных финансовых документов, подтверждающих благополучное состояние потенциального заемщика или наличие у него ликвидного залога (разновидность – получение кредита физическим лицом под залог фактически не принадлежащей ему квартиры);
- получение кредита на основании фальсифицированных финансовых гарантий от третьих лиц;
- получение кредита специально созданной для этого фирмой с последующим исчезновением ее с рынка.

Основным ***методом защиты от подобной угрозы*** является эффективное информационное обеспечение сделки на стадии ее подготовки. В отношении новых для банка клиентов традиционная технологией проверки кредитоспособности должна быть дополнена новыми элементами. В частности, служба безопасности банка должна собрать информацию о самом заемщике (учредители, время выхода на рынок, деловая репутация и т.п.), а также об условиях обеспечения кредита. Например, при использовании залога, представителям банка желательно лично ознакомиться с предлагаемым имуществом и подтвердить как право собственности, так и заявленную стоимость. Кроме того, с учетом угрозы коррупции соответствующих банковских служащих желательно введение в технологию кредитования принципа «двух подписей» не связанных отношениями соподчиненности специалистов.

5.5. Защита банка от угрозы хищений высоколиквидных активов

Рассматриваемая разновидность угроз имущественной безопасности банка актуальна для любой кредитно-финансовой организации, постоянно использующей в своей деятельности наиболее привлекательные для потенциальных злоумышленников виды ценностей – наличные денежные средства, золото, ценные бумаги на предъявителя. Ос-

[6] Финансовый менеджмент в кредитно-финансовых организациях, Кредитные операции коммерческих банков, Риск-менеджмент в кредитно-финансовых организациях и т.п.

новной формой реализации угроз являются кражи, осуществляемые с применением разнообразных технических средств.

Для отражения рассматриваемых угроз банк должен использовать дополняющие друг друга инженерно-технические и организационные методы. К ***методам инженерно-технического характера*** относятся:

- специальные хранилища для ценностей, т.е. сейфы и кладовые различной емкости, конструкции и стоимости;
- средства дополнительной технической защиты помещений, предназначенных для хранения ценностей (решетки, металлические двери и т.п.);
- средства для наблюдения за охраняемыми помещениями (открытые и скрытые видеокамеры);
- сигнализации различной конструкции.

К ***методам организационного характера*** относятся используемые процедуры защиты от несанкционированного доступа в защищаемые помещения и вскрытия хранилищ (порядок обходов охранниками банка, хранение ключей и кодов доступа, правила действий охраны при возникновении угрожающей ситуации и т.п.).

При профилактике рассматриваемых угроз следует учитывать, что главной причиной, которая вынудит потенциального злоумышленника отказаться от попытки кражи, является отсутствие информации об используемых конкретным банком средствах защиты. Поэтому любая информация об этих средствах должна относится к категории абсолютно конфиденциальной.

5.6. Защита банка от ограблений

Рассматриваемая форма угроз имущественной безопасности банка в современных условиях не относится к числу наиболее вероятных, поскольку у злоумышленников появились более безопасные и, главное, прибыльные возможности (мошенничество, хакерство и пр.). Вместе с тем, имеющийся опыт показывает, что кредитно-финансовые организации по-прежнему находятся в «зоне повышенного риска». В отечественных условиях вероятность этой угрозы существенно выше из-за большей распространенности преступлений насильственного характера. Следует учитывать, что ограбление имеет особую опасность, поскольку сопровождается угрозой личной безопасности граждан из числа сотрудников и клиентов банка.

Основными ***формами реализации подобных угроз*** являются:

- ограбление инкассаторов банка в момент транспортировки наличных денег;
- ограбление путем проникновения в помещения самого банка.

Вероятность реализации угрозы ограбления зависит от нескольких факторов:

- размеров банка (в наиболее угрожаемом положении находятся небольшие банки, располагающие худшими возможностями для защиты);
- специализации банка (определяющей масштабы его работы с наличными денежными средствами);
- степени криминагенности региона размещения банка;
- территориального расположения банка и его клиентов (в наиболее угрожаемом положении находятся банки, расположенные в менее людных районах города и имеющие протяженные маршруты транспортировки денег).

Основной принцип защиты от рассматриваемой угрозы предполагает ***обеспечение приоритета безопасности человека над безопасностью защищаемого имущества***. В первую очередь он реализуется при попытке ограбления в помещении банка, где могут находиться десятки посторонних людей. Поэтому служба безопасности банка не вправе своими действиями подвергать их хотя бы гипотетической угрозе.

Исходя из сформулированного выше принципа, основное внимание должно уделяться методам профилактического характера. Так, ***для профилактики угроз ограбления в помещении банка*** могут использоваться методы технического и организационного характера, исключающие возможность проникновения в помещение вооруженных лиц (система металлодетекторов, двойные двери, система видеонаблюдения за входом и т.п.). Для ***профилактики угроз ограбления инкассаторов*** основное внимание следует сосредоточить на постоянном изменении маршрутов движения инкассаторских автомобилей, надежности используемых машин, профессиональной подготовке их водителей.

Выводы

1. Специфика уставной деятельности кредитно-финансовых организаций, прежде всего – наличие у них разноплановой конфиденциальной информации и высоколиквидных активов, предполагает необходимость значительно большего внимания к проблеме обеспечения собственной безопасности, чем для предприятий большинства других отраслей.
2. Основным фактором, определяющим дополнительные требования к эффективности системы обеспечения собственной безопасности, является автоматическое перенесение потерь банка от реализованных угроз на его клиентов и связанный с этим ущерб имиджу, следовательно – конкурентным позициям.
3. Основным требованием к системе обеспечения собственной безопасности банка является комплексный подход к организации защиты от всех возможных угроз, исключающий наличие незащищенных или плохо защищенных объектов.
4. Основным принципом организации системы безопасности банка является «принцип разумной достаточности», предполагающий соразмерность затрат на защиту конкретного объекта степени размерам потерь от реализованных в его адрес угроз.
5. При формировании перечня используемых методов защиты от возможных угроз безопасности банка однозначный приоритет должны иметь методы профилактического характера (и лишь затем – пресекающего и карающего).
6. В процессе организации и последующего управления деятельностью службы безопасности необходимо уделять особое внимание вопросу рационального ограничения ее полномочий. В случае их превышения банк может подвергнуться разнообразным санкциям со стороны государства (от прямого уголовного преследования за нарушение Уголовного Кодекса РФ до необходимости компенсации морального ущерба сотрудникам банка, чьи конституционные права оказались нарушенными действиями рассматриваемой службы).
7. Выбор варианта стратегии обеспечения собственной безопасности определяется, в первую очередь, двумя факторами – избранным рынком (большая потенциальная рентабельность – большая вероятность угроз) и степенью агрессивности конкурентной стратегии.
8. Приоритетным объектом защиты в рамках системы является конфиденциальная информация, имеющаяся в распоряжении банка. В свою очередь, приоритет в системе информационной безопасности банка должна иметь конфиденциальная информация, составляющая банковскую тайну, что вытекает из статуса кредитно-финансовой организации как «особо доверенного лица» для своей клиентуры.
9. Развитие информатики и связанное с этим широкое распространение компьютерных технологий в банковском деле определило расширение перечня возможных угроз как информационной, так и имущественной безопасности кредитно-финансовых организаций. В современных условиях защита банка от несанкционированного проникновения в его компьютерные сети (для последующего вмешательства в финансовые операции или перехвата информации) стала приоритетной задачей службы безопасности.
10. Главной особенностью организации системы безопасности российских банков является необходимость большего внимание к защите от угроз со стороны собственных сотрудников. Основными причинами низкого уровня лояльности банковских служащих выступают, с одной стороны, специфический трудовой менталитет россиян и, с другой стороны, недостаточное внимание к проблемам персонального менеджмента со стороны руководства многих отечественных банков. В этой связи, важнейшей задачей по профилактике подобных угроз определяется формирование в трудовом коллективе кредитно-финансовой организации «корпоративного духа», предполагающего наличие уважения и доверия со стороны сотрудников к своему работодателю.

Список рекомендуемой литературы

1. Конституция РФ. М., 1993.
2. Гражданский кодекс РФ, ч. I, 1994, ч. II, 1995.
3. Уголовный кодекс РФ, 1996.
4. Закон РФ «О безопасности» от 05.03.1992, Российская газета, 06.05.1992.
5. Закон РФ «О частной детективной и охранной деятельности в РФ» от 11.03.1992, Российская газета, 30.04.1992.
6. Закон РФ «Об информации, информатизации и защите информации» от 20.02.1995, Российская газета, 22.02.1995.
7. Постановление Правительства РФ «О перечне сведений, которые не могут составлять коммерческую тайну» от 05.12.1991 № 35 – М.: «Юридический вестник», № 1, 1991.
8. Аппаратура охранной сигнализации. Справочник. МПО – Спецавтоматика.
9. Бизнес и безопасность. Толковый терминологический словарь. – М.: «Бек», 1995.
10. Гайкович Ю.В., Першин А.С. Безопасность электронных банковских систем. – М.: Менатеп – Информ, 1997.
11. Группа личной охраны. Методическая разработка. – М.:«Арсин Лтд.», 1996.
12. Абрамов А., Никулин О., Петрушин А. Системы управления доступом. – М.: «Оберег – РБ», 1998.
13. Бородин И. Концепция корпоративной безопасности // Материалы международной научно-практической конференции: проблемы корпоративной безопасности, Одесса: «Консалтинг», 1998. с. 5-24.
14. Кисилев О. Памятка офицеру охраны. – М.: «Ось – 89», 1994.
15. Козлов С., Иванов Е. Предпринимательство и безопасность. Т.1, Т.2. – М.: «Универсум», 1991.
16. Крысин А. Безопасность предпринимательской деятельности. – М.: Москва, «Финансы и кредит», 1996.
17. Лукашин В. Информационная безопасность. Учебно-практическое пособие. – М.: МЭСИ, 1999.
18. Организация и современные методы защиты информации / Под ред. А.Гиева и А.Шаваева – М.: «Банковский деловой центр», 1998.
19. Поздняков Е. Защита объектов. – М.: «Банковский деловой центр», 1997.
20. Шаваев А. Концептуальные основы обеспечения безопасности негосударственных объектов экономики. – М.: Академия экономической безопасности, 1994.