Концепция безопасности

1. Общие положения

Концепция безопасности коммерческого банка (кредитной организации) представляет собой научно обоснованную систему взглядов на определение основных направлений, условий и порядка практического решения задач защиты банковского дела от противоправных действий и недобросовестной конкуренции.

Под безопасностью коммерческого банка понимается состояние защищенности интересов владельцев, руководства и клиентов банка, материальных ценностей и информационных ресурсов от внутренних и внешних угроз.

Обеспечение безопасности является неотъемлемой составной частью деятельности коммерческого банка (кредитной организации). Состояние защищенности представляет собой умение и способность кредитной организации надежно противостоять любым попыткам криминальных структур или недобросовестных конкурентов нанести ущерб законным интересам банка.

Объектами безопасности являются:

- персонал (руководство, ответственные исполнители, сотрудники);
- финансовые средства, материальные ценности, новейшие технологии;
- информационные ресурсы (информация с ограниченным доступом, составляющая коммерческую тайну, иная конфиденциальная информация, предоставленная в виде документов и массивов независимо от формы и вида их представления).

Субъектами правоотношений при решении проблемы безопасности являются:

- государство (Российская Федерация) как собственник ресурсов, создаваемых, приобретаемых и накапливаемых за счет средств государственных бюджетов, а также информационных ресурсов, отнесенных к категории государственной тайны;
- Центральный банк Российской Федерации, осуществляющий денежно-кредитную политику страны;
- коммерческий банк как юридическое лицо, являющееся собственником финансовых, а также информационных ресурсов, составляющих служебную, коммерческую и банковскую тайну;
- другие юридические и физические лица, в том числе партнеры и клиенты по финансовым отношениям, задействованные в процессе функционирования коммерческого банка как внутри страны, так и во внешнефинансовых связях (органы государственной власти, исполнительные органы, организации, привлекаемые для оказания услуг в области безопасности, обслуживающий персонал, клиенты и др.);
- службы безопасности коммерческих банков и частные охранно-детективные структуры.

Концепция определяет цели и задачи системы безопасности, принципы ее организации, функционирования и правовые основы, виды угроз безопасности и

ресурсы, подлежащие защите, а также основные направления разработки системы безопасности, включая правовую, организационную и инженерно-техническую защиту.

Положения концепции могут служить методическими рекомендациями для руководителей коммерческих банков и служб безопасности при определении политики в области банковской безопасности.

2. Цели и задачи системы безопасности

Главной целью системы безопасности является обеспечение устойчивого функционирования банка и предотвращение угроз его безопасности, защита законных интересов кредитной организации от противоправных посягательств, охрана жизни и здоровья персонала, недопущения хищения финансовых и материально-технических средств, уничтожения имущества и ценностей, разглашения, утраты, утечки, искажения и уничтожения служебной информации, нарушения работы технических средств, обеспечения производственной деятельности, включая и средства информатизации.

Другими целями концепции являются:

- формирование целостного представления о системе безопасности банка и взаимоувязка различных элементов этой системы, определение путей реализации мероприятий, обеспечивающих необходимый уровень надежной защищенности объектов;
- повышение имиджа банка и роста прибыли за счет обеспечения высокого качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов.

Задачами системы безопасности являются:

- прогнозирование и своевременное выявление и устранение угроз безопасности персоналу и ресурсам банка; причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развитию;
- отнесение информации к категории ограниченного доступа (государственной, служебной, банковской и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), а других ресурсов - к различным уровням уязвимости (опасности) и подлежащих сохранению;
- создание механизма и условий оперативного реагирования на угрозы безопасности и проявление негативных тенденций в функционировании банка;
- эффективное пресечение угроз персоналу и посягательств на ресурсы на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерным действиям физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение стратегических целей банка.

3. Принципы организации и функционирования системы безопасности

Организация и функционирование системы безопасности должны соответствовать следующим принципам:

1. Комплексность:

- обеспечение безопасности персонала, материальных и финансовых ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями;
- обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и использования, во всех режимах функционирования;
- способность системы к развитию и совершенствованию в соответствии с изменениями условий функционирования банка.

Комплексность достигается:

- обеспечением соответствующего режима и охраны КБ;
- организацией специального делопроизводства с ориентацией на защиту коммерческих секретов и банковской тайны;
- мероприятиями по подбору и расстановке кадров;
- широким использованием технических средств безопасности и защиты информации;
- развернутой информационно-аналитической и детективной деятельностью.

Комплексность реализуется совокупностью правовых, организационных и инженерно-технических мероприятий.

2. Своевременность - упреждающий характер мер обеспечения безопасности.

Своевременность предполагает постановку задач по комплексной безопасности на ранних стадиях разработки системы безопасности на основе анализа и прогнозирование финансовой обстановки, угроз безопасности банка, а также разработку эффективных мер предупреждения посягательств на законные интересы.

3. Непрерывность - считается, что злоумышленники только и ищут возможность, как бы обойти защитные меры, прибегая для этого к легальным и нелегальным методам.

4. Активность. Защищать интересы банка необходимо с достаточной степенью настойчивости, широко используя маневр силами и средствами обеспечения безопасности и нестандартные меры защиты.

5. Законность. Предполагает разработку системы безопасности на основе федерального законодательства в области банковской деятельности, информатизации и защиты информации, частной охранной деятельности и других нормативных актов по безопасности, утвержденных органами государственного управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений.

6. Обоснованность. Используемые возможности и средства защиты должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и соответствовать установленным требованиям и нормам.

7. Экономическая целесообразность и сопоставимость возможного ущерба и затрат на обеспечение безопасности (критерий «эффективность - стоимость»). Во всех случаях стоимость системы безопасности должна быть меньше размера возможного ущерба от любых видов риска.

8. Специализация. Предполагается привлечение к разработке и внедрению мер и средств защиты специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Эксплуатация технических средств и реализация мер безопасности должны осуществляться профессионально подготовленными специалистами службы безопасности банка, его функциональных и обслуживающих подразделений.

9. Взаимодействие и координация. Означает осуществление мер обеспечения безопасности на основе четкой взаимосвязи соответствующих подразделений и служб, сторонних специализированных организаций в этой области, координации их усилий для достижения поставленных целей, а также сотрудничества с заинтересованными объединениями и взаимодействия с органами государственного управления и правоохранительными органами.

10. Совершенствование. Предусматривает совершенствование мер и средств защиты на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах разведки и промышленного шпионажа, нормативно-технических требований, достигнутого отечественного и зарубежного опыта.

11. Централизация управления. Предполагает самостоятельное функционирование системы безопасности по единым правовым, организационным, функциональным и методологическим принципам и централизованным управлением деятельностью системы безопасности.

4. Объекты защиты

К объектам, подлежащим защите от потенциальных угроз и противоправных посягательств, относятся:

- персонал банка (руководящие работники, производственный персонал, имеющий непосредственный доступ к финансам, валюте, ценностям, хранилищам, осведомленные в сведениях, составляющих банковскую и коммерческую тайну, работники внешнеэкономических служб и другие;
- финансовые средства, валюта, драгоценности;
- информационные ресурсы с ограниченным доступом, составляющие служебную и коммерческую тайну, а также иная конфиденциальная информация на бумажной, магнитной, оптической основе, информационные массивы и базы данных, программное обеспечение, информативные физические поля различного характера;
- средства и системы информатизации (автоматизированные системы и вычислительные сети различного уровня и назначения, линии телеграфной, телефонной, факсимильной, радио- и космической связи, технические средства передачи информации, средства размножения и отображения информации, вспомогательные технические средства и системы);
- материальные средства (здания, сооружения, хранилища, техническое оборудование, транспорт и иные средства);

- технические средства и системы охраны и защиты материальных и информационных ресурсов.

Все объекты, в отношении которых могут быть осуществлены угрозы безопасности или противоправные посягательства, имеют различную потенциальную уязвимость с точки зрения возможного материального или морального ущерба. Исходя из этого они должны быть классифицированы по уровням уязвимости (опасности), степени риска.

Наибольшую уязвимость представляют финансовые и валютные средства, особенно в процессе транспортировки, информационные ресурсы и некоторые категории персонала.

5. Основные виды угроз интересам коммерческого банка

Ухудшение состояния криминогенной обстановки в стране, усиление межрегиональных связей организованных преступных групп, рост их финансовой мощи и технической оснащенности дает основание полагать, что тенденция к осложнению оперативной обстановки вокруг коммерческих банков в ближайшее будущее сохранится. Отсюда определение и прогнозирование возможных угроз и осознание их опасности необходимы для обоснования, выбора и реализации защитных мероприятий, адекватных угрозам интересам банка.

В процессе выявления, анализа и прогнозирования потенциальных угроз интересам банка в рамках концепции учитываются объективно существующие внешние и внутренние условия, влияющие на их опасность. Таковыми являются:

- нестабильная политическая, социально-экономическая обстановка и обострение криминогенной ситуации;
- невыполнение законодательных актов, правовой нигилизм, отсутствие ряда законов по жизненно важным вопросам;
- снижение моральной, психологической и производственной ответственности граждан.

На стадии концептуальной проработки вопросов безопасности коммерческого банка представляется возможным рассмотрение общего состава потенциальных угроз. Конкретные перечни, связанные со спецификой и банка, и условий требуют определенной детализации и характерны для этапа разработки конкретного проекта системы безопасности.

В общем плане к угрозам безопасности личности относятся:

- похищения и угрозы похищения сотрудников, членов их семей и близких родственников;
- убийства, сопровождаемые насилием, издевательствами и пытками;
- психологический террор, угрозы, запугивание, шантаж, вымогательство;
- нападение с целью завладения денежными средствами, ценностями и документами.

Преступные посягательства в отношении помещений (в том числе и жилых), зданий и персонала проявляются в виде:

- взрывов;
- обстрелов из огнестрельного оружия;
- минирования, в том числе с применением дистанционного управления;
- поджогов;
- нападения, вторжения, захватов, пикетирования, блокирования;
- повреждения входных дверей, решеток, ограждений, витрин, мебели, а также транспортных средств личных и служебных;
- технологические аварии, пожары.

Цель подобных акций:

- нанесение серьезного морального и материального ущерба;
- срыв на длительное время нормального функционирования;
- вымогательство значительных сумм денег или каких-либо льгот (кредиты, отсрочка или погашение платежей и т.п.) перед лицом террористической угрозы.

Угрозы финансовым ресурсам проявляются в виде:

- невозврата кредитных ссуд;
- мошенничества со счетами и вкладами;
- подложных платежных документов и пластиковых карт;
- хищения финансовых средств из касс и инкассаторских машин.

Угрозы информационным ресурсам проявляются в виде:

- разглашения конфиденциальной информации;
- утечки конфиденциальной информации через технические средства обеспечения производственной деятельности различного характера и исполнения;
- несанкционированного доступа к охраняемым сведениям со стороны конкурентных организаций и преступных формирований.

Осуществление угроз информационным ресурсам может быть произведено:

- путем неофициального доступа и съема конфиденциальной информации;
- путем подкупа лиц, работающих в банке или структурах, непосредственно связанных с его деятельностью;
- путем перехвата информации, циркулирующей в средствах и системах связи и вычислительной техники с помощью технических средств разведки и съема информации, несанкционированного доступа к информации и преднамеренных программно-математических воздействий на нее в процессе обработки и хранения;
- путем подслушивания конфиденциальных переговоров, ведущихся в служебных помещениях, служебном и личном автотранспорте, на квартирах и дачах;
- через переговорные процессы между банком и иностранными или отечественными фирмами, используя неосторожное обращение с информацией;
- через отдельных сотрудников банка, стремящихся заполучить больший, чем их зарплата, доход или имеющих иную корыстную либо личную заинтересованность.

6. Правовые основы системы безопасности

Правовые основы безопасности коммерческого банка определяют соответствующие положения Конституции Российской Федерации, Закон «О безопасности», федеральные законы «О Центральном банке Российской Федерации», «О банках и банковской деятельности» и другие нормативные акты.

Правовая защита персонала банков, материальных и экономических интересов банков и их клиентов от преступных посягательств обеспечивается на основе норм Уголовного и Уголовно-процессуального кодексов, законов Российской Федерации о прокуратуре, о федеральной службе безопасности, о милиции, об оперативно-розыскной деятельности, о частной детективной и охранной деятельности, об оружии и др.

Защиту имущественных и иных материальных интересов и деловой репутации коммерческих банков призваны обеспечивать также гражданское, гражданско-процессуальное и арбитражное и арбитражно-процессуальное законодательство.

Правовую основу безопасности кредитных отношений банков с клиентами составляют законодательные акты, регулирующие возможность применения различных способов обеспечения исполнения обязательств. Гражданский кодекс РФ позволяет применять удержание, залог, поручительство и банковскую гарантию. Наиболее надежным способом обеспечения выполнения кредитных обязательств является залог. Правовое регулирование залоговых отношений осуществляется при помощи ряда законодательных актов и норм, их которых наиболее важными являются ГК РФ (ст. 334-358), Закон РФ «О залоге» от 29.05.92 N 2872-1, Гражданский процессуальный кодекс РФ (ст. 399-405), Временное положение о согласовании залоговых сделок (утверждено распоряжением Госкомимущества РФ от 21.04.94 N 890-р), Основные положения о залоге недвижимого имущества - ипотеке (одобрено распоряжением заместителя Председателя СМ РФ от 22.12.93 N 96-рз).

Обеспечение информационной безопасности в банковской системе регулируется законами Российской Федерации: «О банках и банковской деятельности», «О коммерческой тайне», «О персональных данных», «Об информации, информационных технологиях и о защите информации».

Важное значение в этом деле имеют указы Президента Российской Федерации «О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам» от 08.05.93 N 644, «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» от 03.04.95 N 334.

При практическом решении задач обеспечения безопасности банковской деятельности необходимо опираться также и на следующие правовые нормативные акты:

- постановление Правительства РСФСР от 05.12.91 N 35 «О перечне сведений, которые не могут составлять коммерческую тайну»;
- «Положение о сертификации средств защиты информации», утвержденное постановлением Правительства Российской Федерации от 26.06.95 N 608 «О сертификации средств защиты информации»;
- Положение о государственной системе защиты информации от ИТР и от утечки по техническим каналам, утвержденное постановлением Правительства РФ от 15.09.93 N 912-51;

- «Положение о государственном лицензировании деятельности в области защиты информации», утвержденное совместным решением Гостехкомиссии и ФАПСИ при Президенте Российской Федерации от 27.04.94 N 10.

Существующие правовые условия обеспечения банковской безопасности в основном позволяют государственным и иным правоохранительным и охранным структурам организовывать противостояние противоправным посягательствам на банковскую безопасность в различных ее аспектах.

Успешное и эффективное решение задач обеспечения безопасности конкретного банка достигается формированием системы внутренних нормативных актов, инструкций, положений, правил, регламентов и функциональных обязанностей сотрудников линейных подразделений и служб, в том числе и службы безопасности. Требования по правовому обеспечению безопасности предусматриваются во всех структурно-функциональных правовых документах, начиная с Устава коммерческого банка и кончая функциональными обязанностями каждого сотрудника. Необходимым условием обеспечения безопасности банка является совокупность правил входа (выхода) лиц в помещения банка, вноса (выноса) документов, денежных средств и материальных ценностей.

7. Техническое обеспечение безопасности банка

Техническое обеспечение безопасности должно базироваться:

- на системе стандартизации и унификации;
- на системе лицензирования деятельности;
- на системах сертификации средств защиты;
- на системе сертификации ТС и ПС объектов информатизации;
- на системе аттестации защищенных объектов информатизацией.

Основными составляющими обеспечения безопасности ресурсов КБ являются:

- система физической защиты (безопасности) материальных объектов и финансовых ресурсов;
- система безопасности информационных ресурсов.

Система физической защиты (безопасности) материальных объектов и финансовых ресурсов должна предусматривать:

- систему инженерно-технических и организационных мер охраны;
- систему регулирования доступа;
- систему мер (режима) сохранности и контроль вероятных каналов утечки информации;
- систему мер возврата материальных ценностей (или компенсации).

Система охранных мер должна предусматривать:

- многорубежность построения охраны (территории, здания, помещения) по нарастающей к наиболее ценной оберегаемой конкретности;

- комплексное применение современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;
- надежную инженерно-техническую защиту вероятных путей несанкционированного вторжения в охраняемые пределы;
- устойчивую (дублированную) систему связи и управления всех взаимодействующих в охране структур;
- высокую подготовку и готовность основных и резервных сил охраны к оперативному противодействию нарушителя;
- самоохрану персонала.

Система регулирования доступа должна предусматривать:

- объективное определение «надежности» лиц, допускаемых к банковской деятельности;
- максимальное ограничение количества лиц, допускаемых на объекты КБ;
- установление для каждого работника (или посетителя) дифференцированного по времени, месту и виду деятельности права доступа на объект;
- четкое определение порядка выдачи разрешений и оформление документов для входа (въезда) на объект;
- определение объемов контрольно-пропускных функций на каждом проходном и проездном пункте;
- оборудование контрольно-пропускных пунктов (постов) техническими средствами, обеспечивающими достоверный контроль проходящих, объективную регистрацию прохода и предотвращение несанкционированного (в том числе силового) проникновения посторонних лиц;
- высокую подготовленность и защищенность персонала (нарядов) контрольно-пропускных пунктов.

Система мер (режим) сохранности ценностей и контроля должна предусматривать:

- строго контролируемый доступ лиц в режимные зоны (зоны обращения и хранения финансов);
- максимальное ограничение посещений режимных зон лицами, не участвующими в работе;
- максимальное сокращение количества лиц, обладающих досмотровым иммунитетом;
- организацию и осуществление присутственного (явочного) и дистанционного - по техническим каналам (скрытого) контроля за соблюдением режима безопасности;
- организацию тщательного контроля любых предметов и веществ, перемещаемых за пределы режимных зон;
- обеспечение защищенного хранения документов, финансовых средств и ценных бумаг;
- соблюдение персональной и коллективной материальной и финансовой ответственности в процессе открытого обращения финансовых ресурсов и материальных ценностей;
- организацию тщательного контроля на каналах возможной утечки информации;
- оперативное выявление причин тревожных ситуаций в режимных зонах, пресечение их развития или ликвидацию во взаимодействии с силами охраны.

Система мер возврата утраченных материальных и финансовых ресурсов слагается из совместных усилий объектовых служб безопасности и государственных органов охраны правопорядка и безопасности.

На объектовую службу безопасности возлагается:

- обнаружение противоправного изъятия финансовых средств из обращения или хранения;
- оперативное информирование правоохранительных органов о событиях и критических ситуациях;
- возможность установления субъекта и время акции;
- проведение поиска возможного «схрона» утраченных средств в районе объекта.

Дальнейший поиск и возврат пропавших ресурсов организуется в установленном порядке через соответствующие органы правопорядка и безопасности.

Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, технических, программных и криптографических средств и мер по защите информации в процессе традиционного документооборота при работе исполнителей с конфиденциальными документами и сведениями, при обработке информации в автоматизированных системах различного уровня и назначения, при передаче по каналам связи, при ведении конфиденциальных переговоров.

При этом основными направлениями реализации технической политики обеспечения информационной безопасности в этих сферах деятельности являются:

- защита информационных ресурсов от хищения, утраты, уничтожения, разглашения, утечки, искажения и подделки за счет несанкционированного доступа (НСД) и специальных воздействий;
- защита информации от утечки вследствие наличия физических полей за счет акустических и побочных электромагнитных излучений и наводок (ПЭМИН) на электрические цели, трубопроводы и конструкции зданий.

В рамках указанных направлений технической политики обеспечения информационной безопасности необходима:

- реализация разрешительной системы допуска исполнителей (пользователей) к работам, документам и информации конфиденциального характера;
- ограничение доступа исполнителей и посторонних лиц в здания, помещения, где проводятся работы конфиденциального характера, в том числе на объекты информатики, на которых обрабатывается (хранится) информация конфиденциального характера;
- разграничение доступа пользователей к данным автоматизированных систем различного уровня и назначения;
- учет документов, информационных массивов, регистрация действий пользователей информационных систем, контроль за несанкционированным доступом и действиями пользователей;
- криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;
- снижение уровня и информативности ПЭМИН, создаваемых различными элементами технических средств обеспечения производственной деятельности и автоматизированных информационных систем;
- снижение уровня акустических излучений;
- электрическая развязка цепей питания, заземления и других цепей технических средств, выходящих за пределы контролируемой территории;
- активное зашумление в различных диапазонах;
- противодействие оптическим и лазерным средствам наблюдения;

проверка технических средств и объектов информатизации на предмет выявления включенных в них закладных устройств;

- предотвращение внедрения в автоматизированные информационные системы программ вирусного характера.

Защита информационных ресурсов от несанкционированного доступа должна предусматривать:

- обоснованность доступа, когда исполнитель (пользователь) должен иметь соответствующий уровень допуска для ознакомления с документацией (информацией) определенного уровня конфиденциальности и ему необходимо ознакомление с данной информацией или необходимы действия с ней для выполнения производственных функций;
- персональную ответственность, заключающуюся в том, что исполнитель (пользователь) должен нести ответственность за сохранность доверенных ему документов (носителей информации, информационных массивов), за свои действия в информационных системах;
- надежность хранения, когда документы (носители информации, информационные массивы) хранятся в условиях, исключающих несанкционированное ознакомление с ними, их уничтожение, подделку или искажение;
- разграничение информации по уровню конфиденциальности, заключающееся в предупреждении показания сведений более высокого уровня конфиденциальности в документах (носителях информации, информационных массивах) с более низким уровнем конфиденциальности, а также предупреждение передачи конфиденциальной информации по незащищенным линиям связи;
- контроль за действиями исполнителей (пользователей) с документацией и сведениями, а также в автоматизированных системах и системах связи;
- очистку (обнуление, исключение информативности) оперативной памяти, буферов при освобождении пользователем до перераспределения этих ресурсов между другими пользователями;
- целостность технической и программной среды, обрабатываемой информации и средств защиты, заключающаяся в физической сохранности средств информатизации, неизменности программной среды, определяемой предусмотренной технологией обработки информации, выполнении средствами защиты предусмотренных функций, изолированности средств защиты от пользователей.

Требование обоснованности доступа реализуется в рамках разрешительной системы допуска к работам, документам и сведениям, в которой устанавливается: кто, кому, в соответствии с какими полномочиями, какие документы и сведения (носители информации, информационные массивы) для каких действий или для какого вида доступа может предоставить и при каких условиях, и которая предполагает определение для всех пользователей автоматизированных систем информационных и программных ресурсов, доступных им для конкретных операций (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

Положение о персональной ответственности реализуется с помощью:

- росписи исполнителей в журналах, карточках учета, других разрешительных документах, а также на самих документах;

- индивидуальной идентификации пользователей и инициированных ими процессов в автоматизированных системах;
- проверки подлинности (аутентификации) исполнителей (пользователей) на основе использования паролей, ключей, магнитных карт, цифровой подписи, а также биометрических характеристик личности как при доступе в автоматизированные системы, так и в выделенные помещения (зоны).

Условие надежности хранения реализуется с помощью:

- хранилищ конфиденциальных документов, оборудованных техническими средствами охраны в соответствии с установленными требованиями, доступ в которые ограничен и осуществляется в установленном порядке;
- выделения помещений, в которых разрешается работа с конфиденциальной документацией, оборудованных сейфами и металлическими шкафами, а также ограничения доступа в эти помещения;
- использования криптографического преобразования информации в автоматизированных системах.

Правило разграничения информации по уровню конфиденциальной реализуется с помощью:

- предварительно учтенных тетрадей для ведения конфиденциальных записей или носителей информации, предназначенных для информации определенного уровня секретности.

Система контроля за действиями исполнителей реализуется с помощью:

- организационных мер контроля при работе исполнителей с конфиденциальными документами и сведениями;
- регистрации (протоколирования) действий пользователей с информационными и программными ресурсами автоматизированных систем с указанием даты и времени, идентификаторов запрашивающего и запрашиваемых ресурсов, вида взаимодействия и его результата, включая запрещенные попытки доступа;
- сигнализации о несанкционированных действиях пользователей.

Очистка памяти осуществляется организационными и программными мерами, а целостность автоматизированных систем обеспечивается комплексом программно-технических средств и организационных мероприятий.

7.1. Защита информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН)

Основным направлением защиты информации от утечки за счет ПЭМИН является уменьшение отношения информативного сигнала к помехе до предела, определяемого «Нормами эффективности защиты АСУ и ЭВМ от утечки информации за счет ПЭМИН», при котором восстановление сообщений становится принципиально невозможным. Решение этой задачи достигается как снижением уровня излучений информационных сигналов, так и увеличением уровня помех в соответствующих частотных диапазонах.

Первый способ реализуется выбором системно-технических и конструкторских решений при создании технических средств ЭВТ в «защищенном исполнении», а также рациональным выбором места размещения технических средств относительно направлений возможного перехвата информативного сигнала.

Второй способ реализуется в основном за счет применения активных средств защиты в виде «генераторов шума» и специальной системы антенн.

7.2. Защита информации в линиях связи

К основным видам линий связи, используемых для передачи информации, можно отнести проводные (телефонные, телеграфные), радио и радиорелейные, тропосферные и космические линии связи.

При необходимости передачи по ним конфиденциальной информации основным направлением защиты информации, передаваемой по всем видам линий связи, от перехвата, искажения и навязывания ложной информации является использование крипто-логического преобразования информации, а на небольших расстояниях, кроме того, использование защищенных волоконно-оптических линий связи.

Для защиты информации должны использоваться средства криптографической защиты данных гарантированной стойкости для определенного уровня конфиденциальности передаваемой информации и соответствующая ключевая система, обеспечивающая надежный обмен информацией и аутентификацию (подтверждение подлинности) сообщений.

7.3. Безопасное использование технических средств информатизации

Одним из методов технической разведки и промышленного шпионажа является внедрение в конструкцию технических средств информатизации закладных устройств перехвата, трансляции информации или вывода технических средств из строя.

В целях противодействия такому методу воздействия на объекты информатики, для технических средств информатизации, предназначенных для обработки конфиденциальной информации, в обязательном порядке проводится проверка этих средств, осуществляемая специализированными организациями с помощью специальных установок и оборудования, как правило, в стационарных условиях в соответствии с установленными требованиями.

7.4. Защита речевой информации при проведении конфиденциальных переговоров

Исходя из возможности перехвата речевой информации при проведении разговоров конфиденциального характера с помощью внедрения закладных устройств, акустических, виброакустических и лазерных технических средств разведки, противодействие этим угрозам должно осуществляться всеми доступными средствами и методами.

В связи с интенсивным внедрением в деятельность КБ автоматизированных систем организационно-финансового управления, технического и другого назначения, используемых для обработки конфиденциальной информации, для учета финансовых средств, локальных, региональных и глобальных вычислительных сетей и интеграции в них значительных по объему и важных по содержанию информационных ресурсов, проблеме безопасности информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи, следует уделить особое внимание.

7.5. Обеспечение качества в системе безопасности

Необходимой составляющей системы безопасности должно быть обеспечение качества работ и используемых средств и мер защиты, нормативной базой которого является система стандартов и других руководящих нормативно- технических и методических документов по безопасности, утвержденных федеральными органами государственного управления в соответствии с их компетенцией и определяющие нормы защищенности информации и требования в различных направлениях защиты информации.

В соответствии с требованиями этой НТД должны проводиться предпроектное обследование и проектирование информационных систем, заказ средств защиты информации и контроля, предполагаемых к использованию в этих системах, аттестация объектов информатики, а также контроль защищенности информационных ресурсов.

К основным стандартам и нормативно-техническим документам в области защиты информации от несанкционированного доступа (НСД) относятся:

- комплект руководящих документов Гостехкомиссии России (1992 г.), в том числе «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации», «Положение по организации разработки, изготовления и эксплуатации программы и технических средств защиты информации от НСД в АС и СВТ».

В совокупности с системой стандартизации единую систему обеспечения качества продукции и услуг по требованиям безопасности информации составляют:

- сертификация средств и систем вычислительной техники и связи по требованиям безопасности информации;
- лицензирование деятельности по оказанию услуг в области защиты информации;
- аттестация объектов информатики по требованиям безопасности информации.

В соответствии с требованиями этих систем право оказывать услуги сторонним организациям в области защиты информации предоставлено только организациям, имеющим на этот вид деятельности разрешение (лицензию). Средства и системы вычислительной техники и связи, предназначенные для обработки (передачи) секретной информации, средства защиты и контроля эффективности защиты такой информации подлежат обязательной сертификации по требованиям безопасности информации, а объекты информатики, предназначенные для обработки секретной и иной конфиденциальной информации, являющейся собственностью государства, а также для ведения секретных переговоров подлежат обязательной аттестации по требованиям безопасности информации.

При разработке системы комплексной защиты информации объекта автоматизации необходимо максимально использовать имеющиеся сертифицированные по требованиям безопасности информации средства вычислительной техники и связи, средства защиты и контроля защищенности, разрабатывая или заказывая оригинальные технические или программные средства защиты только в случаях, когда имеющимися средствами нельзя достигнуть необходимых результатов. Исходя из этого при разработке автоматизированных систем различного уровня и назначения серьезное внимание следует уделить выбору технических средств и общесистемного матобеспечения. Этими же обстоятельствами следует руководствоваться при выборе стратегии развития систем информатизации.

8. Управление системой безопасности КБ

Действующие в настоящее время и разрабатываемые законодательные и иные нормативные акты предусматривают право КБ на выработку собственной концепции системы безопасности и создания соответствующей службы как системы исполнительных органов, реализующей эту концепцию.

Исходя из представленных в концепции задач, принципов организации и функционирования системы безопасности, основных угроз безопасности КБ, целесообразно выделить следующие основные направления деятельности КБ по обеспечению его безопасности:

- информационно-аналитических исследований и прогнозных оценок безопасности, в том числе экономической;
- безопасности персонала;
- сохранности и физической защиты финансовых средств и объектов;
- безопасности информационных ресурсов.

Основными задачами направления информационно-аналитических исследований и прогнозных оценок безопасности являются:

- добывание и анализ информации о мировом и национальном рынках и прогнозирование их развития;
- организация работ по выявлению конфиденциальной информации, обоснованию уровня ее конфиденциальности и документальному оформлению в виде перечней сведений, подлежащих защите;
- сбор экономической и научно-технической информации для обеспечения эффективности деловых сношений с зарубежными и отечественными партнерами, выявление в их числе несостоятельных, ненадежных предпринимателей, а также лиц, связанных с криминальными структурами;
- учет официальных претензий правоохранительных и контролирующих органов к возможным партнерам на финансовом рынке, фирмам, банкам и т.п.;
- изучение, анализ и оценка криминальной обстановки, в том числе состояния экономической преступности в денежно-кредитной сфере по стране и в регионе;
- выявление и прогнозирование уязвимых мест в денежно-кредитной деятельности, реальных и потенциальных угроз безопасности КБ, разработка и осуществление комплекса оперативных и долговременных мер по их предупреждению и нейтрализации;
- анализ и прогнозирование негативных тенденций социально-экономического развития КБ с точки зрения влияния на ее безопасность;
- информационное обеспечение руководства КБ в области безопасности;
- координация деятельности подразделений службы безопасности и обеспечения взаимодействия со всеми структурными подразделениями КБ в решении проблемы безопасности.

Главной заботой о безопасности персонала является охрана личности от любых противоправных посягательств на его жизнь, материальные ценности и личную информацию.

Основными задачами направления сохранности и физической защиты продукции и объектов являются:

- установление режима охраны производственных объектов и объектов жизнедеятельности;
- осуществление допускного и пропускного режимов;
- обеспечение защищенного хранения ценностей и документов (носителей информации), оснащение современными инженерно-техническими средствами охраны;
- организация физической защиты продукции в процессе ее внутриобъектовой транспортировки;
- осуществление контроля за сохранностью продукции на всех стадиях технологического процесса;
- организация личной безопасности определенной категории руководящего состава и ведущих специалистов из так называемой группы повышенного риска;
- обеспечение взаимодействия всех структур, участвующих в обеспечении физической защиты.

Основными задачами направления безопасности информационных ресурсов являются:

- организация и осуществление разрешительной системы допуска исполнителей к работе с документами и сведениями ограниченного доступа;
- организация хранения и обращения с конфиденциальными документами (носителями информации);
- осуществление закрытой переписки и шифрованной связи;
- организация и координация работ по защите информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи;
- обеспечение безопасности в процессе проведения конфиденциальных совещаний, переговоров;
- осуществление контроля за сохранностью конфиденциальных документов (носителей информации), за обеспечением защиты информации, обрабатываемой и передаваемой средствами и системами вычислительной техники и связи.

Основными задачами в работе с персоналом банка являются:

- Набор персонала: создание резерва потенциальных кандидатов по всем должностям. Набор персонала, как правило, проводится из внутренних (перемещение и продвижение по службе своих сотрудников) и внешних (найм по объявлениям и по личным рекомендациям) источников. Основным требованием при этом должны стать объективная оценка не только поступающего на работу сотрудника, но и предлагаемой ему работы.
- Отбор кандидатов. К основным группам качеств для сравнения кандидатов относятся: профессиональные, образовательные, организационные и личные. Основным требованием при отборе является тщательное изучение деловых, моральных и этических данных каждого кандидата путем глубокого изучения трудового прошлого кандидата. В процессе анализа сведений о кандидате следует пользоваться услугами органов внутренних дел, оказываемых ими в соответствии с приказом МВД РФ за № 319 от 1994 г. В соответствии с этим приказом органы внутренних дел должны оказывать платные услуги о наличии (отсутствии) судимости кандидата и сведения о лицах, находящихся в розыске.
- Заключение контракта и получение у сотрудника добровольного согласия на соблюдение требований, регламентирующих режим безопасности и сохранения коммерческой и банковской тайн.

- Обучение кандидатов перед допуском к работе предусматривает введение в должность, обучение установленным правилом выполнения порученного дела, обеспечения безопасности и защиты информации.
- Текущий контроль (мониторинг) за деятельностью сотрудника по повышению его бдительности в отношении угроз безопасности банка.
- Своевременное выявление и устранение конфликтных ситуаций в работе с персоналом.

Учитывая территориальную разбросанность и различный характер деятельности структурных подразделений КБ, необходимость наличия в значительной их части подразделений службы безопасности, а также наличие республиканских нормативных актов, определяющих порядок обеспечения охраны объектов, продукции и транспортировки продукции, представляется невозможным в настоящее время организовать единую службу безопасности КБ с централизованным административным подчинением.

В этих условиях целесообразно создать территориальную распределенную службу безопасности с централизованным организационно-методическим управлением и координацией деятельности по единым принципам и правилам.

Служба безопасности должна подчиняться непосредственно руководителю коммерческого банка. Целесообразно, если позволяют возможности, чтобы начальник службы безопасности состоял в ранге заместителя руководителя КБ, который административно управлял бы службой информационно-аналитических исследований и прогнозных оценок безопасности и оперативно-методически руководил подразделениями служб сохранности и физической защиты ценностей и объектов и безопасности информационных ресурсов, создаваемых для выполнения конкретных задач в соответствии с настоящей концепцией в структурных подразделениях КБ и координировал бы их деятельность.

Вопросы технической безопасности по направлениям деятельности службы безопасности должны решаться совместно с руководством и подразделениями, отвечающими за соответствующее направление научно-технического развития.

При разработке и реализации системы безопасности и организации ее службы безопасности определенная часть сотрудников службы безопасности может быть привлечена для выполнения конкретных работ (консультаций) на договорной основе (по контракту) из числа соответствующего профиля высококвалифицированных специалистов.

9. Предложения по программе создания системы безопасности

В целом создание и обеспечение функционирования системы комплексной безопасности с учетом положений настоящей концепции должны быть разработаны следующие документы:

- Устав (положение) службы безопасности.
- Перечень сведений, составляющих коммерческую тайну.
- Организационно-распорядительные документы, регламентирующие порядок и правила:
    - обеспечения сохранности коммерческой тайны;

    - режима и охраны объектов защиты, включая требования по пропускному и внутриобъектовому режиму;
    - по учету и контролю финансов, обеспечения их сохранности в процессе операций, хранения и транспортировки;
    - обеспечения защиты информации, обрабатываемой и передаваемой в автоматизированных системах и средствах связи.

Для осуществления технической политики в области обеспечения физической и информационной защиты необходимо разработать и реализовать комплекс мероприятий:

- по оснащению важнейших объектов и помещений средствами и системами физической защиты и контроля;
- по обеспечению технической, программной и криптографической защиты информации в системах информатизации и связи;
- по обеспечению защиты речевой информации в помещениях, выделенных для ведения конфиденциальных переговоров.

Программа создания системы безопасности должна предусматривать приоритеты реализации наиболее важных и актуальных направлений обеспечения безопасности, с учетом выделяемых финансовых ресурсов, а также предусматривать привлечение к ее выполнению специализированных организаций, имеющих практический опыт работы по рассматриваемой проблеме и лицензии на соответствующий вид деятельности.

В целях обеспечения нормальной работы службы безопасности в повседневных условиях рекомендуется разработка «Оперативного плана службы безопасности по обеспечению защиты банка». Данным планом предусматриваются конкретные и четкие действия сотрудников банка и службы безопасности при возникновении критических ситуаций типа:

- нападение грабителей;
- исчезновение наличных денежных средств;
- нападение на сотрудника банка;
- пожар, взрыв и другое повреждение здания или имущества как в дневное, так и в ночное время.

Предусматриваются действия как в момент наступления ситуации, в ходе ее развития и по завершению. Главная цель - предупредить наступление, уменьшить ущерб, сохранить следы (улики) для последующей работы по ликвидации ущерба.

10. Принципы и направления взаимодействия между коммерческим банком и правоохранительными органами в области безопасности

Какой бы совершенной ни была самоорганизация безопасности коммерческого банка, она не обеспечит предотвращение преступных посягательств без взаимодействия

кредитного учреждения с соответствующими правоохранительными органами и прежде всего милицией.

Организационно-правовой основой такого взаимодействия являются:

- конституционные принципы равенства защиты всех форм собственности;
- законы Российской Федерации о милиции, об оперативно-розыскной деятельности, о прокуратуре и другие нормативно-правовые акты;
- Соглашение между Министерством внутренних дел Российской Федерации и Ассоциацией российских банков о взаимодействии в области обеспечения банковской безопасности.

Целями сотрудничества являются: предупреждение и раскрытие преступных посягательств на персонал коммерческих банков, денежные средства и ценности.

Приоритетными направлениями взаимодействия банка и территориального органа внутренних дел должны быть:

- Обмен информацией:
  - о фактах (способах) совершения хищений денежных средств в коммерческих банках с использованием подложных банковских документов, кредитных карточек, подделки иных документов;
  - о физических лицах, работающих в коммерческих банках, вкладчиках и других клиентах, подозреваемых в совершении правонарушений;
  - о юридических лицах, являющихся клиентами банка, совершающих банковские операции, имеющие подозрительный характер, в целом о банковских операциях, вызывающих обоснованные сомнения в целесообразности их проведения.
- Разработка совместных мер:
  - противодействия предполагаемым (реальным) фактам общеуголовных проявлений в банковской системе, угрозам убийства, либо нанесения тяжких телесных повреждений, уничтожения имущества коммерческих банков, их руководителей, сотрудников и членов их семей;
  - по технической укрепленности и оборудованию средствами сигнализации объектов банка;
  - по созданию так называемой «горячей линии» между банковским и территориальным органом внутренних дел (милицией);
  - участия в формировании централизованного, регионального банка данных о предприятиях различных форм собственности, недобросовестных участниках кредитно-денежных отношений;
- Работа по подбору, расстановке и профессиональная подготовка кадров служб банковской безопасности:
  - осуществление совместной проверки кандидатур на работу в службу банковской безопасности с использованием информационных возможностей органов внутренних дел, сведений о судимости и т.д.;
  - проведение совместной разработки и введение правил об ответственности персонала коммерческих банков за противоправное использование, либо разглашение коммерческой (банковской) тайны с учетом диспозиции ст. 183 УК РФ «Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну»;
  - использование помощи милиции в обучении и повышении квалификации кадров службы безопасности банка.