



ГАЗПРОМБАНК

АКЦИОНЕРНЫЙ БАНК ГАЗОВОЙ ПРОМЫШЛЕННОСТИ «ГАЗПРОМБАНК»
(Закрытое акционерное общество)

УТВЕРЖДЕНА

**Решением Правления
АБ «Газпромбанк» (ЗАО)**

**« 27 » июня 2007 г.
(протокол № 27)**

**ПОЛИТИКА
в области обеспечения безопасности
АБ «Газпромбанк» (ЗАО)**

**МОСКВА
2007**

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ	3
2. СПИСОК ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ.....	3
3. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ БЕЗОПАСНОСТИ.....	4
4. ПРИНЦИПЫ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ.....	4
5. КЛАССИФИКАЦИЯ РИСКОВ (УГРОЗ)	6
6. КЛАССИФИКАЦИЯ ОБЪЕКТОВ ЗАЩИТЫ	6
7. УЧАСТНИКИ (СУБЪЕКТЫ) СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ	7
8. МЕРОПРИЯТИЯ, ИСПОЛЬЗУЕМЫЕ ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ	7
9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	10

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика в области обеспечения безопасности АБ «Газпромбанк» (ЗАО) (далее – Политика) определяет цели и задачи системы безопасности, принципы ее организации и функционирования, виды угроз и объекты защиты, а также мероприятия, используемые при обеспечении безопасности.

1.2. Политика разработана в соответствии с документами АБ «Газпромбанк» (ЗАО), определяющими стратегические задачи и направления деятельности, действующим законодательством, нормативными актами Правительства Российской Федерации, Банка России и других государственных органов.

1.3. Основными направлениями системы безопасности являются безопасность бизнес-процессов, информационно-аналитическая работа, защита информации, техническая безопасность, физическая безопасность, противопожарная безопасность.

1.4. Приведенные в Политике мероприятия не исключают использования альтернативных вариантов по мере развития технологии обеспечения безопасности. Разработка технических деталей, в том числе регламентов взаимодействия подразделений, порядка распределения и делегирования полномочий в процессе обеспечения безопасности, относится к конкретным нормативным и методическим материалам.

1.5. Вопросы обеспечения информационной безопасности, отнесения информации к категории ограниченного доступа, а также организации и ведения конфиденциального делопроизводства описываются отдельными внутренними нормативными актами АБ «Газпромбанк» (ЗАО).

2. СПИСОК ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

2.1. **Банк** – АБ «Газпромбанк» (ЗАО).

2.2. **Безопасность** — отсутствие недопустимого риска.

2.3. **Бизнес-процесс** — последовательность технологически связанных операций по предоставлению банковских продуктов и/или осуществлению конкретного вида обеспечивающей деятельности Банка.

2.4. **Контрагент** – сторона (потенциальная сторона) по сделке и/или договору с Банком.

2.5. **Объект противоправного посягательства** — конкретный материальный или нематериальный ресурс или бизнес-процесс (направление деятельности), на который направлено (или может быть направлено) противоправное посягательство.

2.6. **Опасность (угроза) (в целях данного документа)** — источник потенциального ущерба объекту противоправного посягательства, причинение которого может воспрепятствовать достижению Банком уставных целей.

2.7. **Подразделения безопасности Банка** – Служба (департамент) безопасности Банка, а также отделы и управления, входящие в ее состав, или служба (отдел) безопасности филиала Банка.

2.8. **Система обеспечения безопасности банковской деятельности (система безопасности)** — совокупность взаимосвязанных мер, при реализации которых потенциально опасные для Банка обстоятельства предупреждены, а действия пресечены либо сведены к такому уровню, при котором не способны нанести ущерб

установленному порядку банковской деятельности (функционированию Банка, сохранению и воспроизводству имущества и инфраструктуры Банка) и воспрепятствовать достижению Банком уставных целей.

2.9. **Субъект противоправного посягательства** — лицо, причастное к реализации угроз.

2.10. **Требования безопасности Банка** — система условий, запретов, ограничений и других обязательных требований, содержащихся в федеральных законах и иных нормативных правовых актах, а также в нормативных внутренних документах Банка, соблюдение которых призвано обеспечить безопасность деятельности Банка.

2.11. **Участники (субъекты) системы обеспечения безопасности** — все подразделения и сотрудники Банка, участвующие в организационных и технологических мероприятиях, направленных на своевременное выявление, оценку, мониторинг угроз (и их последствий) и связанных с управлением рисками в деятельности Банка.

2.12. **Эффективность системы безопасности Банка** — критерий выполнения системой своей основной целевой функции по обеспечению защиты объекта от угроз, отнесенный к затратам на создание, функционирование и поддержку системы.

3. ЦЕЛИ И ЗАДАЧИ СИСТЕМЫ БЕЗОПАСНОСТИ

3.1. Главными целями системы безопасности являются обеспечение устойчивого функционирования Банка и предотвращение угроз его безопасности, защита законных интересов Банка от противоправных посягательств, охрана жизни и здоровья сотрудников и посетителей Банка.

3.2. Задачами системы безопасности являются:

- анализ и прогнозирование вероятных угроз;
- предупреждение угроз (меры организационного, охранного, инженерно-технического и аналитического характера);
- выявление готовящихся и совершенных противоправных посягательств на интересы Банка;
- пресечение угроз, возмещение причиненного ущерба;
- взаимодействие с правоохранительными органами в сфере обеспечения безопасности;
- разработка и контроль соблюдения установленных требований безопасности;
- обеспечение непрерывности бизнеса во внештатных и кризисных ситуациях.

4. ПРИНЦИПЫ ОРГАНИЗАЦИИ И ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ

Организация и функционирование системы безопасности проводятся в соответствии со следующими принципами:

4.1. **Комплексность и полнота защиты.** Приоритетной задачей каждого сотрудника Банка является безопасность проведения любой операции в интересах и в рамках банковской деятельности. Защита Банка и каждого из элементов его структуры осуществляется с использованием всего арсенала законодательно определенных средств и методов, находящихся в распоряжении Банка.

4.2. **Системность.** Безопасность Банка обеспечивается взаимосвязанным и взаимодополняющим функционированием комплекса регулирующих и надзорных мер со стороны государства, системы аналитических, организационных, распорядительных решений и практических мер со стороны Банка. Реализация мер защиты в рамках Банка осуществляется с учетом того, что применение всех средств (мероприятий) обеспечения безопасности осуществляется в режиме системного согласования мероприятий, и каждое из них должно рассматриваться как часть единой системы обеспечения банковской безопасности.

4.3. **Взаимодействие.** В обеспечении системы безопасности в пределах своей компетенции участвуют все подразделения Банка, которые действуют во взаимосвязи друг с другом и с подразделениями безопасности Банка.

Организация взаимодействия с частными детективными и охранными структурами, с подразделениями безопасности других хозяйствующих субъектов, а также с государственными органами, выполняющими правоохранительные функции, осуществляется подразделениями безопасности Банка.

4.4. **Экономическая целесообразность.** Затраты на обеспечение безопасности Банка должны оцениваться с точки зрения их сопоставимости с вероятностью реализации потенциальных угроз и тяжестью возможных последствий (технологические сбои, утрата репутации, материальный ущерб).

4.5. **Приоритет мер предупредительного характера.** Интересы обеспечения безопасности Банка связаны преимущественно с применением таких средств и методов, которые позволяют воспрепятствовать преступным намерениям субъектов посягательства, предупредить совершение преступления. Меры предупреждения посягательств на интересы Банка являются предпочтительными и должны реализовываться преимущественно перед другими. С целью минимизации потерь Банка от реализации угроз техногенного или природного характера разрабатываются планы работ при возникновении чрезвычайных, нештатных и аварийных ситуаций, испытание и актуализация которых проводятся на плановой основе.

4.6. **Законность.** Система безопасности Банка создается и функционирует в строгом соответствии с Конституцией Российской Федерации, федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, нормативными правовыми актами субъектов Российской Федерации, а также нормативными актами министерств и ведомств и внутренними нормативными актами Банка.

4.7. **Соблюдение рекомендаций Банка России.** Банк рассматривает в качестве обязательных рекомендации Центрального банка Российской Федерации по обеспечению безопасности, в том числе по реализации принципов «знай своего клиента» и «знай своего служащего», а также стандартов информационной безопасности.

4.8. **Сочетание гласности и конфиденциальности.** Деятельность системы безопасности осуществляется гласно, однако, в необходимых случаях в интересах защиты имущества, информации и других объектов гражданских прав Банка применяются методы и средства конфиденциального характера, использование которых не нарушает конституционных прав граждан.

4.9. **Подконтрольность и подотчетность Председателю Правления Банка.** Полученные подразделением безопасности материалы о фактах посягательства на интересы Банка используются по усмотрению Председателя Правления Банка (за исключением случаев обязательного информирования правоохранительных органов, предусмотренных законодательством), а также с учётом требований Порядка сбора и

Газпромбанк

Служба (департамент) безопасности

Политика в области обеспечения безопасности АБ «Газпромбанк» (ЗАО)

регистрации данных о рискованных событиях операционного риска в АБ «Газпромбанк» (ЗАО), утвержденным Председателем Правления Банка 20.11.2006 г. № 79.

4.10. **Развитие и совершенствование.** Система безопасности Банка создается, развивается и совершенствуется на основе использования средств и методов, разработанных современной наукой, рекомендаций по их наиболее эффективному применению, с учетом опыта борьбы с преступностью в банковской сфере отечественных и зарубежных правоохранительных структур, а также обобщения и анализа собственного опыта.

5. КЛАССИФИКАЦИЯ РИСКОВ (УГРОЗ)

5.1. Классификация рисков (угроз) проводится с целью оптимизации путей управления различными типами рисков (в т.ч. выработка принципов управления каждым типом риска) с учетом их специфики.

5.2. Классификация рисков по сочетанию факторов возникновения, по направлениям деятельности Банка, по типам последствий рискованного события проводится в соответствии с Политикой по управлению операционным риском в АБ «Газпромбанк» (ЗАО), утвержденной Решением Правления АБ «Газпромбанк» (ЗАО) от 16 июня 2006 г. (протокол № 25).

6. КЛАССИФИКАЦИЯ ОБЪЕКТОВ ЗАЩИТЫ

Основными объектами преступных посягательств на безопасность Банка являются:

6.1. **Бизнес-процессы.**

6.2. **Репутация Банка** - информация, характеризующая Банк как делового партнера, и деловые связи (деловые отношения с действующими либо потенциальными партнерами).

6.3. **Контрагенты Банка и их представители, находящиеся на территории Банка, а также сотрудники Банка.**

6.4. **Имущество Банка:**

- наличные деньги, ценные бумаги, в том числе депозитные сертификаты, а также безналичные деньги и валютные ценности;

- имущественные права на предметы залога и иные имущественные права, принадлежащие Банку;

- здания, оборудование и инвентарь, мебель, автомобили и т.п.

6.5. **Результаты интеллектуальной деятельности**, в том числе исключительные права на них (интеллектуальная собственность).

6.6. **Платежные средства, не являющиеся ценными бумагами**, но служащие средством получения наличных денег, — кредитные либо расчетные пластиковые карты, платежные документы (в том числе платежные поручения) и т.д.;

6.7. **Информация, составляющая коммерческую, банковскую или служебную тайну**, а также сведения ограниченного распространения.

7. УЧАСТНИКИ (СУБЪЕКТЫ) СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

7.1. Система обеспечения безопасности носит комплексный характер, охватывает все подразделения Банка и включает организационные и технологические мероприятия, направленные на своевременное выявление, оценку, мониторинг и максимальное снижение всех видов рисков.

7.2. Требования по обеспечению безопасности должны неукоснительно соблюдаться всеми работниками Банка в процессе исполнения своих должностных обязанностей.

7.3. Мониторинг качества мер по обеспечению безопасности Банка проводится в рамках риск-аудита операционных рисков. Подразделения, участвующие в процессе проведения риск-аудита, и их функции определяются в соответствии с внутренними нормативными документами Банка, регламентирующими порядок проведения риск-аудита операционных рисков.

7.4. Дочерние и зависимые общества Банка в качестве самостоятельных юридических лиц несут ответственность за организацию и эффективное функционирование собственной системы безопасности.

7.5. Мониторинг состояния обеспечения безопасности в дочерних и зависимых обществах проводится в рамках проведения риск-аудита дочерних и зависимых обществ с соблюдением требований действующего законодательства и с учетом специфики организации документооборота между Банком и сторонней организацией.

8. МЕРОПРИЯТИЯ, ИСПОЛЬЗУЕМЫЕ ПРИ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ

8.1. Мероприятия, используемые в целях обеспечения эффективного функционирования системы безопасности, подразделяются на **превентивные** (используемые в целях предупреждения противоправных посягательств на интересы Банка), **сопровождающие** (используемые с целью своевременного выявления настораживающих признаков) и **локализующие** (призванные уменьшить нанесенный Банку ущерб в результате реализовавшегося рискового события).

Превентивные мероприятия:

8.2. В целях предупреждения противоправных посягательств на интересы Банка участники системы обеспечения безопасности в пределах своей компетенции проводят следующие мероприятия:

8.2.1. Получение, накопление и анализ информации о причинах и условиях, способствующих совершению противоправных посягательств в банковской сфере (на основе изучения опыта деятельности правоохранительных органов, частных служб безопасности, собственного опыта Банка), и подготовка предложений по их устранению.

8.2.2. Накопление информации о фактах противоправных посягательств на интересы Банка.

8.2.3. Выявление и анализ недостатков в организационной, технической и технологической защите направлений деятельности Банка либо отдельных операций, облегчающих реализацию преступного замысла (оценка уязвимости Банка от угроз), в

том числе проведение санкционированных специальных экспериментов по проверке надежности и эффективности мер защиты Банка. Разработка рекомендаций по устранению недостатков.

8.2.4. Разработка средств и методов повышения надежности защиты конкретных участков деятельности Банка:

- подготовка методических рекомендаций по выявлению признаков противоправных посягательств на интересы Банка;
- обучение персонала выявлению признаков противоправных посягательств на интересы Банка и действиям по их предупреждению и пресечению;
- участие в совершенствовании мер технической защиты зданий и помещений Банка, его информационной инфраструктуры;
- участие в разработке технологии бизнес-процессов, не позволяющих преступникам использовать выявленные ранее способы совершения преступлений;
- участие в подборе персонала Банка, организации допуска сотрудников к работе с наличными деньгами, ценными бумагами, в том числе депозитными сертификатами, а также платежными средствами, не являющимися ценными бумагами, но служащими средством получения наличных денег, - кредитными либо расчетными пластиковыми картами, платежными документами (платежными поручениями) и т.д., безналичными деньгами, валютными ценностями и охраняемой информацией;
- принятие мер, направленных на недопущение занятия должностей в филиалах Банка и их внутренних структурных подразделениях лицами, находящимися в близком родстве или свойстве (родители, супруги, братья, сестры, сыновья, дочери, а также братья, сестры, родители и дети супругов), если их работа связана с непосредственной подчиненностью или подконтрольностью одного из них другому.

8.2.5. Выявление в действиях потенциальных контрагентов признаков возможных преступных посягательств и подготовка экспертных заключений для уполномоченных коллегиальных органов о рисках Банка для целей выработки обоснованных решений по методу управления риском.

8.2.6. Участие в разработке и осуществлении мероприятий правового, организационного и поискового характера в целях ограждения кадрового состава Банка от проникновения лиц с противоправными устремлениями на стадии отбора кандидатов на работу.

Сопровождающие мероприятия:

8.3. В целях своевременного выявления признаков противоправных посягательств на интересы Банка и обеспечения состояния защищенности, участники системы обеспечения безопасности в пределах своей компетенции проводят следующие мероприятия:

8.3.1. Осуществление комплекса мероприятий по защите информации и информационных технологий Банка (в т.ч. интернет-технологий) в соответствии с требованиями действующего законодательства и внутренних нормативных документов Банка.

8.3.2. Информирование руководства и заинтересованных подразделений Банка относительно выявленных негативных факторов и событий в деятельности контрагента.

8.3.3. Осуществление комплекса мероприятий по защите от злоупотребления полномочиями и коммерческого подкупа путем осуществления следующих действий:

- проверка соблюдения уполномоченными лицами Банка установленных процедур проведения банковских операций и полномочий по принятию решений (по составу и объему операций) с целью выявления факта умышленных действий, причинивших ущерб интересам Банка;

- установление факта проведения сделок и операций, наносящих Банку ущерб;

- осуществление контроля над областями потенциального конфликта интересов в соответствии с внутренними нормативными документами Банка;

- установления факта вовлечения Банка в коммерческие взаимоотношения с лицами, получающими доходы преступным путем или осуществляющими легализацию таких доходов.

8.3.4. Организация и осуществление мер по защите помещений, выделенных для хранения и обработки конфиденциальных материалов.

8.3.5. Организация технической защиты путем:

- защиты помещений, предназначенных для ведения конфиденциальных переговоров;

- защиты средств и систем информатизации (средства вычислительной техники, автоматизированные системы различного уровня и назначения на базе средств вычислительной техники, средств и систем связи и передачи данных, технических средств приема, передачи и обработки информации, средств изготовления, тиражирования документов, программных средств (операционных систем, систем управления базами данных, другого общесистемного и прикладного программного обеспечения);

- защиты технических средств и систем, не обрабатывающих непосредственно конфиденциальную информацию, но размещенных в помещениях, где обрабатывается (циркулирует) конфиденциальная информация (с целью предупредить незаконное получение конфиденциальной информации путем перехвата);

- периодической проверки технических средств и служебных помещений на предмет наличия возможно внедренных электронных устройств перехвата информации («закладок»).

8.3.6. Организация охраны и физической защиты путем:

- охраны имущества Банка, персонала и посетителей Банка от противоправных посягательств;

- организации пропускного режима в помещения Банка с целью недопущения несанкционированного доступа в них;

- постоянного контроля состояния и эффективности защиты помещений и имущества Банка.

8.3.7. Выявление фактов распространения заведомо ложных сведений, наносящих вред репутации Банка. Своевременное реагирование на негативные публикации в средствах массовой информации.

Локализующие мероприятия:

8.4. В целях уменьшения нанесенного Банку ущерба в результате реализовавшегося рискованного события участники системы обеспечения безопасности в пределах своей компетенции проводят следующие мероприятия:

8.4.1. Проведение внутренних расследований по фактам нарушения требований безопасности, выработка предложений по совершенствованию системы безопасности. Участие в проведении служебных расследований для установления вины нарушителя, выявления причин и условий, способствовавших совершению проступка; анализ дисциплинарных проступков и правонарушений, совершенных работниками Банка и разработка мер их предупреждения.

8.4.2. Документирование фактических данных, имеющих отношение к событию, с целью использования в случае необходимости в качестве оснований при назначении дисциплинарного взыскания, либо доказательств на следствии и в суде (в соответствии с Порядком сбора и регистрации данных о рискованных событиях операционного риска в АБ «Газпромбанк» (ЗАО) (№79 от 20.11.2006).

8.4.3. Принятие неотложных мер по защите жизни и здоровья сотрудников и посетителей Банка, а также материальных ценностей от противоправных посягательств, информирование о выявленных фактах правоохранительных органов и взаимодействие с ними.

8.4.4. На стадии прекращения трудовых отношений с работниками, причинившими ущерб интересам Банка, — выявление и фиксация фактов, служащих основанием для расторжения договора.

8.4.5. В рамках работы с проблемными активами - урегулирование задолженности путем взаимодействия с правоохранительными и судебными органами (в т.ч. службой судебных приставов), оказание содействия в получении информации в порядке, предусмотренном действующим законодательством и внутренними нормативными актами Банка.

9. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

9.1. Ответственность за соблюдение Политики возлагается на каждого сотрудника, вовлеченного в процесс обеспечения безопасности, в части вопросов, относящихся к его компетенции.

9.2. Политика утверждается Правлением Банка.

9.3. Все изменения в Политику вносятся на основании решения Правления Банка.