



*Национальный Корпоративный Банк*

*Лицензия № 3422*

**УТВЕРЖДЕНА**  
**решением Совета Директоров**  
**АКБ «НАЦКОРПБАНК» ОАО**

**Протокол № 7 от 21 июня 2010 г.**

**СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**  
**АКБ «НАЦКОРПБАНК» ОАО**

**ПОЛИТИКА ИНФОРМАЦИОННОЙ**  
**БЕЗОПАСНОСТИ**  
**ОСНОВНЫЕ ПРИНЦИПЫ**

**ИБ-100**

**МОСКВА**  
**2010**

 <p><i>Национальный Корпоративный Банк</i></p>	<p><b>КОРПОРАТИВНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p>	<p><b>ИБ-100</b> Действует с 01.07.2010</p>
<p>Система менеджмента информационной безопасности</p>	<p><b>ОСНОВНЫЕ ПРИНЦИПЫ</b></p>	<p>страница 2 из 8</p>

## I. ВВЕДЕНИЕ

### 1. Основные положения

1.1. «Политика информационной безопасности. Основные положения» (далее - Политика) АКБ «НАЦКОРПБАНК» ОАО (далее - Банк) определяет на корпоративном уровне цели и основные принципы системы обеспечения информационной безопасности Банка и вместе с другими документами системы менеджмента информационной безопасности (ИБ) устанавливает системно связанную совокупность правил, требований и руководящих принципов в области обеспечения ИБ, которыми руководствуется Банк в своей деятельности.

### 2. Термины и определения

2.1. **Информационный актив** — Информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для Банка; находящаяся в распоряжении Банка и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

2.2. **Информационная сфера** — собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.

2.3. **Комплекс БР ИББС** — Комплекс документов в области стандартизации Банка России "Обеспечение информационной безопасности организаций Банковской системы Российской Федерации".

2.4. **Система менеджмента информационной безопасности (СМИБ)** — Часть менеджмента организации банковской системы Российской Федерации, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

 <p><i>Национальный Корпоративный Банк</i></p>	<p><b>КОРПОРАТИВНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p>	<p><b>ИБ-100</b> Действует с 01.07.2010</p>
<p>Система менеджмента информационной безопасности</p>	<p><b>ОСНОВНЫЕ ПРИНЦИПЫ</b></p>	<p>страница 3 из 8</p>

## **II. ЦЕЛИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИБ**

### **3. Область применения**

3.1. Настоящая Политика распространяется на все структурные подразделения Банка и обязательна к исполнению всеми его работниками и должностными лицами при использовании информационных ресурсов Банка.

3.2. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах Банка, а также в договорах с контрагентами.

3.3. Положения настоящей Политики обязательны для исполнения работниками и представителями других организаций, являющихся контрагентами Банка, при использовании ими информационных ресурсов Банка в рамках заключенных Банком договоров.

### **4. Объекты защиты**

4.1. Информация (информационные ресурсы), составляющая коммерческую, банковскую тайну или иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, а также любая открытая (общедоступная) информация, необходимая для деятельности Банка, независимо от формы и вида ее представления;

4.2. Процессы обработки информации в информационных системах Банка, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

4.3. Информационная инфраструктура, включающая технические и программные средства обработки и анализа информации, средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены чувствительные элементы информационной среды Банка.

### **5. Цели обеспечения информационной безопасности**

5.1. Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

5.2. Целями обеспечения информационной безопасности являются минимизация ущерба от реализации угроз информационной безопасности и повышение деловой репутации и корпоративной культуры Банка.

 <p><i>Национальный Корпоративный Банк</i></p>	<p><b>КОРПОРАТИВНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p>	<p><b>ИБ-100</b> Действует с 01.07.2010</p>
<p>Система менеджмента информационной безопасности</p>	<p><b>ОСНОВНЫЕ ПРИНЦИПЫ</b></p>	<p>страница 4 из 8</p>

## **6. Принципы обеспечения информационной безопасности**

- 6.1. Информация является важнейшим активом Банка и ее защита является обязанностью каждого сотрудника.
- 6.2. Доступ к информации предоставляется только тем лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.
- 6.3. Для каждого информационного ресурса определяется уполномоченное лицо (распорядитель или менеджер), отвечающее за предоставление к нему доступа и эффективное функционирование мер защиты информации.
- 6.4. Сотрудники Банка проходят подготовку, инструктирование и проверку знаний в области информационной безопасности.
- 6.5. Система управления информационной безопасностью Банка строится на основе отраслевых, национальных и международных стандартов в области обеспечения и управления информационной безопасностью.
- 6.6. Риски, связанные с информационной безопасностью, рассматриваются как часть операционного риска и контролируются в рамках существующей в Банке системы оценки и управления банковскими рисками.
- 6.7. Необходимость внедрения мер защиты информации определяется требованиями нормативных документов, а также возможным влиянием реализации угроз информационной безопасности на финансовые результаты деятельности Банка и его деловую репутацию.

 <p><i>Национальный Корпоративный Банк</i></p>	<p><b>КОРПОРАТИВНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p> <p><b>ОСНОВНЫЕ ПРИНЦИПЫ</b></p>	<p><b>ИБ-100</b></p> <p>Действует с 01.07.2010</p>
		<p>Система менеджмента информационной безопасности</p>

### **III. СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА**

#### **7. Система менеджмента информационной безопасности**

7.1. Система менеджмента информационной безопасности (СМИБ) представляет собой составную часть корпоративной системы управления Банком, которая направлена на содействие достижению целей Банка путем обеспечения защищенности его информационной сферы.

#### **8. Состав документов системы менеджмента информационной безопасности первого и второго уровня**

8.1. Состав документов корпоративной политики информационной безопасности, относящихся к первому уровню документации:

- **[ИБ-100]** — «Политика информационной безопасности. Основные принципы».
- **[ИБ-101]** — «Политика информационной безопасности. Концепция».

8.2. Состав частных политик обеспечения информационной безопасности по областям, относящихся к второму уровню документации:

- **[ИБ-111]** — «Политика обеспечения мониторинга и менеджмента инцидентов информационной безопасности».
- **[ИБ-121]** — «Политика обеспечения непрерывности и восстановления бизнеса».
- **[ИБ-122]** — «Политика обеспечения информационной безопасности при ведении информационных архивов».
- **[ИБ-131]** — «Политика обеспечения информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу».
- **[ИБ-132]** — «Политика обеспечения информационной безопасности при управлении доступом к информационным ресурсам».
- **[ИБ-141]** — «Политика обеспечения информационной безопасности при использовании средств криптографической защиты информации».
- **[ИБ-142]** — «Политика обеспечения информационной безопасности персональных данных».
- **[ИБ-151]** — «Политика обеспечения информационной безопасности средствами защиты от вредоносных программ».
- **[ИБ-161]** — «Политика обеспечения информационной безопасности при использовании автоматизированных банковских систем».
- **[ИБ-171]** — «Политика обеспечения информационной безопасности при использовании телекоммуникационных систем и вычислительных сетей».
- **[ИБ-172]** — «Политика обеспечения информационной безопасности при

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>КОРПОРАТИВНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p> <p align="center"><b>ОСНОВНЫЕ ПРИНЦИПЫ</b></p>	<p align="center"><b>ИБ-100</b> Действует с 01.07.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 6 из 8</p>

использовании электронной почты и ресурсов сети Интернет».

– **[ИБ-181]** — «Политика обеспечения ИБ методами физической защиты».

8.3. Другие документы обеспечения информационной безопасности, относящиеся ко второму уровню:

– **[ИБ-200]** — «План мероприятий по обеспечению информационной безопасности».

– **[ИБ-201]** — «Положение о документации системы менеджмента информационной безопасности».

8.4. Состав прочих документов обеспечения информационной безопасности, относящихся ко второму, а также к третьему и четвертому уровню, определяются положениями документов, перечисленных в п.п. 8.2-8.3 Политики.

8.5. Наименования и индексы документов, указанные в п.п. 8.1-8.3, могут быть уточнены в процессе их разработки и принятия.

 <p><i>Национальный Корпоративный Банк</i></p>	<p><b>КОРПОРАТИВНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p>	<p><b>ИБ-100</b> Действует с 01.07.2010</p>
<p>Система менеджмента информационной безопасности</p>	<p><b>ОСНОВНЫЕ ПРИНЦИПЫ</b></p>	<p>страница 7 из 8</p>

## **IV. УПРАВЛЕНИЕ СИСТЕМОЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

### **9. Руководство**

9.1. Общее руководство обеспечением информационной безопасности Банка осуществляют Совет Директоров, Правление и Председатель Правления Банка.

9.2. Правление Банка назначает Куратора СМИБ из числа заместителей Председателя Правления Банка или директоров Департаментов. Куратор СМИБ не должен быть одновременно куратором информационных технологий.

9.3. Председатель Правления назначает Координатора СМИБ, который организует текущую деятельность по созданию и поддержке функционирования СМИБ.

9.4. Ответственность за реализацию мероприятий системы информационной безопасности и общий контроль за соблюдением требований информационной безопасности в Банке несет начальник Управления банковских информационных технологий Департамента банковских технологий.

9.5. Руководители структурных подразделений Банка несут ответственность за обеспечение выполнения требований ИБ в своих подразделениях.

### **10. Контроль и аудит**

10.1. Председатель Правления назначает Контролера документации СМИБ, который контролирует исполнению документов СМИБ.

10.2. Для оценки СМИБ применяется самооценка и внешний аудит.

10.3. Служба внутреннего контроля (СВК) Банка осуществляет контроль за уровнем информационной безопасности Банка в рамках проводимых проверок СВК Банка, согласно планов, утвержденных Советом Директоров Банка.

### **11. Ответственность**

11.1. Нарушения требований Политики и иных внутренних нормативных документов Банка, входящих в СМИБ, а равно несоблюдение мер, предусмотренных Системой обеспечения информационной безопасности, сотрудниками Банка влечет применение к ним дисциплинарных мер взыскания вплоть до увольнения.

 <p><i>Национальный Корпоративный Банк</i></p>	<p><b>КОРПОРАТИВНАЯ ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ</b></p> <p><b>ОСНОВНЫЕ ПРИНЦИПЫ</b></p>	<p><b>ИБ-100</b></p> <p>Действует с 01.07.2010</p>
		<p>Система менеджмента информационной безопасности</p>

## **V. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

### **12. Ввод в действие и исключения**

12.1. Политика утверждается и вводится в действие решением Совета Директоров Банка.

12.2. Исключения (допускаемые отступления от требований) Политики устанавливаются решением Правления Банка на срок не более шести месяцев подряд.

12.3. Формулировка области действия временных исключений должна носить конкретный ограниченный характер.

### **13. Условия и порядок контроля актуальности и пересмотра**

13.1. Плановая проверка актуальности Политики проводится ежегодно с целью определения необходимости ее пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обеспечению информационной безопасности. Плановая проверка актуальности Политики проводится Координатором СМИБ или начальником Управления банковских информационных технологий Департамента банковских технологий не позднее двадцатого числа месяца ввода в действие последней редакции документа по состоянию на первый день этого месяца. В результате проверки устанавливается возможность продления или необходимость пересмотра действующей редакции Политики. Информация о проведенной проверке заносится в прилагаемый Лист записей о проверках актуальности документа.

13.2. Пересмотр Политики производится по решению Правления Банка по результатам плановой проверки актуальности, в случае выявления несоответствия определенного Политикой комплекса защитных мер фактам зафиксированных инцидентов информационной безопасности, при существенных изменениях в бизнес-процессах или при изменениях нормативной базы в области обеспечения информационной безопасности.

13.3. Пересмотр Политики осуществляет Координатор СМИБ или специально назначаемая Правлением рабочая группа, которые готовят предложения по частичной переработке документа (выпуск/издание редакции с изменениями), либо полной (существенной) переработке документа (перевыпуск/переиздание в новой редакции).

13.4. Контроль исполнения Политики осуществляет Контролер документации СМИБ.