



*Национальный Корпоративный Банк*  
Лицензия № 3422


**УТВЕРЖДЕНА**  
**решением Совета Директоров**  
**АКБ «НАЦКОРПБАНК» ОАО**  
**Протокол № 12 от 11 ноября 2010 г.**

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

**ПОЛИТИКА ОБЕСПЕЧЕНИЯ**  
**ИНФОРМАЦИОННОЙ**  
**БЕЗОПАСНОСТИ ПРИ**  
**ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ**  
**ДАННЫХ**

**ИБ-142**

**МОСКВА**  
**2010**

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 2 из 16</p>

## 1. Общие положения

1.1. Политика обеспечения информационной безопасности при обработке персональных данных (далее – Политика) АКБ «НАЦКОРПБАНК» ОАО (далее – Банк) является нормативным документом, определяющим общие принципы обеспечения безопасности персональных данных (далее – ПДн) и организационно-технические меры по защите ПДн в информационных системах персональных данных (далее – ИСПДн) Банка.

1.2. Настоящая Политика разработана на основе анализа требований действующего законодательства Российской Федерации и нормативных документов, регламентирующих вопросы защиты ПДн, с учетом современного состояния и стратегии развития информационных технологий, целей, задач и правовых основ создания и эксплуатации информационных систем, режимов функционирования, а также на основе анализа модели угроз безопасности ПДн.

1.3. Политика служит основой для разработки комплекса организационных и технических мер по обеспечению защиты персональных данных в ИСПДн Банка, а также нормативных и методических документов, обеспечивающих жизненный цикл системы защиты персональных данных Банка.

## 2. Нормативные ссылки и указатель документов СМИБ

2.1. [ИБ-100] — «Политика информационной безопасности. Основные принципы».

2.2. [ИБ-101] — «Политика информационной безопасности. Концепция».


2.3. Стандарт Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций Банковской системы Российской Федерации. Общие положения».

## 3. Термины и определения:

3.1. **Персональные данные** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

3.2. **Обработка персональных данных** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.3. **Конфиденциальность персональных данных** — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным,

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 3 из 16</p>

требование не допускать их распространения без согласия субъекта или иного законного основания.

**3.4. Распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**3.5. Использование персональных данных** — действия (операции) с персональными данными, совершаемые должностным лицом Организации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов либо иным образом затрагивающих их права и свободы или права и свободы других лиц.

**3.6. Блокирование персональных данных** — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**3.7. Уничтожение персональных данных** — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.


**3.8. Обезличивание персональных данных** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**3.9. Общедоступные персональные данные** — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**3.10. Информация** — сведения (сообщения, данные) независимо от формы их представления.

#### **4. Правовые основы обеспечения безопасности ПДн в ИСПДн Банка**

4.1. Политика разработана в целях реализации требований Федерального закона № 152-ФЗ от 27.07.2006 года «О персональных данных» по обеспечению безопасности ПДн, обрабатываемых в ИСПДн Банка.

 <p><b>Национальный Корпоративный Банк</b></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 4 из 16</p>

## 5. Цели обработки персональных данных

5.1. Целью обработки указанных выше персональных данных является:

- осуществление возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О рынке ценных бумаг», «О несостоятельности (банкротстве) кредитных организаций», «О страховании вкладов физических лиц в банках Российской Федерации», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», нормативными актами Банка России, а также Уставом и нормативными актами Банка;
- организация учета служащих кредитной организации для обеспечения соблюдения законов и иных нормативно-правовых актов, содействия служащему в трудоустройстве, обучении, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», а также Уставом и нормативными актами Банка.


5.2. Цели обработки персональных данных, относящихся к каждому отдельному бизнес-процессу Банка определены в документе СМИБ [ИБ-642] «Перечень персональных данных».

## 6. Основные цели и задачи обеспечения безопасности персональных данных

6.1. Основной целью обеспечения безопасности персональных данных является минимизация ущерба (как непосредственного, так и опосредованного), возникающего вследствие возможной реализации угроз безопасности персональных данных.

6.2. Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту персональных данных и может проявляться в виде:

- нанесения вреда здоровью субъекта персональных данных;
- незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта;
- потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием персональных данных;

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 5 из 16</p>

- нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь.

6.3. Опосредованный ущерб связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с персональными данными.

6.4. Основной задачей обеспечения безопасности персональных данных, при их обработке в ИСПДн Банка, является предотвращение утечки персональных данных по техническим каналам, несанкционированного доступа к ним, предупреждение преднамеренных программно-технических воздействий с целью их разрушения (уничтожения) или искажения в процессе обработки, передачи и хранения.


## **7. Общие принципы обеспечения безопасности персональных данных в ИСПДн Банка**

7.1. Построение системы защиты персональных данных Банка и ее функционирование осуществляются в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность и адекватность;
- персональная ответственность;
- минимизация полномочий;
- гибкость;
- открытость алгоритмов и механизмов защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- знание своих партнеров и работников;
- наблюдаемость и оцениваемость;
- обязательность контроля и оценки.

### **7.1.1. Законность**

Защита ПДн в ИСПДн Банка основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите ПДн и учитывает лучшие мировые практики.

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДА Н Н Ъ Х</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 6 из 16</p>

#### 7.1.2. Системность

Системный подход к построению СЗПДн предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн Банка.

#### 7.1.3. Комплексность

Безопасность ПДн обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер, реализованных в Банке.

Применение различных средств и технологий защиты информации перекрывает все существенные (значимые) каналы реализации угроз безопасности ПДн и не содержит слабых мест в согласовании применяемых средств и технологии защиты информации.

В Банке обеспечен отраслевой подход к разработке рекомендаций (требований) по защите ПДн с учетом особенностей обработки ПД в ИСПДн Банка.

СЗПДн Банка строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа (далее – НСД) к ПДн, но и с учетом возможности повышения уровня защиты по мере выявления новых источников угроз безопасности ПДн, развития способов и средств их реализации в ИСПДн.

Система защиты ПДн Банка строится на основе единой технической политики, с использованием функциональных возможностей информационных технологий, реализованных в информационной системе и имеющихся систем и средств защиты в соответствии с разработанной моделью угроз **СМИБ [ИБ-342]**. При создании системы защиты ПДн могут использоваться системы и средства защиты информации, используемые в Банке для обеспечения безопасности коммерческой тайны и иной конфиденциальной информации.

#### 7.1.4. Непрерывность


Защита ПДн обеспечивается на всех технологических этапах обработки ПДн и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

#### 7.1.5. Своевременность

Принимаемые меры по обеспечению безопасности ПДн носят упреждающий характер.

В Банке принимаются необходимые меры по защите ПДн до начала обработки ПДн, которые обеспечивают надлежащий уровень безопасности ПДн.

Система защиты ПДн разрабатывается одновременно с разработкой и развитием ИСПДн Банка, что позволяет учитывать требования по безопасности ПДн при

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДА Н Н Ъ Х</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 7 из 16</p>

проектировании и модернизации ИСПДн.

#### 7.1.6. Преемственность и непрерывность совершенствования

На основе результатов анализа функционирования ИСПДн и системы защиты ПДн, с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного положительного опыта в сфере защиты информации, осуществляется постоянное совершенствование мер и средств защиты ПДн.

В Банке определены действия, необходимые для устранения причин потенциальных несоответствий требованиям по безопасности ПДн с целью предотвратить их повторное появление. Предпринимаемые предупреждающие действия соответствуют возможным негативным последствиям.

#### 7.1.7. Разумная достаточность и адекватность

Состояние и стоимость реализации мер защиты с рисками, связанными с обработкой и характером защищаемых ПДн.

Анализ рисков нарушения безопасности ПДн проводится в целях определения влияния системы защиты информации на вероятность реализации угроз безопасности ПДн с учетом уязвимостей (дефектов) ИТ - инфраструктуры Банка.

Программно-технические средства защиты не существенно ухудшают основные функциональные характеристики и производительность ИСПДн Банка.

#### 7.1.8. Персональная ответственность

Ответственность за обеспечение безопасности ПДн и ИСПДн Банка возлагается на каждого работника в пределах его полномочий.

Распределение обязанностей и полномочий работников Банка обеспечивает выявление виновных лиц в случаях нарушения безопасности ПДн.

Роли и обязанности сотрудников определены и документально подтверждены в соответствии с документом **СМИБ [ИБ-131]**.

#### 7.1.9. Минимизация полномочий

Предоставление и использование прав доступа к ПДн ограничено и управляемо.


Пользователям предоставляются минимальные права доступа к ПДн и ИСПДн только в соответствии с производственной необходимостью.

Доступ к ПДн предоставляется только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

Пользователю запрещены все операции с ПДн за исключением тех, которые разрешены явно.

#### 7.1.10. Гибкость

В процессе функционирования ИСПДн могут меняться ее характеристики, а также объем и категории обрабатываемых в Банке ПДн.

 <p><b>Национальный Корпоративный Банк</b></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 8 из 16</p>

Для обеспечения возможности варьирования уровня защищенности ПДн, система защиты ПДн Банка обладает определенной гибкостью.

#### 7.1.11. Открытость алгоритмов и механизмов защиты

Защита ПДн осуществляется не только за счет сокрытия структуры, технологий и алгоритмов функционирования системы защиты ПДн.

Знание указанных характеристик системы защиты ПДн не дает возможности преодоления защиты возможными нарушителями безопасности ПДн, включая разработчиков средств защиты.

#### 7.1.12. Научная обоснованность и техническая реализуемость

Уровень рекомендаций и требований по защите ПДн Банка соответствует имеющемуся уровню развития информационных технологий и средств защиты информации.

При создании и эксплуатации системы защиты ПДн, сотрудники Управления банковских информационных технологий и Группы информационной безопасности ориентируются на лучшие современные отечественные и зарубежные технические решения и практику защиты информации.

#### 7.1.13. Специализация и профессионализм

Реализация мер по обеспечению безопасности ПДн и эксплуатация системы защиты ПДн осуществляется профессионально подготовленными специалистами Банка.

#### 7.1.14. Знание своих партнеров и работников

В Банке осуществляется сбор информации о сотрудниках и партнерах, что позволяет минимизировать вероятность реализации угроз безопасности ПДн, источники которых связаны с человеческим фактором.


В Банке реализуется кадровая политика (тщательный подбор персонала и мотивация работников), позволяющая исключить или минимизировать возможность нарушения безопасности ПДн своими работниками.

#### 7.1.15. Наблюдаемость и оцениваемость обеспечения безопасности персональных данных

Предлагаемые Банком меры по обеспечению безопасности ПДн спланированы так, чтобы результат их применения был явно наблюдаем (прозрачен) и мог быть оценен федеральными органами исполнительной власти, осуществляющими функции по контролю и надзору в пределах своих полномочий.

#### 7.1.16. Обязательность контроля и оценки

С целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн в Банке определены процедуры для постоянного контроля использования систем обработки и защиты ПДн, а

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 9 из 16</p>

результаты контроля регулярно анализируются.

## **8. Общие методы обеспечения безопасности персональных данных**

### **8.1. Классификация методов обеспечения безопасности персональных данных**

Методы обеспечения безопасности ПДн разделяются на:

- административно-правовые;
- организационно-технические;
- экономические.

По времени применения методы обеспечения безопасности ПДн разделяются на:

- превентивные;
- восстановительные.


#### **8.1.1. Административно-правовые методы**

К административно-правовым методам защиты относятся нормы действующего законодательства и внутренние организационно-распорядительные документы Банка, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе обработки и использования ПДн, а также устанавливающие ответственность за нарушения этих правил, препятствуя неправомерному использованию ПДн и являющиеся сдерживающим фактором для реализации угроз безопасности потенциальными нарушителями.

#### **8.1.2. Организационно-технические методы**

Организационно-технические методы защиты основаны на использовании организационных мер, различных программных, аппаратных и программно - аппаратных средств, входящих в состав системы защиты ПДн и выполняющих функции защиты информации, направленных на решение следующих задач:

- строгий учет всех подлежащих защите ресурсов (персональных данных, сервисов, каналов связи, серверов, автоматизированных рабочих мест и т.д.);
- предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременного обнаружения фактов НСД к ПДн;
- недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- постоянного контроля за обеспечением уровня защищенности ПДн.

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДА Н Н Ы Х</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 10 из 16</p>

#### 8.1.3. Экономические методы

Экономические методы обеспечения безопасности ПДн включают в себя:

- разработку программ обеспечения безопасности ПДн и определение порядка их финансирования.
- разработку мер поощрения и наложения штрафных санкций за соблюдение или не соблюдение установленных правил и процедур обработки ПДн.

#### 8.1.4. Превентивные методы

Превентивные методы противодействия угрозам безопасности ПДн осуществляются на основе эффективного применения в процессе эксплуатации ИСПДн комплекса организационных, технических и технологических мероприятий, а также методов и средств обеспечения функциональной устойчивости и безопасности работы ИСПДн.


Организационные мероприятия по обеспечению безопасности ПДн являются мероприятиями общего характера по организации деятельности персонала, эксплуатирующего ИСПДн, порядку применения информационных технологий в зданиях и сооружениях, систематическому применению мер по недопущению вывода ИСПДн из строя.

Технические мероприятия по обеспечению безопасности ПДн заключаются в обслуживании, поддержании и управлении требуемым составом технических средств, обеспечивающих обработку ПДн в защищенном режиме.

Технологические мероприятия по обеспечению безопасности ПДн направлены на правильную реализацию функций и заданных алгоритмов работы ИСПДн, технологий обработки ПДн и защиту программ и ПДн от преднамеренных и непреднамеренных нарушений.

#### 8.1.5. Восстановительные методы

Планирование восстановительных методов определяется системой документов, устанавливающих требования к обязательным мероприятиям, проводимым заблаговременно и после возникновения нарушений, угрожающих штатному функционированию ИСПДн.

 <p><b>Национальный Корпоративный Банк</b></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДА Н Н Ъ Х</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p>Система менеджмента информационной безопасности</p>		<p align="center">страница 11 из 16</p>

## **9. Общие мероприятия по обеспечению безопасности персональных данных**

9.1. Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн в Банке несут сотрудники УБИТ ДБТ и Группы ИБ.

9.2. Основными мероприятиями по организации и техническому обеспечению безопасности ПДн в ИСПДн являются:

- мероприятия по организации обеспечения безопасности ПДн, включая классификацию ИСПДн;
- мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн, включающие мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн;
- мероприятия по защите ПДн от несанкционированного доступа и определению порядка выбора средств защиты ПДн при их обработке в ИСПДн.

9.3. Перечень реализуемых мероприятий по защите ПДн при их обработке в ИСПДн Банка определяется на основании анализа актуальности угроз, рисков безопасности ПДн и профилей защиты ПДн для ИСПДн Банка, в соответствии с нормативными и методическими документами Банка России.


9.4. В соответствии с нормативными документами Федеральной службы по техническому и экспортному контролю:

- осуществляется обеспечение защиты (некриптографическими методами) информации;
- проводятся мероприятия по предотвращению утечки информации по техническим каналам;
- проводятся мероприятия по предотвращению несанкционированного доступа к информации, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, и блокирования доступа к ней.

9.5. В соответствии с нормативными документами Федеральной службы безопасности Российской Федерации:

- устанавливаются особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах;
- проводятся мероприятия по обнаружению компьютерных атак.

Мероприятия по обеспечению безопасности ПДн включают в себя:

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДА Н Н Н Х</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 12 из 16</p>

- управление доступом:
  - идентификация и аутентификация;
  - физическая защита;
- регистрацию и учет;
- обеспечение конфиденциальности;
- обеспечение целостности;
- обеспечение доступности;
- обеспечение достоверности (аутентичности);
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия;
- анализ защищенности;
- обнаружение вторжений;
- обеспечение безопасности мобильных рабочих мест;
- обеспечение безопасного доступа к сетям международного информационного обмена.

#### 9.6. Идентификация и аутентификация


Управление доступом к ПДн осуществляется на основе принципа минимизации полномочий. Стандартным методом доступа является ролевой доступ, для чего определяются совокупности типов доступа - групповых прав и полномочий доступа пользователей (ролей), предоставляемых пользователям. Количество таких ролей ограничено и подразумевает возможность эффективного управления. Назначение прав и полномочий конкретным пользователям осуществляется путем назначения им соответствующих ролей.

Каждый пользователь для получения соответствующих прав доступа при подключении к ИСПДн проходит процедуру идентификации, при этом используются уникальные признаки и имена. При этом подлинность личности пользователя проверяется. Стандартное средство проверки подлинности (аутентификации) – пароль.

#### 9.7. Физическая защита

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации.

Размещение, специальное оборудование, охрана и организация режима в помещениях исключают возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами

 <p><b>Национальный Корпоративный Банк</b></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДА Н Н Ъ Х</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 13 из 16</p>

ведущихся там работ.

#### 9.8. Регистрация и учет

В ИСПДн ведутся контрольные журналы, регистрирующие действия пользователей с ПДн. Должны быть установлены процедуры применения мониторинга действий с ПДн, а результаты действий пользователей должны регулярно просматриваться.

#### 9.9. Обеспечение целостности

Банк обеспечивает целостность программных средств защиты в составе системы защиты ПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты ПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ.

Обеспечение целостности реализуется преимущественно операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

#### 9.10. Антивирусная защита

Для обеспечения безопасности ПДн и программно-аппаратной среды ИСПДн, осуществляющей обработку этой информации, применяются специальные средства антивирусной защиты согласно документу СМИБ **[ИБ-151]**.


#### 9.11. Обеспечение безопасного межсетевого взаимодействия

Для осуществления разграничения доступа к ресурсам ИСПДн при межсетевом взаимодействии применяется межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами. Межсетевой экран устанавливается между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран входит в состав защищаемой сети. Для него путем настроек отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Межсетевое экранирование обеспечивает:

- скрытие внутренней сетевой структуры ИСПДн;
- разрешение только такого входящего и исходящего трафика, который является необходимым для работы ИСПДн;
- блокирование любого входящего и исходящего трафика, не разрешенного явно.

#### 9.12. Анализ защищенности

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДА Н Н Н Х</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 14 из 16</p>

Анализ защищенности реализуется на основе использования средств тестирования (анализа защищенности) и контроля (аудита) безопасности информации.

Для гарантии того, что СЗИ успешно выполняют свои функции, разработаны процедуры контроля изменений конфигураций СЗИ и сетевых устройств. Для выполнения этих процедур в информационно-телекоммуникационной среде Оператора связи должна быть создана система анализа защищенности, выполняющая следующие функции:

- контроль настроек сетевых устройств, СЗИ и программно-технического обеспечения ИСПДн;
- анализ уязвимостей настроек СЗИ, сетевых устройств или уязвимостей операционных систем или прикладного программного обеспечения.

#### 9.13. Обнаружение вторжений

Обнаружение вторжений реализуется с использованием в составе системы защиты ПДн Банка программных и (или) программно-аппаратных средств (систем) обнаружения вторжений, использующих комбинированные методы обнаружения атак, включающие в себя сигнатурные методы и методы выявления аномалий.

#### 9.14. Криптографическая защита


Для защиты ПДн, передаваемых между ИСПДн по каналам связи, выходящим за пределы контролируемой зоны, используются защищенные каналы связи, включая доверенные каналы и защищенные волоконно-оптические линии связи.

При использовании открытых и неконтролируемых каналов связи для защиты ПДн применяются средства криптографической защиты информации (далее – СКЗИ). Как отдельно, так и комплексно, используются следующие криптографические методы:

- шифрование, как средство обеспечения конфиденциальности информации;
- электронная цифровая подпись, как средство обеспечения подлинности и юридической значимости электронного документа;
- криптографическая аутентификация, как средство подтверждения санкционированности доступа субъекта к объекту;
- управление ключами, как необходимая составная часть систем с СКЗИ, которая применяется в целях изготовления, учета, распределения, хранения и уничтожения ключевых элементов.
- Подробное описание применения СКЗИ в Банке в документе СМИБ **[ИБ-141]**.

#### 9.15. Обеспечение безопасного доступа к сетям международного информационного обмена

Доступ ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе к международной

 <p><i>Национальный Корпоративный Банк</i></p>	<p align="center"><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ</b></p>	<p align="center"><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p align="center">Система менеджмента информационной безопасности</p>		<p align="center">страница 15 из 16</p>

компьютерной сети Интернет допускается только с использованием специально предназначенных для этого средств защиты информации.

При принятии Банком решений об использовании сети «Интернет» необходимо учитывать следующие положения:

- сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение).
- провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет;
- существует вероятность атаки злоумышленников на оборудование, программное обеспечение и информационные ресурсы, подключенные/доступные из сети Интернет;
- гарантии по обеспечению безопасности ПДн при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются.

## **10. Условия и порядок пересмотра и контроля**


10.1. Плановая проверка актуальности Политики производится ежегодно с целью определения необходимости ее пересмотра для обеспечения соответствия предусмотренного комплекса мероприятий реальным условиям и актуальным требованиям к обеспечению безопасности персональных данных обрабатываемых в ИСПДн Банка. Плановая проверка актуальности Политики проводится координатором СМИБ. 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.

10.2. Внеочередной пересмотр Политики производится по решению координатора СМИБ, в случае выявления неадекватности определенного Политикой комплекса мероприятий реально возникшим в Банке непредвиденным обстоятельствам.

10.3. Рабочие изменения (в рамках поддержки документа) могут вноситься в текст информационных (справочных или рекомендуемых) Приложений к настоящей Политике для учета актуальных изменений и не требуют утверждения.

10.4. Пересмотр Политики осуществляет координатор СМИБ, который готовит предложения по частичной переработке документа (выпуск редакции с изменениями), либо полной переработке документа (перевыпуск в новой редакции).

10.5. Контроль исполнения Политики осуществляет Контролер документации СМИБ.

 <p><i>Национальный Корпоративный Банк</i></p>	<p><b>ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДА Н Н Ъ Х</b></p>	<p><b>ИБ-142-10</b> Действует с 01.12.2010</p>
<p>Система менеджмента информационной безопасности</p>		<p>страница 16 из 16</p>

## **11. Ответственность**

11.1. Нарушение требований Политики сотрудниками Банка влечет ответственность, предусмотренную документом [ИБ-100].

