УТВЕРЖДЕНО:
Советом директоров
ПАО КБ "САММИТ БАНК"
Протокол № 51
от " 24 " апреля 2015 г.
Председатель Совета директоров

_____ Игнатенко Ю.В.

ПОЛОЖЕНИЕ

«Политика ПАО КБ "САММИТ БАНК" в отношении организации обработки и обеспечения безопасности персональных данных»

I. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Настоящее Положение детализирует положения «Политики информационной безопасности ПАО КБ «САММИТ БАНК» применительно к организации обработки и обеспечения безопасности персональных данных (далее ПДн) и является внутренним документом, определяющим цели, задачи и принципы подхода Банка в отношении организации обработки персональных данных и предусматривает комплекс взаимосвязанных мер и мероприятий, направленных на обеспечение безопасности персональных данных работников, клиентов, посетителей и иных субъектов.

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», нормативными требованиями Банка России и другими федеральными законами и нормативными правовыми актами действующего законодательства РФ.

1.3. Настоящее Положение распространяется на все технологические процессы Банка связанные с обработкой и обеспечением защиты персональных данных субъектов, и обязательна для применения всеми работниками Банка.

1.4. Положение является общедоступным документом, декларирующим концептуальные основы деятельности Банка при обработке и защите персональных данных.

II. ЦЕЛИ И ПРИНЦИПЫ ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

2.1. Банк, как оператор, осуществляет обработку ПДн физических лиц в рамках требований законодательства Российской Федерации в целях:

- осуществления возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: от 02.12.1990 № 395-1 «О банках и банковской деятельности», от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг», от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле», от 23.12.2003 № 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации», от 30.12.2004 № 218-ФЗ «О кредитных историях», от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ), от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты

Российской Федерации», нормативными актами Банка России, а также Уставом Банка и внутренними нормативными документами;

- организации учета работников Банка (кандидатов на работу) для обеспечения соблюдения требований законов и иных нормативно-правовых актов, содействия в трудоустройстве, обучении, добровольном страховании всех видов, продвижении по службе, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в системе обязательного пенсионного страхования, Законом № 152-ФЗ, а также Уставом Банка и внутренними нормативными документами;

2.2. Необходимость обеспечения безопасности персональных данных в наше время объективная реальность. Информация о человеке всегда имела большую ценность, но сегодня она превратилась в самый дорогой товар. Именно поэтому персональные данные нуждаются в самой серьезной защите.

Необходимость принятия мер по защите персональных данных (далее ПДн) вызвана также возросшими техническими возможностями по копированию и распространению информации. Уровень информационных технологий достиг того предела, когда самозащита информационных прав уже не является эффективным средством против посягательств на частную жизнь.

С развитием средств электронной коммерции и доступных средств массовых коммуникаций возросли также и возможности злоупотреблений, связанных с использованием собранной и накопленной информации о человеке. Появились и эффективно используются злоумышленниками средства интеграции и быстрой обработки персональных данных, создающие угрозу правам и законным интересам человека.

Деятельность Банка невозможна без обработки информации о человеке. Банк хранит и обрабатывает данные о сотрудниках, клиентах, партнерах, поставщиках и других физических лицах. Утечка, потеря или несанкционированное изменение персональных данных приводит к невосполнимому ущербу, а порой и к полной остановке Банка. Поэтому **целью настоящего Положения являются определение особенностей обработки и обеспечения безопасности персональных данных, а также минимизация ущерба, который может возникнуть вследствие воздействия угроз информационной безопасности, приводящих к нарушению требуемых свойств безопасности персональных данных.**

2.3. С целью **поддержания деловой репутации**, обеспечения защиты прав и свобод человека и гражданина, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, выполнения норм федерального законодательства Банк считает **важнейшими задачами**: обеспечение легитимности обработки персональных данных в бизнес процессах Банка и обеспечение надлежащего уровня безопасности обрабатываемых в Банке персональных данных.

2.4. Понимая важность и ценность информации о человеке, а также заботясь о соблюдении прав своих акционеров, работников, клиентов, **Банк, выстраивая систему организации** обработки и обеспечения безопасности персональных данных, руководствуется следующими **принципами**:

- законность целей и способов обработки персональных данных;
- добросовестность обработки персональных данных;
- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе, а также полномочиям Банка как оператора персональных данных;
- соответствие объемов и характера обрабатываемых персональных данных и способов обработки персональных данных целям обработки персональных данных;
- достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных (ИСПДн).

2.5. Руководство Банка **осознает** важность и необходимость обеспечения безопасности персональных данных и **поощряет** постоянное совершенствование системы защиты персональных данных, обрабатываемых в рамках выполнения основной деятельности Банка.

III. СТРУКТУРА ОРГАНОВ УПРАВЛЕНИЯ СИСТЕМОЙ ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

3.1. В Банке установлен следующий порядок участия органов управления **системой организации** обработки и обеспечения безопасности персональных данных

3.1.1. ***Полномочия Совета директоров Банка***:

- утверждение и периодический пересмотр внутренних документов по общей банковской стратегии и по политике управления **системой организации** обработки и обеспечения безопасности персональных данных;
- создание организационной структуры Банка, соответствующей основным принципам управления **системой организации** обработки и обеспечения безопасности персональных данных;
- оценка эффективности и качества управления **системой организации** обработки и обеспечения безопасности персональных данных;
- контроль за деятельностью Правления Банка по управлению **системой организации** обработки и обеспечения безопасности персональных данных;

Совет директоров несет конечную ответственность за создание и функционирование адекватной и эффективной системы внутреннего контроля, системы управления организации обработки и обеспечения безопасности персональных данных.

3.1.2. ***Полномочия Правления Банка***:

- разработка/актуализация и обеспечение функционирования системы управления организации обработки и обеспечения безопасности персональных данных, включая их оценку, мониторинг и контроль;
- развитие процессов, призванных выявлять, измерять, отслеживать и контролировать банковские риски в сфере управления системой организации обработки и обеспечения безопасности персональных данных;
- образование подотчетных Правлению Банка органов коллегиального управления (Комитета по управлению активами и пассивами и др.) с целью рассмотрения и принятия решений, касающихся обеспечения непрерывного и эффективного процесса управления системой организации обработки и обеспечения безопасности персональных данных Банка;
- предоставление на заседания Совета директоров (не реже двух раз в год) отчетов по оценке качества управления системой организации обработки и обеспечения безопасности персональных данных;
- оперативное информирование Совета директоров о любых материальных убытках, которые могут повлечь за собой существенный риск наложения санкций, финансовых убытков или потери репутации.

Правление Банка несет ответственность за реализацию стратегии и Политики по управлению системой организации обработки и обеспечения безопасности персональных данных, утвержденной Советом директоров, за поддержку организационной структуры с четким распределением сфер ответственности и обеспечением эффективного осуществления делегированных полномочий, а также за результаты управления системой организации обработки и обеспечения безопасности персональных данных.

3.1.3. ***Комитет по управлению активами и пассивами*** участвует в реализации системы организации обработки и обеспечения безопасности персональных данных в рамках утвержденной «Политики по управлению рисками в ПАО КБ "САММИТ БАНК"».

3.2. Для обеспечения требований законодательства в сфере персональных данных и настоящего Положения назначено **Лицо, ответственное за организацию обработки персональных данных** в обязанности которого включены следующие функции:

- доводить до сведения работников Банка положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Лицо, ответственное за организацию обработки персональных данных, подотчетно президенту Банка (Председателю Правления).

3.3. Для обеспечения непрерывного и эффективного функционирования и развития системы управления информационной безопасностью в Банке и как ее составляющей части - организации обработки и обеспечения безопасности персональных данных, учитывая характер и масштабы деятельности Банка, сформирована служба информационной безопасности, ответственная за координацию управления **системой организации** обработки и обеспечения безопасности персональных данных и выполняющая следующие функции:

- разработка и согласование проектов внутрибанковских документов, регламентирующих обработку и обеспечение безопасности персональных данных;
- разработка и (или) апробация методик оценки банковских рисков при обработке и обеспечения безопасности персональных данных;
- осуществление внутреннего контроля соблюдения работниками Банкам нормативно – правовых актов, регулирующих обработку персональных данных, в том числе требований к защите персональных данных;
- информирование работников Банка о положениях законодательства РФ о персональных данных, внутрибанковских документов, регламентирующих обработку персональных данных, требований к защите персональных данных;
- организация приема и обработки обращений и запросов субъектов персональных данных их представителей и осуществление контроля за приемом и обработкой таких обращений и запросов;
- подготовка уведомления об обработке персональных данных, направляемого Уполномоченному органу;
- ведение перечней и классификаторов, использующихся при обработке персональных данных;
- постоянный контроль отдельных направлений банковской деятельности, в целях выполнения требований и положений настоящего Положения и прочих внутрибанковских документов, регламентирующих обработку в Банке персональных данных;
- разработка системы обеспечения безопасности ПДн, обеспечивающей нейтрализацию предполагаемых угроз. При этом ввод в эксплуатацию и использование средств и систем защиты информации должны осуществляться в соответствии с документацией на них;
- осуществление проверки готовности средств защиты информации, а также контроль их использования;
- проведение анализа происходящих нарушений порядка обработки и защиты ПДн, разработки и принятие мер по предотвращению возможных опасных последствий;
- проведение обучения лиц, использующих средства защиты информации, применяемые в автоматизированных системах, правилам работы с ними;
- выработка предложений по совершенствованию процессов обработки персональных данных в Банке с целью недопущения нарушений требований и положений настоящего Положения и прочих внутрибанковских документов, регламентирующих обработку в Банке персональных данных;
- своевременное информирование руководства и Правления Банка по вопросам касательно обработки персональных данных и о случаях, приведших к нарушениям законодательных требований при обработке персональных данных в Банке или предпосылках к таким случаям;
- проведение разбирательств и расследований по фактам нарушения требований и положений настоящего Положения и прочих внутрибанковских документов, регламентирующих обработку в Банке персональных данных.

Служба информационной безопасности несет ответственность за каждодневную реализацию Политики, за эффективное функционирование и развитие процесса управления системой организации обработки и обеспечения безопасности персональных данных.

IV. ОБЩИЕ ПРАВИЛА И МЕТОДЫ УПРАВЛЕНИЯ СИСТЕМОЙ ОРГАНИЗАЦИИ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.

4.1. Настоящее Положение распространяется на персональные данные, полученные как до, так и после утверждения настоящего Положения.

4.2. **Банк раскрывает информацию** о политике по управлению **системой организации** обработки и обеспечения безопасности персональных данных, а также о методах и процедурах контроля и другую информацию в рамках требований законодательства РФ.

4.3. Банк осуществляет уведомление уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку ПДн. Банк добросовестно и в соответствующий срок осуществляет актуализацию сведений, указанных в уведомлении.

4.4. Банк добивается того, чтобы все реализуемые Банком мероприятия по организационной и технической защите персональных данных осуществлялись на законных основаниях, в том числе в соответствии с требованиями законодательства Российской Федерации по вопросам обработки персональных данных.

4.5. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей, не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

4.6. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки, избыточность обрабатываемых данных Банком не допускается.

4.7. При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных, Банк принимает необходимые меры (обеспечивает их принятие) по удалению или уточнению неполных или неточных данных.

4.8. Банк не размещает персональные данные субъекта персональных данных в общедоступных источниках без его предварительного согласия, кроме случаев, установленных законодательством Российской Федерации, когда такое согласие не требуется.

4.9. Банк осуществляет трансграничную передачу персональных данных.

4.10. Работники Банка, осуществляющие обработку ПДн в ИСПДн, должны быть проинформированы о факте обработки ими ПДн и категориях обрабатываемых ПДн при предоставлении доступа к ИСПДн, а также должны быть ознакомлены под личную подпись со всей содержащейся в должностных инструкциях и соответствующих ВНД совокупностью требований Банка по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

4.11. При обработке ПДн на бумажных носителях следует руководствоваться «Положением о неавтоматизированной обработке персональных данных в ПАО КБ "САММИТ БАНК"».

4.12. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4.13. Сроки обработки персональных данных определяются в соответствии с требованиями законодательства РФ и нормативными документами Банка России

V. ВЗАИМОДЕЙСТВЕ БАНКА И НАДЗОРНЫХ ОРГАНОВ.

5.1. Банк предоставляет информацию Надзорным органам по их запросам и / или в ходе проверок, проводимых в установленном соответствующими законодательными и нормативными актами порядке.

5.2. При проведении проверки Банк:

- обеспечивает необходимые условия для ее проведения;
- по требованию должностных лиц Надзорных органов, проводящих проверку, организовывает доступ к оборудованию и в помещения, где осуществляется обработка персональных данных;
- предоставляет необходимую информацию и документацию для достижения целей проверки;

5.3. Банк предоставляет информацию, необходимую для осуществления контроля и надзора за выполнением требований к обработке персональных данных, установленных законодательством РФ и отдельными нормативными актами:

- **Банку России**
- **Уполномоченному органу**

в пределах их компетенции и с правом ознакомления с персональными данными, обрабатываемыми в Банке.

5.4. Банк предоставляет информацию, необходимую для осуществления контроля и надзора за выполнением требований к обработке персональных данных в информационных системах персональных данных, установленных Правительством РФ:

- Федеральному органу исполнительной власти, уполномоченному в области обеспечения Безопасности;
- Федеральным органу исполнительной власти, уполномоченному в области противодействия техническим разведкам и технической защиты информации

в пределах их компетенции и без права ознакомления с персональными данными, обрабатываемыми в таких информационных системах.

VI. ВНУТРЕННИЙ КОНТРОЛЬ И МЕТОДЫ УПРАВЛЕНИЯ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Внутренний контроль обработки персональных данных в Банке осуществляется в целях мониторинга и оценки фактического состояния защищенности персональных данных, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования процесса обработки и обеспечения безопасности персональных данных.

6.1.2. Система контроля управления организации обработки и обеспечения безопасности персональных данных предусматривает следующие уровни:

– *руководители структурных подразделений Банка* обеспечивают ежедневное соблюдение работниками Банка требований настоящего Положения и прочих внутрибанковских документов, регулирующих обработку и защиту персональных данных;

– *служба информационной безопасности* несет ответственность за каждодневную реализацию Политики, за эффективное функционирование и развитие процесса управления системой организации обработки и обеспечения безопасности персональных данных;

– *комитет Банка (КУАП)* рассматривает и принимает решения, касающиеся обеспечения непрерывного и эффективного процесса управления системой организации обработки и обеспечения безопасности персональных данных Банка;

– *лицо, ответственное за организацию обработки персональных данных* осуществляет внутренний контроль за соблюдением Банком и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных на постоянной основе;

– *Правление Банка* контролирует обеспечение функционирования системы управления организации обработки и обеспечения безопасности персональных данных, включая их оценку, мониторинг и контроль;

– *Совет директоров* осуществляет общий контроль функционирования **системы организации** обработки и обеспечения безопасности персональных данных.

6.1.3. Решения, принимаемые одним из уровней системы контроля управления процессом обработки и обеспечения безопасности персональных данных в рамках своих полномочий, являются обязательными для всех субъектов более низких уровней.

6.1.4. *Служба внутреннего контроля Банка* проводит периодические проверки состояния системы контроля организации обработки и обеспечения безопасности персональных данных, включающие:

- проверку полноты применения и эффективности проводимой Банком Политики в отношении организации обработки и обеспечения безопасности персональных данных,

- проверку качества управления процессом обработки и обеспечения безопасности персональных данных;

- контроль за эффективностью принимаемых подразделениями и органами управления по результатам проверок мер, обеспечивающих снижение уровня нарушений порядка обработки и защиты персональных данных или решений о их приемлемости и принятии.

6.2. Мероприятия внутреннего контроля обработки и обеспечения безопасности персональных данных направлены на решение следующих задач:

- Обеспечение соблюдения работниками Банка требований настоящего Положения и прочих внутрибанковских документов, регулирующих обработку и защиту персональных данных.
- Обеспечение работоспособности и эффективности технических средств информационных систем, в которых обрабатываются персональные данные и средств защиты персональных данных, их соответствия требованиям надзорных органов.

6.3. Решение вышеуказанных задач достигается за счет:

- **Выявления** нарушений установленного порядка обработки персональных данных и своевременное предотвращение негативных последствий таких нарушений.
- **Оценки** компетентности работников, задействованных в обработке персональных данных.
- **Принятия** корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки персональных данных, так и в работе технических средств информационных систем, в которых обрабатываются персональные данные.
- **Разработки** рекомендаций по совершенствованию порядка обработки и обеспечения безопасности персональных данных по результатам контрольных мероприятий.
- **Осуществления контроля исполнения** рекомендаций и указаний по устранению нарушений.

6.4. Контроль обеспечения безопасности персональных данных включает в себя в том числе:

- Проведение проверок деятельности работниками Банка, допущенных к работе с персональными данными в ИСПДн, на соответствие порядку обработки и обеспечения безопасности персональных данных, установленному настоящим Положением и другими нормативными документами, регламентирующими обработку персональных данных.
- Проведение проверок состояния защищенности персональных данных, обрабатываемых в информационных системах, включая проверку доступов пользователей к персональным данным, выполнение требований по защите ИСПДн, корректности работы системы защиты персональных данных.
- Проведение проверок состояния защищенности персональных данных, обрабатываемых без использования средств автоматизации, и условий хранения материальных носителей персональных данных.

6.5. Нарушение порядка обработки и защиты персональных данных является Инцидентом в Банке, фиксируется и расследуется.

6.6. В соответствии с выявленными актуальными угрозами Банк применяет необходимые и достаточные правовые, организационные и технические меры по обеспечению безопасности персональных данных, включающие в себя использование прошедших в установленном порядке процедур оценки соответствия средств защиты информации, обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по недопущению подобных инцидентов в дальнейшем, восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним, установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, учет машинных носителей персональных данных, а также контроль и оценку эффективности принимаемых мер по обеспечению безопасности персональных данных

6.7. Восстановление персональных данных и процесса их обработки, нарушенных по причине нештатных ситуаций, регламентируется банковским порядком обеспечения непрерывности и восстановления деятельности (План ОНиВД).

VII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.

7.1. Настоящее Положение является внутренним общедоступным документом Банка и подлежит размещению на официальном сайте Банка. Вступает в силу со дня его утверждения Советом Директоров Банка.

7.2. Настоящее Положение подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, а также по инициативе Банка.

7.3. Ответственность работников Банка, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Банка.

7.4. В целях создания и обеспечения функционирования системы организации обработки и обеспечения безопасности персональных данных с учетом положений настоящей политики Банком разрабатываются документы по защите персональных данных, о порядке обработки персональных данных, о неавтоматизированной обработке персональных данных. Данный список не является окончательным. Банк издает приказы, утверждает инструкции, составляет акты, разрабатывает необходимые внутрибанковские документы в целях соблюдения настоящего Положения.