Банк ЗЕНИТ Сочи (акционерное общество)

Приложение № 6
к приказу Председателя Правления
АО Банк ЗЕНИТ Сочи
от 28.12.2015 № 384/1-ОВ

УТВЕРЖДЕНО
Правлением АО Банк ЗЕНИТ Сочи
Протокол от 25.12.2015 № 108

ПОЛИТИКА

по обеспечению информационной безопасности банковского технологического процесса обработки персональных данных
(частная политика)

г. Сочи

Информация
о частной политике по обеспечению ИБ при организации банковского технологического процесса обработки персональных данных

Область действия документа	Обеспечение информационной безопасности при организации банковского технологического процесса обработки персональных данных
Редакция	Редакция № 1.0
Цель документа	Определение порядка организации банковского технологического процесса обработки персональных данных
Владелец документа	АО Банк ЗЕНИТ Сочи
Разработчик	ОИБ УЭБР
Структурные подразделения-пользователи	Все структурные и обособленные подразделения Банка.

Содержание

1. Общие положения

1.1. Под банковским технологическим процессом обработки персональных данных Банка подразумевается процесс обработки персональных данных (ПДн).

1.2. Настоящая Политика устанавливает требования к обеспечению информационной безопасности банковского технологического процесса обработки персональных данных.

1.3. Руководство Банка обеспечивает выполнение требований настоящей Политики путем назначения ответственного за обработку ПДн.

1.4. Руководство Банка обеспечивает контроль выполнения требований настоящей Политики в области ИБ путем назначения ответственного за обеспечение ИБ ПДн.

1.5. Руководство Банка обеспечивает выполнение требований к организации хранения машинных носителей ПДн путем назначения ответственного за организацию хранения машинных носителей ПДн.

2. Порядок идентификации ПДн

2.1. Банк определил следующий принцип отнесения данных к ПДн:

- в случае, если совокупность данных является необходимой и достаточной для идентификации субъекта ПДн, такие данные считаются персональными.
- иначе данные персональными не считаются.

2.2. На данный момент Банк осуществляет обработку следующих видов ПДн:

- ПДн клиентов;
- ПДн работников;
- ПДн соискателей;
- ПДн посетителей.

2.3. Обработка ПДн осуществляется в Банке смешанным образом с использованием автоматизированных средств обработки и без использования автоматизированных средств.

3. Порядок учета ПДн

3.1. Все идентифицированные ПДн подлежат их учету. Учет ПДн выполняется в Банке путем формирования ресурсов ПДн. Под ресурсом ПДн Банк определяет совокупность ПДн, объединенных общими целями обработки.

3.2. Каждый ресурс ПДн подлежит документированию по форме, определенной **Приложением 1**, с указанием в перечне ресурсов следующих данных:

- цели обработки ПДн;
- перечень обрабатываемых ПДн;
- сроки хранения ПДн;
- условия прекращения обработки;
- перечень ИСПДн, в которых ПДн обрабатываются;
- категория ПДн;
- количество субъектов ПДн.

3.3. Перечень ресурсов ПДн подлежит пересмотру и актуализации под контролем отдела ИБ с периодичностью не реже 1 раза в 6 месяцев, а также в каждом случае возникновения существенных изменений в порядке и способах обработки ПДн.

3.4. Все данные, указанные в перечне, анализируются при пересмотре. При этом выполняется сравнение содержания и объема обрабатываемых ПДн с установленными целями обработки, а также актуализация количества субъектов ПДн.

3.5. Для каждого ресурса ПДн Банк устанавливает частный порядок обработки ПДн и контролирует его выполнение.

3.6. Банк обеспечивает возможность ознакомления субъектов ПДн с частным порядком обработки ПДн путем размещения данного порядка в открытом для субъектов ПДн доступе.

4. Порядок учета ИСПДн

4.1. Обработка ПДн осуществляется в Банке автоматизированным и неавтоматизированным образом. Автоматизированная обработка ПДн осуществляется в автоматизированных системах.

4.2. Банк установил следующий критерий отнесения АС к ИСПДн:

- если в АС осуществляется автоматизированная обработка любого ресурса ПДн, данная АС относится к ИСПДн;
- иначе АС к ИСПДн не относится.

4.3. Банк формирует перечень ИСПДн по форме, приведенной в **Приложении 2**. В перечне ИСПДн Банк указывает следующую информацию о каждой ИСПДн:

- места хранения ПДн;
- компоненты, задействованных в обработке ПДн;
- уровень защищенности ИСПДн;
- меры защиты ПДн.

4.4. Данный перечень подлежит его пересмотру и актуализации под контролем отдела ИБ с периодичностью не реже 1 раза в 1 год, а также в случае возникновения существенных изменений в инфраструктуре Банка.

5. Порядок классификации ИСПДн

5.1. Каждая ИСПДн Банка подлежит ее классификации в соответствии с порядком, определенным Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5.2. В целях классификации ИСПДн Банк формирует комиссию по классификации и приказом назначает членов данной комиссии.

5.3. Члены комиссии на основании модели угроз и нарушителей определяют угрозы, актуальные для ИСПДн и выполняют ее классификацию.

5.4. Результаты классификации регистрируются соответствующим актом Акт определения уровня актуальных угроз (**Приложение 3**) и Акт определения уровня защищенности (**Приложение 4**).

6. Порядок работы с ТСЗИ

6.1. В целях снижения рисков ИБ ПДн, Банк использует сертифицированные по требованиям безопасности информации средств защиты информации в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

6.2. Банк составляет перечень используемых технических средств защиты информации с указанием в перечне цели применения технического средства.

6.3. Банк устанавливает требования к обеспечению доверенной поставки технических средств защиты информации в следующей комплектации:

- верифицированный дистрибутив ПО;
- формуляр с указанием контрольной суммы дистрибутива;
- специальный голографический знак соответствия.

6.4. Ответственным за обеспечение ИБ ПДн обеспечивается безопасное хранение ТСЗИ в следующей комплектации:

- сертификат ТСЗИ;
- формуляр ТСЗИ;
- дистрибутив ТСЗИ;
- эксплуатационная документация ТСЗИ;
- техническое задание на внедрение;
- стандарт конфигурирования/паспорт конфигурации.

7. Порядок предоставления доступа к ПДн

7.1. Предоставление доступа работникам к ПДн обеспечивается в соответствии с положениями *Политики по обеспечению ИБ при управлении доступом и регистрацией*. При этом, перед предоставлением работнику доступа к ПДн, служебная записка на предоставление доступа подлежит ее согласованию с работником, ответственным за обеспечение ИБ ПДн.

7.2. В Банке формируется перечень работников, имеющих доступ к ПДн.

7.3. При предоставлении работнику доступа к ПДн, данные о работнике вносятся в перечень работников, имеющих доступ к ПДн.

7.4. Перечень работников, имеющих доступ к ПДн, подлежит его утверждению руководством Банка.

7.5. Перечень работников, имеющих доступ к ПДн, подлежит его актуализации и пересмотру не реже 1 раза в 1 год с участием работника, ответственного за обеспечение ИБ ПДн.

7.6. Работникам, имеющим доступ к ПДн, предоставляется утвержденный перечень работников.

7.7. Работникам, имеющим доступ к ПДн, разрешается осуществлять передачу ПДн только работникам, указанным в перечне.

7.8. Перед предоставлением доступа к ПДн, а также не реже 1 раза в 1 год, работники, обладающие доступом к ПДн, подлежат ознакомлению с требованиями положений законодательства РФ и внутренними документами организации БС РФ, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

7.9. По результатам ознакомления, работники ставят подпись в Журнале ознакомления, содержащего следующие данные:

- перечень документов для ознакомления;
- ФИО, должность;
- дата;
- подпись.

8. Порядок учета помещений

8.1. Банк обеспечивает формирование перечня помещений, в которых осуществляется обработка ПДн.

8.2. Перечень помещений подлежит его актуализации и пересмотру не реже 1 раза в 1 год работником, ответственным за обеспечение ИБ ПДн.

8.3. Доступ работников в помещения, в которых ведется обработка, осуществляется на основании перечня работников, имеющих доступ к ПДн.

9. Порядок работы с носителями ПДн

9.1. Хранение ПДн осуществляется на бумажных и машинных носителей ПДн. При фиксации ПДн на материальных носителях обеспечивается их обособление от иной

зафиксированной на материальном носителе информации путем использования выделенных разделов материальных носителей.

9.2. ПДн, относимые к разным ресурсам ПДн, подлежат хранению на разных материальных носителях ПДн.

9.3. Все машинные носители ПДн подлежат их инвентаризации и учету. В Банке формируется перечень машинных носителей ПДн с указанием уникального идентификатора машинного носителя и категории обрабатываемых ПДн.

9.4. Перечень машинных носителей подлежит пересмотру не реже 1 раза в 1 год работником, ответственным за обеспечение ИБ ПДн.

9.5. Все машинные носители ПДн подлежат их хранению в серверной комнате Банка.

9.6. Доступ к машинным носителям ПДн разрешен лишь работникам, которым предоставлен доступ в серверную комнату Банка.

9.7. Любой вынос машинных носителей, содержащих ПДн, должен быть зафиксирован в журнале учета с указанием, как минимум, старого и нового места хранения, а также причины перемещения машинного носителя.

9.8. Любой вынос машинных носителей, содержащих ПДн, за пределы Компании, включая передачу их третьим лицам, должен утверждаться руководством Компании.

9.9. Пересылку машинных носителей ПДн следует осуществлять только доверенным курьером или иным способом, который может быть тщательно проконтролирован.

9.10. Перед осуществлением выноса машинного носителя ПДн, вся информация, содержащаяся на носителе, должна быть уничтожена в соответствии с порядком, определенным *Инструкцией по учету и выводу из обращения носителей информации*.

10. Порядок взаимодействия с РНК

10.1. Банк обеспечивает направление уведомления об обработке ПДн в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (РНК).

10.2. Ответственный за обработку ПДн обеспечивает отслеживание изменений в данных, содержащихся в уведомлении и обеспечивает направление в уполномоченный орган информации об изменениях в течении 10 дней с момента их принятия.

10.3. Ответственный за обработку ПДн в случае получения соответствующего запроса уполномоченного органа предоставляет уполномоченному органу все необходимые сведения, указанные в запросе, в течении 30 дней со дня его получения.

10.4. Ответственный за обработку ПДн в случае получения соответствующего запроса обеспечивает уточнение, блокирование или уничтожение недостоверных или полученных незаконным путем ПДн в течении 30 дней со дня его получения.

10.5. В случае возникновения такой необходимости, Банк направляет уполномоченному органу обращения субъектов ПДн, связанные с неправомерной обработкой ПДн.

11. Порядок получения согласия на обработку

11.1. Для каждого ресурса ПДн Банк определяет необходимость получения письменного согласия на обработку ПДн у субъекта ПДн.

11.2. Банк определяет необходимость получения письменного согласия у субъекта ПДн на обработку ПДн в следующих случаях:

- поручение обработки ПДн другому лицу;
- внесение ПДн в общедоступные источники;
- обработка специальных категорий ПДн;
- обработка биометрических ПДн;
- осуществление трансграничной передачи ПДн;
- обработка ПДн в целях продвижения товаров, работ, услуг;

- обработка ПДн в целях политической агитации;
- принятие решений, порождающих юридические последствия в отношении субъекта ПДн, затрагивающих его права и законные интересы.

11.3. Форма согласия на обработку ПДн и порядок его получения определяется частным порядком обработки ПДн для каждого ресурса ПДн.

12. Порядок прекращения обработки ПДн

12.1. Банк обеспечивает прекращение обработки ПДн, осуществляемой Банком или обработчиком, действующим по поручению Банка, по достижению целей обработки ПДн.

12.2. Банк обеспечивает прекращение обработки ПДн, осуществляемой Банком или обработчиком, действующим по поручению Банка, в случае выявления факта неправомерной обработки ПДн, если обеспечить правомерную обработку не представляется возможным.

12.3. Банк обеспечивает прекращение обработки ПДн, осуществляемой Банком или обработчиком, действующим по поручению Банка, в случае получения соответствующего обращения субъекта ПДн.

12.4. Прекращение обработки ПДн осуществляемой Банком, обеспечивается путем применения к ПДн процедур уничтожения либо обезличивания.

12.5. Прекращение обработки ПДн, осуществляемой обработчиком, действующим по поручению Банка, обеспечивается путем направления обработчику уведомления с требованием прекратить обработку ПДн и уведомить Банк по результатам прекращения обработки.

13. Порядок уточнения ПДн

13.1. Уточнение ПДн обеспечивается Банком в случае получения соответствующего запроса от субъекта ПДн или уполномоченного органа, а также в случае выявления неточностей в обрабатываемых ПДн субъекта.

13.2. Уточнение ПДн, обрабатываемых в АС обеспечивается путем внесения изменений в обрабатываемые ПДн с использования встроенных функциональных возможностей АС.

13.3. Уточнение ПДн, обрабатываемых на бумажном носителе, обеспечивается путем формирования нового бумажного носителя с уточненными данными. При этом старый носитель подлежит его уничтожению.

13.4. Внесение изменений в ПДн обеспечивается с использованием данных, указанных субъектом ПДн в обращении субъекта, или путем предоставления субъектом этих данных при личном посещении Банка.

13.5. Банк обеспечивает направление субъекту соответствующего запроса на уточнение в случае необходимости получения точных данных.

14. Порядок блокирования ПДн

14.1. Банк обеспечивает блокирование ПДн в каждом случае разбирательства по фактам неправомерной обработки ПДн.

14.2. Банк обеспечивает блокирование ПДн в каждом случае невозможности выполнения уничтожения ПДн и обезличивание ПДн в установленные нормативно либо законодательно сроки. При этом, Банк осуществляет блокирование ПДн на срок, не превышающий 6 месяцев с последующим уничтожением заблокированных ПДн.

14.3. Банк осуществляет блокирование ПДн путем обеспечения технического или организационного запрета редактирования, использования и распространения ПДн. Технический запрет реализуется встроенными функциональными возможностями АС. Организационный запрет организуется путем издания и доведения до работника соответствующего указа.

14.4. Блокирование ПДн, содержащихся на отдельных носителях ПДн, выполняется путем ограничения доступа к данному носителю.

14.5. По результатам блокирования подлежит заполнению Акт об уничтожении (блокировании) ПДн (**Приложение 5**).

15. Порядок уничтожения ПДн

15.1. Банк осуществляет уничтожение ПДн при достижении целей обработки ПДн в течении 30 дней со дня достижения цели, или передает ПДн на архивное хранение в случае, если архивное хранение ПДн требуется для выполнения требований законодательства РФ.

15.2. В случае, если уничтожение ПДн не представляется возможным, Банк осуществляет затирание части ПДн в целях невозможности идентификации по оставшимся данным субъекта ПДн.

15.3. Гарантированное уничтожение ПДн с бумажных носителей осуществляется путем уничтожения бумажного носителя.

15.4. Гарантированное уничтожение ПДн с электронных носителей осуществляется в соответствии с *Инструкцией по учету и выводу из обращения носителей информации*.

15.5. По результатам уничтожения подлежит заполнению Акт об уничтожении (блокировании) ПДн (**Приложение 5**).

16. Права и обязанности

16.1. Ответственным работникам вверяется в обязанность обеспечение выполнения положений настоящей Политики.

16.2. Ответственные работники назначаются руководством Банка всеми необходимыми полномочиями для выполнения требований настоящей Политики.

16.3. Ответственные работники имеют право обращаться к другим работникам Банка с целью обеспечения выполнения требований настоящей Политики.

16.4. Работники Банка обязаны выполнять требования ответственных работников, касающиеся выполнения требований настоящей Политики и несут ответственность за их выполнение.

16.5. Ответственные работники имеют право вносить предложения, по применению дисциплинарных и иных взысканий по отношению к работникам, не соблюдающим требования положений настоящей Политики.

17. Записи о результатах выполнения

Настоящая Политика порождает следующие записи, свидетельствующие о ее выполнении:

Таблица 17-1. Записи о выполнении

№	Название и содержание записи	Момент внесения записи	Место хранения
1	**Перечень ресурсов ПДн** Цель обработки ПДн; Перечень обрабатываемых ПДн; Сроки хранения ПДн; Условия прекращения обработки; Перечень ИСПДн, в которых ПДн обрабатываются;	– При выявлении новых ресурсов – Не реже 1 раза в 1 год	ОИБ УЭБР

№	Название и содержание записи	Момент внесения записи	Место хранения
	Категория ПДн; Количество субъектов ПДн.		
2	**Перечень ИСПДн:** Места хранения ПДн; Компоненты, задействованные в обработке; Уровень защищенности ИСПДн; Меры защиты ПДн.	– При выявлении новых ИСПДн – Не реже 1 раза в 1 год	ОИБ УЭБР
3	**Акт определения уровня актуальных угроз**	– При классификации ИСПДн	ОИБ УЭБР
4	**Акт определения уровня защищенности**	– При классификации ИСПДн	ОИБ УЭБР
5	**Перечень ТСЗИ:** Информация о ТСЗИ; Срок действия лицензии; Цель использования.	– При приобретении ТСЗИ – Не реже 1 раза в 1 год	ОИБ УЭБР
6	**Приказ о назначении ответственного за обработку ПДн**	– При назначении ответственного и его смене	Аппарат управления
7	**Приказ о назначении ответственного за обеспечение ИБ ПДн**	– При назначении ответственного и его смене	Аппарат управления
8	**Приказ о назначении ответственного за организацию хранения машинных носителей ПДн**	– При назначении ответственного и его смене	Аппарат управления
9	**Приказ о создании комиссии по классификации ИСПДн**	– При классификации ИСПДн	Аппарат управления
10	**Комплектация ТСЗИ:** Сертификат ТСЗИ; Формуляр ТСЗИ; Дистрибутив ТСЗИ; Эксплуатационная документация ТСЗИ; Техническое задание на внедрение; Стандарт конфигурирования/паспорт конфигурации.	– При приобретении ИСПДн	УА ОИБ УЭБР
11	**Перечень работников, имеющих доступ к ПДн:** ФИО, должность; Отметка об утверждении.	– При предоставлении доступа к ИСПДн – Не реже 1 раза в 1 год	ОИБ УЭБР
12	**Журнал ознакомления:** Перечень документов для ознакомления; ФИО, должность; Дата; Подпись.	– При предоставлении доступа к ПДн – Не реже 1 раза в 1 год	ОИБ УЭБР

№	Название и содержание записи	Момент внесения записи	Место хранения
13	**Перечень помещений, в которых осуществляется обработка ПДн**	– Не реже 1 раза в 1 год	ОИБ УЭБР
14	**Перечень машинных носителей ПДн:** Идентификатор носителя; Категория обрабатываемых ПДн.	– При вводе, выводе из эксплуатации и перемещении носителя – Не реже 1 раза в 1 год	ОИБ УЭБР
15	**Уведомление об обработке ПДн**	– Перед осуществлением обработки ПДн; – При изменении сведений, содержащихся в уведомлении.	ОИБ УЭБР
16	**Акт об уничтожении (блокировании) ПДн**	– В каждом случае уничтожения (блокирования) ПДн	ОИБ УЭБР

Приложение 1

Перечень ресурсов ПДн, обрабатываемых в АО «Банк ЗЕНИТ Сочи»

Таблица 1. <Название ресурса>

Название ресурса:	
Цель обработки ПДн:	•
Обрабатываемые данные:	•
Категория ПДн:	•
Количество субъектов ПДн:	•
Срок хранения ПДн:	•
Условие прекращения обработки ПДн:	•
Используемые ИСПДН:	•
Необходимость письменного согласия субъекта:	•

Приложение 2

Перечень ИСПДн АО «Банк ЗЕНИТ Сочи»

Таблица 1. <Название ИСПДн>

Название:	
Краткое описание:	
Цель обработки ПДн:	•
Обрабатываемые данные:	•
Категория ПДн:	•
Категория субъектов ПДн:	•
Количество субъектов ПДн:	•
Тип актуальных угроз	•
Необходимый уровень защищенности ПДн:	•
Срок обработки ПДн:	•
Используемые АС:	•
Места хранения ПДН:	•
Компоненты ИСПДн:	•
Меры защиты:	•

Приложение 3

«Утверждаю»
Председатель Правления
_____ И.Н.Сосин

«____» _____ г.

Акт определения уровня актуальных угроз

_____

(наименование информационной системы персональных данных)

В соответствии с порядком определения уровня актуальных угроз, утвержденным Постановлением Правительства РФ от 1 ноября 2012 года №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" комиссия в составе:

Роль	ФИО	Должность
Председатель:		
Члены комиссии:		

Изучив актуальную модель угроз информационной безопасности Компании, решила признать неактуальными угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе персональных данных Компании, и определить информационной системе персональных данных

_____

(наименование информационной системы персональных данных)

3 (третий) уровень актуальных угроз.

Председатель комиссии:

Члены комиссии:

Приложение 4

«Утверждаю»
Председатель Правления
_____ И.Н.Сосин

«____» _____ г.

Акт определения уровня защищенности

_____

(наименование информационной системы персональных данных)

Рассмотрев следующие исходные данные на информационную систему персональных данных:

Критерий классификации	Значение критерия
Категория обрабатываемых персональных данных:	• Специальные • Биометрические • Общедоступные • Иные
Объем обрабатываемых персональных данных:	☐ < 100000 субъектов ПДн ☐ > 100000 субъектов ПДн
Категория субъектов ПДн:	• Сотрудники • Клиенты
Тип актуальных угроз:	• 1 тип • 2 тип • 3 тип

в соответствии с порядком определения уровня защищенности, утвержденным Постановлением Правительства РФ от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» комиссия в составе:

Роль	ФИО	Должность
Председатель:		
Члены комиссии:		

решила установить информационной системе персональных данных:

(наименование информационной системы персональных данных)

необходимость обеспечения **3 (третьего)** уровня защищенности персональных данных при их обработке в этой информационной системе.

Председатель комиссии:

Члены комиссии:

Приложение 5

«Утверждаю»
Председатель Правления
_____ И.Н.Сосин

«____» _____ г.

АКТ
об уничтожении (блокировании) персональных данных

Произведя отбор следующих персональных данных (носителей персональных данных):

№ п/п	Наименование носителя	Номер носителя	ФИО субъекта ПДн	Причина

Комиссия в составе:

Роль	ФИО	Должность
Председатель:		
Члены комиссии:		

Установила, что данные подлежат:

- уничтожению
- блокированию до дд.мм.гггг
- блокированию с последующим уничтожением дд.мм.гггг

Председатель комиссии:

Члены комиссии:

Данные заблокированы/уничтожены

Блокировка/уничтожение выполнено следующим способом:

Блокировку/уничтожение выполнил: