БАНК РОССИИ
АССОЦИАЦИЯ РОССИЙСКИХ БАНКОВ
АССОЦИАЦИЯ РЕГИОНАЛЬНЫХ БАНКОВ РОССИИ (АССОЦИАЦИЯ «РОССИЯ»)

Методические рекомендации

по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации

(на основе комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»)

2010

Содержание

I. Введение

В Банк России, Ассоциацию российских банков и Ассоциацию региональных банков России (Ассоциацию «Россия») поступают многочисленные обращения организаций банковской системы Российской Федерации (БС РФ) по вопросу применения положений Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»). Банками отмечается, что выполнение норм Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных является крайне важной задачей и способствует защите интересов граждан.

С целью выполнения в организациях банковской системы Российской Федерации (далее - БС РФ) требований Федерального закона "О персональных данных" и требований (рекомендаций) Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор), Федеральной службы безопасности Российской Федерации (далее – ФСБ России) и Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) Центральный банк Российской Федерации при участии Роскомнадзора, ФСБ России, ФСТЭК России (далее – Регуляторы, если по смыслу не требуется детализация), Ассоциации российских банков (далее - АРБ) и Ассоциации региональных банков России (Ассоциации «Россия») разработал отраслевые документы по приведению организаций БС РФ в соответствие с требованиями законодательства в области персональных данных. Эти документы включают:

1. Четыре документа, входящие в комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» (далее – Комплекс БР ИББС):

- Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации» (РС БР ИББС-2.4) (далее – Отраслевая модель угроз).

- Доработанные в части требований по обработке и обеспечению безопасности персональных данных в соответствии с Отраслевой моделью угроз стандарты Банка России отраслевого применения СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (далее - стандарт Банка России СТО БР ИББС-1.0) и СТО БР ИББС-1.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».

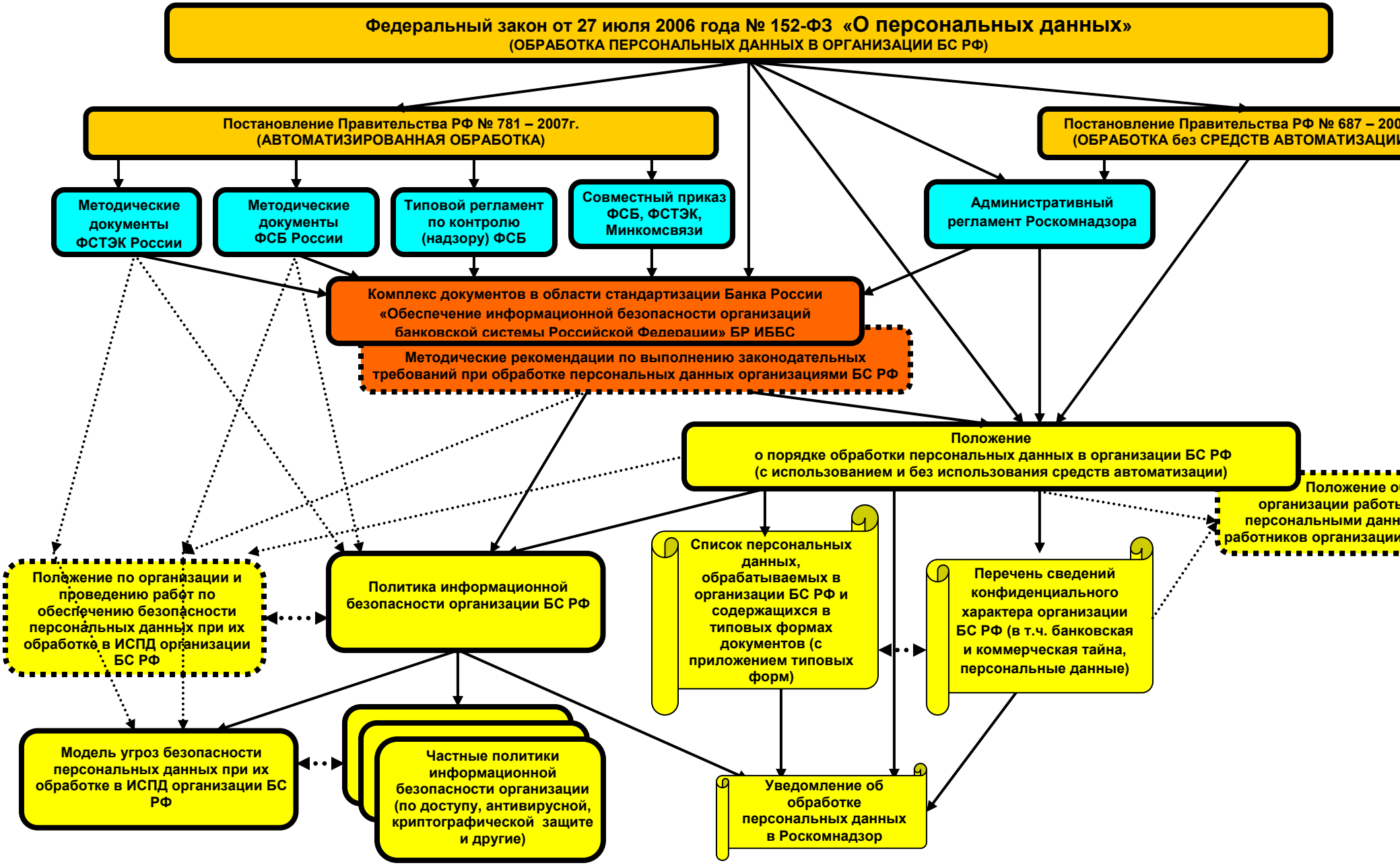
- Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации» (далее – рекомендации в области стандартизации Банка России РС БР ИББС-2.3).

2. Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях БС РФ (далее – Методические рекомендации).

Методические рекомендации разработаны Ассоциацией российских банков и Ассоциацией региональных банков России (Ассоциацией «Россия») совместно с Банком России для обеспечения методической поддержки применения организациями БС РФ Комплекса БР ИББС.

Место вышеуказанной документации показано на примерной структурной схеме документационного обеспечения выполнения законодательных требований при обработке персональных данных в организациях БС РФ (Рис.1).

Рис 1 Примерная структурная схема верхних уровней документационного обеспечения выполнения законодательных требований при обработке персональных данных в организации БС РФ



II. Общие положения

Отраслевая модель угроз разработана на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», рекомендованной ФСТЭК России, и содержит перечень угроз безопасности персональным данным, актуальных для организаций БС РФ.

Стандарты Банка России Банка России позволяют обеспечить защиту персональных данных, обрабатываемых как в информационных системах персональных данных (ИСПДн), т.е. в системах, целью создания которых является обработка персональных данных и к защите которых требования и рекомендации по обеспечению безопасности персональных данных предъявляют ФСБ России и ФСТЭК России, так и в иных автоматизированных банковских системах, в которых персональные данные обрабатываются совместно с информацией, защищаемой в соответствии с требованиями, установленными для этой информации (режим защиты сведений, составляющих банковскую тайну, коммерческую тайну и др.).

При введении Стандартов Банка России в организации БС РФ приказом требования по получению лицензий на деятельность по технической защите конфиденциальной информации и требования аттестации ИСПДн не являются обязательными (в соответствии с пунктом 9.6 СТО БР ИББС-1.0-2010).

В случае применения организацией БС РФ для обеспечения безопасности персональных данных шифровальных (криптографических) средств защиты информации (далее - СКЗИ), организации БС РФ обязаны получать лицензии ФСБ России в соответствии с законодательством Российской Федерации.

Рекомендации содержат набор практик, способствующих выполнению в организациях БС РФ требований Стандартов Банка России и тем самым – выполнению требований Федерального закона «О персональных данных», а также требований и рекомендаций Регуляторов.

III. Особенности и ограничения

В соответствии с Федеральным законом от 27 декабря 2002г. № 184-ФЗ «О техническом регулировании» все стандарты носят рекомендательный характер.

Вместе с тем, в случае введения их в организации БС РФ приказом, стандарты принимают статус документов, обязательных для выполнения в этой организации. В этом случае организация БС РФ добровольно принимает на себя обязательство внедрить Стандарты Банка России, оценить соответствие организации БС РФ его требованиям (с использованием стандарта Банка России СТО БР ИББС-1.2) и официально подтвердить это, направив в адрес Банка России и территориальных органов Регуляторов – Роскомнадзора, ФСТЭК России, ФСБ России (в пределах их полномочий) «Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0».

Если организация БС РФ не вводит Стандарты Банка России приказом, то ее деятельность при обработке персональных данных подлежит оценке при осуществлении надзора и контроля уполномоченными государственными органами на соответствие требованиям нормативных документов Регуляторов в области персональных данных, без учета отраслевых особенностей банковской сферы деятельности, отраженных в Комплексе БР ИББС.

IV. Программа действий по приведению организации БС РФ в соответствие с требованиями Федерального закона «О персональных данных»

1. Принятие решения о присоединении или не присоединении к Стандартам Банка России. Подготовка и выпуск приказа.

2. Создание комиссии по приведению организации БС РФ в соответствие с требованиями Федерального закона «О персональных данных». Указанная комиссия будет координировать работы по приведению организации БС РФ в соответствие с требованиями Стандартов Банка России и настоящих рекомендаций и по проведению самооценки.

3. Разработка плана по приведению организации БС РФ в соответствие с требованиями Федерального закона «О персональных данных» (в соответствие с требованиями Стандартов Банка России).

4. Формирование перечня обрабатываемых персональных данных, а также формулирование целей и оснований для обработки этих данных.

5. Определение и выработка условий и принципов обработки персональных данных в организации БС РФ.

6. Составление перечня систем организации БС РФ, в которых обрабатываются персональные данные. Выделение ИСПДн и проведение их классификации.

7. Принятие решения о вводе в действие в организации БС РФ Отраслевой модели угроз. Разработка, в случае необходимости, собственной частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных организации БС РФ.

8. Оценка возможности обезличивания персональных данных. Проведение обезличивания. Проведение, в случае необходимости, повторной классификации ИСПДн.

9. Оценка существующих защитных мер на предмет соответствия требованиям Стандартов Банка России.

10. Решение вопроса о выделении необходимых материальных, кадровых и финансовых ресурсов для реализации мероприятий, предусмотренных планом мероприятий.

11. Реализация плана, включая выпуск необходимых документов. Доработка уже существующих документов с целью их соответствия требованиям Федерального закона «О персональных данных».

12. Проведение контроля в форме:

- Оценки соответствия организации БС РФ положениям стандарта Банка России СТО БР ИББС-1.0-2010 внешней организацией (аудита).
- Самооценки соответствия организации БС РФ положениям стандарта Банка России СТО БР ИББС-1.0-2010.

13. Выпуск документа о подтверждении соответствия организации БС РФ требованиям стандарта Банка России СТО БР ИББС-1.0 с указанием соответствия в целом и по направлениям Регуляторов - Роскомнадзора, ФСБ России и ФСТЭК России (в пределах их полномочий).

14. Направление этого документа в адрес Банка России и территориальных органов Регуляторов (по готовности, но не позже 31 декабря 2010 года, в дальнейшем – один раз в три года).

V. Комментарии к программе действий

а. Создание комиссии по приведению организации БС РФ в соответствие с требованиями Федерального закона «О персональных данных» (пункт 2 программы действий)

Перед началом работ по приведению организации БС РФ в соответствие с требованиями Федерального закона «О персональных данных» организационно-распорядительным порядком создается комиссия, на которую

будет возлагаться реализация приведенных выше этапов. В состав данной комиссии входят представители юридического подразделения, подразделений общей и информационной безопасности, подразделений информатизации (разработки и обеспечения банковских технологий и обработки информации), кадровой службы (отдела кадров), управления делами (делопроизводства), подразделений по работе с клиентами (физическими лицами), а также представители других структурных подразделений, имеющих непосредственное отношение в организации БС РФ к сфере действия Федерального закона «О персональных данных».

Целесообразно, чтобы председатель комиссии был одновременно назначен ответственным за выполнение законодательных требований при обработке персональных данных в организации БС РФ.

Одной из задач комиссии является классификация информационных систем персональных данных.

После выполнения плана по приведению организации БС РФ в соответствие требованиям Федерального закона «О персональных данных» рекомендуется продолжить работу комиссии на постоянной основе.

b. Разработка плана по приведению в соответствие (пункт 3 программы действий)

Все этапы программы действий (кроме первого) могут быть детализированы в поэтапном плане по приведению организации БС РФ в соответствие с требованиями Федерального Закона «О персональных данных».

Данный поэтапный план утверждается с указанием конкретных сроков реализации каждого этапа.

c. Типовой перечень персональных данных (пункт 4 программы действий)

В организации БС РФ рекомендуется сформировать перечень персональных данных с указанием целей и сроков их обработки (в т.ч. и хранения). Это позволит облегчить решение ряда задач, например:

разработка положения о защите персональных данных и иной организационно-распорядительной документации в области обработки персональных данных;

планирование и реализация мероприятий по защите персональных данных;

разработка уведомления в Роскомнадзор;

реагирование на запросы субъектов персональных данных.

При составлении Перечня персональных данных организация БС РФ может воспользоваться примерным перечнем, приведенным в Приложении 3.

При составлении перечня персональных данных, обрабатываемых организацией БС РФ, важно определить цели и сроки такой обработки. Например, если для регистрации паспортных данных посетителей организации БС РФ выбрана цель - «однократный проход посетителей на территорию организации БС РФ», то покидание посетителем организации БС РФ приводит к необходимости уничтожения зафиксированных персональных данных. Этого требует Федеральный закон «О персональных данных», так как по достижению цели обработки персональные данные должны быть уничтожены. Это пример некорректно выбранной цели. Теперь приведем пример некорректно выбранного срока хранения персональных данных. Если во внутренних документах организации БС РФ написано, что «хранение персональных данных персонала организации БС РФ осуществляется в течение срока действия трудового договора», то организация БС РФ может столкнуться с ситуацией, когда персональные данные уволенного работника должны быть удалены, а сделать это невозможно, так как эти данные должны быть использованы при предоставлении отчетности в органы Федеральной налоговой службы, Пенсионный Фонд Российской Федерации, Фонд обязательного медицинского страхования и т.п. С целью упрощения определения целей и сроков обработки персональных данных организация БС РФ может воспользоваться формулировками, приведенными в Перечне персональных данных, обрабатываемых организацией БС РФ (Приложение 3).

Данный этап также позволит выделить персональные данные, которые потребуют особых условий обработки – видео и фотоизображения человека, геометрия руки и дактилоскопия, голосовые данные в центрах обработки вызовов и т.п.

При наличии в организации БС РФ утвержденного Перечня сведений конфиденциального характера допускается включить в него новый пункт – «персональные данные» (вместо разработки и утверждения отдельного Перечня обрабатываемых персональных данных). Это позволит легитимным образом распространить уже существующие режимы конфиденциальности, а

также разработанную по этим вопросам нормативно-распорядительную документацию, и на обрабатываемые в организации БС РФ персональные данные.

При обработке персональных данных клиентов организации БС РФ рекомендуется минимизировать обработку персональных данных, отнесенных Федеральным законом «О персональных данных» (статья 10) к специальным категориям персональных данных.

d. Классификация ИСПДн (пункт 6 программы действий)

В связи с тем, что согласно статье 19 Федерального закона «О персональных данных» операторы обязаны защитить персональные данные от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий, то все ИСПДн организации БС РФ относятся к категории специальных в соответствии с пунктом 8 Порядка проведения классификации информационных систем персональных данных, утвержденного приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

Автоматизированные системы, в которых обрабатываются персональные данные, но целью работы которых не является обработка персональных данных, включаются в перечень систем, обрабатывающих персональные данные, но не классифицируются как ИСПДн.

По результатам классификации ИСПДн составляется Акт классификации.

e. Разработка частной модели угроз (пункт 7 программы действий)

В соответствии с пунктом 16 Порядка проведения классификации информационных систем персональных данных, утвержденного приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля

2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» для специальных информационных систем персональных данных должна быть разработана модель угроз безопасности персональных данных.

В качестве модели угроз безопасности персональных данных при их обработке в ИСПДн организация БС РФ может использовать Отраслевую модель угроз, содержащую актуальные угрозы безопасности персональных данных при обработке в ИСПДн организаций БС РФ (применительно к большинству организаций БС РФ) и согласованную с Регуляторами.

В случае необходимости, в организации БС РФ может быть составлена частная модель угроз безопасности персональных данных при их обработке в ИСПДн организации БС РФ (далее – частная модель угроз), учитывающая особенности обработки персональных данных в конкретной организации БС РФ.

В качестве методики выбора актуальных для организации БС РФ угроз и последующего составления частной модели угроз используются рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 «Обеспечение информационной безопасности организаций БС РФ. Методика оценки рисков нарушения информационной безопасности.

f. Оценка возможности обезличивания персональных данных (пункт 8 программы действий)

Персональные данные, обрабатываемые в ИСПДн, можно обезличить с целью понижения уровня требований по обеспечению безопасности. Согласно Федеральному закону «О персональных данных» обезличивание – это действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Полностью обезличить все персональные данные невозможно – в информационных системах всегда будут присутствовать технические средства (например, автоматизированные рабочие места операционистов или принтеры), на которых будет происходить процесс, обратный обезличиванию, - для целей сверки данных, печати на принтере, отправки по электронной почте и т.п.

На основе анализа национальных и международных стандартов[1] может быть составлен следующий список алгоритмов обезличивания персональных данных (см. Таблица 1).

[1] NIST SP800-122 «Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)», BS10012:2009 «Data protection – Specification for a personal information management system», ISO 25237:2008 «Health informatics – Pseudonymization»

Таблица 1. Алгоритмы обезличивания персональных данных (ПДн)

Алгоритм обезличивания	Описание	Примечание
Абстрагирование ПДн	Сделать ПДн менее точными путем группирования общих или непрерывных характеристик	Например, вместо указания конкретного возраста использовать кодификаторы (18-25 лет – 2, 26-33 года – 3 и т.д.)
Скрытие ПДн	Удалить все или часть записи ПДн, не требуемой для деятельности кредитной организации	
Внесение шума в ПДн	Добавить небольшое количество посторонней информации в ПДн	
Замена ПДн	Переставить поля одной записи ПДн с теми же самыми полями другой аналогичной записи	
Замена данных средним значением	Заменить выбранные данные средним значением для группы ПДн	
Разделение ПДн на части	Использование таблиц перекрестных ссылок	Например, вместо одной таблицы использовать две – одна с ФИО и идентификатором субъекта ПДн, вторая – с тем же идентификатором субъекта ПДн и остальной частью ПДн
Использование специальных алгоритмов	Маскирование ПДн или подмена определенных символов другими	
Использование алгоритмов криптографического преобразования	Хэширование или шифрование	

g. Реализация плана и документирование процесса обработки персональных данных (пункт 11 программы действий)

Обеспечение безопасности персональных данных осуществляется в соответствии с доработанными для использования в целях защиты персональных данных и согласованными с Регуляторами Стандартами Банка России.

Организация работ по обработке и обеспечению безопасности персональных данных сопровождается разработкой различных документов в соответствии с требованиями федерального законодательства, требованиями и рекомендациями Регуляторов. Эти документы разрабатываются в организации БС РФ и предъявляются Регуляторам в случае проведения ими контроля и надзора за соответствием обработки персональных данных законодательным требованиям. Примерный перечень документов приведен в Таблице 2, типовые шаблоны части этих документов приведены в приложениях к данным рекомендациям.

Таблица 2. Перечень документов

№ п/п	Документ	Ссылка*	Примечание
1	Приказ о создании комиссии по приведению организации БС РФ в соответствие с требованиями Федерального закона «О персональных данных».	Раздел V пункт a Рекомендаций	Одной из задач комиссии является классификация информационных систем персональных данных. Шаблон документа – в Приложении 1
2	План по приведению организации БС РФ в соответствие требованиям Федерального закона «О персональных данных».	Раздел V пункт b Рекомендаций	В Приложении 2 приведен пример такого плана
3	Перечень персональных данных, обрабатываемых организацией БС РФ в своей деятельности.	Раздел V пункт c Рекомендаций	В Приложении 3 приведен примерный перечень, который может быть скорректирован (сокращен или дополнен) в зависимости от специфики деятельности организации БС РФ
4	Приказ о назначении ответственного за обеспечение безопасности персональных данных (структурного подразделения или должностного лица).	Пункт 13 Постановления Правительства № 781 Приказ ФСТЭК	Шаблон документа – в Приложении 4. Допускается возложение ответственности на существующее в организации БС РФ подразделение (например, на службу безопасности) с внесением изменений в Положение о данном структурном подразделении.
5	Список лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей.	Пункт 14 Постановления Правительства № 781	Возможно существование перечня (списка) в электронном виде, при условии предоставления работникам прав доступа в ИСПДн только на основании распорядительного документа в документально зафиксированном в организации БС РФ порядке. В случае необходимости (в частности, перед проведением проверок) может быть распечатан на бумажный носитель в виде базы пользователей, например, Active Directory или определенной ИСПДн.

6	Список систем, в которых обрабатываются персональные данные.	Раздел V пункт d Рекомендаций	Шаблон документа – в Приложении 5
7	Акт классификации информационных систем персональных данных организации БС РФ.	Пункт 18 Приказа Раздел V пункт d Рекомендаций	Шаблон документа – в Приложении 6
8	Заключение о возможности эксплуатации средств защиты информации.	Пункт 12 Постановления Правительства № 781	Шаблон документа – в Приложении 7. Заключение составляется по результатам проверки готовности средств защиты информации к использованию. Допускается издание актов ввода в эксплуатацию АБС, в состав которых входят средства и системы защиты информации.
9	Политика информационной безопасности организации БС РФ, в части разделов, касающихся обеспечения безопасности персональных данных.	Постановление Правительства № 781 Пункт 16 Приказа Регламент ФСБ Документы ФСБ Приказ ФСТЭК	1. Разрабатывается на основе положений стандарта Банка России СТО БР ИББС-1.0-2010 2. Включаются требования: - по обеспечению безопасности персональных данных в организации БС РФ как при обработке персональных данных в ИСПДн, так и вне ИСПДн; - (в случае использования СКЗИ) по обеспечению безопасности персональных данных при помощи СКЗИ; - по хранению носителей персональных данных; - организации допуска и защиты помещений, в которых обрабатываются персональные данные; - и др. 3. Может быть единым документом (политика информационной безопасности организации БС РФ, включающая разделы, касающиеся обеспечения безопасности персональных данных) или комплектом документов (набор частных политик, включающих разные аспекты обеспечения безопасности персональных данных)
10	План проведения контроля (как внутреннего	Пункт 12	1. Разрабатывается на основе положений

	контроля, так и контроля с привлечением внешних независимых проверяющих организаций) обеспечения безопасности персональных данных.	Постановления Правительства № 781	стандарта Банка России СТО БР ИББС-1.0-2010 2. Включает, в частности, контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.
11	Документы, подтверждающие постановку на учет средств защиты информации, применяемых в организации БС РФ для обеспечения безопасности персональных данных.	Пункт 12 Постановления Правительства № 781	Такими документами могут, в частности, являться справки о постановке на балансовый учет
12	Журнал учета носителей персональных данных.	Пункт 12 Постановления Правительства № 781	Шаблон документа – в Приложении 8. Журнал нумеруется, брошюруется, скрепляется печатью и подписывается работником, на которого возложены соответствующие обязанности
13	Эксплуатационная и техническая документация на средства и системы защиты информации.	Пункт 12 Постановления Правительства № 781	Предоставляется разработчиком или поставщиком средств и систем защиты информации Является описанием системы защиты персональных данных
14	Частная модель угроз безопасности персональных данных в организации БС РФ.	Пункт 12 Постановления Правительства № 781 Пункт 16 Приказа Регламент ФСБ Документы ФСБ Приказ ФСТЭК	См Раздел V пункт е Рекомендаций
15	Уведомление об обработке персональных данных.	Статья 22 Закона Пункт 64.1.1 регламента Роскомнадзора	Типовая форма уведомления и рекомендации по ее заполнению на официальном интернет-сайте Роскомнадзора www.rsoc.ru
16	Положение о порядке обработки персональных данных.	Пункты 64.1.5, 64.1.7 регламента Роскомнадзора	1. Разрабатывается на основе положений раздела 7.10 стандарта Банка России СТО БР ИББС-1.0-2010. 2. Содержит в том числе: порядок и условия обработки специальных категорий и

			биометрических персональных данных, порядок и условия трансграничной передачи персональных данных, порядок обработки персональных данных, осуществляемой без использования средств автоматизации (если такая обработка есть в организации БС РФ).
17	Документ, определяющий процедуру допуска работников организации БС РФ к работе с персональными данными.	Пункт 67.1 регламента Роскомнадзора	Такими документами могут быть, например, утвержденная процедура допуска, распорядительные документы организации БС РФ и т.п.
18	Должностные регламенты/инструкции лиц, имеющих доступ и (или) осуществляющих обработку персональных данных.	Пункт 67.1 регламента Роскомнадзора	Могут быть написаны явно или содержаться в иных документах, устанавливающих права, полномочия и обязанности работников организации БС РФ, имеющих доступ к информации, защищаемой в соответствии с действующим законодательством
19	Типовые формы документов, содержащие персональные данные.	Пункт 67.1 регламента Роскомнадзора	Под типовой формой документа понимается шаблон, бланк документа или другая унифицированная форма документа, разрабатываемая организацией с целью сбора ПДн. Требования к типовым формам установлены Постановлением Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"
20	Журналы (реестры, книги), содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию организации БС РФ, или в иных аналогичных целях.	Пункт 67.1 регламента Роскомнадзора	Требования к ведению установлены Постановлением Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" Шаблон журнала разовых пропусков – в

			Приложении 9. Журнал может вестись как в бумажном, так и в электронном виде. В случае ведения журнала в электронном виде в конце установленного периода времени журнал распечатать, пронумеровать, сброшюровать, скрепить печатью и подписать работником, на которого возложены соответствующие обязанности
21	Договоры с субъектами персональных данных	Пункт 67.1 регламента Роскомнадзора	
22	Типовая форма письменного согласия субъектов персональных данных на обработку их персональных данных.	Пункт 64.1.4 регламента Роскомнадзора	Шаблон документа – в Приложении 10
23	Документы, содержащие письменные согласия субъектов персональных данных на обработку их персональных данных.	Пункт 64.1.4 регламента Роскомнадзора	Письменные согласия получает организация БС РФ в установленных законодательством случаях от клиентов и работников организации БС РФ, от их родственников, и других субъектов, персональные данные которых обрабатывает организация БС РФ
24	Журналы (книги) учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных организацией БС РФ.	Пункт 67.1 регламента Роскомнадзора	Шаблон документа – в Приложении 11 Журналы могут вестись как в бумажном, так и в электронном виде. В случае ведения журнала в электронном виде в конце установленного периода времени журнал распечатать, пронумеровать, сброшюровать, скрепить печатью и подписать работником, на которого возложены соответствующие обязанности
25	Акт об уничтожении персональных данных субъекта(ов) персональных данных (в случае достижения цели обработки).	Пункт 64.1.6 регламента Роскомнадзора	Шаблон документа – в Приложении 12
26	Документы, содержащие свидетельства выполнения организацией предписаний об	Пункт 64.1.3 регламента Роскомнадзора	1. В том случае, если ранее проводились проверки.

	устранении ранее выявленных нарушений законодательства Российской Федерации в области персональных данных.		2. Примерами таких документов могут быть планы устранения выявленных нарушений и свидетельства выполнения выявленных нарушений
27	Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-2010	Разделы III и IV Рекомендаций	Шаблон документа – в Приложении 13

В случае использования организацией БС РФ для обеспечения безопасности персональных данных средств криптографической защиты информации (СКЗИ) помимо определенных выше документов разрабатываются следующие документы:

28	Акты ввода СКЗИ в эксплуатацию. Документы, содержащие описание соответствия размещения и монтажа СКЗИ требованиям документации на СКЗИ.	Регламент ФСБ Документы ФСБ	Допускается не составлять акты ввода СКЗИ в эксплуатацию. При этом составляется заключение о возможности эксплуатации СКЗИ (по результатам проверки готовности СКЗИ к использованию и соответствия размещения, монтажа и настроек СКЗИ требованиям документации на СКЗИ). Шаблон документа – в Приложении 7. Допускается издание актов ввода в эксплуатацию АБС, в состав которых входят СКЗИ.
29	Журнал поэкземплярного учета СКЗИ.	Регламент ФСБ Документы ФСБ	Шаблон документа – в Приложении 14
30	Порядок организации контроля за соблюдением условий использования СКЗИ.	Регламент ФСБ Документы ФСБ	Может быть написан явно или содержаться в Методике внутреннего контроля безопасности организации БС РФ
31	Договора на приобретение СКЗИ организации БС РФ (купли-продажи, обмена).	Регламент ФСБ Документы ФСБ	
32	Лицензии и сертификаты на используемые СКЗИ (или разрешения ФСБ на использования СКЗИ).	Регламент ФСБ Документы ФСБ	
33	Эксплуатационная документация на СКЗИ.	Регламент ФСБ Документы ФСБ	Предоставляется разработчиком или поставщиком средств и систем защиты

			информации
34	Приказ о назначении лиц (пользователей СКЗИ), допущенных к работе с ключами СКЗИ.	Регламент ФСБ Документы ФСБ	Шаблон документа – в Приложении 15
35	Документы, подтверждающие функциональные обязанности работников организации БС РФ.	Регламент ФСБ Документы ФСБ	Должностные инструкции и регламенты.
36	Документы, подтверждающие прохождение обучения работников организации БС РФ.	Регламент ФСБ Документы ФСБ	Сертификаты, справки, отчеты и др.
37	Журнал учета криптографических ключей.	Регламент ФСБ Документы ФСБ	Шаблон документа – в Приложении 16
38	Акт о комиссионном уничтожении криптографических ключей.	Регламент ФСБ Документы ФСБ	Шаблон документа – в Приложении 17

*** В столбце приведены сокращенные названия документов:**

1. Рекомендации – Рекомендации по выполнению законодательных требований при обработке персональных данных в организации БС РФ.
2. Закон - Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных"
3. Постановление Правительства № 781 - Постановление Правительства РФ от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"
4. Приказ - Приказ Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных"
5. Приказ ФСТЭК – Приказ федеральной службы по техническому и экспортному контролю от 5 февраля 2010 года № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»
6. Документы ФСБ - «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утверждены Руководством 8 Центра ФСБ России 21 февраля 2008 года)
7. Регламент ФСБ - Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утвержден Руководством 8 Центра ФСБ России 08 августа 2009 года № 149/7/2/6-1173)

8. Регламент Роскомнадзора - Административный регламент проведения проверок Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных (утвержден приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций № 630 от 01.12.2009 года).

Приложение 1

ПРИКАЗ

О создании комиссии по приведению

_____
(наименование организации БС РФ)

в соответствие с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»

С целью исполнения законодательных требований при обработке персональных данных в _____
(наименование организации БС РФ)

ПРИКАЗЫВАЮ:

1. Создать комиссию по приведению_____
(наименование организации БС РФ)

в соответствие с требованиями Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» в составе:

Председатель комиссии:

ФИО	Должность

Члены комиссии:

ФИО	Должность

2. Возложить на созданную комиссию задачу по классификации информационных систем персональных данных, а также иные задачи по приведению_____
(наименование организации БС РФ)

в соответствие с требованиями Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных».

2. Контроль за исполнением настоящего приказа оставляю за собой.

<Руководитель организации>: _____ / /

«___» _____20__ г.

Приложение 2
Утверждаю
<руководитель организации БС РФ>
ФИО

_____
«___» _____20__ г.

План приведения _____
(наименование организации БС РФ)

в соответствие с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»

№ п/п	Наименование мероприятия	Основание (нормативный акт)	Форма реализации	Статус реализации	Срок выполнения	Ответственное лицо	Примечание
1.	Изучить бизнес-процессы организации БС РФ и технологические процессы обработки информации.						
2.	Идентифицировать и описать все бизнес-процессы (технологические процессы), в рамках которых обрабатываются ПДн.						
3.	Определить какие программные и технические средства используются в технологических						

	процессах, в рамках которых обрабатываются ПДн.						
4.	Определить работников организации (должности), участвующих в технологических процессах, в рамках которых обрабатываются ПДн.						
5.	Определить состав обрабатываемых в организации ПДн (тип, категория, объем).		Проект перечня ПДн				
6.	Определить цели, правовое основание, условия и принципы обработки ПДн.		Проект перечня ПДн				
7.	Определить, выполняется ли обработка специальных категорий ПДн. Если да, то на каком основании.		Проект перечня ПДн				
8.	Определить к какому типу защищаемой (коммерческая тайна, банковская тайна и др.) информации относятся ПДн.		Проект перечня ПДн				
9.	Сопоставить объем собираемых ПДн целям обработки (убрать		Перечень ПДн				

	избыточные данные).						
10.	Определить срок хранения ПДн.		Перечень ПДн или отдельный нормативный акт				
11.	Определить необходимость получения согласия на обработку ПДн и для тех случаев, когда необходимо, получить такое согласие в письменном виде.		Согласие субъектов на обработку ПДн				
12.	Сообщать субъекту ПДн о целях обработки при сборе сведений, составляющих ПДн.		Скорректированные формы договоров с субъектами персональных данных				
13.	Определить ПДн, получаемые не непосредственно от субъекта ПДн, и для таких случаев уведомить субъектов.		Типовая форма уведомления субъектов				
14.	Определить порядок передачи ПДн сторонним организациям и лицам.						
15.	Определить договорные взаимоотношения, в		Изменение форм договоров и				

	рамках которых выполняется передача ПДн третьей стороне и внести в такие договора требования об обеспечении конфиденциальности передаваемых ПДн.		заключение дополнительных соглашений к действующим договорам				
16.	Определить, выполняется ли трансграничная передача ПДн. Если да, то убедиться что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, или в противном случае имеется обоснование для такой передачи.						
17.	Определить порядок реагирования на запросы со стороны субъектов ПДн и предоставления им их ПДн, внесения изменений, прекращения		Регламент реагирования на обращения субъектов. Журналы (книги) учета обращений				

	обработки ПДн		субъектов персональных данных. Типовая форма ответа на запросы				
18.	Определить порядок уничтожения ПДн после достижения целей обработки		Инструкция по уничтожению ПДн. Акт об уничтожении персональных данных				
19.	Определить необходимость уведомления уполномоченного органа по защите ПДн о начале обработки ПДн. Если необходимость есть, то составить и отправить уведомление		Уведомление Роскомнадзора				
20.	Определить структурное подразделение или должностное лицо, ответственное за обеспечение безопасности ПДн		Приказ о назначении ответственного				
21.	Провести анализ систем организации и составить перечень		Список систем, в которых				

	систем, в которых обрабатываются персональные данные. Выделить ИСПДн.		обрабатываются персональные данные				
22.	Выявить ИСПДн (в том числе государственные) и их границы (в рамках организации БС РФ), в отношении которых организация не определяет цели обработки и требования по защите (например, передача отчетности в Пенсионный фонд, ФНС, ФОМС и др.)						Обеспечение безопасности ПДн в таких системах следует осуществлять в соответствии с предъявляемыми их организатором (владельцем) требованиями
23.	Разработать модель угроз ПДн		Приказ о вводе в действие в организации БС РФ Отраслевой модели угроз или Частная модель угроз безопасности ПДн организации БС РФ				
24.	Провести классификацию ИСПДн		Акты классификации ИСПДн				

25.	Оценить необходимость и возможности обезличивания ПДн. Провести обезличивание ПДн. При необходимости провести повторную классификацию ИСПДн						
26.	Определить требования и меры по обеспечению безопасности ПДн		Политика информационной безопасности или отдельный документ				
27.	Разработать требования по обеспечению безопасности ПДн при обработке в ИСПДн		Политика информационной безопасности или отдельный документ, содержащий требования по обеспечению безопасности ПДн				
28.	Разработать должностные инструкции персоналу ИСПДн в части		Должностные инструкции персонала и журнал				

	обеспечения безопасности ПДн при их обработке в ИСПДн		инструктажа				
29.	Определить порядок действий должностных лиц в случае возникновения нештатных ситуаций		Журнал учета нештатных ситуаций				
30.	Определить порядок проведения контроля обеспечения безопасности ПДн		Политика информационной безопасности или отдельный документ				
31.	Анализ существующих защитных мер на предмет соответствия требованиям Стандартов Банка России и требованиям, определенным на этапах 19, 20						
32.	Выявление невыполненных в организации требований Стандартов Банка России и требований, определенных на этапах 19, 20, принятие решений о создании системы защиты персональных данных,						

	доработке ИСПДн, доработке документов организации БС РФ и др.						
33.	Организовать разработку системы обеспечения безопасности персональных данных на основе положений ГОСТ 34 серии.		Приказы, Распоряжения, Договоры с организациями, которые проводят работы по созданию системы защиты информации, Документы в соответствии с положениями ГОСТ 34 серии				
34.	Разработать систему защиты в соответствии с положениями Стандартов Банка России, и требованиями, определенным на этапах 19, 20.						
35.	Разработка технических заданий на создание системы защиты.		Технические задания. Частные технические				

	Разработка частных технических заданий на доработку ИСПДн.		задания				
36.	Вести учет носителей ПДн, СЗИ, в том числе поэкземплярный учет СКЗИ, криптографических ключей		Справки Журналы учета				
37.	Назначить приказом ответственного пользователя СКЗИ, имеющего необходимый уровень квалификации		Приказ о назначении ответственного за СКЗИ				
38.	Обеспечить размещение, специальное оборудование, охрану и организацию режима в помещениях, где установлены СКЗИ или хранятся криптографические ключи						
39.	Определить подразделения и назначить лиц, ответственных за эксплуатацию средств защиты информации с их обучением по направлению обеспечения		Приказы, распоряжения				

	безопасности ПДн						
40.	Провести обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними		Документы о прохождении обучения				
41.	Доработка существующих документов и разработка новых документов с целью приведения документов организации в соответствие с требованиями Федерального закона «О персональных данных» и Стандартов Банка России		Документы				
42.	Определить необходимость получения лицензий (в соответствии с пунктами 9.6 и 9.7 СТО БР ИББС-1.0-2010)		Лицензии				
43.	Проводить разбирательство и составление заключений по фактам несоблюдения условий хранения носителей		Журнал учета нештатных ситуаций				

	персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений						
44.	Выполнять постоянный контроль обеспечения безопасности ПДн		Справки, отчеты				
45.	Провести самооценку соответствия информационной безопасности (в том числе обеспечения безопасности персональных данных) требованиям СТО БР ИББС-1.0-20….		Отчет о результатах. План устранения выявленных недостатков				
46.	Провести внешнюю оценку соответствия информационной		Отчет и Заключение. План				

	безопасности (в том числе обеспечения безопасности персональных данных) требованиям СТО БР ИББС-1.0-20….		устранения выявленных недостатков				
47.	Подготовить и утвердить «Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-2010»		Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-2010				
48.	Направить «Подтверждение соответствия организации БС РФ стандарту Банка России СТО БР ИББС-1.0-2010»						
49.	Выполнять постоянный контроль обеспечения безопасности ПДн		Справки, отчеты, заключения				

Приложение 3

Утверждаю
<руководитель организации БС РФ>
ФИО

_____
«___» _____20__ г.

Перечень персональных данных, обрабатываемых в

_____
(наименование организации БС РФ)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Перечень персональных данных, подлежащих защите в

_____
(наименование организации БС РФ)

(далее – Перечень), разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Уставом _____ (далее Организации).
(наименование организации БС РФ)

2. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Сведениями, составляющими персональные данные, в _____
(наименование организации БС РФ)
является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе:

2.1. Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения.

2.2. Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.

2.3. Характеристики, идентифицирующие физиологические особенности человека и на основе которых можно установить его личность.

2.4. Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.

2.5. Номера телефонов (мобильного и домашнего), в случае их регистрации на субъекта персональных данных или по адресу его места жительства (по паспорту).

2.6. Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома,

свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения).

2.7. Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения).

2.8. Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса и телефона организации, а также реквизитов других организаций с полным наименование занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения).

2.9. Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней.

2.10. Содержание и реквизиты трудового договора с работником Организации или гражданско-правового договора с гражданином.

2.11. Сведения о заработной плате (номера счетов для расчета с работниками, данные зарплатных договоров с клиентами, в том числе номера их спецкартсчетов, данные по окладу, надбавкам, налогам и другие сведения).

2.12. Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии\снятии на(с) учет(а) и другие сведения).

2.13. Сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2НДФЛ супруга(и), данные документов по долговым обязательствам, степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения).

2.14. Сведения об имуществе (имущественном положении):

- автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств);

- недвижимое имущество (вид, тип, способ получения, общие характеристики, стоимость, полные адреса размещения объектов недвижимости и другие сведения);

- банковские вклады (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов, вид, срок размещения, сумма, условия вклада и другие сведения);

- кредиты (займы), банковские счета (в том числе спецкартсчета), денежные средства и ценные бумаги, в том числе в доверительном управлении и на доверительном хранении (данные договоров с клиентами, в том числе номера счетов, спецкартсчетов, номера банковских карт, кодовая информация по банковским картам, коды кредитных историй, адреса приобретаемых объектов недвижимости, сумма и валюта кредита или займа, цель кредитования, условия кредитования, сведения о залоге, сведения о приобретаемом объекте, данные по ценным бумагам, остатки и суммы движения по счетам, тип банковских карт, лимиты и другие сведения).

2.15. Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.

2.16. Сведения об идентификационном номере налогоплательщика.

2.17. Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).

2.18. Сведения, указанные в оригиналах и копиях приказов по личному составу Организации и материалах к ним.

2.19. Сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) работников Организации.

2.20. Материалы по аттестации и оценке работников Организации.

2.21. Материалы по внутренним служебным расследованиям в отношении работников Организации.

2.22. Внутрибанковские материалы по расследованию и учету несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами.

2.23. Сведения о временной нетрудоспособности работников Организации.

2.24. Табельный номер работника Организации.

2.25. Сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения).

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Целью обработки указанных выше персональных данных является:

- осуществление возложенных на Организацию 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 Организации;

- 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 Организации.

4. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Сроки обработки указанных выше персональных данных определяются в соответствие со сроком действия договора с субъектом ПДн, приказом Росархива от 06.10.2000 «Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения», сроком исковой давности, а также иными требованиями законодательства и нормативными документами Банка России.

Приложение 4

ПРИКАЗ

О назначении ответственного за обеспечение безопасности персональных данных в

_____
(наименование организации БС РФ)

С целью приведения_____
(наименование организации БС РФ)

в соответствие с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и исполнения законодательных требований при обработке персональных данных

ПРИКАЗЫВАЮ:

1. Назначить ответственным за обеспечение безопасности персональных данных

_____.
(наименование подразделения организации БС РФ) или (ФИО, должность)

2. Контроль за исполнением настоящего приказа оставляю за собой.

<Руководитель организации>: _____ / /

«___» _____20__ г.

Приложение 5

Утверждаю
<руководитель организации БС РФ>
ФИО

_____
«___» _____20__ г.

Список систем

_____,
(наименование организации БС РФ)

в которых обрабатываются персональные данные

№ п/п	Наименование системы	Цель создания ИСПДн	Разработчик ИСПДн	Эксплуатирующее ИСПДн подразделение	Исходные данные[2]	Примечания
1	2	3	4	5	6	7

Должностные лица, участвовавшие в составлении списка:

_____ *(должность)*	_____ *(ФИО)*	_____ *(подпись)*	_____ *20__ г.*
_____ *(должность)*	_____ *(ФИО)*	_____ *(подпись)*	_____ *20__ г.*
...	...	...	...

[2] Содержание столбца определяется решением комиссии по приведению организации БС РФ в соответствие требованиям Федерального закона «О персональных данных»

Приложение 6
Утверждаю
<руководитель организации БС РФ>
ФИО
_____
«___» _____20__ г.

Акт классификации информационных систем персональных данных

_____
(наименование организации БС РФ)

СОГЛАСОВАНО
Должность

_____ _____
(подпись) (ФИО)
"___" _____ 20__ г.

СОГЛАСОВАНО
Должность

_____ _____
(подпись) (ФИО)
"___" _____ 20__ г.

СОГЛАСОВАНО
Должность

_____ _____
(подпись) (ФИО)
"___" _____ 20__ г.

СОГЛАСОВАНО
Должность

_____ _____
(подпись) (ФИО)
"___" _____ 20__ г.

№ п/п	Наименование ИСПДн	Цель создания ИСПДн (цель обработки ПДн)	Разработчик ИСПДн	Эксплуатирующее ИСПДн подразделение	Исходные данные ИСПДн[3]	Класс ИСПДн[4]	Примечания
1	2	3	4	5	6	7	8

Должностные лица, составившие Акт классификации ИСПДн

_____	_____	_____	_____ 20__ г.
(должность)	(ФИО)	(подпись)	
_____	_____	_____	_____ 20__ г.
(должность)	(ФИО)	(подпись)	
…	…	…	…

[3] Содержание столбца определяется решением решением комиссии по приведению организации БС РФ в соответствие требованиям Федерального закона «О персональных данных». Могут содержаться следующие данные:

- Перечень персональных данных, которые обрабатываются в ИСПДн.
- Категория обрабатываемых персональных данных - в том случае, если в организации БС РФ проводится классификация персональных данных, в соответствии с пунктом 7.10.3 стандарта Банка России СТО БР ИББС-1.0-2010.
- Объем обрабатываемых персональных данных - количество субъектов персональных данных, персональные данные которых обрабатываются в ИСПДн.
- Виды обработки персональных данных - заполняется в соответствии с частью 3 статьи 3 Федерального закона «О персональных данных».
- Характеристики безопасности - Конфиденциальность, целостность, доступность и другие свойства безопасности персональных данных.
- Структура ИСПДн, Наличие подключения ИСПДн к сетям связи общего пользования и сетям международного информационного обмена, Режим обработки персональных данных, Режим разграничения прав доступа пользователей к ИСПДн, Местонахождение технических средств ИСПДн - заполняется в соответствии с пунктами 9-13 Порядка проведения классификации информационных систем персональных данных, утвержденного приказом ФСТЭК, ФСБ и Минсвязи от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»

[4] В соответствии с определенными критериями классификации (пункт 7.11.3 стандарта Банка России СТО БР ИББС-1.0-2010)

Приложение 7

Утверждаю
<руководитель структурного подразделения
или должностное лицо, ответственное
за обеспечение безопасности
персональных данных>
ФИО

_____
«___» _____2009 г.

ЗАКЛЮЧЕНИЕ
о возможности эксплуатации средств(-а)/системы защиты информации

_____
(наименование средств(-а)/системы защиты информации)

в информационной системе персональных данных

_____
(наименование ИСПДн)

В соответствии с _____
(приказ, положение о защите ПДн и др.)

комиссией в составе:

	ФИО	**Должность**
Председатель		
Члены комиссии		

проведена установка и адаптация средств(-а)/системы защиты информации_____
(наименование средств(-а)/системы защиты информации)

на _____,
(автоматизированные рабочие места, сервера и др.)

входящие в состав информационной системы персональных данных _____.
(наименование ИСПДн)

1. Системное и прикладное программное обеспечение.
2. Информация о настройках средств(-а)/системы защиты информации от несанкционированного доступа.
3. Выполнение требований по сертификации средств(-а)/системы защиты информации.
4. Вывод о возможности эксплуатации:

Средство(-а)/система защиты информации _____ готово(-а) к эксплуатации в ИСПДн _____.

Председатель комиссии: _____ / /
Члены комиссии: _____ / /
_____ / /

Приложение 8

Журнал учета носителей персональных данных

Журнал начат «____» _____ 200__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 200__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№ п/п	Регистрационный номер	Дата учета	Тип / емкость носителя	Серийный номер	Отметка о постановке на учет (ФИО, подпись, дата)	Отметка о снятии с учета (ФИО, подпись, дата)	Местоположение носителя	Сведения об уничтожении носителя / стирании информации
1	2	3	4	5	6	7	8	9

Приложение 9

Журнал учета разовых пропусков

Журнал начат «____» _____ 200__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 200__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

Номер пропуска	**Номер заявки на выдачу пропуска**	**ФИО посетителя**	**Наименование принимающего структурного подразделения**	**ФИО должностного лица, подписавшего пропуск**	**Время начала действия пропуска**	**Вид документа, с которым пропуск действителен**	**Место посещения**	**Фактическое время выхода**	**Отметка о возврате пропуска**	**Подпись дежурного бюро пропусков**
1	2	3	4	5	6	7	8	9	10	11

Приложение 10

Согласие на обработку персональных данных

Я, _____
(ФИО)

_____,
данные паспорта (или иного документа, удостоверяющего личность)

не возражаю против обработки _____
(наименование организации БС РФ)

(адрес _____) , включая

_____
_____,
перечисление видов обработки (сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение)

следующих моих персональных данных:

_____,
(перечень персональных данных)

обрабатываемых с целью

_____,
(цель обработки персональных данных)

в течение

_____.
(указать срок действия согласия)

Настоящее согласие может быть отозвано мной в письменной форме.

Настоящее согласие действует до даты его отзыва мною путем направления в _____
(наименование организации БС РФ)

письменного сообщения об указанном отзыве в произвольной форме, если иное не установлено законодательством Российской Федерации.

"____" _____20___г. _____
(подпись) (ФИО)

Приложение 11

Журнал учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных

_____
(наименование организации БС РФ)

Журнал начат «____» _____ 200__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 200__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№ п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи / отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8

Приложение 12

Разрешаю уничтожить
<руководитель структурного подразделения
или должностное лицо, ответственное
за обеспечение безопасности
персональных данных>
ФИО

_____
«___» _____2009 г.

Акт об уничтожении персональных данных

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации _____ информация, записанная на них в процессе эксплуатации, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего подлежит уничтожению носителей
(цифрами и прописью)

После утверждения акта перечисленные носители сверены с записями в акте и на указанных носителях персональные данные уничтожены путем _____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

После утверждения акта перечисленные носители сверены с записями в акте и уничтожены путем

_____.
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Уничтоженные носители с книг и журналов учета списаны.

Председатель комиссии: _____ / /
Члены комиссии: _____ / /
_____ / /

Примечание:
1. Акт составляется раздельно на каждый способ уничтожения носителей.
2. Все листы акта, а так же все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

Приложение 13

Подтверждение соответствия *«Наименование организации БС РФ» юридический адрес* стандарту Банка России СТО БР ИББС-1.0-2010

Настоящее Подтверждение соответствия является документальным удостоверением того, что в результате проведения оценки соответствия *«Наименование организации БС РФ»* положениям стандарта Банка России СТО БР ИББС-1.0-2010 *«Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (далее – СТО БР ИББС-1.0)*

с использованием стандартов Банка России СТО БР ИББС-1.2-2010 *«Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организации БС РФ требованиям СТО БР ИББС-1.0»* и СТО БР ИББС–1.1-2007 *«Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности»*

были получены следующие результаты:

1. Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих обработку персональных данных (регулятор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Роскомнадзор):

_____;

2. Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации (регулятор – Федеральная служба по техническому и экспортному контролю, ФСТЭК России):

_____;

3. Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных при использовании средств криптографической защиты информации (регулятор - Федеральная служба безопасности Российской Федерации, ФСБ России):

_____;

4. Итоговый уровень соответствия информационной безопасности организации БС РФ требованиям СТО БР ИББС-1.0 (регулятор - Центральный банк Российской Федерации):

_____.

Оценка соответствия была проведена в форме внешней оценки соответствия *«Наименование организации БС РФ»* положениям СТО БР ИББС-1.0 *«Наименование проверяющей организации»* по состоянию на *«__.__.20__»*.

Оценка соответствия была проведена в форме самооценки соответствия *«Наименование организации БС РФ»* положениям СТО БР ИББС-1.0 по состоянию на *«__.__.20__»*.

<Руководитель организации>: _____ / /

«___» _____20__ г

Приложение 14

Журнал учета средств криптографической защиты информации

Журнал начат «____» _____ 200__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 200__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№ п.п.	Наименование СКЗИ	Регистрационный номер СКЗИ	Отметка о получении		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств ИСПДН			Примечание
			От кого получены	Дата и номер сопроводи-тельного письма	Ф.И.О. пользователя СКЗИ, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12

Приложение 15

ПРИКАЗ

Об назначении работников, допущенных к работе с ключами средств криптографической защиты информации

С целью исполнения законодательных требований, а также требований внутренних документов_____
(наименование организации БС РФ)

при обработке персональных данных

ПРИКАЗЫВАЮ:

1. Утвердить список работников _____,
(наименование структурного подразделения организации БС РФ) или (наименование организации БС РФ)

допущенных к работе с ключами средств криптографической защиты информации.

2. Контроль за исполнением настоящего приказа оставляю за собой.

<Руководитель комиссии>: _____ / /
«___» _____20__г

Приложение
к приказу от «___» _____20__г. № _____

Список работников,
допущенных к работе с ключами средств криптографической защиты информации

№ п/п	Наименование СКЗИ	Название должности	ФИО	Наименование ИСПДн

Руководитель структурного подразделения
или должностное лицо, ответственное
за обеспечение безопасности
персональных данных _____ / /
от «___» _____20__г.

Приложение 16

Журнал учета криптографических ключей

Журнал начат «____» _____ 200__ г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 200__ г.
Должность
_____ / ФИО должностного лица /

На _____ листах

№ п.п.	Номера экземпляров (криптографические номера) ключевых документов	Номера серий криптографических ключей	Наименование СКЗИ	Отметка о получении		Отметка о выдаче		Отметка об уничтожении ключевых документов		
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя	Дата	Дата уничтожения	Ф.И.О. пользователя СКЗИ, производившего уничтожение	Номер акта или расписка об уничтожении
1	2	3	4	5	6	7	8	12	13	14

Приложение 17

Утверждаю
<руководитель структурного подразделения
или должностное лицо, ответственное
за обеспечение безопасности
персональных данных>
ФИО

_____
«___» _____2009 г.

Акт о комиссионном уничтожении криптографических ключей

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

провела уничтожение криптографических ключей:

№ п/п	Дата	Тип носителя ключа	Регистрационный номер носителя ключа	Наименование СКЗИ	Примечание

Всего носителей криптографических ключей _____
(цифрами и прописью)

На указанных носителях криптографические ключи уничтожены путем _____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители криптографических ключей уничтожены путем _____
_____.
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.п.)

Председатель комиссии: _____ / /

Члены комиссии: _____ / /
_____ / /

Приложение 17

Типовые ошибки при реализации требований законодательства о персональных данных

В таблице приведены типовые и распространенные ошибки кредитных организаций, допускаемые при реализации законодательства о персональных данных, которые выявляются Роскомнадзором, ФСТЭК России и ФСБ России в процессе исполнения ими функций государственного контроля и надзора.

Таблица 3.

№ п/п	Типовая ошибка	Сфера компетенции регулятора
1.	Отсутствует согласие субъекта ПДн на обработку его ПДн	Роскомнадзор
2.	Не уничтожены ПДн после обращения субъекта	
3.	Не послано уведомление субъекту об уничтожении его ПДн	
4.	Предоставление ПДн третьим лицам без согласия субъекта ПДн	
5.	Не соответствие реальной обработки ПДн заявленным целям обработки	
6.	Прямой маркетинг без получения предварительного согласия субъекта ПДн	
7.	Обработка ПДн без уведомление Роскомнадзора	
8.	Отсутствие в договоре с третьими лицами условия обеспечения конфиденциальности	
9.	Отсутствие требований по технической защите персональных данных в ТЗ и проектной документации	ФСТЭК России
10.	Незавершенность классификации ИСПДн или ее ошибочность	
11.	Невыполнение работ по анализу угроз информационной безопасности	
12.	Незавершенность разработки необходимого комплекта организационно-распорядительной документации	
13.	Отсутствие необходимых мер и сервисов защиты информации	

14.	Непринятие мер по учету машинных носителей	
15.	Отсутствие в должностных регламентах ответственных лиц за защиту персональных данных и их полномочий по контролю за выполнением требований по защите	
16.	Отсутствие достаточного количества квалифицированных специалистов	
17.	Использование средств криптозащиты, отличающихся от эталонных сертифицированных версий	ФСБ России
18.	Невыполнение отдельных требований по порядку эксплуатации криптосредств, предусмотренных технической документацией	
19.	Несовершенство отдельных подготовленных оператором документов, регламентирующих вопросы обеспечения безопасности в конкретной организации	