РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.3-2010

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дата введения: 2010-06-21

Издание официальное

Москва
2010

Предисловие

1. ПРИНЯТЫ И ВВЕДЕНЫ в действие Распоряжением Банка России от 21 июня 2010 года № Р-705.

2. ВВЕДЕНЫ ВПЕРВЫЕ.

Содержание

Введение

В соответствии с действующим стандартом Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0) важнейшим условием реализации целей деятельности Банка России является обеспечение необходимого и достаточного уровня информационной безопасности организаций банковской системы Российской Федерации (БС РФ), их активов, к которым в том числе относятся персональные данные и банковские технологические процессы, в рамках которых они обрабатываются.

Стандартом СТО БР ИББС-1.0 с целью выполнения в организациях БС РФ требований законодательства Российской Федерации в области персональных данных определены требования по обработке персональных данных и по обеспечению информационной безопасности (ИБ) банковских технологических процессов, в рамках которых обрабатываются персональные данные (далее — требования СТО БР ИББС-1.0 в области персональных данных).

Настоящий документ содержит детализирующие требования по обеспечению безопасности персональных данных, выполнение которых способствует реализации в организациях БС РФ требований СТО БР ИББС-1.0 в области персональных данных и обеспечивает нейтрализацию актуальных для организаций БС РФ угроз безопасности персональных данных, содержащихся в рекомендациях в области стандартизации Банка России РС БР ИББС-2.x-20xx “Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций БС РФ”.

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

Дата введения: 2010-06-21

1. Область применения

Настоящие рекомендации распространяются на организации БС РФ, реализующие требования стандарта СТО БР ИББС-1.0 в области персональных данных, в рамках построения/совершенствования системы обеспечения информационной безопасности организации БС РФ.

Настоящий документ применяется в организации БС РФ путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних нормативных и методических документах организаций БС РФ.

Рекомендательный статус документа допускает, что его отдельные требования по решению организации БС РФ могут быть заменены иными требованиями, обеспечивающими эквивалентный (аналогичный) уровень безопасности персональных данных.

2. Нормативные ссылки

В настоящих рекомендациях в области стандартизации Банка России использованы нормативные ссылки на следующие документы в области стандартизации Банка России:

СТО БР ИББС-1.0;

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” (далее — СТО БР ИББС-1.2).

3. Термины и определения

В настоящих рекомендациях применены термины в соответствии со СТО БР ИББС-1.0.

4. Обозначения и сокращения

АРМ — автоматизированное рабочее место;
БС — банковская система;
ИБ — информационная безопасность;
ИСПДн — информационная система персональных данных;
ЛВС — локальная вычислительная сеть;
ОС — операционная система;
ПО — программное обеспечение;

РФ — Российская Федерация;
СКЗИ — средства криптографической защиты информации;
СУБД — система управления базы данных.

5. Общий подход к определению требований по обеспечению безопасности персональных данных в информационных системах персональных данных

5.1. Выбор требований по обеспечению безопасности персональных данных в информационных системах персональных данных (ИСПДн) осуществляется в зависимости от результатов классификации ИСПДн.

5.2. В соответствии с действующим стандартом СТО БР ИББС-1.0 все ИСПДн организаций БС РФ относятся к специальным. ИСПДн организации БС РФ классифицируются на основе категорий обрабатываемых в ИСПДн персональных данных. Выделяются следующие основные классы ИСПДн:

ИСПДн обработки специальных категорий персональных данных (далее — ИСПДн-С);

Примечание.

В соответствии с Федеральным законом от 27 июля 2006 года “О персональных данных” [1] к специальным категориям персональных данных относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.

ИСПДн обработки биометрических персональных данных (далее — ИСПДн-Б);

Примечание.

В соответствии с Федеральным законом от 27 июля 2006 года “О персональных данных” [1] к биометрическим персональным данным относятся сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность.

ИСПДн обработки персональных данных, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным (далее — ИСПДн-И);

ИСПДн обработки общедоступных и (или) обезличенных персональных данных (далее — ИСПДн-Д).

Примечание.

В соответствии с Федеральным законом от 27 июля 2006 года “О персональных данных” [1] к общедоступным персональным данным относятся персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

В соответствии с Федеральным законом от 27 июля 2006 года “О персональных данных” [1] обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

5.3. Для обеспечения выполнения требований СТО БР ИББС-1.0 в ИСПДн организации БС РФ для каждой ИСПДн должны быть реализованы:

— общие требования по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн любого класса (раздел 6.1 настоящих рекомендаций);
— требования по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн соответствующего класса (разделы 6.2—6.5 настоящих рекомендаций).

5.4. Связь положений СТО БР ИББС-1.0 и требований настоящего документа, необходимых для реализации этих положений, приведена в Приложении.

5.5. При проведении оценок соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0 (самооценок и внешних оценок соответствия) вопросы частных показателей СТО БР ИББС-1.2 в части банковских технологических процессов, в рамках которых обрабатываются персональные данные, детализируются и конкретизируются вопросами, составленными на основе требований настоящего документа. Перечень указанных детализирующих и конкретизирующих вопросов, а также подход к проведению оценок соответствия ИБ содержатся в СТО БР ИББС-1.2.

6. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных

6.1. Общие требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных любого класса

6.1.1. Требования по обеспечению безопасности персональных данных в ИСПДн в общем случае реализуются комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации.

Организация выполнения и (или) реализация требований по обеспечению безопасности персональных данных должна осуществляться структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, либо на договорной основе организацией — контрагентом организации БС РФ, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Допускается возложение ответственности за организацию работы по обеспечению безопасности персональных данных на существующее в организации БС РФ подразделение (например, на службу ИБ).

Реализация требований по обеспечению безопасности персональных данных должна осуществляться по согласованию и под контролем службы ИБ организации БС РФ.

6.1.2. Создание ИСПДн организации БС РФ должно включать разработку и согласование (утверждение) предусмотренной техническим заданием организационно-распорядительной, проектной и эксплуатационной документации на создаваемую систему. В документации должны быть отражены вопросы обеспечения безопасности обрабатываемых персональных данных.

Разработка концепций, технических заданий, проектирование, создание и тестирование, приемка и ввод в действие ИСПДн должны осуществляться по согласованию и под контролем структурного подразделения или должностного лица (работника) организации БС РФ, ответственного за обеспечение безопасности персональных данных, и службы ИБ организации БС РФ.

6.1.3. Все информационные активы, принадлежащие ИСПДн организаций БС РФ, должны быть защищены от воздействий вредоносного кода. В организации БС РФ должны быть определены и документально зафиксированы требования по обеспечению безопасности персональных данных средствами антивирусной защиты и порядок проведения контроля реализации этих требований в соответствии с требованиями пункта 7.5 СТО БР ИББС-1.0.

6.1.4. В организации БС РФ должна быть определена система контроля доступа, позволяющая осуществлять контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации ИСПДн.

6.1.5. Руководители эксплуатирующих и обслуживающих ИСПДн подразделений организации БС РФ обеспечивают безопасность персональных данных при их обработке в ИСПДн.

Работники, осуществляющие обработку персональных данных в ИСПДн, должны действовать в соответствии с инструкцией (руководством, регламентом и т.п.), входящей в состав эксплуатационной документации на ИСПДн, и соблюдать требования документов организации БС РФ по обеспечению ИБ.

6.1.6. Обязанности по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению ИБ ИСПДн организации БС РФ, возлагаются приказами (распоряжениями) на администраторов информационной безопасности ИСПДн.

6.1.7. Порядок действий администратора информационной безопасности ИСПДн и персонала, занятых в процессе обработки персональных данных, должен быть определен инструкциями (руководствами), которые готовятся разработчиком ИСПДн в составе эксплуатационной документации на ИСПДн.

Указанные инструкции (руководства):

устанавливают требования к квалификации администратора информационной безопасности и персонала в области защиты информации, а также актуальный перечень защищаемых объектов и правила его обновления;

содержат в полном объеме актуальные (по времени) данные о полномочиях пользователей;

содержат данные о технологии обработки информации в объеме, необходимом для администратора информационной безопасности;

устанавливают порядок и периодичность анализа журналов регистрации событий (архивов журналов);

регламентируют другие действия администратора информационной безопасности и персонала, предусмотренные настоящими рекомендациями.

Параметры конфигурации средств защиты и механизмов защиты информации от НСД, используемых в зоне ответственности администратора информационной безопасности, определяются в эксплуатационной документации на ИСПДн. Порядок и периодичность проверок установленных параметров конфигурации устанавливаются в эксплуатационной документации или регламентируются внутренним документом организации БС РФ, при этом проверки должны проводиться не реже чем раз в год.

6.1.8. В организации БС РФ должен быть определен и документально зафиксирован порядок доступа в помещения, в которых размещаются технические средства ИСПДн и хранятся носители персональных данных, предусматривающий контроль доступа в помещения посторонних лиц и наличие препятствий для несанкционированного проникновения в помещения.

Указанный порядок должен быть разработан структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение режима физической безопасности организации БС РФ и согласован структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и службой ИБ организации БС РФ.

6.1.9. Пользователи и обслуживающий персонал ИСПДн не должны осуществлять несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование персональных данных. С этой целью организационно-техническими мерами должно быть запрещено несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование персональных данных, в том числе с использованием отчуждаемых (сменных) носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующих различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото- и видеосъемки.

6.2. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки общедоступных и (или) обезличенных персональных данных

6.2.1. Процессы обработки персональных данных, а также порядок установки, настройки, эксплуатации и восстановления необходимых технических и программных средств регламентируются разработчиком ИСПДн в проектной и эксплуатационной документации.

6.2.2 Идентификация и аутентификация (проверка подлинности) субъекта доступа при входе в ИСПДн обеспечиваются по идентификатору (коду) и периодически обновляемому паролю длиной не менее шести буквенно-цифровых символов.

При наличии технической возможности количество последовательных неудачных попыток ввода пароля должно быть ограничено — от 3 до 5 попыток. При превышении указанного количества средства защиты и механизмы защиты должны блокировать возможность дальнейшего ввода пароля, включая правильное значение пароля, до вмешательства администратора информационной безопасности.

Порядок формирования и смены паролей, а также контроля исполнения этих процедур регламентируется разработчиком ИСПДн в эксплуатационной документации в инструкциях (руководствах) администраторов информационной безопасности.

6.2.3. Передача персональных данных должна осуществляться только при условии обеспечения их целостности с помощью защитных мер, механизмов и средств, применяемых по согласованию со структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных.

6.3. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки персональных данных, не являющихся биометрическими, не относящихся к специальным категориям и к общедоступным или обезличенным

6.3.1. Для информационных систем обработки персональных данных, не являющихся биометрическими, не относящихся к специальным категориям и к общедоступным или обезличенным, применяются все требования по обеспечению безопасности, определенные в разделе 6.2, а также следующие требования.

6.3.2. Выполнение функций обеспечения безопасности персональных данных в ИСПДн должно обеспечиваться средствами защиты информации, прошедшими в установленном по-

рядке процедуру оценки соответствия, а также комплексом встроенных механизмов защиты электронных вычислительных машин (ЭВМ), операционных систем (ОС), систем управления базами данных (СУБД), прикладного программного обеспечения (ПО).

6.3.3. На стадии ввода в действие разработчиком ИСПДн должны быть выполнены настройки средств и механизмов обеспечения безопасности, не допускающие несанкционированного изменения пользователем предоставленных ему полномочий. Разработчиком ИСПДн должен быть определен порядок постоянного контроля фактического состояния указанных настроек на предмет их соответствия установленным правилам.

Указанный порядок должен быть согласован структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и согласован службой ИБ организации БС РФ.

6.3.4. Регистрация входа в ИСПДн (выхода из ИСПДн) субъекта доступа является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

— дата и время входа в систему (выхода из системы) субъекта доступа;
— идентификатор субъекта, предъявленный при запросе доступа;
— результат попытки входа: успешная или неуспешная (несанкционированная);
— идентификатор (адрес) устройства (компьютера), используемого для входа в систему.

6.3.5. В ИСПДн не должно быть субъекта доступа, имеющего полномочия, а при возможности и технические средства по уничтожению и модификации информации, содержащейся в журнале регистрации событий, указанном в пункте 6.3.4.

Очистка журналов регистрации событий регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн. Перед очисткой журналов регистрации событий должно производиться архивирование содержащейся в них информации путем перемещения информации в соответствующий архив.

Операция по архивированию журнала регистрации событий должна, в свою очередь, регистрироваться с указанием времени и идентификатора работника, выполнившего операцию, в качестве первой записи в действующем журнале регистрации событий.

Архивы журналов регистрации событий уничтожаются только администратором информационной безопасности, в зоне ответственности которого находятся данные архивы, не ранее чем через три года с момента появления последней записи в данной архивной копии.

6.3.6. В организации БС РФ должен быть определен и документально зафиксирован порядок постановки на учет и снятия с учета машинных носителей, предназначенных для размещения персональных данных.

Снятие с учета машинных носителей, на которых были размещены персональные данные, производится по акту путем стирания с них информации средствами гарантированного стирания информации или по акту путем их уничтожения.

Процедура стирания информации регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн в зависимости от применяемого средства гарантированного стирания.

При наличии технической возможности осуществляется очистка освобождаемых областей памяти на носителях, ранее использованных для хранения персональных данных.

6.3.7. Состав и назначение ПО ИСПДн должны быть определены и зафиксированы документально в соответствии с требованиями пункта 7.9.7 СТО БР ИББС-1.0.

6.3.8. Порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО, должен быть регламентирован. Эталонные копии ПО должны быть учтены, доступ к ним должен быть регламентирован. Соответствующие регламенты в виде инструкций, руководств готовятся разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

6.3.9. Сохранность и целостность программных средств ИСПДн и персональных данных являются обязательными и обеспечиваются в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн.

Средства восстановления функций обеспечения безопасности персональных данных в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств.

Порядок создания и сопровождения резервных копий, включающий способ и периодичность копирования, процедуры создания, учета, хранения, использования (для восстановления) и уничтожения резервных копий, регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

6.3.10. Восстановление функций обеспечения безопасности персональных данных в ИСПДн в случае нештатной ситуации должно осуществляться администратором ИСПДн с обязательным привлечением администратора информационной безопасности ИСПДн (при необходимости — с привлечением специалистов структурного подразделения или должностного лица (работника) организации БС РФ, ответственного за обеспечение безопасности персональных данных, и службы ИБ организации БС РФ). Процедура восстановления должна быть регламентирована разработчиком ИСПДн в эксплуатационной документации на ИСПДн.

6.3.11. Подключение ИСПДн к ИСПДн другого класса или к сети Интернет осуществляется с использованием средств межсетевого экранирования (межсетевых экранов), которые обеспечивают выполнение следующих функций:

фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;

регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

возможность проверки (контроля) целостности программной и информационной частей средства межсетевого экранирования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования);

фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

восстановление свойств межсетевого экрана после сбоев и отказов оборудования (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования);

возможность проведения регламентного тестирования реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления (в том числе с применением внешних программных средств, не встроенных в средство межсетевого экранирования).

6.4. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки биометрических персональных данных

6.4.1. Для информационных систем обработки биометрических персональных данных применяются все требования по обеспечению безопасности, определенные в разделе 6.3, а также требования, установленные Постановлением Правительства от 6 июля 2008 г. № 512 “Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных” [2].

6.5. Требования по обеспечению безопасности персональных данных, обрабатываемых в информационных системах обработки специальных категорий персональных данных

6.5.1. Для информационных систем обработки специальных категорий персональных данных применяются все требования по обеспечению безопасности, определенные в разделе 6.3, а также следующие требования.

6.5.2. Идентификация информационных ресурсов (например, информационных массивов, баз данных, файлов, обрабатывающих их программ), содержащих персональные данные, должна осуществляться по логическим именам.

6.5.3. Контроль доступа субъектов к защищаемым информационным ресурсам в соответствии с правами доступа указанных субъектов является обязательным.

6.5.4. Регистрация печати материалов, содержащих персональные данные, является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

— дата и время печати;
— спецификация устройства печати (логическое имя (номер) внешнего устройства);
— полное наименование (вид, шифр, код) материала;
— идентификатор субъекта доступа, запросившего печать материала;

— объем фактически отпечатанного материала (количество страниц, листов, копий) и результат печати: успешная (весь объем) или неуспешная.

6.5.5. Регистрация запуска программ и процессов, осуществляющих доступ к защищаемым информационным ресурсам, является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

— дата и время запуска;
— имя (идентификатор) программы (процесса, задания);
— идентификатор субъекта доступа, запросившего программу (процесс, задание);
— результат попытки запуска: успешная или неуспешная (несанкционированная);
— дата и время попытки доступа к защищаемому информационному ресурсу;
— имя (идентификатор) защищаемого информационного ресурса;
— вид запрашиваемой операции (например, чтение, запись, модификация, удаление);
— результат попытки доступа: успешная или неуспешная (несанкционированная).

6.5.6. Регистрация изменений полномочий субъектов доступа и статуса объектов доступа (защищаемых информационных ресурсов) является обязательной. В журнале регистрации событий, который ведется в электронном виде ИСПДн, указываются следующие параметры:

— дата и время изменения;
— содержание изменения с указанием идентификатора субъекта доступа, чьи полномочия подверглись изменению, или логического имени защищаемого информационного ресурса, чей статус изменился;
— идентификатор администратора информационной безопасности, осуществившего изменение.

6.5.7. В ИСПДн не должно быть субъекта доступа, имеющего полномочия, а при возможности и технические средства по уничтожению и модификации информации, содержащейся в журналах регистрации событий, указанных в пунктах 6.5.4—6.5.6.

Очистка журналов регистрации событий регламентируется разработчиком ИСПДн в эксплуатационной документации на ИСПДн. Перед очисткой журналов регистрации событий должно производиться архивирование содержащейся в них информации путем перемещения информации в соответствующий архив.

Операция по архивированию журнала регистрации событий должна, в свою очередь, регистрироваться с указанием времени и идентификатора работника, выполнившего операцию, в качестве первой записи в действующем журнале регистрации событий.

Архивы журналов регистрации событий уничтожаются только администратором информационной безопасности, в зоне ответственности которого находятся данные архивы, не ранее чем через три года с момента появления последней записи в данной архивной копии.

6.5.8. С целью недопущения изменения состава ПО ИСПДн, комплекс средств автоматизации которой представляет собой автономное, изолированное на физическом уровне в соответствии с эталонной моделью взаимодействия открытых систем — моделью OSI, автоматизированное рабочее место (АРМ) работника или работников, из ПО должны быть исключены программные средства, предназначенные для разработки и отладки ПО (либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения). Если стандартные программные средства общего назначения (например, MS Office) не обеспечивают возможности выборочного удаления из них средств разработки и отладки ПО, допускается использование этих программных средств при условии, что документально введен запрет использования отдельных их компонент (средств разработки и отладки ПО).

6.5.9. В ИСПДн, комплекс средств автоматизации которой включает одно или несколько сетевых АРМ, сетевого оборудования и серверов, технические и программные средства, предназначенные для разработки и отладки ПО либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения, должны располагаться в сегментах локальной вычислительной сети (ЛВС), изолированных (на уровне не выше сетевого в соответствии с эталонной моделью взаимодействия открытых систем — моделью OSI) от сегментов, задействованных в обработке персональных данных.

Параметры настроек технических и программных средств, обеспечивающих указанное разделение, а также процедура контроля этих параметров настроек регламентируются разработчиком в эксплуатационной документации на ИСПДн.

Стандартные программные средства общего назначения (например, MS Office), которые не обеспечивают возможности выборочного удаления из них средств разработки и отладки ПО, могут быть использованы в сегментах, задействованных в обработке персональных данных, при условии, что документально введен запрет использования отдельных их компонент (средств разработки и отладки ПО).

6.5.10. Передача персональных данных между подразделениями организации БС РФ по телекоммуникационным каналам и линиям связи, не принадлежащим организации БС РФ или не пролегающим только по территории организации БС РФ, должна осуществляться только при обеспечении их защиты с помощью организации виртуальных частных сетей (Virtual Private Network — VPN) или иных защитных мер, механизмов и средств, применение которых определяется структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и согласовывается со службой ИБ организации БС РФ.

6.5.11. Передача персональных данных по телекоммуникационным каналам и линиям связи между подразделениями организации БС РФ, с одной стороны, и внешними организациями, с другой стороны, должна осуществляться с использованием сертифицированных средств криптографической защиты или иных защитных механизмов, применение которых определяется структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и согласовывается со службой ИБ организации БС РФ.

В случае использования СКЗИ должны быть выполнены требования нормативных правовых актов ФСБ России.

В случае обмена информацией с другой организацией правила использования СКЗИ должны быть определены соглашением сторон, в частности, условиями договора.

При отсутствии указанной технической возможности передача персональных данных в электронном виде осуществляется на магнитных и других съемных носителях. Порядок такой передачи должен быть согласован со структурным подразделением или должностным лицом (работником) организации БС РФ, ответственным за обеспечение безопасности персональных данных, и со службой ИБ организации БС РФ.

6.5.12. Подключение ИСПДн к ИСПДн другого класса или к сети Интернет осуществляется с использованием средств межсетевого экранирования (межсетевых экранов), которые должны иметь подтвержденный сертификатом класс защиты не ниже четвертого при возможности информационного обмена между всеми компонентами защищаемой ИСПДн без использования компонентов других автоматизированных банковских систем организации БС РФ (в иных случаях — не ниже третьего класса). Указанные классы защиты устанавливаются в соответствии с руководящим документом “Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации”, утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 года.

Приложение

Таблица соответствия положений СТО БР ИББС-1.0, частных показателей СТО БР ИББС-1.2, положений РС БР ИББС-2.3, положений Приказа ФСТЭК от 5.02.2010 № 58 [3], положений ISO/IEC 17799-2005 [4]

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
7.2.1	М1.1	6.1.5			6.1.1, 6.1.3, 8.1.1, 8.2.1, 8.2.3
		6.1.6			
		6.1.7			
		6.3.10			
7.2.2	М1.3	6.1.5			6.1.3, 8.2.3
		6.1.6			
		6.1.7			
		6.3.10			
	М1.4	6.1.5			
		6.1.6			
		6.1.7			
		6.3.10			
7.2.3	М1.9	6.3.5	2.1		6.1.3, 10.1.3
		6.5.7	2.1		
7.2.6	М1.13	6.1.7			8.1.2, 8.2
	М1.14	6.1.7			
7.2.8	М1.19	6.1.5			8.1.3, 8.2.3
7.3.1	М2.1	6.1.1	1.3		10.1.4, 10.3.2, 12
		6.1.2			
		6.2.1			
		6.3.2	2.1		
		6.3.8			
		6.5.8		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
7.3.2	М2.2	6.1.1	1.3		6.1.2, 6.1.3, 10.3.2, 12.1.1, 12.5
		6.1.2			
7.3.3	М2.3	6.1.1	1.3		6.1.2, 6.1.3, 12
		6.1.2			
7.3.4	М2.4	6.1.1	1.3		10.2
7.3.5	М2.5	6.1.2			10.1.1, 10.2, 10.3.2, 10.7.4, 12.5.1
		6.1.7			
		6.3.10			
		6.4.1			
	М2.6	6.1.2			
		6.1.7			
		6.3.10			
		6.4.1			
	М2.7	6.5.9		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
7.3.7	М2.10	6.5.9		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	10.1.4, 10.3.2, 12.4.2, 15.2.2
7.3.8	М2.11	6.1.7			15.2
	М2.12	6.1.7			

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
7.3.9	М2.13	6.3.7			10.2.1, 10.2.3
		6.3.8			10.4.1, 10.5
		6.3.9	2.1	2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	10.10.1, 12.4.1, 12.5.1, 12.5.2, 12.5.3
		6.3.10			
		6.5.8		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
	М2.14	6.3.7			
		6.3.8			
		6.3.9	2.1	2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
7.3.11	М2.16	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	10.5, 10.7.2, 10.10.3, 12.4.1
	М2.17	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
7.4.1	М3.1	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	7.1.1, 7.1.3, 10.7, 11.1
		6.4.1	2.1		11.6
	М3.2	6.1.7			
		6.5.3	2.1	4.3а	
7.4.2	М3.3	6.4.1			11
	М3.4	6.3.2	2.1		12.1
		6.3.3			
		6.4.1			
		6.5.2	2.1	4.2а, 4.3а	
		6.5.3	2.1	4.3а	
		6.5.10	2.1		
		6.5.11	2.1		
		6.5.12	2.1, 2.4, 2.6–2.11	3.4, 4.4	
7.4.3	М3.5	6.1.4	2.1		10.4, 10.5, 10.7
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	11, 12.2, 12.5.1
		6.5.2	2.1	4.2а, 4.3а	
		6.5.3	2.1	4.3а	
	М3.6	6.1.4	2.1		
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	
		6.5.3	2.1	4.3а	
	М3.7	6.1.4	2.1		
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	
		6.4.1	2.1		
		6.5.3	2.1	4.3а	
	М3.8	6.1.4	2.1		
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	
		6.4.1	2.1		
		6.5.3	2.1	4.3а	
	М3.9	6.2.3	2.1, 2.4, 2.10		
		6.4.1	2.1		
	М3.10	6.4.1	2.1		

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
	М3.11	6.1.7			
		6.3.4	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.3.5	2.1		
		6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.4.1	2.1		
		6.5.4	2.1	4.1б, 4.2б, 4.3б	
		6.5.5	2.1	4.1б, 4.2б, 4.3б	
		6.5.6	2.1	4.1б, 4.2б, 4.3б	
		6.5.7	2.1		
	М3.12	6.1.7			
		6.3.4	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.3.5	2.1		
		6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.4.1	2.1		
		6.5.4	2.1	4.1б, 4.2б, 4.3б	
		6.5.5	2.1	4.1б, 4.2б, 4.3б	
		6.5.6	2.1	4.1б, 4.2б, 4.3б	
		6.5.7	2.1		
7.4.4	М3.14	6.1.7			10.10
	М3.15	6.1.7			
	М3.16	6.1.7			
	М3.17	6.1.7			
7.4.5	М3.18	6.1.8	2.1		9.1.2
	М3.19	6.1.8	2.1		9.1.5
	М3.20	6.1.8	2.1		
7.5.1	М4.1	6.1.3	2.1, 2.3		10.4.1
	М4.5	6.1.3	2.1, 2.3		
7.6.1	М5.1	6.2.3	2.1, 2.4, 2.10		10.6, 10.8, 10.9.2
		6.3.11	2.1, 2.4, 2.6–2.10	2.4	11.4, 11.7.2
		6.5.12	2.1, 2.4, 2.6–2.11	3.4, 4.4	
7.6.7	М5.15	6.2.3	2.1, 2.4, 2.10		10.4.1
		6.3.11	2.1, 2.4, 2.6–2.10	2.4	10.8.1, 10.8.4
		6.5.12	2.1, 2.4, 2.6–2.11	3.4, 4.4	11.4.6
7.6.10	М5.23	6.2.3	2.1, 2.4, 2.10		10.6
		6.3.11	2.1, 2.4, 2.6–2.10	2.4	11.4
		6.5.12	2.1, 2.4, 2.6–2.11	3.4, 4.4	
7.7.1	М6.1	6.5.10	2.1		10.8.1, 10.9.1
		6.5.11	2.1		11.5.2, 11.7.1
7.7.2	М6.3	6.4.1			12.2.3, 12.3
	М6.4	6.4.1			15.1.6
7.9.2	М8.1	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	7.2, 10.7
		6.4.1	2.1		
7.9.3	М8.3	6.1.2			7.1.1, 7.1.3, 7.2

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
7.9.4	М8.4	6.1.6			6.1.1, 6.1.3, 8.1.1
		6.3.5	2.1		
		6.3.10			
		6.5.7	2.1		
7.9.5	М8.5	6.1.2			10.10.2
		6.1.6			12.1
		6.1.7			15.2
		6.3.5	2.1		
		6.3.10			
		6.5.7	2.1		
7.9.6	М8.6	6.2.1			10.1.1, 10.2, 10.3.2, 10.7.4, 12.5.1
		6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
	М8.7	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.4.1	2.1		
	М8.8	6.5.9		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
7.9.7	М8.9	6.3.7			10.1.1, 10.3.2, 10.10.2, 12, 15.2
	М8.10	6.3.7			
7.9.8	М8.12	6.1.7			15.2
		6.5.9		2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	
7.9.9	М8.13	6.3.9	2.1	2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	10.1.1, 10.5, 13.2.1, 14.1.1, 14.1.3
		6.3.10			
7.11.3	М10.2	5.2	1.4		7.1, 7.2
	М10.3	5.2	1.4		
8.2.2	М11.9	6.1.8	2.1		6.1.1, 6.1.3 8.1.1
		6.2.3	2.1, 2.4, 2.10		
		6.3.3			
		6.4.1			
		6.5.11	2.1		
	М28.9	6.1.8	2.1		
		6.2.3	2.1, 2.4, 2.10		
		6.3.3			
		6.4.1			
		6.5.11	2.1		
		6.1.8	2.1		
8.3.1	М12.2	5.2	1.4		7.1, 7.2 10.7
		6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.4.1	2.1		
8.3.2	М12.3	5.2	1.4		7.1, 7.2 10.7
		6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	
		6.4.1	2.1		
8.3.3	М12.4	5.2	1.4		7.1, 7.2, 10.7

СТО БР ИББС-1.0	СТО БР ИББС-1.2	РС БР ИББС-2.3	Приказ ФСТЭК от 5.02.2010 № 58		ISO/IEC 17799-2005 (ISO/IEC 27002-2005)
			Положение о методах и способах защиты информации в ИСПДн	приложение к Положению о методах и способах защиты информации в ИСПДн	
8.6.2	М15.6	6.1.2			5, 6.1.5
		6.1.6			10.1.1, 10.7.4
		6.1.7			15.2
		6.1.9	2.1		
		6.2.1			
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	
		6.3.5	2.1		
		6.3.8			
		6.5.7	2.1		
	М15.7	6.1.2			
		6.1.6			
		6.1.7			
		6.2.1			
		6.3.8			
	М15.8	6.1.6			
		6.1.7			
		6.1.9	2.1		
		6.2.2	2.1	2.1а, 2.2а, 2.3а, 3.1а, 3.2а, 3.3а, 4.1а, 4.2а, 4.3а	
		6.3.5	2.1		
		6.3.8			
		6.5.7	2.1		
8.7.1	М16.1	6.1.5			4.2,
	М29.1	6.1.5			6.1.1, 6.1.2, 10.1
8.8.2	М17.2	6.3.6	2.1	2.1б, 2.2б, 2.3б, 3.1б, 3.2б, 3.3б, 4.1б, 4.2б, 4.3б	5, 6.1, 10, 11, 12
		6.4.1	2.1		
8.11.2	М20.2	6.3.10			14
8.11.3	М20.3	6.3.9	2.1	2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	14
8.11.5	М20.5	6.3.9	2.1	2.1в, 2.2в, 2.3в, 3.1в, 3.2в, 3.3в, 4.1в, 4.2в, 4.3в	10.1.4, 10.3.1, 10.5, 12.2, 12.5, 12.6, 13.4, 14
8.12.1	М21.1	6.1.7			10.10
		6.1.9	2.1		
		6.3.3			
8.12.6	М21.7	6.1.7			6.1.1, 6.1.3,
		6.1.9	2.1		8.1.1, 8.2.1,
	М21.8	6.1.7			10.10
	М32.1	6.1.7			
		6.1.9	2.1		
	М32.2	6.1.7			

Библиография

[1] Федеральный закон “О персональных данных” от 27 июля 2006 г. № 152-ФЗ.
[2] Постановление Правительства от 6 июля 2008 г. № 512 “Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных”.
[3] Приказ Федеральной службы по техническому и экспортному контролю от 5 февраля 2010 г. № 58 “Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных”.
[4] ISO/IEC 17799-2005 Information technology — Security techniques — Code of practice for information security management.

Ключевые слова: банковская система Российской Федерации, персональные данные, безопасность, информационная система персональных данных.