Приложение А1.17

к Порядку документирования при создании, развитии, тестировании, вводе в эксплуатацию, эксплуатации и сопровождении, выводе из эксплуатации компонентов информационно-телекоммуникационной системы Банка России

**Центральный Банк Российской Федерации  
(Банк России)**

*Шаблон заполнения листа утверждения приведен в приложении А (А3) к Порядку документирования при создании, развитии, тестировании, вводе в эксплуатацию, эксплуатации и сопровождении, выводе из эксплуатации компонентов информационно-телекоммуникационной системы Банка России*

|  |
| --- |
| *поле 1 – должности и подписи лиц, утвердивших и (или) согласовавших документ* |

|  |
| --- |
| *поле 2 – наименование ИТ-решения*  *Наименование документа* |

Лист утверждения

Обозначение документа

|  |
| --- |
| *поле 3 – должности и подписи лиц, подготовивших и согласовавших документ* |

<Год выпуска>

**Центральный Банк Российской Федерации  
(Банк России)**

**Утвержден**

<Обозначение листа утверждения документа> – ЛУ

**<полное наименование КомпонентА ИТС>**

Регламент подключения пользователей

<Обозначение документа>

на \_\_\_\_\_\_\_листах

<Год выпуска>

[Предисловие является вводной частью документа, в которой приводятся назначение и общие сведения о документе, в том числе с указанием номера проекта или заявки, номера договора, в рамках которого проводятся работы по созданию компонента ИТС, стандартов, положений и других руководящих документов Банка России, с учетом требований которых разработан документ. Предисловие не имеет названия и не включается в содержание документа.]

**Содержание**

[Обозначения и сокращения 4](#_Toc83308311)

[Термины и определения 5](#_Toc83308312)

[1 Общие сведения 6](#_Toc83308313)

[2 Описание ролевой модели 7](#_Toc83308314)

[3 Участники процесса согласования заявок 8](#_Toc83308315)

[4 Порядок предоставления и прекращения предоставления прав логического доступа пользователей к ресурсам доступа 9](#_Toc83308316)

[5 Контроль предоставления доступа 13](#_Toc83308317)

# Обозначения и сокращения

| Сокращение | Расшифровка сокращения |
| --- | --- |
| СУЗ | Сервис управления заявками |
| СУД | Сервис управления и контроля прав доступа |

# Термины и определения

| Термин | Определение |
| --- | --- |
|  |  |
|  |  |

# Общие сведения

[В разделе должны быть указаны сведения общего характера, необходимые для работы с настоящим регламентом:

1. назначение и область действия документа (наименование ресурсов доступа компонентов ИТС, порядок предоставления логического доступа к которым определяет регламент);
2. назначение ресурсов доступа компонента ИТС;
3. основание для разработки регламента (наименование и реквизиты нормативных документов Банка России, определяющих необходимость разработки и требования к содержанию документа);
4. сведения о разработке и согласовании документа (наименование подразделения или организации – разработчика документа и подразделений, согласовавших документ);
5. сведения о компонентах ИТС и сервисах обеспечения информационной безопасности (далее – ИБ), задействованных в технологическом процессе предоставления и прекращения предоставления доступа к ресурсам доступа;
6. сведения об эксплуатационном подразделении ресурсов доступа;
7. сведения о распорядителе логического доступа.]

# Описание ролевой модели

[В разделе должны быть указаны:

1. перечень ролей пользователей ресурсов доступа (для каждой роли указываются наименование роли, описание роли, права, требуемые для реализации данной роли);
2. требования к совмещению ролей (перечисляются роли, которые не могут быть одновременно назначены одному и тому же пользователю).

*Назначение одному лицу ролей администратора автоматизированной системы Банка России и администратора ИБ автоматизированной системы Банка России в той же автоматизированной системе Банка России не допускается.*

*Назначение одному лицу ролей эксплуатационного персонала, в том числе администратора автоматизированной системы Банка России, администратора ИБ автоматизированной системы Банка России, администратора систем управления базами данных, и роли контролера эксплуатации в той же автоматизированной системе Банка России не допускается, за исключением случаев возникновения в информационно-телекоммуникационной системе Банка России инцидентов, зафиксированных в соответствии с требованиями нормативных и (или) иных актов Банка России;*

1. требования к назначению на роли (перечисляются роли, назначение на которые требует документального оформления, в частности издания организационно-распорядительного документа).]

# Участники процесса согласования заявок

[В разделе должны быть указаны перечень и описание ролей работников, которым предоставлено право согласования заявок на предоставление и прекращение предоставления логического доступа к ресурсам доступа.]

# Порядок предоставления и прекращения предоставления прав логического доступа пользователей к ресурсам доступа

[В разделе должны быть приведены:

1. описание формы и содержания заявок на предоставление и прекращение предоставления логического доступа к ресурсам доступа (форма и содержание заявок должны соответствовать требованиям пунктов 1.4 и 1.5 приложения к Положению Банка России от 22.11.2019 № 701-П «О требованиях к обеспечению информационной безопасности при доступе к объектам и ресурсам информационно-телекоммуникационной системы Банка России» (с изменениями), описание заявок может быть приведено в приложении к регламенту).

*Заявки включают следующую информацию:*

* *дату формирования заявки;*
* *для пользователей и эксплуатационного персонала – фамилию, имя, отчество (последнее при наличии), должность субъекта доступа, осуществляющего логический доступ, и наименование структурного подразделения субъекта доступа;*
* *для программных сервисов – наименование программного процесса (сервиса) и при необходимости наименование учетной записи, используемой для осуществления логического доступа; фамилия, имя, отчество (последнее при наличии), должность субъекта доступа, сформировавшего заявку, а также обоснование необходимости предоставления логического доступа;*
* *наименования ресурсов доступа, к которым предоставляется логический доступ (наименования автоматизированных систем Банка России, их подсистем, прикладных программных комплексов, баз данных, ресурсов локальных вычислительных сетей), или наименования ресурсов доступа, к которым прекращается или приостанавливается логический доступ (наименования автоматизированных систем Банка России, прикладных программных комплексов, баз данных, ресурсов локальных вычислительных сетей в соответствии с ранее оформленной заявкой на предоставление логического доступа);*
* *запрашиваемые для субъекта доступа права логического доступа, роли и атрибуты доступа;*
* *сроки предоставления логического доступа.*

*В дополнение к указанной информации в базе заявок в зависимости от специфики фиксируется следующая информация:*

* *наименование и (или) идентификаторы учетных записей;*
* *при предоставлении логического доступа эксплуатационному персоналу с использованием административной учетной записи – IP-адрес или иная информация, позволяющая однозначно определить принадлежность средства вычислительной техники, с которого осуществляется логический доступ, субъекту доступа;*
* *иные данные, необходимые для однозначной идентификации объекта и субъекта доступа;*
* *иная информация, определяемая эксплуатационным подразделением и необходимая для предоставления логического доступа;*

1. описание порядка предоставления и прекращения предоставления прав доступа к ресурсам доступа (краткое описание процесса регистрации, согласования и исполнения заявок на предоставление и прекращение доступа).

*Предоставление (прекращение) логического доступа к ресурсам доступа осуществляется на основании заявки, сформированной с использованием СУЗ, с учетом следующих требований.*

*При предоставлении (прекращении) логического доступа субъектам доступа заявка формируется работником Банка России, которому предоставляется логический доступ, или его непосредственным руководителем.*

*Заявка подписывается (подтверждается) руководителем (заместителем руководителя) структурного подразделения центрального аппарата, территориального учреждения или другого подразделения Банка России, ее сформировавшего.*

*При предоставлении логического доступа эксплуатационному персоналу и программным сервисам к ресурсам доступа заявка формируется работником эксплуатационного подразделения или его непосредственным руководителем и утверждается руководителем (заместителем руководителя) территориального учреждения или другого подразделения Банка России, для центрального аппарата Банка России – директором Департамента информационных технологий.*

*Для ресурсов доступа, распорядителем логического доступа к которым является Комитет Банка России по управлению данными, при условии соответствия запрашиваемого логического доступа матрице доступа (профилю структурного подразделения, а также ресурсам доступа, разрешенным структурному подразделению Банка России или субъекту доступа) СУЗ обеспечивает согласование заявки на предоставление логического доступа. В случае необходимости, определяемой матрицей доступа, СУЗ обеспечивает согласование указанной в настоящем абзаце заявки с Департаментом безопасности Банка России.*

*Для ресурсов доступа, распорядителем логического доступа к которым является структурное подразделение центрального аппарата, территориального учреждения или другого подразделения Банка России, СУЗ обеспечивает согласование заявки на предоставление логического доступа со всеми структурными подразделениями Банка России и в порядке, определенном регламентом предоставления доступа, а также утверждение заявки распорядителем логического доступа к ресурсам доступа.*

*Для ресурсов доступа, распорядителем логического доступа к которым является Комитет Банка России по управлению данными, при условии несоответствия запрашиваемого логического доступа матрице доступа СУЗ информирует структурное подразделение Банка России, сформировавшее заявку, о невозможности предоставления логического доступа к указанным ресурсам доступа и обеспечивает возможность формирования заявки на внесение изменений в матрицу доступа структурным подразделением Банка России, запрашивающим логический доступ. Заявка на внесение изменений в матрицу доступа направляется подразделением Банка России для рассмотрения в Департамент статистики, утверждения Комитетом Банка России по управлению данными.*

*В случае возникновения необходимости изменения для субъекта доступа перечня ресурсов доступа, к которым ему предоставляется логический доступ, запрашиваемых прав доступа, сроков предоставления логического доступа требуются формирование и согласование новой заявки.*

*Прекращение логического доступа к ресурсам доступа осуществляется на основании заявки или автоматически СУД, на основании приказа Банка России по личному составу о переводе или увольнении работника – субъекта доступа или по истечении указанного в заявке срока предоставления логического доступа.*

*Заявка на прекращение логического доступа формируется в том числе в случае изменения должностных обязанностей субъекта доступа, в результате которого не требуется продолжение предоставления логического доступа.*

*Логический доступ уволенных работников Банка России прекращается в день увольнения субъекта доступа.*

*Заявки на прекращение доступа для пользователей должны формироваться структурным подразделением работника и подписываться (подтверждаться) руководителем (заместителем руководителя) сформировавшего их структурного подразделения центрального аппарата, территориального учреждения или другого подразделения Банка России.*

*Заявки на прекращение доступа для эксплуатационного персонала и программных сервисов должны формироваться эксплуатационным подразделением и подтверждаться руководителем (заместителем руководителя) территориального учреждения или другого подразделения Банка России, для центрального аппарата Банка России – директором Департамента информационных технологий;*

1. схемы и описание схем согласования заявок (приводятся схемы и описание схем согласования заявок, рекомендуемая форма которых определена типовым регламентом подключения пользователей автоматизированных систем с использованием Централизованной системы управления правами доступа пользователей);
2. описание порядка делегирования полномочий на согласование заявок.]

# Контроль предоставления доступа

[В разделе должны быть приведены:

1. краткое описание порядка хранения утвержденных заявок на предоставление и прекращение предоставления доступа к ресурсам доступа и порядка получения информации из заявок, находящихся на хранении (отчетов из «базы заявок»).

*Факт предоставления, изменения прав, прекращения логического доступа фиксируется в базе заявок СУЗ. Информация об исполненных заявках должна храниться в базе заявок СУЗ в течение трех лет со дня прекращения предоставления логического доступа, предоставленного на основании указанных в настоящем абзаце заявок.*

*СУЗ обеспечивает информирование структурного подразделения Банка России, сформировавшего заявку, о ее выполнении или о причинах невозможности ее выполнения. Информация о выполнении заявки должна быть доступна контролеру эксплуатации автоматизированной системы Банка России, а также регулярно выгружаться в сервис мониторинга и анализа событий ИБ.*

*СУЗ обеспечивает хранение базы заявок способом, позволяющим сформировать:*

* *для каждого конкретного субъекта доступа – перечень ресурсов доступа, к которым этому субъекту предоставляется логический доступ;*
* *для конкретного ресурса доступа – перечень субъектов доступа и программных сервисов, которым предоставляется или был предоставлен логический доступ к этому ресурсу, с указанием:*
* *данных о субъектах доступа и программных сервисах, которым предоставлен логический доступ (фамилия, имя, отчество (последнее при наличии), должность субъекта доступа, наименование структурного подразделения субъекта доступа),*
* *данных о программных сервисах, которым предоставлен логический доступ (фамилия, имя, отчество (последнее при наличии), должность работника эксплуатационного подразделения субъекта доступа, за которым закреплена техническая учетная запись, используемая программным сервисом);*
* *прав доступа;*
* *наименований и (или) идентификаторов учетных записей;*
* *сроков предоставления прав доступа.*

*СУЗ обеспечивает фиксацию и хранение всех заявок на изменение прав логического доступа к ресурсам доступа, а также информации об их исполнении, внесенной автоматически или работниками эксплуатационного подразделения;*

1. сведения о работниках, которым предоставлено право доступа к информации из «базы заявок» и на которых возложены обязанности по контролю за соблюдением требований по осуществлению логического доступа к ресурсам доступа;
2. перечень контролируемых требований по осуществлению логического доступа из нормативных документов.

*В случае планируемого длительного (более 41 календарного дня, а для районов Крайнего Севера и приравненных к ним местностей – более 62 календарных дней, когда в соответствии с законодательством Российской Федерации за субъектом доступа сохраняется место работы) отсутствия субъекта доступа на рабочем месте или временного отсутствия при необходимости использования учетной записи для осуществления логического доступа руководитель структурного подразделения центрального аппарата, территориального учреждения или другого подразделения Банка России субъекта доступа должен сформировать с использованием СУД заявку на блокировку соответствующих учетных записей субъекта доступа.*

*На основании утвержденной заявки блокирование соответствующих учетных записей должно осуществляться администратором ИБ автоматизированной системы Банка России или автоматически СУД. При отсутствии технической возможности блокирования учетных записей должен осуществляться отзыв прав соответствующих учетных записей, выполняемый администратором ИБ автоматизированной системы Банка России или автоматически СУД.*

*Администраторы ИБ автоматизированной системы Банка России, контролеры эксплуатации автоматизированной системы Банка России или иные работники соответствующего подразделения безопасности и защиты информации должны осуществлять контроль, направленный на выявление фактов неиспользования пользователями и (или) эксплуатационным персоналом предоставленного им права на осуществление логического доступа на протяжении периода времени, превышающего 90 дней, и в случае выявления таких фактов формировать заявку на блокирование неиспользуемых учетных записей. Информация о неиспользовании пользователями и (или) эксплуатационным персоналом предоставленного им права на осуществление логического доступа должна направляться с использованием Системы автоматизации документооборота и делопроизводства Банка России руководителям их структурных подразделений для принятия решения о необходимости продолжения предоставления логического доступа;*

1. порядок осуществления указанного контроля.]

При разработке данного документа необходимо учитывать требования Типового регламента подключения пользователей автоматизированных систем с использованием Централизованной системы управления правами доступа пользователей, а также требования пункта 3.23 Положения 701-П «О требованиях к обеспечению информационной безопасности при доступе к объектам и ресурсам информационно-телекоммуникационной системы Банка России» (с изменениями).