

Наименование финансовой организации:	Сведения о поставщике услуг (опросный лист заполняется в разрезе одного поставщика услуг) (в случае наличия, например, 10 поставщиков услуг заполняются 10 отдельных excel-файлов)			
ИНН финансовой организации:	№	Вопросы	Ответ финансовой организации	Комментарии /пояснения
	1	2	3	4
Полное фирменное наименование поставщика услуг:	1. Общий перечень вопросов			
	1.1	Поставщик услуг обрабатывает банковскую тайну и иную информацию ограниченного доступа (ограничение доступа к которой устанавливается федеральными законами)?		
ИНН / TIN поставщика услуг	1.2	Поставщик услуг обрабатывает защищаемую информацию (за исключением банковской тайны и иной информации ограниченного доступа)?		
	1.3	Поставщик услуг в рамках удаленного доступа к объектам информационной инфраструктуры финансовой организации имеет доступ к банковской тайне и иной информации ограниченного доступа?		
Дата заполнения опросного листа:	1.4	Поставщик услуг в рамках удаленного доступа к объектам информационной инфраструктуры финансовой организации имеет доступ к защищаемой информации (за исключением банковской тайны и иной информации ограниченного доступа)?		
	1.5	Поставщик услуг имеет удаленный доступ к объектам информационной инфраструктуры финансовой организации без доступа к защищаемой информации?		

Ф.И.О. отв. исполнителя:	1.6	Имеется ли у финансовой организации стратегия выхода на случай прекращения договора с поставщиком услуг (например, альтернативные решения или планы перехода, чтобы иметь возможность прекратить или перевести текущую деятельность и данные от поставщика услуг на эти решения контролируемым и достаточно проверенным способом, принимая во внимание вопросы размещения данных и поддержания непрерывности деятельности на этапе перехода)?		
	1.7	Сколько времени потребуется финансовой организации для перехода на другого поставщика услуг (менее 1 месяца; более 1 месяца, но менее 1 года; более 1 года)?		
Контакты отв. исполнителя:	2. Вопросы к соглашению с поставщиком услуг			
	2.1	Содержит ли соглашение с поставщиком услуг SLA для осуществления контроля за соблюдением поставщиком услуг требований к операционной надежности и защиты информации, а также обязанность поставщика услуг обеспечить их пороговые значения?		
	2.2	Содержит ли соглашение с поставщиком услуг условия привлечения поставщиком услуг субподрядчиков, включая: - предварительное уведомление финансовой организации о передаче на субподряд технологических процессов; - право расторгнуть договор с поставщиком услуг, если запланированные поставщиком услуг изменения в части привлечения субподрядчиков могут отрицательно сказаться на оценке риска аутсорсинга?		
	2.3	Содержит ли соглашение с поставщиком услуг ответственность поставщика услуг за ненадлежащее предоставление услуг?		
	2.4	Содержит ли соглашение с поставщиком услуг порядок возмещения потерь финансовой организации, возникших по вине поставщика услуг?		
	2.5	Содержит ли соглашение с поставщиком услуг условия внесения изменений и досрочного расторжения договора с поставщиком услуг?		

	2.6	Содержит ли соглашение с поставщиком услуг состав информации, предоставляемой поставщиком услуг, в рамках контроля финансовой организацией за элементами информационных систем, переданными на аутсорсинг?		
	2.7	Содержит ли соглашение с поставщиком услуг требование о соблюдении поставщиком услуг уровня защиты информации, определенного национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»?		
	2.8	Содержит ли соглашение с поставщиком услуг требование о соблюдении уровня защиты информации в отношении процесса 1 «Обеспечение защиты информации при управлении доступов», определенного пунктом 7.2 ГОСТ Р 57580.1-2017, согласно методике оценки соответствия защиты информации, определенной ГОСТ Р 57580.2-2018?		
	2.9	Содержит ли соглашение с поставщиком услуг требования о соблюдении поставщиком услуг уровня защиты информации в отношении процесса 5 «Предотвращение утечек информации», определенного пунктом 7.6 ГОСТ Р 57580.1-2017, согласно методике оценки соответствия защиты информации, определенной ГОСТ Р 57580.2-2018?		
	2.10	Содержит ли соглашение с поставщиком услуг требование о привлечении поставщика услуг при проведении Банком России и федеральными органами исполнительной власти надзорных (контрольных) мероприятий, включая обеспечение возможности: - предоставления финансовой организацией по запросу в ее адрес данных, относящихся к выполнению технологических процессов, технологических участков технологических процессов, реализуемых поставщиком услуг, включая данные, которые принадлежат поставщику услуг, необходимые Банку России и федеральным органам исполнительной власти в рамках проведения надзорных (контрольных) мероприятий; - своевременного информирования финансовой организацией Банка России об инцидентах защиты информации и операционной надежности?		

**3. Обработка защищаемой информации с использованием объектов информационной инфраструктуры поставщика услуг
(вопросы к соглашению с поставщиком услуг)**

3.1	Содержит ли соглашение с поставщиком услуг требование о предотвращении несанкционированного доступа к данным финансовой организации и ее клиентов?		
3.2	Содержит ли соглашение с поставщиком услуг требование о передаче данных финансовой организации и ее клиентов только по защищенным каналам сетевого взаимодействия или положения, предусматривающие возможность реализовать защиту каналов сетевого взаимодействия финансовой организации самостоятельно?		
3.3	Содержит ли соглашение с поставщиком услуг требование о двухсторонней аутентификации, а также контроле целостности данных финансовой организации и ее клиентов при их передаче по каналам сетевого взаимодействия?		
3.4	Содержит ли соглашение с поставщиком услуг требование об обеспечении защиты аутентификационных данных, а также иных данных, с применением которых может осуществляться доступ к системам хранения данных поставщика услуг, содержащим данные финансовой организации и ее клиентов?		
3.5	Содержит ли соглашение с поставщиком услуг требование о защите машинных носителей информации, используемых в рамках систем хранения данных поставщика услуг, на которых осуществляется хранение данных финансовой организации и ее клиентов?		
3.6	Содержит ли соглашение с поставщиком услуг требование о применении механизмов, направленных на обнаружение фактов нарушения целостности и восстановление данных финансовой организации и ее клиентов в рамках систем хранения данных поставщика услуг?		

	3.7	Содержит ли соглашение с поставщиком услуг требование о возможности применения финансовой организацией средств криптографической защиты информации для защиты данных финансовой организации и ее клиентов, в том числе возможности хранения ключевой информации средств криптографической защиты информации на собственном оборудовании финансовой организации?		
	3.8	Содержит ли соглашение с поставщиком услуг требование о защите образов виртуальных машин, в рамках которых обрабатываются данные финансовой организации и ее клиентов, в целях недопущения возможности их запуска неавторизованными субъектами доступа?		
	3.9	Содержит ли соглашение с поставщиком услуг требование о реализации доступа к данным финансовой организации и ее клиентов согласно реализуемой модели управления доступом?		
	3.10	Содержит ли соглашение с поставщиком услуг требование о регистрации результатов выполнения действий субъектов доступа, связанных с осуществлением доступа к данным финансовой организации и ее клиентов, а также положения, предусматривающие возможность выявления аномальной активности субъектов доступа при выполнении таких действий?		
	3.11	Содержит ли соглашение с поставщиком услуг требование о гарантированном удалении по запросу финансовой организации ее данных и данных ее клиентов (включая созданные резервные копии), аутентификационных данных, а также иных данных, с применением которых может осуществляться доступ к системам хранения данных поставщика услуг, содержащим данные финансовой организации и ее клиентов?		

3.12	Содержит ли соглашение с поставщиком услуг требование об установлении запрета на высвобождение и (или) перераспределение другим пользователям пространства, которое выделено поставщиком услуг финансовой организации для хранения и обработки данных финансовой организации и ее клиентов, аутентификационных данных, а также иных данных, с применением которых может осуществляться доступ к системам хранения данных поставщика услуг, содержащим данные финансовой организации и ее клиентов, до санкционированного удаления таких данных?		
3.13	Содержит ли соглашение с поставщиком услуг требование о гарантированном удалении данных финансовой организации и ее клиентов при выводе поставщиком услуг собственного оборудования из эксплуатации?		
4. Операционная надежность (вопросы к соглашению с поставщиком услуг)			
4.1	Содержит ли соглашение с поставщиком услуг требование о резервном копировании данных финансовой организации и ее клиентов?		
4.2	Содержит ли соглашение с поставщиком услуг требование об обеспечении возможности перемещения (миграции) данных финансовой организации и ее клиентов из систем хранения поставщика услуг, включая обеспечение целостности таких данных при их передаче по защищенным каналам сетевого взаимодействия, поддержание непрерывности сессии такого сетевого взаимодействия, а также обеспечение возможности предварительного резервного копирования передаваемых данных? <i>В случае если обязанность по обеспечению миграции данных конфиденциального характера возложена на поставщика услуг, таким поставщиком услуг во взаимодействии с финансовой организацией осуществляются анализ влияния выбранной схемы миграции данных конфиденциального характера на риск аутсорсинга и разработка мероприятий, направленных на уменьшение негативного влияния такого риска.</i>		

	4.3	Содержит ли соглашение с поставщиком услуг требование об обеспечении необходимой и достаточной производительности объектов информационной инфраструктуры поставщика услуг, их надежной работы (отказоустойчивости), возможности их планового масштабирования, а также оперативного восстановления работоспособности?		
	4.4	Содержит ли соглашение с поставщиком услуг требование о применении отказоустойчивых решений, разделении основных и резервных критичных активов (в том числе в части их резервирования, включая системы резервного хранения, электро- и холодоснабжения/теплоотвода, каналы связи), используемых в рамках обработки и хранения данных, выполняемое в том числе: - созданием резервных центров обработки и хранения данных, обеспечением защиты информации резервных центров обработки и хранения данных на уровне, эквивалентном основным центрам; - раздельным размещением основного и резервного центров обработки и хранения данных для снижения подверженности однотипным угрозам; - подготовкой и тестированием готовности резервных центров обработки и хранения данных к выполнению определенных финансовой организацией технологических процессов; - определением резервных каналов связи и электроснабжения в основных и резервных центрах обработки и хранения данных с обеспечением их максимального разделения для снижения вероятности их вывода из строя; - наличием более одного центра обработки данных?		
	5. Доступ поставщиков услуг к объектам информационной инфраструктуры финансовой организации (вопросы к соглашению с поставщиком услуг)			
	5.1	Содержит ли соглашение с поставщиком услуг требование о передаче данных финансовой организации и ее клиентов только по защищенным каналам сетевого взаимодействия или положения, предусматривающие возможность реализовать защиту каналов сетевого взаимодействия финансовой организации самостоятельно?		

5.2	Содержит ли соглашение с поставщиком услуг требование о двухсторонней аутентификации, а также контроле целостности данных финансовой организации и ее клиентов при их передаче по каналам сетевого взаимодействия?		
5.3	Содержит ли соглашение с поставщиком услуг требование о предоставлении удаленного доступа к объектам информационной инфраструктуры финансовой организации субъектам доступа с использованием устройств, находящихся под контролем системы централизованного управления и мониторинга финансовой организации (системы Mobile Device Management, MDM)?		
5.4	Содержит ли соглашение с поставщиком услуг требование об аутентификации мобильных (переносных) устройств удаленного доступа?		
5.5	Содержит ли соглашение с поставщиком услуг требование об определении правил удаленного доступа и перечня ресурсов доступа, к которым предоставляется удаленный доступ?		

6. Доступ поставщиков услуг к объектам информационной инфраструктуры финансовой организации (меры контроля)

6.1	Передача данных финансовой организации и ее клиентов только по защищенным каналам сетевого взаимодействия		
6.2	Организация двухсторонней аутентификации, а также контроля целостности данных финансовой организации и ее клиентов при их передаче по каналам сетевого взаимодействия		
6.3	Предоставление удаленного доступа к объектам информационной инфраструктуры финансовой организации субъектам доступа с использованием устройств, находящихся под контролем системы централизованного управления и мониторинга финансовой организации (системы Mobile Device Management, MDM)		
6.4	Аутентификация мобильных (переносных) устройств удаленного доступа		
6.5	Определение правил удаленного доступа и перечня ресурсов доступа, к которым предоставляется удаленный доступ		

6.6	Предоставление возможности реализации доступа к данным финансовой организации и ее клиентов согласно реализуемой модели управления доступом		
6.7	Обнаружение и предотвращение вторжений (несанкционированных сетевых подключений) посредством объектов информационной инфраструктуры, используемых поставщиками услуг в рамках своей деятельности		
6.8	Обеспечение возможности регистрации результатов выполнения действий субъектов доступа, связанных с осуществлением доступа к данным финансовой организации и ее клиентов, а также предоставление возможности выявления аномальной активности субъектов доступа при выполнении таких действий		
7. Оценка соответствия поставщика услуг требованиям защиты информации (при наличии)			
7.1	Оценка соответствия поставщика услуг уровню защиты информации в отношении процесса 1 "Обеспечение защиты информации при управлении доступом", определенного пунктом 7.2 ГОСТ Р 57580.1-2017, согласно методике оценки соответствия защиты информации, определенной ГОСТ Р 57580.2-2018 (указывается числовое значение)		
7.2	Оценка соответствия поставщика услуг уровню защиты информации в отношении процесса 5 "Предотвращение утечек информации", определенного пунктом 7.6 ГОСТ Р 57580.1-2017, согласно методике оценки соответствия защиты информации, определенной ГОСТ Р 57580.2-2018 (указывается числовое значение)		
7.3	Оценка соответствия поставщика услуг уровню защиты информации, определенному ГОСТ Р 57580.1-2017 (указывается числовая итоговая оценка в соответствии с пунктом 7.10 ГОСТ Р 57580.2-2018)		

ПОЯСНЕНИЯ ПО ЗАПОЛНЕНИЮ
формы обследования
«Обследование сведений о поставщиках ИТ-услуг»

1. Форма обследования «Обследование сведений о поставщиках ИТ-услуг» (далее – форма обследования) направлена на сбор сведений для следующих поставщиков услуг:

- обрабатывающих защищаемую информацию (финансовой организации и ее клиентов) с использованием своей информационной инфраструктуры, включая облачные услуги;

- отвечающих за операционную надежность технологических процессов, указанных в Положении Банка России от 13.01.2025 № 850-П «Об обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требованиях к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг» и Положении Банка России от 15.11.2021 № 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)»;

- имеющих доступ к объектам информационной инфраструктуры финансовой организации (например, в рамках оказания технической поддержки или разработки программного обеспечения).

2. Форма обследования заполняется отдельно по каждому поставщику услуг. В случае наличия, например, 10 поставщиков услуг заполняются 10 отдельных excel-файлов.

3. Разделы 1 и 2 заполняются для каждого из поставщиков услуг согласно пункту 1 настоящей инструкции.

4. Разделы 3 и 7 заполняются для поставщиков услуг, обрабатывающих защищаемую информацию с использованием своей информационной инфраструктуры.

5. Разделы 4 и 7 заполняются для поставщиков услуг, от которых зависит операционная надежность технологических процессов.

6. Разделы 5 и 6 заполняются для поставщиков услуг, имеющих удаленный доступ к объектам информационной инфраструктуры финансовой организации.

7. В случае если поставщик услуг относится одновременно к нескольким категориям, заполняются все разделы, которые относятся к этим категориям, в соответствии с пунктами 3–6.

8. В графе 3 разделов 1–6 указывается ответ из выпадающего списка (да/нет).

9. В графе 3 раздела 7 указывается числовое значение. В случае отсутствия оценки соответствия поставщика услуг уровню защиты информации графа 3 раздела 7 не заполняется.

10. Обязательны для заполнения данные, указанные в столбце «В»:

- наименование финансовой организации;
- ИНН финансовой организации;
- полное фирменное наименование поставщика услуг;
- ИНН/TIN поставщика услуг;

- дата заполнения опросного листа;
- Ф.И.О. ответственного исполнителя;
- контакты ответственного исполнителя.