Приложение №1 к Приказу № 07-00967/21-(0) от «06» декабря 2021 г.

Об утверждении типовой формы

Договора о привлечении банковского платежного агента

**Договор о привлечении банковского платежного агента № \_\_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| г. Москва  |  «\_\_» \_\_\_\_\_\_\_\_ 202\_ г. |

**Публичное акционерное общество «МТС-Банк»,** именуемое в дальнейшем **«Банк»**, в лице Бизнес-лидера Стрима «Система денежных переводов» Пальчуна Кирилла Викторовича, действующего на основании доверенности № И-24-00089/21-(0) от 12.02.2021, с одной стороны,

и **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, именуемое в дальнейшем «**Банковский платежный агент**» (БПА), в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, совместно именуемые «Стороны», заключили настоящий Договор о нижеследующем:

1. **Предмет договора**
	1. Банк в целях осуществления перевода денежных средств поручает, а Банковский платёжный агент обязуется за вознаграждение осуществлять от имени и за счет Банка, в рамках, установленных п. 1.2. настоящего Договора, следующие действия:
* принимать от физических лиц (далее - плательщики) наличные денежные средства с применением платежных терминалов в целях осуществления операций по переводу денежных средств без открытия банковского счета, не требующих проведения идентификации, в том числе, упрощенной идентификации в соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», а именно: операций по переводу денежных средств в пользу юридических лиц и индивидуальных предпринимателей для оплаты реализуемых товаров, выполняемых работ, оказываемых услуг, использования результатов интеллектуальной деятельности или средств индивидуализации, в пользу органов государственной власти и органов местного самоуправления при условии, что сумма операции не превышает 15 000 (пятнадцати тысяч) рублей;
	1. Перечень и условия совершения операций, подлежащих выполнению Банковским платёжным агентом, содержатся в Приложении №1 к настоящему Договору. Приложение №1 к настоящему Договору может быть изменено по соглашению Сторон путем обмена официальными письмами, подписанными уполномоченными представителями Сторон и(или) путем заключения дополнительного соглашения к настоящему Договору.
1. **Права и обязанности Сторон**
	1. **Банковский платежный агент обязан:**
		1. Осуществлять операции Банковского платежного агента от имени Банка;
		2. Для зачисления в полном объеме полученных от плательщиков наличных денежных средств и/или для зачисления денежных средств плательщиков, поступивших со специальных счетов в других кредитных организациях (включая вознаграждение, указанное в Приложении 1 к Договору, за исключением дополнительного вознаграждения банковского платежного субагента в случае его привлечения для осуществления деятельности по настоящему Договору) использовать специальный банковский счет банковского платежного агента (далее – Специальный банковский счет), открытый в Банке Банковскому платежному агенту (для осуществления деятельности по  настоящему Договору) не позднее, чем в течение 1 (одного) рабочего дня с даты предоставления Банковским платежным агентом необходимых для открытия Специального банковского счета документов в Банк;
		3. Подтверждать принятие наличных денежных средств путем выдачи кассового чека, соответствующего требованиям пункта 2.1.11. настоящего Договора;
		4. Вносить денежные средства, принятые от плательщиков и/или внесенных на другие специальные счета (в других кредитных организациях), на Специальный банковский счет в срок не позднее 3 (третьего) рабочего дня, следующего за днем предоставления плательщиком наличных денежных средств (при осуществлении перевода денежных средств плательщиков со специальных счетов в других кредитных организациях Банковский платежный агент должен обеспечить зачисление таких денежных средств на Специальный банковский счет не позднее 3 (третьего) рабочего дня, следующего за днем предоставления плательщиком наличных денежных средств);
		5. Предоставлять плательщикам и иным лицам информацию, предусмотренную последним абзацем пункта 2.1.11. настоящего Договора в автоматическом режиме;
		6. В рамках исполнения обязательств по настоящему Договору использовать терминалы в соответствии с требованиями законодательства Российской Федерации о применении контрольно-кассовой техники при осуществлении наличных денежных расчетов;
		7. Ежемесячно предоставлять Банку сведения о суммах денежных средств, принятых от плательщиков в соответствии с настоящим Договором Банковским платёжным агентом и привлечёнными им Банковскими платёжными субагентами и зачисленных на Специальные банковские счета в предыдущем календарном месяце. Указанные сведения предоставляются Банковским платежным агентом путем отражения в Акте об оказании услуг (далее - Акт), образец которого изложен в Приложении №2 к настоящему Договору, и направляются в Банк в порядке, предусмотренном пунктом 3.3. настоящего Договора;
		8. Не превышать ставки разрешённого дополнительного вознаграждения, взимаемого с плательщиков за осуществление операций Банковского платежного агента, размер которых согласован Сторонами в Приложении №1 к настоящему Договору;
		9. Принимать и рассматривать претензии плательщиков, связанные с осуществлением Банковским платежным агентом действий, указанных в п.1.1. Договора;
		10. Направлять в Банк следующую информацию:

2.1.10.1. Сведения о своей деятельности в качестве банковского платежного агента по договорам, заключенным с другими операторами по переводу денежных средств (далее – ОПДС), а также в качестве платежного агента, осуществляющего свою деятельность в соответствии с Федеральным законом от 03.06.2009 № 103-ФЗ «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами» в следующем формате: наименование ОПДС/ поставщика (если Банковский платежный агент по данному договору является оператором по приему платежей)/ поставщика и оператора по приему платежей (если Банковский платежный агент по данному договору является платежным субагентом), с которым Банковский платежный агент заключил соответствующий договор, номер и дата заключенного договора, в каком качестве выступает Банковский платежный агент по данному договору (банковский платежный агент/ оператор по приему платежей/ платежный субагент); срок действия договора.

Указанные сведения предоставляются по форме, приведенной в Приложении № 3 настоящего Договора в течение 5 (пяти) рабочих дней с даты заключения Банковским платежным агентом договора с ОПДС/ поставщиком/ оператором по приему платежей в электронном виде на адрес электронной почты Банка psmtsb@mtsbank.ru.

2.1.10.2. Отчеты, содержащие следующие сведения и подтверждающие их документы (форма отчета приведена в Приложении № 5 к Договору):

а) источники поступления денежных средств на банковские счета Банковского платежного агента, в том числе по каждому терминалу, банкомату Банковского платежного агента;

б) направления, объемы и периодичность списаний денежных средств со Специального банковского счета Банковского платежного агента на другие банковские счета.

Указанные сведения предоставляются за квартал в течение 5 (пяти) рабочих дней с даты окончания последнего календарного месяца квартала в электронном виде на адрес электронной почты Банка psmtsb@mtsbank.ru. Одновременно Отчет передается в Банк на бумажном носителе, заверенный подписью уполномоченного лица и печатью Банковского платежного агента, по адресу Банка, указанному в разделе 10 Договора. К Отчету (в электронном виде и на бумажном носителе) должен прилагаться перечень банкоматов и терминалов, посредством которых Банковский платежный агент осуществлял прием денежных средств в отчетном периоде (квартале) с указанием реквизитов соответствующего банкомата/терминала и адреса его установки.

Отчет по форме Приложения № 5 к Договору предоставляется Банковским платежным агентом как по своему Специальному счету, так и по специальным банковским счетам привлеченных БПА банковских платёжных субагентов.

2.1.10.3. Перечень привлеченных платежных субагентов, Банковских платёжных субагентов (с указанием наименования, ИНН, ОГРН, места нахождения и адреса таких платежных агентов/ банковских платежных субагентов), адреса мест осуществления операций Банковского платежного агента и привлечённых им платежных субагентов и Банковских платёжных субагентов, реквизиты договоров, заключенных между Банковским платежным агентом и платежными субагентами/ банковскими платежными субагентами, извещения об изменении любых данных Банковского платежного агента и привлечённых им платежных субагентов и Банковских платёжных субагентов, в том числе места нахождения и адреса, адреса (адресов) электронной почты, контактных телефонов, изменении уполномоченных представителей Банковского платежного агента/субагентов, изменении банковских реквизитов Банковского платежного агента/субагентов и т.д.

Указанные сведения должны быть направлены в течение 3 (трех) рабочих дней с момента заключения настоящего Договора/заключения Банковским платежным агентом договора о привлечении платежного субагента или Банковского платежного субагента/изменения соответствующих данных по адресу электронной почте psmtsb@mtsbank.ru.

2.1.10.4. По запросу Банка:

а) сведения о количестве платежных терминалов и банкоматов с указанием адреса их установки;

б) документы, подтверждающие использование контрольно-кассовой техники в составе платежных терминалов, банкоматов.

Указанные сведения должны быть направлены в Банк в течение 3 (трех) рабочих дней с даты запроса Банка по адресу электронной почте psmtsb@mtsbank.ru.

 2.1.10.5. Информацию и документы (по требованию Банка), необходимые для осуществления контроля Банком за выполнением Банковским платежным агентом требований законодательства Российской Федерации и положений настоящего Договора, в том числе сведения об открытых специальных банковских счетах БПА в других кредитных организациях по форме приведенной в Приложении № 4 настоящего Договора в срок не позднее 3 (трех) рабочих дней от даты направления требования Банка на адрес электронной почты БПА \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_;

* + 1. В соответствии с действующим законодательством использовать контрольно-кассовую технику с фискальной памятью и контрольной лентой, а также соблюдать иные требования законодательства Российской Федерации о применении контрольно-кассовой техники при осуществлении наличных денежных расчетов (в том числе при применении Банковским платежным агентом платежного терминала), подтверждать принятие распоряжений плательщика и наличных денежных средств путем выдачи кассового чека. БПА при осуществлении расчетов с использованием терминалов обязан выдать кассовый чек на бумажном носителе (при этом все реквизиты, напечатанные на кассовом чеке, должны быть четкими и легко читаемыми) и (или) направить плательщику кассовый чек в электронной форме на предоставленные абонентский номер либо адрес электронной почты (при наличии технической возможности для передачи информации плательщику в электронной форме на адрес электронной почты). Кассовый чек, выдаваемый (направляемый) плательщику, согласно требованиям о применении контрольно-кассовой техники, изложенным в Федеральном законе от 22.05.2003 № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации» (далее – Федеральный закон № 54-ФЗ), должен содержать следующую информацию:
* наименование документа – кассовый чек;
* порядковый номер за смену;
* номер смены;
* дата, время и место (адрес) осуществления расчета (при расчете в зданиях и помещениях - адрес здания и помещения с почтовым индексом);
* признак расчета (получение средств от плательщика) – приход;
* наименование операции Банковского платежного агента – прием наличных денежных средств с целью перевода;
* сумма расчета - общая сумма принятых денежных средств от плательщика;
* форма расчета – оплата наличными деньгами;
* регистрационный номер контрольно-кассовой техники;
* заводской номер экземпляра модели фискального накопителя;
* фискальный признак документа;
* адрес сайта уполномоченного органа в сети "Интернет", на котором может быть осуществлена проверка факта записи этого расчета и подлинности фискального признака;
* порядковый номер фискального документа;
* фискальный признак сообщения (для кассового чека или бланка строгой отчетности, хранимых в фискальном накопителе или передаваемых оператору фискальных данных);
* QR-код;
* абонентский номер либо адрес электронной почты плательщику в случае передачи ему кассового чека в электронной форме или идентифицирующих такой кассовый чек признаков и информации об адресе информационного ресурса в сети "Интернет", на котором такой документ может быть получен;
* адрес электронной почты БПА - отправителя кассового чека в электронной форме в случае передачи плательщику кассового чека в электронной форме.

Кассовый чек, выдаваемый (направляемый) плательщику Банковским платежным агентом, может не содержать обязательные реквизиты о ставке и размере налога на добавленную стоимость.

 Дополнительно к требованиям законодательства Российской Федерации, указанным в Федеральном законе № 54-ФЗ и перечисленным выше, кассовый чек должен содержать следующую информацию:

* адрес места осуществления операций Банковского платежного агента;
* наименование и место нахождения Банка и Банковского платежного агента, а также их идентификационные номера налогоплательщика;
* номер лицензии Банка на осуществление банковских операций;
* реквизиты настоящего Договора;
* размер вознаграждения, уплачиваемого плательщиком в виде общей суммы, включающей в том числе вознаграждение Банковского платежного агента в случае его взимания;
* способы подачи претензий и порядок их рассмотрения;
* номера телефонов Банка, Банковского платежного агента и Банковского платежного субагента (в случае его привлечения Банковским платежным агентом).

При использовании Банковским платежным агентом терминала информация, предусмотренная настоящим абзацем, должна предоставляться плательщикам - физическим лицам в автоматическом режиме до начала осуществления каждой операции физическим лицом посредством направления ее на экран терминала (перед печатью кассового чека).

* + 1. До даты внесения Обеспечительного платежа, указанного в п.3.6. Договора, не осуществлять деятельность (операции), предусмотренную п.1.1. Договора;
		2. Использовать программно-аппаратный комплекс Банка (ПО Банка) для исполнения поручения по настоящему Договору (в том числе, для фиксирования информации о каждой операции приема наличных денежных средств, принятых от конкретных плательщиков и обеспечения доступа Банка к данной информации), а также обеспечить использование ПО Банка Банковскими платежными субагентами.
		3. Осуществлять прием денежных средств в соответствии с Правилами работы в ПО Банка (далее – Правила), указанными в Приложении 6 к Договору, а также обеспечить соблюдение Правил Банковскими платежными субагентами.
		4. Соблюдать организационные и технические меры по защите информации в соответствии с Приложением № 8 к настоящему Договору.
	1. **Банковский платежный агент вправе:**
		1. Взимать с плательщика дополнительное вознаграждение за осуществление операций Банковского платежного агента в размере, согласованном Сторонами в Приложении №1 к Договору. Указанное в настоящем [пункте](#Par71) дополнительное вознаграждение полностью поступает в распоряжение Банковского платежного агента и не включается в расчет вознаграждения Банковского платежного агента, предусмотренного настоящим Договором.
		2. Для осуществления видов деятельности, предусмотренных п.1.1. настоящего Договора, привлекать Банковских платежных субагентов на основании Договора о привлечении банковского платежного субагента, образец которого приведен в Приложении №10 к настоящему Договору. Банковский платежный агент вправе вносить изменения в образец при заключении Договора о привлечении банковского платежного субагента, предварительно согласовав их с Банком. При таком привлечении Банковский платежный субагент вправе взимать с плательщиков вознаграждение в размере, установленном заключенным с ним Банковским платежным агентом договором. Размер вознаграждения, взимаемого с плательщика Банковским платежным субагентом и Банковским платежным агентом, в совокупности не может превышать размера вознаграждения, установленного для Банковского платежного агента в Приложении № 1 к настоящему Договору.
	2. **Банк обязан:**

2.3.1. Информировать Банковского платежного агента по адресу электронной почты \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_ о возникновении технических неполадок и иных событий, препятствующих выполнению условий настоящего Договора;

2.3.2. Извещать Банковского платёжного агента об изменении любых данных Банка, указанных в настоящем Договоре, в том числе местонахождения, адреса электронной почты, контактных телефонов, изменении уполномоченных представителей Банка, изменении банковских реквизитов Банка и т.д. Извещение должно быть направлено в течение 3 (трех) рабочих дней с момента изменения соответствующих данных.

* 1. **Банк вправе:**

2.4.1. Осуществлять контроль за соблюдением Банковским платежным агентом условий, установленных статьей 14 Федерального закона «О национальной платежной системе» от 27.06.2011 № 161-ФЗ (далее – Федеральный закон № 161-ФЗ), настоящим Договором и законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Порядок осуществления контроля Банком за деятельностью Банковского платежного агента устанавливается нормативными актами Банка России и [п. 2.4.2.](#Par68) настоящего Договора;

2.4.2. В целях осуществления контроля за соблюдением Банковским платежным агентом условий настоящего Договора, в том числе в части соблюдения правил осуществления расчетов в Российской Федерации, требований ст.14 Федерального закона №161-ФЗ, а также требований Федерального закона № 115-ФЗ:

- проводить проверки в торговой сети Банковского платежного агента или привлечённых им Банковских платёжных субагентов, в том числе с использованием методики «тайный покупатель». Результаты проверки оформляются актами проверки, составленными Банком в одностороннем порядке;

- на основании актов проведенных проверок требовать от Банковского платежного агента устранения выявленных замечаний, принятия мер к недопущению повторных замечаний, устанавливать сроки для выполнения требований Банка. Требования направляются Банком Банковскому платежному агенту по почте в письменном виде либо по электронной почте на адрес \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_. К требованию должен быть приложен акт проверки;

- запрашивать у Банковского платежного агента информацию и документы (заверенные надлежащим образом копии первичных документов, подтверждающих прием денежных средств (контрольные ленты контрольно-кассовой техники, оригиналы заявлений о возврате денежных средств, изменений реквизитов плательщика), а также иную информацию и документы в целях подтверждения исполнения Банковским платежным агентом обязанностей по настоящему Договору;

- направлять запросы в адрес Банковского платежного агента для получения от него информации о всех специальных банковских счетах, предусмотренных частью 3 пункта 3 статьи 14 Федерального закона N 161-ФЗ, открытых Банковскому платежному агенту для целей осуществления деятельности от имени оператора по переводу денежных средств согласно п. 2.1.10.5 настоящего Договора, выписок по указанным специальным банковским счетам, а также необходимых Банку для осуществления контроля копий первичных учетных документов.

2.4.3. В случае возникновении технических неполадок и иных событий, за исключением случаев, указанных в п. 3.6.3 настоящего Договора, препятствующих выполнению условий настоящего Договора, блокировать возможность осуществления Банковским платёжным агентом приема денежных средств, уведомив Банковского платёжного агента за 3 (три) рабочих дня по адресу электронной почты \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_ с указанием причины блокировки;

2.4.4. При несоблюдении Банковским платежным агентом указанных в настоящем Договоре условий его привлечения, требований Федерального закона № 161-ФЗ или законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма принять следующие меры:

* направить Банковскому платежному агенту письменное предупреждение о необходимости приведения его деятельности в соответствие с требованиями заключенного Договора и/или законодательства Российской Федерации с указанием сроков исправления нарушений и условием недопущения нарушений в дальнейшем;
* предъявить Банковскому платежному агенту письменное требование об уплате штрафов (неустойки) в соответствии с Договором на основании выставленного Банком требования (счета) об уплате;
* отказаться от исполнения Договора в одностороннем порядке;

2.4.5. Списывать со Специального банковского счета без дополнительного распоряжения Банковского платежного агента (заранее данный акцепт) денежные средства в размере, необходимом для осуществления переводов денежных средств по поручению плательщиков, и осуществлять перевод денежных средств на счета получателей в соответствии с распоряжениями плательщиков;

2.4.6. Списывать с расчетного счета Банковского платежного агента в Банке №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ без дополнительного распоряжения Банковского платежного агента (заранее данный акцепт) денежные средства в размере, необходимом для погашения задолженности Банковского платежного агента перед Банком, возникшей из настоящего Договора.

2.4.7. Списывать с расчетного счета Банковского платежного агента в Банке № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ без дополнительного распоряжения Банковского платежного агента (заранее данный акцепт) денежные средства в размере суммы вознаграждения, указанного в столбце 5 таблицы п. 1.1. Приложения № 1 к Договору, после перевода денежных средств в указанном размере со Специального банковского счета на расчетный счет Банковского платежного агента в Банке № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, произведенного в соответствии с п. 2.1.4. Договора.

2.5. Банковский платежный агент поручает Банку:

- осуществлять перевод денежных средств со Специального банковского счета на банковские счета получателей средств не позднее следующего рабочего дня после внесения денежных средств/ зачисления денежных средств на основании данных о принятых Банковским платежным агентом у плательщиков суммах денежных средств;

– осуществлять перевод денежных средств со Специального банковского счета на расчетный счет Банковского платежного агента в Банке № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в размере суммы вознаграждения, указанного в столбце 5 таблицы п. 1.1. Приложения № 1 к Договору.

1. **Финансовые условия.**
	1. Банк уплачивает Банковскому платежному агенту вознаграждение за осуществление деятельности банковского платежного агента согласно п.1.1. и п.1.2. настоящего Договора (за выполнение поручения, указанного в п.1.1. и п.1.2. Договора), размер которого определяется в соответствии с Приложением № 1 к настоящему Договору, в том числе НДС по ставке, подлежащей применению в соответствии с законодательством РФ. Приложение № 1 к Договору может быть изменено по соглашению Сторон путем обмена официальными письмами, подписанными уполномоченными представителями Сторон. Официальные письма об изменении Приложения № 1 к Договору должны быть переданы Сторонами друг другу и получены ими не позднее чем за 5 (пять) рабочих дней до введения в действие новой редакции Приложения № 1 к Договору.
	2. Банк рассчитывает вознаграждение Банковскому платежному агенту за приём денежных средств от суммы фактически принятых от плательщиков денежных средств в отчетном (календарном) периоде и перечисленных в пользу получателей денежных средств в отчетном календарном месяце.
	3. Банковский платежный агент не позднее 3 (трех) рабочих дней месяца, следующего за отчетным (календарным), предоставляет Банку на предварительное согласование Акт в электронном виде на адрес электронной почты psmtsb@mtsbank.ru, который согласовывается Банком в течение 3 (трех) рабочих дней. В случае несогласия с данными, указанными в Акте, Банк обязуется в тот же срок предоставить Банковскому платежному агенту свои мотивированные возражения на адрес электронной почты: \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_. Если в течение указанного срока Банк не представил возражений, Акт считается полностью одобренным и принятым Банком.
	4. В течение 3 (трех) рабочих дней с момента согласования Сторонами Акта Банковский платежный агент направляет 2 (два) экземпляра подписанных со своей стороны экземпляров Акта, счет на оплату вознаграждения и счет-фактуру в Банк по адресу, указанному в п.9.2. настоящего Договора. Банк обязан подписать и направить один экземпляр оригинала Акта Банковскому платежному агенту по адресу, указанному в п. 9.2. настоящего Договора, в течение 3 (трех) рабочих дней с даты его получения от Банковского платежного агента.
	5. Не позднее 3 (Трех) рабочих дней с даты подписания Акта Сторонами Банк перечисляет сумму вознаграждения на основании выставленного Банковским платежным агентом счета на оплату и счета-фактуры.
	6. В качестве обеспечения надлежащего исполнения обязательств по настоящему Договору до начала осуществления деятельности, предусмотренной п.1.1. настоящего Договора, Банковский платёжный агент перечисляет Банку обеспечительный платеж (далее - Обеспечительный платеж),  размер которого устанавливается Сторонами в следующем порядке:  Банковский платежный агент уведомляет Банк об установлении суммы Обеспечительного платежа в определенном размере путем направления сообщения по адресу электронной почты psmtsb@mtsbank.ru, за 1 (Один) рабочий день до даты перечисления/изменения суммы Обеспечительного платежа;  если Банк в день получения электронного сообщения от Банковского платежного агента не представит возражений относительно заявленной суммы Обеспечительного платежа на адрес электронной почты: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ , то размер Обеспечительного платежа считается установленным в сумме, указанной в электронном сообщении Банковского платежного агента. Банковский платежный агент вправе в любой момент инициировать изменение размера Обеспечительного платежа, направив в адрес Банка соответствующее электронное сообщение в порядке, предусмотренном настоящим пунктом Договора, и перечислив Банку дополнительную сумму денежных средств (если необходимо). Сумма Обеспечительного платежа НДС не облагается. Уменьшение суммы Обеспечительного платежа возможно только после полного погашения обязательств БПА согласно п. 2.1.4 настоящего Договора и при условии,  что сумма Обеспечительного платежа после ее снижения окажется не меньшей суммы денежных средств, принятых от плательщиков (в соответствии с данными ПО Банка), но не внесенных/не переведенных на Специальный банковский счет согласно п.2.1.4.
		1. Обеспечительный платеж перечисляется Банковским платёжным агентом по реквизитам, которые Банк предоставляет БПА в течение 3 (Трех) рабочих дней после подписания настоящего Договора. На сумму Обеспечительного платежа Банк не начисляет проценты, в том числе проценты по денежному обязательству в соответствии со ст.317.1. ГК РФ.
		2. В случае неисполнения Банковским платёжным агентом в установленные сроки обязательств, предусмотренных п.2.1.4. настоящего Договора, Банк уменьшает Обеспечительный платеж путем перечисления соответствующей суммы получателям в соответствии с условиями настоящего Договора, распоряжениями плательщиков, денежные средства у которых были приняты Банковским платежным агентом. Банк информирует Банковского платежного агента об уменьшении суммы Обеспечительного платежа путем направления электронного сообщения на адрес электронной почты \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_ непосредственно в день уменьшения суммы Обеспечительного платежа. Банковский платежный агент обязан пополнить (восстановить) сумму Обеспечительного платежа до необходимого размера, установленного в порядке, предусмотренном п.3.6. настоящего Договора.
		3. В случае, если сумма денежных средств, принятых от плательщиков (в соответствии с данными ПО Банка), но не внесенных/не переведенных на Специальный банковский счет согласно п.2.1.4 Договора, достигнет размера суммы Обеспечительного платежа, установленного в соответствии с п.3.6. Договора, Банк вправе в одностороннем порядке приостановить (прекратить) прием Банковским платежным агентом (и привлеченными им Банковскими платежными субагентами) денежных средств от плательщиков с последующим направлением Банковскому платежному агенту уведомления по адресу электронной почты \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_. После внесения/зачисления на Специальный банковский счет денежных средств в размере, соответствующем сумме принятых от плательщиков денежных средств (в соответствии с данными ПО Банка) прием Банковским платежным агентом (и привлеченными им Банковскими платежными субагентами) денежных средств от плательщиков по решению Банка возобновляется.
		4. В случае расторжения настоящего Договора Обеспечительный платеж, за вычетом сумм, возможность удержания которых Банком предусмотрена настоящим Договором, подлежит возврату Банком Банковскому платёжному агенту путем перечисления на счет Банковского платёжного агента по реквизитам, которые Банковский платежный агент сообщит Банку письменно, в течение 5 (Пяти) календарных дней с даты расторжения настоящего Договора.
2. **Ответственность Сторон**
	1. Банковский платежный агент обязан возместить Банку реальный ущерб, причиненный в результате неисполнения (ненадлежащего исполнения) обязательств по настоящему Договору, в том числе, суммы уплаченных Банком штрафов в случае привлечения Банка к административной ответственности в связи с допущенными Банковским платежным агентом нарушениями требований ФЗ «О персональных данных» при обработке персональных данных.
	2. Банковский платежный агент в полном объеме несет ответственность перед Банком по всем операциям, совершенным Банковским платежным агентом, его уполномоченными лицами.
	3. В случае неисполнения/ненадлежащего исполнения обязательств Банковского платежного агента при осуществлении расчетов в соответствии с п.2.1.4 настоящего Договора по соблюдению сроков поступления денежных средств на Специальный банковский счет, Банковский платежный агент уплачивает Банку неустойку в размере 0,5 % (Ноль целых пять десятых) процентов от суммы неисполненного обязательства за каждый день неисполнения.
	4. Банк в рамках настоящего Договора не несет ответственности за неисполнение/ненадлежащее исполнение своих обязательств, если это явилось результатом предоставления со стороны Банковского платежного агента неполной/недостоверной информации, используемой Банком для исполнения соответствующих обязательств по настоящему Договору. Банк не несет ответственности по спорам и разногласиям, возникшим между Банковским платежным агентом и Клиентами во всех случаях, когда споры и разногласия не относятся к предмету Договора.
	5. Банк не несет ответственности за убытки Банковского платежного агента либо плательщика, возникшие вследствие злого умысла или ошибки со стороны сотрудников Банковского платежного агента.
	6. Стороны обязуются соблюдать требования антикоррупционного законодательства и не предпринимать никаких действий, которые могут нарушить нормы антикоррупционного законодательства, в связи со своими правами или обязательствами согласно Договору, в том числе (не ограничиваясь) не совершать от своего имени предложение, санкционирование, обещание и осуществление незаконных платежей, включая (но не ограничиваясь) взятки в денежной или любой иной форме, каким-либо физическим или юридическим лицам, включая (но не ограничиваясь) коммерческие организации, органы власти и самоуправления, государственных служащих, частных компаний и их представителей.
	7. В случае нарушения какой-либо из Сторон, указанных в настоящем разделе обязательств, другая сторона имеет право в одностороннем внесудебном порядке отказаться от исполнения Договора. Нарушившей стороне не возмещаются убытки в случае отказа другой стороны от исполнения Договора в соответствии с настоящим пунктом.
	8. В случае получения штрафов со стороны Банка России за недобросовестное выполнение функций по соблюдению требований информационной безопасности, БПА обязуется компенсировать Банку размер штрафов, выставленных со стороны Банка России.
	9. В случае совершения БПА любых несанкционированных отправок денежных переводов от своего имени посредством нарушения безопасности компьютерных систем БПА, последний также компенсируют Банку все убытки и финансовые потери, которые понес Банк в связи с указанными нарушениями.
3. **Срок действия Договора**
	1. Настоящий Договор вступает в силу с момента его подписания Сторонами и действует в течение неопределенного срока.
	2. Досрочное расторжение Договора возможно в следующих случаях:
		1. По соглашению Сторон, оформленному в письменном виде;
		2. По инициативе любой из Сторон. Сторона, отказывающаяся от дальнейшего исполнения настоящего Договора, в письменной форме уведомляет другую сторону о своем намерении расторгнуть Договор не позднее, чем за 60 (шестьдесят) календарных дней до предполагаемой даты расторжения Договора. Уведомление должно быть сделано в письменной форме на бумажном носителе и содержать указание на причину расторжения Договора;
		3. По инициативе Банка при нарушении Банковским платежным агентом любого из условий настоящего Договора;
		4. В иных случаях, предусмотренных настоящим Договором и действующим законодательством Российской Федерации.
	3. В случае несоблюдения Банковским платежным агентом условий его привлечения, предусмотренных настоящим Договором, требований статьи 14 Федерального закона № 161-ФЗ и законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма Банк вправе в одностороннем порядке отказаться от Договора (исполнения Договора). Банк уведомляет Банковского платежного агента об одностороннем отказе от Договора (исполнения Договора) путем направления ему соответствующего письменного уведомления в электронной форме по адресу электронной почты \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_ и на бумажном носителе курьером либо заказным почтовым отправлением с уведомлением о вручении по адресу, указанному в разделе 10 настоящего Договора. Договор в этом случае прекращается с даты, указанной в уведомлении Банка.
	4. Обязательства Сторон по настоящему Договору, возникшие до расторжения/прекращения настоящего Договора, сохраняются вплоть до их полного исполнения.
4. **Конфиденциальность**
	1. Банковский платёжный агент обязуется соблюдать конфиденциальность персональных данных плательщиков и обеспечивать безопасность персональных данных при их обработке. При обработке персональных данных Банковский платёжный агент должен руководствоваться требованиями к защите персональных данных, установленными законодательными актами РФ.
	2. Стороны договорились сохранять в режиме конфиденциальности сведения, составляющие коммерческую тайну каждой из Сторон. Под сведениями, составляющими коммерческую тайну, понимаются не являющиеся общедоступными сведения о деятельности каждой из Сторон, разглашение которых может привести к возникновению убытков и/или негативно повлиять на деловую репутацию любой из Сторон, а также на информацию, которую любая из Сторон идентифицирует как конфиденциальную до или сразу после ее предоставления другой Стороне.
	3. Стороны принимают на себя обязательства не разглашать полученные в ходе исполнения настоящего Договора сведения, составляющие банковскую или иную охраняемую законом тайну, включая, но не ограничиваясь, информацию об операциях, о персональных данных плательщиков.
	4. Информация, составляющая банковскую или иную охраняемую законом тайну, может быть сообщена третьим лицам только при наличии письменного разрешения плательщика, за исключением случаев, предусмотренных действующим законодательством.
	5. В целях обеспечения конфиденциальности при передаче информации между Сторонами, в том числе обрабатываемых персональных данных, Стороны обязуются организовать и использовать только защищенный канал связи.
	6. Факт заключения настоящего Договора и предмет Договора не являются конфиденциальной информацией. К информации, признаваемой в соответствии с настоящим Договором конфиденциальной, не могут относиться сведения, являющиеся в соответствии с требованиями российского законодательства общедоступными.
	7. Обязательства о конфиденциальности сохраняют силу в течение пяти лет после истечения срока действия или расторжения настоящего Договора.
5. **Запрет неправомерного использования и разглашения инсайдерской информации.**
	1. Банк не вправе разглашать или иным образом использовать информацию о ПАО «МТС» и аффилированных лицах ПАО «МТС», их деятельности, ценных бумагах, которая не является общедоступной («инсайдерская информация»), которая стала известной ему в результате реализации прав исполнения обязанностей по настоящему Договору.
	2. Банк не вправе самостоятельно совершать сделки или давать кому-либо поручение (указание) о совершении сделок с ценными бумагами ПАО «МТС» или его аффилированных лиц на основе инсайдерской информации.
	3. Банк не вправе передавать кому-либо инсайдерскую информацию, за исключением случаев передачи инсайдерской информации третьим лицам в процессе реализации прав и выполнения обязанностей по настоящему Договору при условии наличия письменного согласия ПАО «МТС» на такую передачу.
	4. Разрешение и передача инсайдерской информации третьим лицам в процессе исполнения настоящего

Договора должны осуществляться ПАО «МТС» исключительно в случаях, предусмотренных настоящим Договором, и в пределах, необходимых для реализации прав и выполнения обязанностей, предусмотренных настоящим Договором, и в порядке, предусмотренном действующим законодательством и внутренними документами ПАО «МТС».

* 1. Банк не вправе использовать инсайдерскую информацию в целях, не отвечающих целям реализации

прав и исполнения обязанностей по настоящему Договору, в том числе использовать инсайдерскую информацию в своих интересах и в интересах третьих лиц, включая (но не ограничиваясь):

* осуществление торговли на основании инсайдерской информации;
* рекомендации третьим лицам о покупке, продаже, сохранении ценных бумаг ПАО «МТС» на основании инсайдерской информации;
* передачу инсайдерской информации третьим лицам за вознаграждение или без вознаграждения;
* публикацию или распространение инсайдерской информации иным образом.
	1. ПАО «МТС» вправе потребовать от Банка, виновного в неправомерном использовании и распространении инсайдерской информации, возмещения убытков, причиненных ПАО «МТС» указанными неправомерными действиями.
1. **Антикоррупционная оговорка**
	1. В рамках исполнения настоящего Договора Стороны подтверждают, что в своей деятельности придерживаются высоких этических стандартов и обязуются соблюдать требования Применимого антикоррупционного законодательства, и не будут предпринимать никаких действий, которые могут нарушить нормы Применимого антикоррупционного законодательства или стать причиной такого нарушения другой Стороной, в том числе не требовать, не получать, не предлагать, не санкционировать, не обещать и не совершать незаконные платежи напрямую, через третьих лиц или в качестве посредника, включая (но не ограничиваясь) взятки в денежной или любой иной форме, каким-либо физическим или юридическим лицам, включая (но не ограничиваясь) органам власти и самоуправления, государственным служащим, частным компаниям и их представителям.
	2. Стороны обязуются не совершать действий (бездействий), создающих угрозу возникновения конфликта интересов, а также в разумные сроки сообщать другой Стороне о ставших известными ей обстоятельствах, способных вызвать конфликт интересов.
	3. Канал уведомления ПАО «МТС-Банк» для направления (раскрытия) сведений: compliance@mtsbank.ru.
	4. Канал уведомления БПА для направления (раскрытия) сведений: \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_.
	5. Стороны подтверждают, что любые третьи лица, привлеченные для исполнения настоящего Договора, не осуществляют свои действия с целью оказать незаконное влияние на Государственных должностных лиц либо с целью коммерческого подкупа и будут допущены к выполнению договорных обязательств после проведения достаточных проверочных мероприятий привлекающей их Стороной.
	6. Стороны обязуются надлежащим образом вести и хранить всю бухгалтерскую отчетность, и другие документы, подтверждающие расходы, осуществленные по настоящему Договору. Стороны обязуются в полной мере оказывать поддержку в отношении любого расследования и/или аудита, который может проводится в рамках исполнения настоящего Договора. Стороны обязуются охранять всю конфиденциальную информацию, которая может стать им известна в рамках аудита, в соответствии с законодательством РФ.
	7. В случае нарушения одной из Сторон изложенных в п. 8.1 - 8.2. антикоррупционных обязательств, другая Сторона вправе в одностороннем порядке приостановить исполнение своих обязательств по настоящему Договору до устранения причин такого нарушения или отказаться от исполнения Договора, направив об этом письменное уведомление.
	8. Под Применимым антикоррупционным законодательством понимается:

1) российское антикоррупционное законодательство (Федеральный закон от 25.12.2008 г. № 273-ФЗ «О противодействии коррупции», Уголовный Кодекс РФ, Гражданский Кодекс РФ, Кодекс РФ об административных правонарушениях, а также иные Федеральные законы и подзаконные нормативные правовые акты РФ, содержащие нормы, направленные на борьбу с коррупцией.),

2) иные законы по борьбе со взяточничеством и коррупцией, постановления, правила, политики, надзорные указания зарубежных стран, включая Закон США «О противодействии коррупции за рубежом», Закон Великобритании «О взяточничестве» 2010, в той мере, в какой указанные акты применимы к соответствующей Стороне.

* 1. Под Государственным Должностным Лицом понимается:

- любое российское или иностранное, назначаемое или избираемое лицо, занимающее какую-либо должность в законодательном, исполнительном, административном или судебном органе, или международной организации;

- любое лицо, выполняющее какую-либо публичную функцию для государства, в том числе для государственной организации;

- ведущие политические деятели, должностные лица политических партий, включая кандидатов на политические посты, послы, влиятельные функционеры в национализированных областях промышленности или естественных монополиях;

- руководители и сотрудники Государственных органов, учреждений и предприятий, включая врачей, военнослужащих, муниципальных служащих и т.п.;

- лица, о которых известно, что они связаны с государственным должностным лицом родственными, дружескими или деловыми отношениями и (или) действуют от имени и(или) в интересах государственного должностного лица.

1. **Дополнительные условия и заключительные положения**
	1. Во всем остальном, что не предусмотрено настоящим Договором, Стороны руководствуются действующим законодательством Российской Федерации.
	2. Уведомления и/или извещения по настоящему Договору, если иное не установлено настоящим Договором, должны быть совершены в письменной форме, и могут вручаться путём доставки лично под расписку, через курьера, а также посредством заказной или экспресс-почтой по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Адрес ПАО «МТС-Банк» (почтовый): 115432, г. Москва, пр-т Андропова, дом 18, корп. 1.

* 1. Договор составлен в двух экземплярах, по одному для каждой из Сторон.
	2. К настоящему Договору прилагаются и являются его неотъемлемой частью следующие Приложения:

Приложение №1- Перечень и условия совершения операций, подлежащих выполнению Банковским платёжным агентом;

Приложение №2 - Акт об оказании услуг (образец);

Приложение №3 - Сведения о деятельности в качестве банковского платежного агента;

Приложение №4 - Уведомление Банковского платежного агента об открытых специальных банковских счетах;

Приложение № 5 - Отчет Банковского платежного агента ПАО «МТС» за «\_\_\_\_\_\_\_\_\_\_\_\_» 20\_\_\_\_г по Специальному банковскому счету;

Приложение № 6 – Правила работы в программном обеспечении Банка;

Приложение № 7 – Договор о привлечении банковского платежного субагента (образец);

Приложение № 8 – Перечень принимаемых организационных и технических мер по защите информации.

1. **Реквизиты и подписи Сторон:**

|  |  |
| --- | --- |
| Публичное акционерное общество «МТС-Банк»Место нахождения: 115432, Российская Федерация, город Москва, пр-т Андропова, дом 18, корп. 1, ОГРН 1027739053704, ИНН 7702045051, К/счет 30101810600000000232 в ГУ Банка России по Центральному федеральному округу, БИК 044525232 Бизнес-лидер Стрима «Система денежных переводов»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | Банковский платежный агент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Юридический адрес: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ИНН \_\_\_\_\_\_\_\_\_\_КПП \_\_\_\_\_\_\_\_\_р/с № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_БИК \_\_\_\_\_\_\_\_\_к/с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_/мп |

**Приложение №1**

**к Договору о привлечении банковского платежного агента**

**№\_\_\_\_\_\_\_\_\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.**

**Перечень и условия совершения операций, подлежащих выполнению Банковским платёжным агентом**

1. Проведение операций по приёму от физических лиц денежных средств в целях осуществления переводов без открытия банковского счета в пользу юридических лиц, перечисленных в п. 1.1 настоящего Приложения для оплаты работ/услуг, при условии, что такие переводы в соответствии с Федеральным законом № 115-ФЗ не требуют проведения идентификации, в том числе упрощенной идентификации:
	1. Перечень получателей переводов, размер вознаграждения:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Наименование юридического лица получателя | Наименование получателя в ПО Банка | Дополнительное вознаграждение (вознаграждение, взимаемое Банковским платежным агентом) | Размер вознаграждения Банковского платежного агента, выплачиваемого Банком, в том числе НДС по ставке, подлежащей применению в соответствии с законодательством РФ (в % от суммы принятых денежных средств плательщиков или в рублях) | Размер вознаграждения, взимаемое Банком с плательщика, НДС не облагается (в % от суммы принятых денежных средств плательщиков или в рублях | Минимальная сумма перевода, руб. | Максимальная сумма перевода, руб. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |

**Подписи Сторон:**

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /мп |

 **Приложение №2**

**к Договору о привлечении банковского платежного агента**

**№ \_\_\_\_\_\_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г.**

|  |  |
| --- | --- |
|  | *Образец***Акт об оказании услуг №\_\_\_\_\_** |
|  | г. Москва \_\_ \_\_\_\_\_\_\_ 20\_\_г. |
|  |  |  |  |
| ООО «\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_», именуемое в дальнейшем «Банковский платежный агент», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и **ПАО «\_\_\_\_\_\_\_\_\_\_\_»**, именуемое в дальнейшем «Банк», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, вместе именуемые «Стороны», составили настоящий АКТ по Договору № \_\_\_\_\_\_\_\_\_\_\_\_от \_\_\_\_\_\_\_\_\_\_\_\_\_ (далее – «Договор») о нижеследующем: |
|  |  |  |  |
| 1. В соответствии с условиями Договора Банковским платежным агентом были оказаны услуги в следующем объеме: |
|  |  |  |  |
| **№ п/п** | **Наименование показателя** | **Значение показателя** | **Единица измерения** |
| 1 | Дата и время начала отчетного периода | \_\_.\_\_.20\_\_ | 00:00:00 |
| 2 | Дата и время окончания отчетного периода | \_\_.\_\_.20\_\_ | 23:59:59 |
| **Обеспечительные платежи** |
| 3 | Сумма Обеспечительного платежа, перечисленная (+)/списанная (-) на счет в Банке в Отчетном периоде (календарном месяце) |  | руб. |
| 4 | Остаток суммы Обеспечительного платежа на конец предыдущего отчетного периода |  | руб. |
| 5 | Остаток суммы Обеспечительного платежа на конец отчетного периода  |  | руб. |
| **Платежи БПА** |
| 6 | Сумма наличных денежных средств, принятых от плательщиков в отчетном периоде  |  | руб. |
| 7 | Сумма наличных денежных средств, принятых от плательщиков в отчетном периоде и Подлежащая зачислению на Специальный банковский счет БПА *ОБРАЗЕЦ* |  | руб. |
| 8 | Сумма наличных денежных средств, принятых от плательщиков и зачисленных на Специальный банковский счет БПА в отчетном периоде |  | руб. |
| 9 | Сумма наличных денежных средств, принятых от плательщиков в отчетном периоде, подлежащая зачислению на Специальные банковские счета БПА в следующем отчетном периоде |  | руб. |
| **Вознаграждение БПА** |
| 10 | Сумма вознаграждения Банковского платежного агента, подлежащая к перечислению Банком за отчетный период, в т.ч. НДС по ставке, подлежащей применению в соответствии с законодательством РФ \_\_\_\_\_\_.\_\_ руб. |  | руб. |
|  |  |  |  |
| 2. Итого подлежит выплате Банковскому платежному агенту вознаграждение за отчетный период в сумме \_\_\_\_\_\_\_\_**.**\_\_ (\_\_\_\_\_\_\_\_) рублей \_\_ копеек, в т.ч. НДС по ставке, подлежащей применению в соответствии с законодательством РФ, составляет \_\_\_\_\_\_.\_\_ руб. 3. Обязательства Банковского платежного агента по оказанию услуг, предусмотренных Договором, выполнены в полном объеме, в соответствии с условиями Договора. 4. Банк не имеет каких-либо претензий по оказанным Банковским платежным агентом услугам за период, указанный в настоящем Акте. 5. Настоящий Акт составлен в двух экземплярах, по одному для каждой из Сторон. |
|  |  |  |  |

 **Банк**  **Банковский платёжный агент**

\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_/

 мп мп

***Образец Акта согласован:***

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /мп |

**Приложение № 3**

**к Договору о привлечении банковского платежного агента**

**№ \_\_\_\_\_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.**

**Сведения о деятельности в качестве банковского платежного агента**

Полное или сокращенное фирменное наименование БПА \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Адрес (место нахождения) БПА \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН \_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование оператора по переводу денежных средств (кроме МТС Банка) / поставщика[[1]](#footnote-2)  | Признак банковского платежного агента[[2]](#footnote-3) | Номер договора, заключенного с другими операторами по переводу денежных средств (кроме МТС Банк) / поставщиками | Дата заключенного договора | Срок действия договора |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /мп |

*ОБРАЗЕЦ*

**Приложение № 4**

**к Договору о привлечении банковского платежного агента**

**№ \_\_\_\_\_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.**

**Уведомление Банковского платежного агента об открытых специальных банковских счетах**

**на дату «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ г.**

Полное или сокращенное фирменное наименование БПА \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Адрес (место нахождения) БПА \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование кредитных организаций, в которых открыты специальные банковские счета банковскому платежному агенту | БИК | № специального банковского счета |
| 1 |  |  |  |
| 2 |  |  |  |

*ОБРАЗЕЦ*

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /мп |

**Приложение № 5**

**к Договору о привлечении банковского платежного агента**

**№ \_\_\_\_\_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.**

**Отчет Банковского платежного агента ПАО «МТС» за «\_\_\_\_\_\_\_\_\_\_\_\_» 20\_\_\_\_г.**

 (месяц)

**по Специальному банковскому счету № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| Поступления на Специальный банковский счет | Списания со Специального банковского счета |
| Источник поступления денежных средств (в т.ч. в разрезе терминалов) | Сумма поступления, руб. | Получатель денежных средств, списанных со Специального банковского счета/номер банковского счета получателя | Сумма списания, руб. | Периодичность списания |
| 1 | 2 | 3 | 4 | 5 |
| 1. Принятые БПА наличные, |  |  |  |  |
| в том числе: |  |  |  |  |
| терминал № \_\_\_\_ |  |  |  |  |
| терминал № \_\_\_\_ |  |  |  |  |
| ….. |  |  |  |  |
| …. |  |  |  |  |
| 2. Перечислено со Специальных банковских счетов БПСА, |  | *ОБРАЗЕЦ* |  |  |
| в том числе: |  |  |  |  |
| наименование БПСА |  |  |  |  |
| Наименование БПСА |  |  |  |  |
| …. |  |  |  |  |
| 3. Перечислено с другого Специального банковского счета БПА |  |  |  |  |
|  |  |  |  |  |
| Итого сумма поступлений на Специальный банковский счет |  | Итого сумма списаний со Специального банковского счета |  |  |

**Подписи Сторон:**

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /мп |

**Приложение № 6**

**к Договору о привлечении банковского платежного агента**

**№ \_\_\_\_\_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.**

**Правила работы в ПО Банка**

1. Общие правила:
	1. Регистрация в ПО Банка Банковского платежного агента/банковского платежного субагента (далее – БПСА) производится сотрудниками Банка на основании заполненной формы Анкеты регистрации агента (далее – Анкета) (Приложение 1 к Приложению 6 к настоящему Договору). Все поля Анкеты являются обязательными к заполнению БПА и БПСА. Анкета направляется Банковским платежным агентом и/или Банковским платежным субагентом на адрес psmtsb@mtsbank.ru, paycenter@mtsbank.ru, в копию необходимо поставить ответственного сотрудника Банковского платежного агента и ответственного сотрудника Банка со стороны бизнеса. Контакты ответственного сотрудника Банка со стороны бизнеса доводятся до сведения ответственного сотрудника Банковского платежного агента путем направления Банком на контактный адрес электронной почты, указанный в 2.3.1 Договора, письма с указанием адреса электронной почты ответственного сотрудника Банка, а также номера телефона.

После регистрации Банковского платежного субагента ответственный сотрудник Банковского платежного агента с ролью «Дилер МТС» в ПО Банка производит повторную генерацию паролей и сертификатов для роли «Дилер агента» и передаёт их ответственному сотруднику Банковского платежного субагента по защищённым каналам связи.

* 1. Другие пользователи Банковского платежного субагента создаются ответственным сотрудником Банковского платежного субагента с ролью «Дилер». Пользователи с ролями, предоставляющими права на создание, изменение и удаление точек, платежей, пользователей и других объектов (например, роль Дилер), обязательно должны использовать тип аутентификации «Сертификат и пароль».

Для создания пользователя с правом изменения параметров Переводов на основании заявления плательщиков либо проведения Переводов после снятия с них блокировки ответственный сотрудник Банковского платежного субагента направляет официальный запрос Банковскому платежному агенту, Банковский платежный агент согласовывает запрос и направляет его ответственному сотруднику Банка по электронной почте. Ответственный сотрудник Банка со стороны бизнеса регистрирует задачу для службы поддержки Банка. По факту создания пользователя ответственный сотрудник службы поддержки Банка направляет уведомление по электронной почте ответственному сотруднику Банка со стороны бизнеса и ответственному сотруднику Банковского платежного агента. Ответственный сотрудник Банковского платежного агента производит повторную генерацию паролей и сертификатов для созданного пользователя и передает их ответственному сотруднику Банковского платежного субагента по защищённым каналам связи Запрос должен быть составлен на официальном бланке Банковского платежного субагента за подписью лица, имеющего право подписи документов от имени Банковского платежного субагента, содержать печать, подпись ответственного сотрудника Банковского платежного агента. Все операции, осуществленные с использованием аутентификационных данных данной роли (логин, пароль и сертификат), считаются легитимными, если Банковский платежный субагент не заявил в Банк об их компрометации. В случае если аутентификационные данные были скомпрометированы, но в Банк информация о компрометации не поступала, операции признаются совершенными от имени Банковского платежного субагента, и все убытки, понесенные Банковским платежным субагентом от совершенных действий, не подлежат возмещению Банком.

* 1. Регистрация точек (терминалов, офисов и других типов), в которых БПА/БПСА осуществляет выполнение своих функций в рамках Договора, производится автоматическим загрузчиком ПО Банка, согласно предоставленному БПА/БПСА файлу по шаблону Приложения №2 к настоящему Приложению. Список точек направляется БПСА по электронной почте на согласование ответственному сотруднику Банковского платежного агента.

После регистрации точек Банковский платежный агент/субагент обязан проверить все параметры загруженных точек, например, дневной лимит приема денежных средств от плательщиков, правила блокирования операций по приему денежных средств, адрес, принадлежность к БПА/БПСА и другие. При необходимости ответственный сотрудник Банковского платежного агента/субагента самостоятельно корректирует параметры.

При регистрации точки «Офис» рекомендуется установить на нее лимит проведения операций по приему денежных средств. При проведении операций в данной точке с использованием корректных аутентификационных данных ответственного сотрудника Банковского платежного агента/БПСА и отсутствии в Банке информации о компрометации аутентификационных данных, операции признаются совершенными от лица Банковского платежного агента/БПСА и не подлежат возмещению со стороны Банка.

* 1. Требования к паролям пользователей ПО Банка:

- Минимальная длина пароля – 8 символов;

- обязательное использование букв в верхнем и нижнем регистрах в пароле;

- обязательное использование цифр в пароле;

- обязательное использование специальных символов в пароле;

- срок действия пароля – 60 дней, затем необходимо произвести смену;

- поериод автоматической блокировки пользователя при неактивности – 30 дней. Для роли «Дилер» – 14 дней.

* 1. Банковский платежный агент/БПСА обязан обеспечить защиту устройств, с которых производится вход в личный кабинет ПО Банка, а также терминалов, на которые установлено ПО Банка:

- на устройствах должны быть установлены и включены средства антивирусной защиты, с настроенным ежедневным обновлением антивирусной базы. Раз в неделю необходимо проводить полное сканирование;

- на устройствах должен быть включён Firewall, защищающий устройство от внешнего подключения;

- доступ к ПО Банка должен быть предоставлен только тем сотрудникам Банковского платежного агента/БПСА, которым по должностным обязанностям требуется предоставление доступа, а также с тем набором прав, которые необходимы для выполнения должностных обязанностей;

- при увольнении сотрудников, имеющих доступ к ПО Банка, ответственный сотрудник Банковского платежного агента/БПСА обязан своевременно блокировать учетные записи пользователей;

- в случае подозрения на компрометацию средств доступа к ПО Банка ответственный сотрудник Банковского платежного агента/БПСА обязан заблокировать учетную запись пользователя или создать новые средства доступа, а так же направить информационное сообщение в Банк для проведения проверки.

* 1. Банковский платежный агент/БПСА обязан контролировать статусы операций (наличие блокировок, ошибок) в личном кабинете, открытом для БПА/БПСА в ПО Банка.
1. Правила взаимодействия с системой фрод-мониторинга Банка:
	1. Все операции осуществляемые по внесению наличных денежных средств через терминалы БПА/БПСА дополнительно анализируются системой внешнего фрод-мониторинга Банка.
	2. Правила, реализованные фрод-мониторингом Банка, при запрете проведения операций в случае противоречия правилам, настроенным в ПО Банка, имеют высший приоритет.
	3. Правила могут быть настроены по инициативе Банковского платежного агента/БПСА в ПО Банка сотрудниками Банка. Для настройки сотруднику БПА/БПСА необходимо направить запрос Банку по электронному адресу psmtsb@mtsbank.ru, paycenter@mtsbank.ru, в копию необходимо поставить ответственного сотрудника Банковского платежного агента и Банка.
	4. Лимиты (на сумму операции по приему наличных денежных средств плательщика в день) на терминалах настраиваются Банковским платежным агентом/БПСА.
	5. Изменение лимитов Банковского платежного агента/БПСА в ПО Банка возможно по инициативе Банковского платежного агента/БПСА. Изменение лимитов производится ответственным сотрудником Банковского платежного агента.
	6. При срабатывании правила внешнего фрод-мониторинга операции присваивается статус «Заблокирована» и субстатус «Заблокировано внешним антифродом». При срабатывании правил, настроенных в ПО Банка, операции присваивается статус «Заблокирована» и субстатус «Правила».
	7. Если при проверке заблокированного платежа Банковский платежный агент/БПСА выявляет факт мошенничества, ответственный сотрудник Банковского платежного агента/БПСА окончательно блокирует (завершает) операцию по приему наличных денежных средств плательщика и сообщает об этом в Банк на электронный адрес psmtsb@mtsbank.ru, paycenter@mtsbank.ru, в копию необходимо поставить ответственного сотрудника Банковского платежного агента и/или указать комментарий к платежу в ПО Банка о подозрении на мошенничество.
	8. Если при проверке платежа со статусом «Заблокировано», с субстатусами «Заблокировано внешним антифродом» или «Правила» Банковский платежного агент/БПСА не усматривает обстоятельств для его окончательной блокировки, ответственный сотрудник Банковского платежного агента/БПСА разблокирует (начинает проведение) платеж. При этом все финансовые убытки, возникшие в результате проведения платежа, несет Банковский платежный агент/БПСА.
	9. По истечении 3х календарных дней в случае не совершения Банковским платежным агентом/БПСА действий, указанных в пп. 2.7 и 2.8 настоящего Приложения, заблокированный платеж разблокируется системой автоматически и/или в ручном режиме ответственным сотрудником Банка. При этом все финансовые убытки, возникшие в результате проведения платежа, несет Банковский платежный агент/БПСА.
	10. Все вопросы по работе системы внешнего фрод-мониторинга Банковский платежный агент/БПСА может направлять по электронной почте на psmtsb@mtsbank.ru, paycenter@mtsbank.ru с указанием стандартной темы письма «Внешний антифрод».
	11. При взаимодействии Банка с Банковским платежным субагентом напрямую в копии писем обязательно необходимо указывать ответственного сотрудника Банковского платежного агента.

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /мп |

 **Приложение № 1 к Приложению 6**

**к Договору о привлечении банковского платежного агента**

**№ \_\_\_\_\_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.**

**Анкета регистрации БПА/БПСА**

|  |
| --- |
| **Регистрация Дилера (администратор БПА/БПСА)** |
| Логин *(не менее 6 латинских символов)*\* |  |
| Тип аутентификации *(Пароль/Сертификат/Пароль+Сертификат)*\* |  |
| ФИО *(полностью)*\* |  |
| График работы\* |  |
| Город\* | *ОБРАЗЕЦ* |
| E-mail\* |  |
| **Регистрация агента** |
| Наименование\* |  |
| Полное наименование\* |  |
| Договор проведения по умолчанию *(Заполняется МТС)* |  |
| Профиль вознаграждения\* *(Заполняется МТС)* |  |
| ИНН\*  |  |
| ОГРН |  |
| КПП |  |
| Адрес\* |  |
| Банк\* |  |
| Адрес банка\* |  |
| БИК\* |  |
| К/С\* |  |
| Спец. Счет\* |  |
| Р/С\* |  |
| Телефоны поддержки\* |  |
| Время работы поддержки |  |
| Расписание работы терминалов агента\* *(в остальное время блокируются)* |  |
| Комментарии |  |
| Плательщик НДС\* *(да/нет)* |  |
| **Информация для формирования акта** |
| Должность руководителя |  |
| ФИО руководителя (родительный падеж)  | ***Пример: Иванова Ивана Ивановича*** |
| ФИО руководителя (именительный падеж)    | ***Пример: Иванов Иван Иванович*** |
| Основание *(доверенность/Устав/свидетельство о регистрации)* |  |
| Наименование компании  |  |

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /мп |

**Приложение № 2 к Приложению 6**

**к Договору о привлечении банковского платежного агента**

**№ \_\_\_\_\_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.**

*ОБРАЗЕЦ*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ID\* терминала | Название | Кладр | Улица | Номер дома | Корпус | Суточный лимит суммы операций по приему наличных денежных средств плательщиков | ID терминала ПЦ\* | ID агента | Индекс | \*\*  |  \*\* | ID параметров точек | ID профилей меню | График работы |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

\* Заполняется Банком

\*\* Оставить поля пустыми

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /мп |

**Приложение №7**

**к договору №\_\_\_\_\_\_\_\_\_\_\_\_\_\_ от \_\_\_\_ \_\_\_\_\_\_\_\_\_ г.**

**о привлечении банковского платежного агента**

**ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ**

1.1. Банк является оператором ПДн клиентов Банка и поручает Банковскому платежному агенту осуществление обработки ПДн Субъектов ПДн. При этом Банк не дает Банковскому платежному агенту задание, которое выходило бы за пределы предмета настоящего договора, и/или за пределы того, что допускается в соответствии с законодательством РФ о ПДн.

1.2. Поручение Банка Банковскому платёжному агенту распространяется на обработку следующих персональных данных Субъектов ПДн: ФИО, реквизиты предъявленного Субъектом ПДн документа, удостоверяющего личность (серию, номер, кем/когда выдан), включая скан копию такого документа, фотографию клиента, дату рождения, место рождения, адрес регистрации, номер телефона, а также иную информацию, предоставленную Субъектом ПДн при заполнении типовых форм Банка, использовать которые Банк поручил в рамках настоящего Договора.

1.3. Поручение обработки персональных данных Субъектов ПДн Банка Банковскому платёжному агенту предполагает осуществление следующих действий: систематизацию, накопление, хранение, уточнение (обновление, изменение), блокирование, уничтожение, сбор, запись, извлечение, использование, обезличивание, передача.

1.4. Целью обработки персональных данных является проведение идентификации/упрощённой идентификации в случаях, предусмотренных пп. 1.5 п.1 ст.7 Федерального закона №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», передача персональных данных Субъектов ПДн в Банк.

1.5. Стороны обязуются обрабатывать персональные данные Субъектов ПДн до наступления одного из следующих событий, в зависимости от того, что наступит ранее:

- получение от другой Стороны уведомления о необходимости прекращения обработки персональных данных Субъектов ПДн;

- достижение Стороной цели обработки персональных данных Субъектов ПДн или утраты необходимости в достижении такой цели;

- прекращение (в т.ч. при отзыве, исполнении, не ограничиваясь указанным) соответствующего поручения на обработку персональных данных.

- прекращения срока обработки, установленного законом и необходимого для исполнения такого закона, либо срока выполнения поручения о передаче персональных данных Субъектов ПДн, установленного настоящим Договором.

1.6. Стороны обязуются уничтожить персональные данные Субъектов ПДн в течение сроков, установленных действующим законодательством, с даты достижения цели обработки персональных данных.

1.7. Стороны обязуются соблюдать конфиденциальность персональных данных и в любом случае обеспечивать безопасность персональных данных на уровне, не ниже уровня, определяемого в соответствии с законодательством о персональных данных. При обработке персональных данных Стороны обязаны принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

1.8. Стороны гарантируют, что от каждого Субъекта ПДн, персональные данные которого передаются другой Стороне, если это требуется в соответствии с условиями действующего законодательства, получено согласие на передачу таких персональных данных другой Стороне и обработку таких персональных данных другой Стороной.

1.9 Стороны обязуются обеспечить безопасность персональных данных посредством:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, проводимых Банковским платежным агентом;

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности.

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

1.10 Стороны осуществляют выбор средств защиты информации при обработке персональных данных в соответствии с нормативными правовыми актами, принятыми Федеральной службой по техническому и экспортному контролю.

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /мп |

**Приложение №8**

**к Договору о привлечении банковского платежного агента**

**№\_\_\_\_\_\_\_\_\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.**

**Перечень принимаемых организационных и технических мер по защите информации[[3]](#footnote-4)**

Перечень мер разработан согласно в соответствии с требованиями Положения ЦБ РФ №719-П[[4]](#footnote-5).

1. Банковские платежные агенты (субагенты) должны обеспечивать защиту информации при участии в осуществлении переводов денежных средств в отношении следующих операций:
* принятие от физического лица наличных денежных средств, в том числе с применением платежных терминалов.
1. К защищаемой информации при совершении банковскими платежными агентами (субагентами) операций, указанных в п.3.1 Положения № 719-П, относится информация:
* Информация, содержащаяся в электронных сообщениях физических лиц;
* Информация, содержащаяся в электронных сообщениях, передаваемых при взаимодействии банковских платежных агентов (субагентов) и операторов по переводу денежных средств, в том числе в электронных сообщениях, составленных банковскими платежными агентами (субагентами) от имени операторов по переводу денежных средств;
* Информация, содержащаяся в реестрах, сформированных на основе электронных сообщений (далее - реестр электронных сообщений) физических лиц. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между банковскими платежными агентами (субагентами) и операторами по переводу денежных средств;
* Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между банковскими платежными агентами (субагентами) и операторами по переводу денежных средств;

# Банковские платежные агенты (субагенты) должны обеспечить реализацию минимального уровня защиты информации для объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1-2017.

1. Банковские платежные агенты (субагенты) должны обеспечить при осуществлении операций, указанных в пункте 1 настоящего Приложения, реализацию мер по обеспечению защиты информации приведенных в таблицах 1 и 2;
2. Информировать Банк об инцидентах нарушения защиты информационной безопасности, в результате которых были нарушены или могли быть нарушены конфиденциальность данных плательщика(ов) или могли быть выполнены неавторизованные платежи. Соответствующие сообщения должны направляться на адрес ib\_bpa@mtsbank.ru, psmtsb@mtsbank.ru. В части контроля выполнения требований 719-П БПА по запросу банка предоставляют Банку отчет, подготовленный проверяющей организацией по результатам оценки соответствия требованиям 719-П в части защиты информации по форме Приложения №9 к настоящему Договор.

АРМ - автоматизированное рабочее место;

АС – автоматизированные системы, в том числе программное обеспечение Банка

ПДн - персональные данные;

ИСПДн - информационные системы персональных данных;

МНИ - машинные носители информации;

НСД - несанкционированный доступ;

ПО - программное обеспечение;

СКЗИ - средства криптографической защиты информации;

СВТ - средство вычислительной техники;

СУБД - система управления базами данных.

Приведенные таблицы содержат меры защиты информации в соответствии с ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

Перечень мер, содержащихся в таблицах 1 и 2 являются обязательными к исполнению всеми Банковскими платежными агентами (субагентами)

Перечень мер, содержащихся в таблицах 3-7 вступает в действие с 01.01.2022 г. в соответствии с требованиями Положения ЦБ РФ №719-П.

# Банковский платежный агент (субагент) должен обеспечить выполнение следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
| 1 | **Обеспечение защиты информации при управлении доступом** |
| 1.2 | Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями |
| 1.3 | Исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа |
| 1.4 | Исключение возможного бесконтрольного изменения пользователями параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации |
| 1.5 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для банковского платежного агента (субагента) (субагента), клиентов и контрагентов. |
| 1.6 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению криптографическими ключами |
| 1.7 | [Идентификация](#sub_3016) и [однофакторная аутентификация](#sub_3028) пользователей |
| 1.8 | Идентификация и однофакторная аутентификация эксплуатационного персонала |
| 1.9 | Аутентификация программных сервисов, осуществляющих логический доступ с использованием [технических учетных записей](#sub_3020) |
| 1.10 | Сокрытие (неотображение) паролей при их вводе субъектами доступа |
| 1.11 | Временная блокировка учетной записи пользователей после выполнения ряда неуспешных последовательных попыток аутентификации на период времени не менее 30 мин. |
| 1.12 | Обеспечение возможности выполнения субъектом логического доступа - работниками банковского платежного агента (субагента) процедуры принудительного прерывания сессии логического доступа и (или) приостановки осуществления логического доступа (с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа) |
| 1.13 | Автоматическое прерывание сессии логического доступа (приостановка осуществления логического доступа) по истечении установленного времени бездействия (неактивности) субъекта логического доступа, не превышающего 15 мин., с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа |
| 1.14 | Выполнение процедуры повторной аутентификации для продолжения осуществления логического доступа после его принудительного или автоматического прерывания (приостановки осуществления логического доступа), предусмотренного мерами 1.12 и 1.13 настоящей таблицы |
| 1.15 | Использование на АРМ субъектов логического доступа встроенных механизмов контроля изменения базовой конфигурации оборудования (пароль на изменение параметров конфигурации системы, хранящихся в энергонезависимой памяти) |
| 1.16 | Запрет на использование технологии аутентификации с сохранением аутентификационных данных в открытом виде в СВТ |
| 1.17 | Запрет на передачу аутентификационных данных в открытом виде по каналам и линиям связи и их передачу куда-либо, кроме средств или систем аутентификации |
| 1.18 | Смена паролей пользователей не реже одного раза в год |
| 1.19 | Смена паролей эксплуатационного персонала не реже одного раза в квартал |
| 1.20 | Использование пользователями паролей длиной не менее восьми символов |
| 1.21 | Использование эксплуатационным персоналом паролей длиной не менее шестнадцати символов |
| 1.22 | Использование при формировании паролей субъектов логического доступа символов, включающих буквы (в верхнем и нижнем регистрах) и цифры |
| 1.23 | Обеспечение возможности самостоятельной смены субъектами логического доступа своих паролей |
| 1.24 | Авторизация логического доступа к ресурсам доступа, в том числе АС |
| 1.25 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа |
| 1.26 | Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа, в том числе АС |
| 1.27 | Запрет выполнения пользователями бизнес-процессов с использованием привилегированных прав логического доступа, в том числе работы пользователей с правами локального администратора АРМ |
| 1.28 | Регистрация осуществления субъектами логического доступа идентификации и аутентификации |
| 1.29 | Регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа, в том числе в АС |
|  | **Обеспечение защиты вычислительных сетей** |
| 1.30 | Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в [ГОСТ Р ИСО/МЭК 7498-1](http://mobileonline.garant.ru/document?id=70146072&sub=0), внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет |
| 1.31 | Межсетевое экранирование внутренних вычислительных сетей банковского платежного агента (субагента), включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в [ГОСТ Р ИСО/МЭК 7498-1](http://mobileonline.garant.ru/document?id=70146072&sub=0) |
| 1.32 | Реализация и контроль информационного взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет в соответствии с установленными правилами и протоколами сетевого взаимодействия |
| 1.33 | Сокрытие топологии внутренних вычислительных сетей банковского платежного агента (субагента) |
| 1.34 | Реализация сетевого взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет через ограниченное количество контролируемых точек доступа |
| 1.35 | Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей банковского платежного агента (субагента) |
| 1.36 | Контроль и обеспечение возможности блокировки нежелательных сообщений электронной почты (SPAM) |
| 1.37 | Применение сетевых протоколов, обеспечивающих защиту подлинности сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии [двухсторонней аутентификации](#sub_3030) при осуществлении логического доступа с использованием телекоммуникационных каналов и (или) линий связи, не контролируемых банковским платежным агентом |
| 1.38 | Реализация защиты информации от раскрытия и модификации, применение двухсторонней аутентификации при ее передаче с использованием сети Интернет, телекоммуникационных каналов и (или) линий связи, не контролируемых банковским платежным агентом |
|  | Защита беспроводных сетей |
| 1.39 | Аутентификация устройств доступа техническими средствами, реализующими функции беспроводного сетевого соединения (точками доступа по протоколу Wi-Fi) |
| 1.40 | Защита информации от раскрытия и модификации при ее передаче с использованием протоколов беспроводного доступа |
|  | **Защита от вредоносного кода** |
| 1.41 | Реализация защиты от вредоносного кода на уровне физических АРМ пользователей и эксплуатационного персонала |
| 1.42 | Реализация защиты от вредоносного кода на уровне виртуальной информационной инфраструктуры |
| 1.43 | Реализация защиты от вредоносного кода на уровне серверного оборудования |
| 1.44 | Реализация защиты от вредоносного кода на уровне контроля почтового трафика |
| 1.45 | Реализация защиты от вредоносного кода на уровне входного контроля устройств и переносных (отчуждаемых) носителей информации |
| 1.46 | Реализация защиты от вредоносного кода на уровне контроля общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) |
| 1.47 | Функционирование средств защиты от вредоносного кода в постоянном, автоматическом режиме, в том числе в части установки их обновлений и сигнатурных баз данных |
| 1.48 | Функционирование средств защиты от вредоносного кода на АРМ пользователей и эксплуатационного персонала в резидентном режиме (в режиме service - для операционной системы Windows, в режиме daemon - для операционной системы Unix), их автоматический запуск при загрузке операционной системы |
| 1.49 | Применение средств защиты от вредоносного кода, реализующих функцию контроля целостности их программных компонентов |
| 1.50 | Контроль отключения и своевременного обновления средств защиты от вредоносного кода |
| 1.51 | Выполнение еженедельных операций по проведению проверок на отсутствие вредоносного кода |
| 1.52 | Использование средств защиты от вредоносного кода различных производителей, как минимум для уровней:- физические АРМ пользователей и эксплуатационного персонала;- серверное оборудование |
| 1.53 | Входной контроль всех устройств и переносных (отчуждаемых) носителей информации (включая мобильные компьютеры и флеш-накопители) перед их использованием в вычислительных сетях банковского платежного агента (субагента) |
| 1.54 | Регистрация операций по проведению проверок на отсутствие вредоносного кода |
| 1.55 | Регистрация фактов выявления вредоносного кода |
| 1.56 | Регистрация сбоев в функционировании средств защиты от вредоносного кода |
| 1.57 | Регистрация сбоев в выполнении контроля (проверок) на отсутствие вредоносного кода |
| 1.58 | Регистрация отключения средств защиты от вредоносного кода |
| 1.59 | Регистрация нарушений целостности программных компонентов средств защиты от вредоносного кода |
|  | **Предотвращение утечек информации** |
| 1.60 | Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при осуществлении вывода МНИ из эксплуатации или вывода из эксплуатации СВТ, в состав которых входят указанные МНИ, а также при необходимости их передачи в сторонние организации |
| 1.61 | Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при передаче (перезакреплении) МНИ между работниками и (или) структурными подразделениями банковского платежного агента (субагента) |

# Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Обеспечение защиты информации при управлении доступом** |
| 2.1 | Контроль соответствия фактического состава разблокированных учетных записей фактическому составу [легальных субъектов](#sub_3024) логического доступа |
| 2.2 | Контроль отсутствия незаблокированных учетных записей:- уволенных работников;- работников, отсутствующих на рабочем месте более 90 календарных дней;- работников внешних (подрядных) организаций, прекративших свою деятельность в организации |
| 2.3 | Контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения |
| 2.4 | Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа) |
| 2.5 | Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа) |
| 2.6 | Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации |
| 2.7 | Контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа |
| 2.8 | Контроль необходимости отзыва прав субъектов логического доступа при изменении их должностных обязанностей |
| 2.9 | Контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа |
| 2.10 | Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 90 дней |
| 2.11 | Реализация контроля со стороны распорядителя логического доступа целесообразности дальнейшего предоставления прав логического доступа, не использованных субъектами на протяжении периода времени, указанного мерой 2.10 настоящей таблицы |
| 2.12 | Реализация возможности определения состава предоставленных прав логического доступа для конкретного ресурса доступа |
| 2.13 | Реализация возможности определения состава предоставленных прав логического доступа для конкретного субъекта логического доступа |
| 2.14 | Определение состава ролей, связанных с выполнением операции (транзакции) в АС, имеющих финансовые последствия для банковского платежного агента (субагента), клиентов и контрагентов, и ролей, связанных с контролем выполнения указанных операций (транзакций), запрет выполнения указанных ролей одним субъектом логического доступа |
| 2.15 | Реализация правил управления правами логического доступа, обеспечивающих запрет совмещения одним субъектом логического доступа ролей, предусмотренных мерой 2.14 настоящей таблицы |
| 2.16 | Запрет использования учетных записей субъектов логического доступа с незаданными аутентификационными данными или заданными по умолчанию разработчиком ресурса доступа, в том числе разработчиком АС |
| 2.17 | Запрет на использование групповых, общих и стандартных учетных записей и паролей, а также прочих подобных методов идентификации и аутентификации, не позволяющих определить конкретного субъекта доступа |
| 2.18 | Хранение копий аутентификационных данных эксплуатационного персонала на выделенных МНИ или на бумажных носителях |
| 2.19 | Реализация защиты копий аутентификационных данных эксплуатационного персонала от НСД при их хранении на МНИ или бумажных носителях |
| 2.20 | Регистрация персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации, реализующих многофакторную аутентификацию |
| 2.21 | Смена аутентификационных данных в случае их [компрометации](#sub_3026) |
| 2.22 | Запрет реализации пользователями бизнес-процессов и технологических процессов банковского платежного агента (субагента) с использованием учетных записей эксплуатационного персонала, в том числе в АС |
| 2.23 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
|  | Защита информации при осуществлении физического доступа |
| 2.24 | Контроль перечня лиц, которым предоставлено право самостоятельного физического доступа в помещения |
| 2.25 | Назначение для всех помещений распорядителя физического доступа |
| 2.26 | Предоставление права самостоятельного физического доступа в помещения по решению распорядителя физического доступа |
| 2.27 | Оборудование входных дверей помещения механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время |
| 2.28 | Контроль состояния общедоступных объектов доступа с целью выявлений несанкционированных изменений в их аппаратном обеспечении и (или) ПО |
| 2.29 | Приведение общедоступных объектов доступа, для которых были выявлены несанкционированные изменения в их аппаратном обеспечении и (или) ПО (до устранения указанных несанкционированных изменений), в состояние, при котором невозможно их использование для осуществления операции (транзакции), приводящей к финансовым последствиям для банковского платежного агента (субагента), клиентов и контрагентов |
| 2.30 | Учет созданных, используемых и (или) эксплуатируемых ресурсов доступа |
| 2.31 | Учет используемых и (или) эксплуатируемых объектов доступа |
| 2.32 | Учет эксплуатируемых общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) |
| 2.33 | Контроль фактического состава созданных, используемых и (или) эксплуатируемых ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) и их корректного размещения в сегментах вычислительных сетей банковского платежного агента (субагента) |
|  | **Контроль целостности и защищенности информационной инфраструктуры** |
| 2.34 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между внутренними вычислительными сетями банковского платежного агента (субагента) и сетью Интернет |
| 2.35 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет |
| 2.36 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный логический доступ к ресурсам доступа, размещенным в вычислительных сетях банковского платежного агента (субагента), подключенных к сети Интернет |
| 2.37 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный удаленный доступ |
| 2.38 | Контроль размещения и своевременного обновления на серверном и сетевом оборудовании ПО средств и систем защиты информации, прикладного ПО, ПО АС, системного ПО и сигнатурных баз средств защиты информации, в том числе с целью устранения выявленных уязвимостей защиты информации |
| 2.39 | Контроль размещения и своевременного обновления на АРМ пользователей и эксплуатационного персонала ПО средств и систем защиты информации, прикладного ПО, ПО АС и системного ПО, в том числе с целью устранения выявленных уязвимостей защиты информации |
| 2.40 | Контроль работоспособности (тестирование) и правильности функционирования АС после выполнения обновлений ПО, предусмотренного мерами [2.38](#sub_3317) и 2.39 настоящей таблицы, выполняемого в сегментах разработки и тестирования |
| 2.41 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации после выполнения обновлений ПО, предусмотренного мерой 2.38 настоящей таблицы |
| 2.42 | Обеспечение возможности восстановления эталонных копий ПО АС, ПО средств и систем защиты информации, системного ПО в случаях нештатных ситуаций |
| 2.43 | Наличие, учет и контроль целостности эталонных значений параметров настроек ПО АС, системного ПО, ПО средств и систем защиты информации, возможность восстановления указанных настроек в случаях нештатных ситуаций |
| 2.44 | Контроль целостности и достоверности источников получения при распространении и (или) обновлении ПО АС, ПО средств и систем защиты информации, системного ПО |
| 2.45 | Контроль состава разрешенного для использования ПО АРМ пользователей и эксплуатационного персонала |
| 2.46 | Исключение возможности установки и (или) запуска неразрешенного для использования ПО АРМ пользователей и эксплуатационного персонала |
|  | **Защита от вредоносного кода** |
| 2.47 | Запрет неконтролируемого открытия самораспаковывающихся архивов и исполняемых файлов, полученных из сети Интернет |
| 2.48 | **Предотвращение утечек информации** |
| 2.49 | Учет и контроль использования МНИ, предназначенных для хранения информации конфиденциального характера |
| 2.50 | Документарное определение порядка использования и доступа к МНИ, предназначенным для хранения информации конфиденциального характера |
| 2.51 | Маркирование учтенных МНИ |
| 2.52 | Регистрация действий по учету и снятию с учета МНИ, предназначенных для хранения информации конфиденциального характера |
| 2.53 | Регистрация фактов стирания информации с МНИ |

# При использовании среды виртуализации Банковский платежный агент (субагент) должен обеспечить выполнение следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Защита среды виртуализации** |
| 3.1 | Идентификация и аутентификация пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам |
| 3.2 | Обеспечение возможности принудительной блокировки (выключения) установленной сессии работы пользователя с виртуальной машиной |
| 3.3 | Регистрация операций, связанных с запуском (остановкой) виртуальных машин |
| 3.4 | Регистрация операций, связанных с созданием и удалением виртуальных машин |
| 3.5 | Регистрация операций, связанных с созданием, изменением, копированием, удалением базовых образов виртуальных машин |
| 3.6 | Регистрация операций, связанных с копированием текущих образов виртуальных машин |
| 3.7 | Регистрация операций, связанных с изменением прав логического доступа к серверным компонентам виртуализации |
| 3.8 | Регистрация операций, связанных с изменением параметров настроек серверных компонентов виртуализации |
| 3.9 | Регистрация операций, связанных с аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации |
| 3.10 | Регистрация операций, связанных с аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам |
| 3.11 | Регистрация операций, связанных с изменением параметров настроек технических мер защиты информации, используемых для реализации контроля доступа к серверным компонентам виртуализации |
| 3.12 | Регистрация операций, связанных с изменением настроек технических мер защиты информации, используемых для обеспечения защиты виртуальных машин |
| 3.13 | Аутентификация мобильных (переносных) устройств удаленного доступа |
| 3.14 | Реализация защиты информации от раскрытия и модификации, применение двухсторонней взаимной аутентификации участников информационного обмена при ее передаче при осуществлении удаленного логического доступа |
| 3.15 | Идентификация, двухфакторная аутентификация и авторизация субъектов доступа после установления защищенного сетевого взаимодействия, выполнения аутентификации |
| 3.16 | Реализация и контроль информационного взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и мобильных (переносных) устройств в соответствии с установленными правилами и протоколами сетевого взаимодействия |
| 3.17 | Обеспечение защиты мобильных (переносных) устройств от воздействий вредоносного кода |
| 3.18 | Стирание информации конфиденциального характера с мобильных (переносных) устройств средствами, обеспечивающими полную перезапись данных, при осуществлении вывода мобильных (переносных) устройств из эксплуатации, а также при необходимости их передачи в сторонние организации, между работниками и (или) структурными подразделениями банковского платежного агента (субагента) |

# При использовании среды виртуализации Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Защита среды виртуализации** |
| 4.1 | Запрет на копирование текущих образов виртуальных машин, использующих СКЗИ, с загруженными криптографическими ключами |
| 4.2 | Запрет на копирование текущих образов виртуальных машин, используемых для реализации технологии виртуализации АРМ пользователей |
| 4.3 | Определение правил удаленного доступа и перечня ресурсов доступа, к которым предоставляется [удаленный доступ](#sub_3045) |

# При использовании собственной разработки программного обеспечения Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Защита информации на этапах жизненного цикла автоматизированных систем и приложений** |
| 5.1 | Документарное определение перечня защищаемой информации, планируемой к обработке в АС |
| 5.2 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) |
| 5.3 | Документарное определение в проектной и эксплуатационной документации на систему защиты информации АС:- состава и порядка применения технических и (или) организационных мер системы защиты информации АС;- параметров настроек технических мер системы защиты информации АС и компонентов информационной инфраструктуры, предназначенных для размещения указанных технических мер |
| 5.4 | Контроль предоставления и обеспечение разграничения доступа в сегментах разработки и тестирования |
| 5.5 | Реализация запрета использования защищаемой информации в сегментах разработки и тестирования |
| 5.6 | Контроль (тестирование) полноты реализации мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) |
| 5.7 | Проведение модернизации АС при изменении требований к составу и содержанию мер системы защиты информации АС (функционально-технические требований к системе защиты информации АС) |
| 5.8 | Документарное определение в проектной и эксплуатационной документации на систему защиты информации АС:- состава и порядка применения клиентами банковского платежного агента (субагента) прикладного ПО и (или) технических и (или) организационных мер защиты информации (далее при совместном упоминании - клиентские компоненты);- параметров настроек клиентских компонентов и информационной инфраструктуры клиентов банковского платежного агента (субагента), предназначенной для размещения клиентских компонентов;- описания мер по обеспечению использования клиентом определенных доверенных версий (сборок) прикладного ПО |
| 5.9 | Размещение и настройка (конфигурирование) технических мер системы защиты информации АС в информационной инфраструктуре, используемой для непосредственной реализации бизнес-процессов или технологических процессов банковского платежного агента (субагента) (далее - промышленная среда), в соответствии с положениями проектной и эксплуатационной документации |
| 5.10 | Контроль (тестирование) полноты реализации мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) в промышленной среде |
| 5.11 | Реализация контроля эксплуатации технических мер системы защиты информации АС в соответствии с положениями проектной и эксплуатационной документации, включающего:- контроль фактического размещения технических мер защиты в промышленной среде;- контроль фактических параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенной для размещения технических мер защиты информации |
| 5.12 | Реализация контроля применения мер системы защиты информации АС |
| 5.13 | Назначение и реализация контроля деятельности лиц, ответственных за эксплуатацию (сопровождение) системы защиты информации АС |
| 5.14 | Обеспечение оперативного устранения выявленных уязвимостей защиты информации АС, включая уязвимости прикладного ПО |
| 5.15 | Регистрация операций по изменению параметров настроек технических мер системы защиты информации АС |
| 5.16 | Принятие мер по обеспечению защиты информации от несанкционированного копирования и распространения |

# Банковский платежный агент (субагент) должен обеспечить выполнение следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Обнаружение инцидентов защиты информации и реагирование на них** |
| 6.1 | Реализация защиты информации об инцидентах защиты информации от НСД, обеспечение целостности и доступности указанной информации |
| 6.2 | Обеспечение возможности доступа к информации об инцидентах защиты информации в течение трех лет |
|  | **Управление инцидентами защиты информации** |
| 6.3 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых техническими мерами, входящими в состав системы защиты информации |
| 6.4 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых АС и приложениями |
| 6.5 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых контроллерами доменов |
| 6.6 | Генерация временных меток для данных регистрации о событиях защиты информации и синхронизации системного времени объектов информатизации, используемых для формирования, сбора и анализа данных регистрации |
| 6.7 | Резервирование необходимого объема памяти для хранения данных регистрации о событиях защиты информации |
| 6.8 | Реализация защиты данных регистрации о событиях защиты информации от НСД при их хранении, обеспечение целостности и доступности хранимых данных регистрации |
| 6.9 | Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет |
| 6.10 | Обеспечение возможности выявления и анализа событий защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД |
| 6.11 | Обеспечение возможности определения состава действий и (или) операций конкретного субъекта доступа |
| 6.12 | Обеспечение возможности определения состава действий и (или) операций субъектов доступа при осуществлении логического доступа к конкретному ресурсу доступа |
| 6.13 | Регистрация доступа к хранимым данным о событиях защиты информации |
|  | **Требования к организации и управлению защитой информации** |
| 6.14 | Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса |

# Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Обнаружение инцидентов защиты информации и реагирование на них** |
| 7.1 | Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации |
| 7.2 | Регистрация информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, полученной от работников, клиентов и (или) контрагентов банковского платежного агента (субагента) |
| 7.3 | Классификация инцидентов защиты информации с учетом степени их влияния (критичности) на предоставление финансовых услуг, реализацию бизнес-процессов и (или) технологических процессов банковского платежного агента (субагента) |
| 7.4 | Установление и применение единых правил получения от работников, клиентов и (или) контрагентов банковского платежного агента (субагента) информации, потенциально связанной с инцидентами защиты информации |
| 7.5 | Установление и применение единых правил регистрации и классификации инцидентов защиты информации в части состава и содержания атрибутов, описывающих инцидент защиты информации, и их возможных значений |
| 7.6 | Установление и применение единых правил реагирования на инциденты защиты информации |
| 7.7 | Определение и назначение ролей, связанных с реагированием на инциденты защиты информации |
| 7.8 | Проведение реагирования на каждый обнаруженный инцидент защиты информации, включающего:- анализ инцидента;- определение источников и причин возникновения инцидента;- оценку последствий инцидента на предоставление финансовых услуг, реализацию бизнес-процессов или технологических процессов банковского платежного агента (субагента);- принятие мер по устранению последствий инцидента;- планирование и принятие мер по предотвращению повторного возникновения инцидента |
| 7.9 | Установление и применение единых правил сбора, фиксации и распространения информации об инцидентах защиты информации |
| 7.10 | Установление и применение единых правил закрытия инцидентов защиты информации |
|  | **Управление инцидентами защиты информации** |
| 7.11 | Контроль формирования данных регистрации о событиях защиты информации объектов информатизации |
|  | **Требования к организации и управлению защитой информации** |
| 7.12 | Документарное определение области применения процесса системы защиты информации для уровней информационной инфраструктуры |
| 7.13 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания организационных мер защиты информации, выбранных банковским платежным агентом и реализуемых в рамках процесса системы защиты информации |
| 7.14 | Документарное определение порядка применения организационных мер защиты информации, реализуемых в рамках процесса системы защиты информации |
| 7.15 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания технических мер защиты информации, выбранных финансовой организацией и реализуемых в рамках процесса системы защиты информации |
| 7.16 | Документарное определение порядка применения технических мер защиты информации, реализуемых в рамках процесса системы защиты информации, включающего:- правила размещения технических мер защиты информации в информационной инфраструктуре;- параметры настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации[\*\*](#sub_3340);- руководства по применению технических мер защиты информации (включающие руководства по эксплуатации, контролю эксплуатации и использованию по назначению технических мер защиты информации);- состав ролей и права субъектов доступа, необходимых для обеспечения применения технических мер защиты информации (включающего эксплуатацию, контроль эксплуатации и использование по назначению мер защиты информации) |
| 7.17 | Реализация учета объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, для уровней информационной инфраструктуры, в том числе объектов доступа, расположенных в публичных (общедоступных) местах (в том числе банкоматах, платежных терминалах) |
| 7.18 | Размещение и настройка (конфигурирование) технических мер защиты информации в информационной инфраструктуре банковского платежного агента (субагента) |
| 7.19 | Контроль (тестирование) полноты реализации технических мер защиты информации |
| 7.20 | Назначение работникам банковского платежного агента (субагента) ролей, связанных с применением мер защиты информации, и установление обязанности и ответственности за их выполнение |
| 7.21 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной инфраструктуры |
| 7.22 | Реализация эксплуатации, использования по назначению технических мер защиты информации |
| 7.23 | Реализация применения организационных мер защиты информации |
| 7.24 | Обучение, практическая подготовка (переподготовка) работников банковского платежного агента (субагента), ответственных за применение мер защиты информации в рамках процесса защиты информации |
| 7.25 | Повышение осведомленности (инструктаж) работников банковского платежного агента (субагента) в области реализации процесса защиты информации, применения организационных мер защиты информации, использования по назначению технических мер защиты информации |
| 7.26 | Контроль фактического состава объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, на соответствие учетным данным |
| 7.27 | Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий:- контроль фактического размещения технических мер защиты информации в информационной инфраструктуре банковского платежного агента (субагента);- контроль фактических параметров настроек технических мер защиты информации и компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации |
| 7.28 | Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий:- контроль назначения ролей, связанных с эксплуатацией и использованием по назначению технических мер защиты информации;- контроль выполнения руководств по эксплуатации и использованию по назначению технических мер защиты информации |
| 7.29 | Периодический контроль (тестирование) полноты реализации технических мер защиты информации |
| 7.30 | Контроль применения организационных мер защиты информации |
| 7.31 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| 7.32 | Проведение проверок знаний работников банковского платежного агента (субагента) в части применения мер защиты информации в рамках процесса системы защиты информации |
| 7.33 | Фиксация результатов (свидетельств) проведения мероприятий по контролю реализации процесса системы защиты информации |
| 7.34 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях:- обнаружения инцидентов защиты информации;- обнаружения недостатков в рамках контроля системы защиты информации |
| 7.35 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях изменения политики банковского платежного агента (субагента) в отношении:- области применения процесса системы защиты информации;- основных принципов и приоритетов в реализации процесса системы защиты информации;- целевых показателей величины допустимого остаточного операционного риска (риск-аппетита), связанного с обеспечением безопасности информации |
| 7.36 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях:- изменений требований к защите информации, определенных правилами платежной системы;- изменений, внесенных в законодательство Российской Федерации, в том числе нормативные акты Банка России |
| 7.37 | Фиксация решений о проведении совершенствования процесса системы защиты информации в виде корректирующих или превентивных действий, например:- пересмотр области применения процесса системы защиты информации;- пересмотр состава и содержания организационных мер защиты информации, применяемых в рамках процесса системы защиты информации;- пересмотр состава технических мер защиты информации, применяемых в рамках процесса системы защиты информации |

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /Мп |

**Приложение №9**

**к Договору о привлечении банковского платежного агента**

**№\_\_\_\_\_\_\_\_\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.**

**Анкета по Информационной безопасности**

|  |  |
| --- | --- |
| Наименование организации: |  |
| Сотрудник, заполнивший анкету:- Фамилия Имя Отчество:- должность:  |  |
| Дата заполнения:  |  |

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Вопрос**  | **Статус выполнения требования (да/нет)** |
|  | **Обеспечение защиты информации при управлении доступом** |  |
| 1.2 | Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями*ОБРАЗЕЦ* |  |
| 1.3 | Исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа |  |
| 1.4 | Исключение возможного бесконтрольного изменения пользователями параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации |  |
| 1.5 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для банковского платежного агента (субагента) (субагента), клиентов и контрагентов. |  |
| 1.6 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению криптографическими ключами |  |
| 1.7 | [Идентификация](#sub_3016) и [однофакторная аутентификация](#sub_3028) пользователей |  |
| 1.8 | Идентификация и однофакторная аутентификация эксплуатационного персонала |  |
| 1.9 | Аутентификация программных сервисов, осуществляющих логический доступ с использованием [технических учетных записей](#sub_3020) |  |
| 1.10 | Сокрытие (неотображение) паролей при их вводе субъектами доступа |  |
| 1.11 | Временная блокировка учетной записи пользователей после выполнения ряда неуспешных последовательных попыток аутентификации на период времени не менее 30 мин. |  |
| 1.12 | Обеспечение возможности выполнения субъектом логического доступа - работниками банковского платежного агента (субагента) процедуры принудительного прерывания сессии логического доступа и (или) приостановки осуществления логического доступа (с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа) |  |
| 1.13 | Автоматическое прерывание сессии логического доступа (приостановка осуществления логического доступа) по истечении установленного времени бездействия (неактивности) субъекта логического доступа, не превышающего 15 мин., с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа |  |
| 1.14 | Выполнение процедуры повторной аутентификации для продолжения осуществления логического доступа после его принудительного или автоматического прерывания (приостановки осуществления логического доступа), предусмотренного мерами 1.12 и 1.13 настоящей таблицы |  |
| 1.15 | Использование на АРМ субъектов логического доступа встроенных механизмов контроля изменения базовой конфигурации оборудования (пароль на изменение параметров конфигурации системы, хранящихся в энергонезависимой памяти)*ОБРАЗЕЦ* |  |
| 1.16 | Запрет на использование технологии аутентификации с сохранением аутентификационных данных в открытом виде в СВТ |  |
| 1.17 | Запрет на передачу аутентификационных данных в открытом виде по каналам и линиям связи и их передачу куда-либо, кроме средств или систем аутентификации |  |
| 1.18 | Смена паролей пользователей не реже одного раза в год |  |
| 1.19 | Смена паролей эксплуатационного персонала не реже одного раза в квартал |  |
| 1.20 | Использование пользователями паролей длиной не менее восьми символов |  |
| 1.21 | Использование эксплуатационным персоналом паролей длиной не менее шестнадцати символов |  |
| 1.22 | Использование при формировании паролей субъектов логического доступа символов, включающих буквы (в верхнем и нижнем регистрах) и цифры |  |
| 1.23 | Обеспечение возможности самостоятельной смены субъектами логического доступа своих паролей |  |
| 1.24 | Авторизация логического доступа к ресурсам доступа, в том числе АС |  |
| 1.25 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа |  |
| 1.26 | Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа, в том числе АС |  |
| 1.27 | Запрет выполнения пользователями бизнес-процессов с использованием привилегированных прав логического доступа, в том числе работы пользователей с правами локального администратора АРМ |  |
| 1.28 | Регистрация осуществления субъектами логического доступа идентификации и аутентификации |  |
| 1.29 | Регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа, в том числе в АС |  |
|  | **Обеспечение защиты вычислительных сетей** |  |
| 1.30 | Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в [ГОСТ Р ИСО/МЭК 7498-1](http://mobileonline.garant.ru/document?id=70146072&sub=0), внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет |  |
| 1.31 | Межсетевое экранирование внутренних вычислительных сетей банковского платежного агента (субагента), включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в [ГОСТ Р ИСО/МЭК 7498-1](http://mobileonline.garant.ru/document?id=70146072&sub=0) |  |
| 1.32 | Реализация и контроль информационного взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет в соответствии с установленными правилами и протоколами сетевого взаимодействия |  |
| 1.33 | Сокрытие топологии внутренних вычислительных сетей банковского платежного агента (субагента) |  |
| 1.34 | Реализация сетевого взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет через ограниченное количество контролируемых точек доступа |  |
| 1.35 | Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей банковского платежного агента (субагента) |  |
| 1.36 | Контроль и обеспечение возможности блокировки нежелательных сообщений электронной почты (SPAM) |  |
| 1.37 | Применение сетевых протоколов, обеспечивающих защиту подлинности сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии [двухсторонней аутентификации](#sub_3030) при осуществлении логического доступа с использованием телекоммуникационных каналов и (или) линий связи, не контролируемых банковским платежным агентом |  |
| 1.38 | Реализация защиты информации от раскрытия и модификации, применение двухсторонней аутентификации при ее передаче с использованием сети Интернет, телекоммуникационных каналов и (или) линий связи, не контролируемых банковским платежным агентом |  |
|  | Защита беспроводных сетей |  |
| 1.39 | Аутентификация устройств доступа техническими средствами, реализующими функции беспроводного сетевого соединения (точками доступа по протоколу Wi-Fi) |  |
| 1.40 | Защита информации от раскрытия и модификации при ее передаче с использованием протоколов беспроводного доступа |  |
|  | **Защита от вредоносного кода** |  |
| 1.41 | Реализация защиты от вредоносного кода на уровне физических АРМ пользователей и эксплуатационного персонала |  |
| 1.42 | Реализация защиты от вредоносного кода на уровне виртуальной информационной инфраструктуры*ОБРАЗЕЦ* |  |
| 1.43 | Реализация защиты от вредоносного кода на уровне серверного оборудования |  |
| 1.44 | Реализация защиты от вредоносного кода на уровне контроля почтового трафика |  |
| 1.45 | Реализация защиты от вредоносного кода на уровне входного контроля устройств и переносных (отчуждаемых) носителей информации |  |
| 1.46 | Реализация защиты от вредоносного кода на уровне контроля общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) |  |
| 1.47 | Функционирование средств защиты от вредоносного кода в постоянном, автоматическом режиме, в том числе в части установки их обновлений и сигнатурных баз данных |  |
| 1.48 | Функционирование средств защиты от вредоносного кода на АРМ пользователей и эксплуатационного персонала в резидентном режиме (в режиме service - для операционной системы Windows, в режиме daemon - для операционной системы Unix), их автоматический запуск при загрузке операционной системы |  |
| 1.49 | Применение средств защиты от вредоносного кода, реализующих функцию контроля целостности их программных компонентов |  |
| 1.50 | Контроль отключения и своевременного обновления средств защиты от вредоносного кода |  |
| 1.51 | Выполнение еженедельных операций по проведению проверок на отсутствие вредоносного кода |  |
| 1.52 | Использование средств защиты от вредоносного кода различных производителей, как минимум для уровней:- физические АРМ пользователей и эксплуатационного персонала;- серверное оборудование |  |
| 1.53 | Входной контроль всех устройств и переносных (отчуждаемых) носителей информации (включая мобильные компьютеры и флеш-накопители) перед их использованием в вычислительных сетях банковского платежного агента (субагента) |  |
| 1.54 | Регистрация операций по проведению проверок на отсутствие вредоносного кода |  |
| 1.55 | Регистрация фактов выявления вредоносного кода |  |
| 1.56 | Регистрация сбоев в функционировании средств защиты от вредоносного кода |  |
| 1.57 | Регистрация сбоев в выполнении контроля (проверок) на отсутствие вредоносного кода |  |
| 1.58 | Регистрация отключения средств защиты от вредоносного кода |  |
| 1.59 | Регистрация нарушений целостности программных компонентов средств защиты от вредоносного кода |  |
|  | **Предотвращение утечек информации** |  |
| 1.60 | Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при осуществлении вывода МНИ из эксплуатации или вывода из эксплуатации СВТ, в состав которых входят указанные МНИ, а также при необходимости их передачи в сторонние организации |  |
| 1.61 | Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при передаче (перезакреплении) МНИ между работниками и (или) структурными подразделениями банковского платежного агента (субагента) |  |

# 2.Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Обеспечение защиты информации при управлении доступом** |  |
| 2.1 | Контроль соответствия фактического состава разблокированных учетных записей фактическому составу [легальных субъектов](#sub_3024) логического доступа |  |
| 2.2 | Контроль отсутствия незаблокированных учетных записей:- уволенных работников;- работников, отсутствующих на рабочем месте более 90 календарных дней;- работников внешних (подрядных) организаций, прекративших свою деятельность в организации |  |
| 2.3 | Контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения |  |
| 2.4 | Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа) |  |
| 2.5 | Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа) |  |
| 2.6 | Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации |  |
| 2.7 | Контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа |  |
| 2.8 | Контроль необходимости отзыва прав субъектов логического доступа при изменении их должностных обязанностей |  |
| 2.9 | Контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа |  |
| 2.10 | Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 90 дней |  |
| 2.11 | Реализация контроля со стороны распорядителя логического доступа целесообразности дальнейшего предоставления прав логического доступа, не использованных субъектами на протяжении периода времени, указанного мерой 2.10 настоящей таблицы |  |
| 2.12 | Реализация возможности определения состава предоставленных прав логического доступа для конкретного ресурса доступа |  |
| 2.13 | Реализация возможности определения состава предоставленных прав логического доступа для конкретного субъекта логического доступа |  |
| 2.14 | Определение состава ролей, связанных с выполнением операции (транзакции) в АС, имеющих финансовые последствия для банковского платежного агента (субагента), клиентов и контрагентов, и ролей, связанных с контролем выполнения указанных операций (транзакций), запрет выполнения указанных ролей одним субъектом логического доступа |  |
| 2.15 | Реализация правил управления правами логического доступа, обеспечивающих запрет совмещения одним субъектом логического доступа ролей, предусмотренных мерой 2.14 настоящей таблицы |  |
| 2.16 | Запрет использования учетных записей субъектов логического доступа с незаданными аутентификационными данными или заданными по умолчанию разработчиком ресурса доступа, в том числе разработчиком АС |  |
| 2.17 | Запрет на использование групповых, общих и стандартных учетных записей и паролей, а также прочих подобных методов идентификации и аутентификации, не позволяющих определить конкретного субъекта доступа |  |
| 2.18 | Хранение копий аутентификационных данных эксплуатационного персонала на выделенных МНИ или на бумажных носителях |  |
| 2.19 | Реализация защиты копий аутентификационных данных эксплуатационного персонала от НСД при их хранении на МНИ или бумажных носителях |  |
| 2.20 | Регистрация персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации, реализующих многофакторную аутентификацию*ОБРАЗЕЦ* |  |
| 2.21 | Смена аутентификационных данных в случае их [компрометации](#sub_3026) |  |
| 2.22 | Запрет реализации пользователями бизнес-процессов и технологических процессов банковского платежного агента (субагента) с использованием учетных записей эксплуатационного персонала, в том числе в АС |  |
| 2.23 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |  |
|  | Защита информации при осуществлении физического доступа |  |
| 2.24 | Контроль перечня лиц, которым предоставлено право самостоятельного физического доступа в помещения |  |
| 2.25 | Назначение для всех помещений распорядителя физического доступа |  |
| 2.26 | Предоставление права самостоятельного физического доступа в помещения по решению распорядителя физического доступа |  |
| 2.27 | Оборудование входных дверей помещения механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время |  |
| 2.28 | Контроль состояния общедоступных объектов доступа с целью выявлений несанкционированных изменений в их аппаратном обеспечении и (или) ПО |  |
| 2.29 | Приведение общедоступных объектов доступа, для которых были выявлены несанкционированные изменения в их аппаратном обеспечении и (или) ПО (до устранения указанных несанкционированных изменений), в состояние, при котором невозможно их использование для осуществления операции (транзакции), приводящей к финансовым последствиям для банковского платежного агента (субагента), клиентов и контрагентов |  |
| 2.30 | Учет созданных, используемых и (или) эксплуатируемых ресурсов доступа |  |
| 2.31 | Учет используемых и (или) эксплуатируемых объектов доступа |  |
| 2.32 | Учет эксплуатируемых общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) |  |
| 2.33 | Контроль фактического состава созданных, используемых и (или) эксплуатируемых ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) и их корректного размещения в сегментах вычислительных сетей банковского платежного агента (субагента) |  |
|  | **Контроль целостности и защищенности информационной инфраструктуры** |  |
| 2.34 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между внутренними вычислительными сетями банковского платежного агента (субагента) и сетью Интернет |  |
| 2.35 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет |  |
| 2.36 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный логический доступ к ресурсам доступа, размещенным в вычислительных сетях банковского платежного агента (субагента), подключенных к сети Интернет |  |
| 2.37 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный удаленный доступ |  |
| 2.38 | Контроль размещения и своевременного обновления на серверном и сетевом оборудовании ПО средств и систем защиты информации, прикладного ПО, ПО АС, системного ПО и сигнатурных баз средств защиты информации, в том числе с целью устранения выявленных уязвимостей защиты информации |  |
| 2.39 | Контроль размещения и своевременного обновления на АРМ пользователей и эксплуатационного персонала ПО средств и систем защиты информации, прикладного ПО, ПО АС и системного ПО, в том числе с целью устранения выявленных уязвимостей защиты информации |  |
| 2.40 | Контроль работоспособности (тестирование) и правильности функционирования АС после выполнения обновлений ПО, предусмотренного мерами [2.38](#sub_3317) и 2.39 настоящей таблицы, выполняемого в сегментах разработки и тестирования |  |
| 2.41 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации после выполнения обновлений ПО, предусмотренного мерой 2.38 настоящей таблицы*ОБРАЗЕЦ* |  |
| 2.42 | Обеспечение возможности восстановления эталонных копий ПО АС, ПО средств и систем защиты информации, системного ПО в случаях нештатных ситуаций |  |
| 2.43 | Наличие, учет и контроль целостности эталонных значений параметров настроек ПО АС, системного ПО, ПО средств и систем защиты информации, возможность восстановления указанных настроек в случаях нештатных ситуаций |  |
| 2.44 | Контроль целостности и достоверности источников получения при распространении и (или) обновлении ПО АС, ПО средств и систем защиты информации, системного ПО |  |
| 2.45 | Контроль состава разрешенного для использования ПО АРМ пользователей и эксплуатационного персонала |  |
| 2.46 | Исключение возможности установки и (или) запуска неразрешенного для использования ПО АРМ пользователей и эксплуатационного персонала |  |
|  | **Защита от вредоносного кода** |  |
| 2.47 | Запрет неконтролируемого открытия самораспаковывающихся архивов и исполняемых файлов, полученных из сети Интернет |  |
| 2.48 | **Предотвращение утечек информации** |  |
| 2.49 | Учет и контроль использования МНИ, предназначенных для хранения информации конфиденциального характера |  |
| 2.50 | Документарное определение порядка использования и доступа к МНИ, предназначенным для хранения информации конфиденциального характера |  |
| 2.51 | Маркирование учтенных МНИ |  |
| 2.52 | Регистрация действий по учету и снятию с учета МНИ, предназначенных для хранения информации конфиденциального характера |  |
| 2.53 | Регистрация фактов стирания информации с МНИ |  |

# При использовании среды виртуализации Банковский платежный агент (субагент) должен обеспечить выполнение следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Защита среды виртуализации** |  |
| 3.1 | Идентификация и аутентификация пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам |  |
| 3.2 | Обеспечение возможности принудительной блокировки (выключения) установленной сессии работы пользователя с виртуальной машиной |  |
| 3.3 | Регистрация операций, связанных с запуском (остановкой) виртуальных машин*ОБРАЗЕЦ* |  |
| 3.4 | Регистрация операций, связанных с созданием и удалением виртуальных машин |  |
| 3.5 | Регистрация операций, связанных с созданием, изменением, копированием, удалением базовых образов виртуальных машин |  |
| 3.6 | Регистрация операций, связанных с копированием текущих образов виртуальных машин |  |
| 3.7 | Регистрация операций, связанных с изменением прав логического доступа к серверным компонентам виртуализации |  |
| 3.8 | Регистрация операций, связанных с изменением параметров настроек серверных компонентов виртуализации |  |
| 3.9 | Регистрация операций, связанных с аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации |  |
| 3.10 | Регистрация операций, связанных с аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам |  |
| 3.11 | Регистрация операций, связанных с изменением параметров настроек технических мер защиты информации, используемых для реализации контроля доступа к серверным компонентам виртуализации |  |
| 3.12 | Регистрация операций, связанных с изменением настроек технических мер защиты информации, используемых для обеспечения защиты виртуальных машин |  |
| 3.13 | Аутентификация мобильных (переносных) устройств удаленного доступа |  |
| 3.14 | Реализация защиты информации от раскрытия и модификации, применение двухсторонней взаимной аутентификации участников информационного обмена при ее передаче при осуществлении удаленного логического доступа |  |
| 3.15 | Идентификация, двухфакторная аутентификация и авторизация субъектов доступа после установления защищенного сетевого взаимодействия, выполнения аутентификации |  |
| 3.16 | Реализация и контроль информационного взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и мобильных (переносных) устройств в соответствии с установленными правилами и протоколами сетевого взаимодействия |  |
| 3.17 | Обеспечение защиты мобильных (переносных) устройств от воздействий вредоносного кода |  |
| 3.18 | Стирание информации конфиденциального характера с мобильных (переносных) устройств средствами, обеспечивающими полную перезапись данных, при осуществлении вывода мобильных (переносных) устройств из эксплуатации, а также при необходимости их передачи в сторонние организации, между работниками и (или) структурными подразделениями банковского платежного агента (субагента) |  |

# 4.При использовании среды виртуализации Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Защита среды виртуализации** |  |
| 4.1 | Запрет на копирование текущих образов виртуальных машин, использующих СКЗИ, с загруженными криптографическими ключами |  |
| 4.2 | Запрет на копирование текущих образов виртуальных машин, используемых для реализации технологии виртуализации АРМ пользователей |  |
| 4.3 | Определение правил удаленного доступа и перечня ресурсов доступа, к которым предоставляется [удаленный доступ](#sub_3045) |  |

# При использовании собственной разработки программного обеспечения Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Защита информации на этапах жизненного цикла автоматизированных систем и приложений** |  |
| 5.1 | Документарное определение перечня защищаемой информации, планируемой к обработке в АС |  |
| 5.2 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС)*ОБРАЗЕЦ* |  |
| 5.3 | Документарное определение в проектной и эксплуатационной документации на систему защиты информации АС:- состава и порядка применения технических и (или) организационных мер системы защиты информации АС;- параметров настроек технических мер системы защиты информации АС и компонентов информационной инфраструктуры, предназначенных для размещения указанных технических мер |  |
| 5.4 | Контроль предоставления и обеспечение разграничения доступа в сегментах разработки и тестирования |  |
| 5.5 | Реализация запрета использования защищаемой информации в сегментах разработки и тестирования |  |
| 5.6 | Контроль (тестирование) полноты реализации мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) |  |
| 5.7 | Проведение модернизации АС при изменении требований к составу и содержанию мер системы защиты информации АС (функционально-технические требований к системе защиты информации АС) |  |
| 5.8 | Документарное определение в проектной и эксплуатационной документации на систему защиты информации АС:- состава и порядка применения клиентами банковского платежного агента (субагента) прикладного ПО и (или) технических и (или) организационных мер защиты информации (далее при совместном упоминании - клиентские компоненты);- параметров настроек клиентских компонентов и информационной инфраструктуры клиентов банковского платежного агента (субагента), предназначенной для размещения клиентских компонентов;- описания мер по обеспечению использования клиентом определенных доверенных версий (сборок) прикладного ПО |  |
| 5.9 | Размещение и настройка (конфигурирование) технических мер системы защиты информации АС в информационной инфраструктуре, используемой для непосредственной реализации бизнес-процессов или технологических процессов банковского платежного агента (субагента) (далее - промышленная среда), в соответствии с положениями проектной и эксплуатационной документации |  |
| 5.10 | Контроль (тестирование) полноты реализации мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) в промышленной среде |  |
| 5.11 | Реализация контроля эксплуатации технических мер системы защиты информации АС в соответствии с положениями проектной и эксплуатационной документации, включающего:- контроль фактического размещения технических мер защиты в промышленной среде;- контроль фактических параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенной для размещения технических мер защиты информации |  |
| 5.12 | Реализация контроля применения мер системы защиты информации АС |  |
| 5.13 | Назначение и реализация контроля деятельности лиц, ответственных за эксплуатацию (сопровождение) системы защиты информации АС |  |
| 5.14 | Обеспечение оперативного устранения выявленных уязвимостей защиты информации АС, включая уязвимости прикладного ПО |  |
| 5.15 | Регистрация операций по изменению параметров настроек технических мер системы защиты информации АС |  |
| 5.16 | Принятие мер по обеспечению защиты информации от несанкционированного копирования и распространения |  |

# Банковский платежный агент (субагент) должен обеспечить выполнение следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Обнаружение инцидентов защиты информации и реагирование на них** |  |
| 6.1 | Реализация защиты информации об инцидентах защиты информации от НСД, обеспечение целостности и доступности указанной информации |  |
| 6.2 | Обеспечение возможности доступа к информации об инцидентах защиты информации в течение трех лет |  |
|  | **Управление инцидентами защиты информации** |  |
| 6.3 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых техническими мерами, входящими в состав системы защиты информации |  |
| 6.4 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых АС и приложениями |  |
| 6.5 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых контроллерами доменов |  |
| 6.6 | Генерация временных меток для данных регистрации о событиях защиты информации и синхронизации системного времени объектов информатизации, используемых для формирования, сбора и анализа данных регистрации |  |
| 6.7 | Резервирование необходимого объема памяти для хранения данных регистрации о событиях защиты информации |  |
| 6.8 | Реализация защиты данных регистрации о событиях защиты информации от НСД при их хранении, обеспечение целостности и доступности хранимых данных регистрации |  |
| 6.9 | Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет |  |
| 6.10 | Обеспечение возможности выявления и анализа событий защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД |  |
| 6.11 | Обеспечение возможности определения состава действий и (или) операций конкретного субъекта доступа |  |
| 6.12 | Обеспечение возможности определения состава действий и (или) операций субъектов доступа при осуществлении логического доступа к конкретному ресурсу доступа*ОБРАЗЕЦ* |  |
| 6.13 | Регистрация доступа к хранимым данным о событиях защиты информации |  |
|  | **Требования к организации и управлению защитой информации** |  |
| 6.14 | Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса |  |

# Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Обнаружение инцидентов защиты информации и реагирование на них** |  |
| 7.1 | Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации |  |
| 7.2 | Регистрация информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, полученной от работников, клиентов и (или) контрагентов банковского платежного агента (субагента) |  |
| 7.3 | Классификация инцидентов защиты информации с учетом степени их влияния (критичности) на предоставление финансовых услуг, реализацию бизнес-процессов и (или) технологических процессов банковского платежного агента (субагента) |  |
| 7.4 | Установление и применение единых правил получения от работников, клиентов и (или) контрагентов банковского платежного агента (субагента) информации, потенциально связанной с инцидентами защиты информации |  |
| 7.5 | Установление и применение единых правил регистрации и классификации инцидентов защиты информации в части состава и содержания атрибутов, описывающих инцидент защиты информации, и их возможных значений |  |
| 7.6 | Установление и применение единых правил реагирования на инциденты защиты информации |  |
| 7.7 | Определение и назначение ролей, связанных с реагированием на инциденты защиты информации |  |
| 7.8 | Проведение реагирования на каждый обнаруженный инцидент защиты информации, включающего:- анализ инцидента;- определение источников и причин возникновения инцидента;- оценку последствий инцидента на предоставление финансовых услуг, реализацию бизнес-процессов или технологических процессов банковского платежного агента (субагента);- принятие мер по устранению последствий инцидента;- планирование и принятие мер по предотвращению повторного возникновения инцидента |  |
| 7.9 | Установление и применение единых правил сбора, фиксации и распространения информации об инцидентах защиты информации |  |
| 7.10 | Установление и применение единых правил закрытия инцидентов защиты информации |  |
|  | **Управление инцидентами защиты информации** |  |
| 7.11 | Контроль формирования данных регистрации о событиях защиты информации объектов информатизации |  |
|  | **Требования к организации и управлению защитой информации** |  |
| 7.12 | Документарное определение области применения процесса системы защиты информации для уровней информационной инфраструктуры |  |
| 7.13 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания организационных мер защиты информации, выбранных банковским платежным агентом и реализуемых в рамках процесса системы защиты информации |  |
| 7.14 | Документарное определение порядка применения организационных мер защиты информации, реализуемых в рамках процесса системы защиты информации |  |
| 7.15 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания технических мер защиты информации, выбранных финансовой организацией и реализуемых в рамках процесса системы защиты информации*ОБРАЗЕЦ* |  |
| 7.16 | Документарное определение порядка применения технических мер защиты информации, реализуемых в рамках процесса системы защиты информации, включающего:- правила размещения технических мер защиты информации в информационной инфраструктуре;- параметры настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации[\*\*](#sub_3340);- руководства по применению технических мер защиты информации (включающие руководства по эксплуатации, контролю эксплуатации и использованию по назначению технических мер защиты информации);- состав ролей и права субъектов доступа, необходимых для обеспечения применения технических мер защиты информации (включающего эксплуатацию, контроль эксплуатации и использование по назначению мер защиты информации) |  |
| 7.17 | Реализация учета объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, для уровней информационной инфраструктуры, в том числе объектов доступа, расположенных в публичных (общедоступных) местах (в том числе банкоматах, платежных терминалах) |  |
| 7.18 | Размещение и настройка (конфигурирование) технических мер защиты информации в информационной инфраструктуре банковского платежного агента (субагента) |  |
| 7.19 | Контроль (тестирование) полноты реализации технических мер защиты информации |  |
| 7.20 | Назначение работникам банковского платежного агента (субагента) ролей, связанных с применением мер защиты информации, и установление обязанности и ответственности за их выполнение |  |
| 7.21 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной инфраструктуры |  |
| 7.22 | Реализация эксплуатации, использования по назначению технических мер защиты информации |  |
| 7.23 | Реализация применения организационных мер защиты информации |  |
| 7.24 | Обучение, практическая подготовка (переподготовка) работников банковского платежного агента (субагента), ответственных за применение мер защиты информации в рамках процесса защиты информации |  |
| 7.25 | Повышение осведомленности (инструктаж) работников банковского платежного агента (субагента) в области реализации процесса защиты информации, применения организационных мер защиты информации, использования по назначению технических мер защиты информации |  |
| 7.26 | Контроль фактического состава объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, на соответствие учетным данным |  |
| 7.27 | Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий:- контроль фактического размещения технических мер защиты информации в информационной инфраструктуре банковского платежного агента (субагента);- контроль фактических параметров настроек технических мер защиты информации и компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации |  |
| 7.28 | Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий:- контроль назначения ролей, связанных с эксплуатацией и использованием по назначению технических мер защиты информации;- контроль выполнения руководств по эксплуатации и использованию по назначению технических мер защиты информации |  |
| 7.29 | Периодический контроль (тестирование) полноты реализации технических мер защиты информации |  |
| 7.30 | Контроль применения организационных мер защиты информации |  |
| 7.31 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование*ОБРАЗЕЦ* |  |
| 7.32 | Проведение проверок знаний работников банковского платежного агента (субагента) в части применения мер защиты информации в рамках процесса системы защиты информации |  |
| 7.33 | Фиксация результатов (свидетельств) проведения мероприятий по контролю реализации процесса системы защиты информации |  |
| 7.34 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях:- обнаружения инцидентов защиты информации;- обнаружения недостатков в рамках контроля системы защиты информации |  |
| 7.35 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях изменения политики банковского платежного агента (субагента) в отношении:- области применения процесса системы защиты информации;- основных принципов и приоритетов в реализации процесса системы защиты информации;- целевых показателей величины допустимого остаточного операционного риска (риск-аппетита), связанного с обеспечением безопасности информации |  |
| 7.36 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях:- изменений требований к защите информации, определенных правилами платежной системы;- изменений, внесенных в законодательство Российской Федерации, в том числе нормативные акты Банка России |  |
| 7.37 | Фиксация решений о проведении совершенствования процесса системы защиты информации в виде корректирующих или превентивных действий, например:- пересмотр области применения процесса системы защиты информации;- пересмотр состава и содержания организационных мер защиты информации, применяемых в рамках процесса системы защиты информации;- пересмотр состава технических мер защиты информации, применяемых в рамках процесса системы защиты информации |  |

**Приложение №10**

**к Договору о привлечении банковского платежного агента**

**№ \_\_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_ 20\_\_ г.**

*Образец*

**Договор о привлечении банковского платежного субагента №\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| г.\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г. |

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем **«Банковский платежный агент»**, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, а также договора о привлечении банковского платёжного агента №\_\_\_\_ от \_\_\_\_\_\_\_\_г. (далее - Договор о привлечении банковского платёжного агента), заключённого с ПАО «МТС-Банк», генеральная лицензия Банка России №2268 от 17.12.2014 (далее – «Банк»), с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем **«Банковский платежный субагент»**, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_, с другой стороны, совместно именуемые «Стороны», заключили настоящий Договор о нижеследующем:

**1. Предмет договора**

1.1. Банковский платёжный агент в целях осуществления перевода денежных средств поручает, а Банковский платёжный субагент обязуется за вознаграждение осуществлять от имени и за счет Банка, в рамках, установленных п. 1.2. настоящего Договора, следующие действия:

- принимать от физических лиц (далее - плательщики) наличные денежные средства с применением платежных терминалов в целях осуществления операций по переводу денежных средств без открытия банковского счета, не требующих проведения идентификации, в том числе, упрощенной идентификации в соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», а именно: операций по переводу денежных средств в пользу юридических лиц и индивидуальных предпринимателей для оплаты реализуемых товаров, выполняемых работ, оказываемых услуг, использования результатов интеллектуальной деятельности или средств индивидуализации, в пользу органов государственной власти и органов местного самоуправления при условии, что сумма операции не превышает 15 000 (пятнадцати тысяч) рублей;

1.2. Перечень и условия совершения операций, подлежащих выполнению Банковским платёжным субагентом, содержатся в Приложении №1 к настоящему Договору. Приложение № 1 к настоящему Договору может быть изменено по соглашению Сторон путем обмена официальными письмами, подписанными уполномоченными представителями Сторон и(или) путем заключения дополнительного соглашения к настоящему Договору.

**2. Права и обязанности Сторон**

**2.1.** Обязанности Банковского платежного субагента:

**2.1.1.** Банковский платежный субагент обязан:

- осуществлять операции Банковского платежного субагента от имени Банка;

- использовать специальный банковский счет банковского платежного субагента № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, открытый в банке – (наименование банка), БИК банка - \_\_\_\_\_\_\_\_\_\_, корсчет банка - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, (далее – Специальный банковский счет) для зачисления в полном объеме полученных от плательщиков наличных денежных средств;

- подтверждать принятие наличных денежных средств путем выдачи кассового чека, соответствующего требованиям пункта 2.1.3. настоящего Договора;

- вносить наличные денежные средства, принятые от плательщиков/осуществлять перевод денежных средств, принятых от плательщиков и внесенных на другие специальные счета (в других кредитных организациях), на Специальный банковский счет в срок не позднее рабочего дня, следующего за днем предоставления плательщиком наличных денежных средств (при осуществлении перевода денежных средств плательщиков со специальных счетов в других кредитных организациях Банковский платежный субагент должен обеспечить поступление таких денежных средств на Специальный банковский счет не позднее рабочего дня, следующего за днем предоставления плательщиком наличных денежных средств);

- предоставлять плательщикам и иным лицам информацию, предусмотренную последним абзацем пункта 2.1.3. настоящего Договора в автоматическом режиме;

- в рамках исполнения обязательств по настоящему Договору использовать терминалы в соответствии с требованиями законодательства Российской Федерации о применении контрольно-кассовой техники при осуществлении наличных денежных расчетов;

- на регулярной основе (ежемесячно до 10 числа месяца, следующего за отчетным календарным месяцем) предоставлять Банковскому платёжному агенту сведения о суммах денежных средств, принятых от плательщиков в соответствии с настоящим Договором и зачисленных на Специальный банковский счет в предыдущем календарном месяце. Указанные сведения предоставляются Банковским платежным субагентом в рамках отчета, составляемого в виде сводной информации в свободной форме, и направляются по электронной почте на адрес \_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_, с последующим направлением оригиналов по почтовому адресу Банковского платёжного агента, указанному в разделе 9 Договора;

- не превышать ставки разрешённого дополнительного вознаграждения, взимаемого с плательщиков за осуществление операций Банковского платежного субагента, размер которых согласован Сторонами в Приложении №1 к настоящему Договору;

- принимать и рассматривать претензии плательщиков, связанные с осуществлением Банковским платежным субагентом действий, указанных в п.1.1. Договора.

**2.1.2.** Банковский платежный субагент обязан направлять Банковскому платёжному агенту следующую информацию:

- ежедневно, до 11 ч. по московскому времени, информировать Банковского платёжного агента о полученных Банковским платежным субагентом распоряжениях и суммах денежных средств плательщиков за предыдущий календарный день путём направления сведений посредством электронной почты на адрес \_\_\_\_\_\_@\_\_\_\_\_\_\_\_, используя формат отчёта в соответствии с Приложением №4 к настоящему Договору, и обеспечить своевременность и точность передаваемых данных;

- сообщить Банковскому платёжному агенту в письменном виде или по электронной почте \_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_ о местонахождении (об изменении местонахождения) мест осуществления операций Банковского платежного субагента в срок не позднее дня, следующего за днем установления (изменения) местонахождения такого места;

- извещать Банковского платёжного агента об изменении любых данных Банковского платежного субагента, указанных в настоящем Договоре, в том числе местонахождения, адреса (адресов) электронной почты, контактных телефонов, изменении уполномоченных представителей Банковского платежного субагента, изменении банковских реквизитов Банковского платежного субагента и т.д. Извещение должно быть направлено в течение 2 (двух) рабочих дней с момента изменения соответствующих данных;

- предоставить сведения о своей деятельности в качестве банковского платежного агента (субагента) по договорам, заключенным с другими операторами по переводу денежных средств (далее – ОПДС), а также в качестве платежного агента, осуществляющего свою деятельность в соответствии с Федеральным законом от 03.06.2009 № 103-ФЗ «О деятельности по приему платежей физических лиц, осуществляемой платежными агентами» по форме, приведенной в Приложении № 3 к настоящему Договору в течение 5 (пяти) рабочих дней с даты заключения Банковским платежным субагентом договора с ОПДС / поставщиком / оператором по приему платежей в электронном виде на адрес электронной почты \_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_;

- представлять по требованию Банковского платёжного агента информацию и документы, необходимые для осуществления контроля Банковским платёжным агентом за выполнением Банковским платежным субагентом требований законодательства Российской Федерации и положений настоящего Договора, в том числе сведения об открытых специальных банковских счетах Банковский платежный субагента в других кредитных организациях по форме приведенной в Приложении №4 настоящего Договора в срок не позднее 3 (трех) рабочих дней от даты направления требования на адрес электронной почты Банковского платежного субагента \_\_\_\_\_\_@\_\_\_\_\_\_\_\_.

**2.1.3.** Банковский платежный субагент обязан в соответствии с действующим законодательством использовать контрольно-кассовую технику с фискальной памятью и контрольной лентой, а также соблюдать иные требования законодательства Российской Федерации о применении контрольно-кассовой техники при осуществлении наличных денежных расчетов (в том числе при применении Банковским платежным субагентом платежного терминала), подтверждать принятие распоряжений плательщика и наличных денежных средств путем выдачи кассового чека.

Банковский платежный субагент при осуществлении расчетов с использованием терминалов обязан выдать кассовый чек на бумажном носителе (при этом все реквизиты, напечатанные на кассовом чеке, должны быть четкими и легко читаемыми) и (или) направить плательщику кассовый чек в электронной форме на предоставленные абонентский номер либо адрес электронной почты (при наличии технической возможности для передачи информации плательщику в электронной форме на адрес электронной почты). Кассовый чек, выдаваемый (направляемый) плательщику, согласно требованиям о применении контрольно-кассовой техники, изложенным в Федеральном законе от 22.05.2003 № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении расчетов в Российской Федерации» (далее – Федеральный закон № 54-ФЗ), должен содержать следующую информацию:

* наименование документа – кассовый чек;
* порядковый номер за смену;
* номер смены;
* дата, время и место (адрес) осуществления расчета (при расчете в зданиях и помещениях - адрес здания и помещения с почтовым индексом);
* признак расчета (получение средств от плательщика) – приход;
* наименование операции Банковского платежного субагента – прием наличных денежных средств с целью перевода;
* сумма расчета - общая сумма принятых денежных средств от плательщика;
* форма расчета – оплата наличными деньгами;
* регистрационный номер контрольно-кассовой техники;
* заводской номер экземпляра модели фискального накопителя;
* фискальный признак документа;
* адрес сайта уполномоченного органа в сети "Интернет", на котором может быть осуществлена проверка факта записи этого расчета и подлинности фискального признака;
* порядковый номер фискального документа;
* фискальный признак сообщения (для кассового чека или бланка строгой отчетности, хранимых в фискальном накопителе или передаваемых оператору фискальных данных);
* QR-код;
* абонентский номер либо адрес электронной почты плательщику в случае передачи ему кассового чека в электронной форме или идентифицирующих такой кассовый чек признаков и информации об адресе информационного ресурса в сети "Интернет", на котором такой документ может быть получен;
* адрес электронной почты Банковского платежного субагента - отправителя кассового чека в электронной форме в случае передачи плательщику кассового чека в электронной форме.

Кассовый чек, выдаваемый (направляемый) плательщику Банковским платежным субагентом, может не содержать обязательные реквизиты о ставке и размере налога на добавленную стоимость.

 Дополнительно к требованиям законодательства Российской Федерации, указанным в Федеральном законе № 54-ФЗ и перечисленным выше, кассовый чек должен содержать следующую информацию:

* адрес места осуществления операций Банковского платежного субагента;
* наименование и место нахождения Банка и Банковского платежного субагента, а также их идентификационные номера налогоплательщика;
* номер лицензии Банка на осуществление банковских операций;
* реквизиты настоящего Договора;
* размер вознаграждения, уплачиваемого плательщиком в виде общей суммы, включающей в том числе вознаграждение Банковского платежного субагента в случае его взимания;
* способы подачи претензий и порядок их рассмотрения;
* номера телефонов Банка и Банковского платежного субагента.

При использовании Банковским платежным субагентом терминала информация, предусмотренная настоящим абзацем, должна предоставляться плательщикам - физическим лицам в автоматическом режиме до начала осуществления каждой операции физическим лицом посредством направления ее на экран терминала (перед печатью кассового чека).

**2.2.** Банковский платежный субагент вправе:

**2.2.2.** Взимать с плательщика дополнительное вознаграждение за осуществление операций Банковского платежного субагента в размере, согласованном Сторонами в Приложении №1 к Договору. Указанное в настоящем [пункте](#Par71) дополнительное вознаграждение полностью поступает в распоряжение Банковского платежного субагента и не включается в расчет вознаграждения Банковского платежного субагента, предусмотренного настоящим Договором.

**2.3.** Банковский платёжный агент обязан:

- информировать Банковского платежного субагента по адресу электронной почты \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_ о возникновении технических неполадок и иных событий, препятствующих выполнению условий настоящего Договора;

- извещать Банковского платёжного субагента об изменении любых данных Банка, Банковского платёжного агента, указанных в настоящем Договоре, в том числе местонахождения, адреса электронной почты, контактных телефонов, изменении уполномоченных представителей Банковского платёжного агента, изменении банковских реквизитов Банковского платёжного агента и т.д. Извещение должно быть направлено в течение 3 (трех) рабочих дней с момента изменения соответствующих данных;

**-** оплачивать услуги Банковского платежного субагента.

**2.4.** Банковский платёжный агент вправе:

**2.4.1.** осуществлять контроль за соблюдением Банковским платежным субагентом условий, установленных статьей 14 Федерального закона «О национальной платежной системе» от 27.06.2011 № 161-ФЗ (далее – Федеральный закон № 161-ФЗ), настоящим Договором;

Порядок осуществления контроля Банковским платёжным агентом за деятельностью Банковского платежного субагента устанавливается нормативными актами Банка России и [п. 2.4.2.](#Par68) настоящего Договора.

**2.4.2.** В целях осуществления контроля за соблюдением Банковским платежным субагентом условий настоящего Договора, в том числе в части соблюдения правил осуществления расчетов в Российской Федерации, требований ст.14 Федерального закона №161-ФЗ, а также требований Федерального закона № 115-ФЗ;

- проводить проверки в торговой сети Банковского платежного субагента, в том числе с использованием методики «тайный покупатель». Результаты проверки оформляются актами, составленными Банковским платёжным агентом в одностороннем порядке;

- на основании актов проведенных проверок требовать от Банковского платежного субагента устранения выявленных замечаний, принятия мер к недопущению повторных замечаний, устанавливать сроки для выполнения требований Банковского платёжного агента. Требования направляются Банковским платёжным агентом Банковскому платежному субагенту по почте в письменном виде либо по электронной почте на адрес \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_\_. К требованию должен быть приложен акт проверки;

 - запрашивать у Банковского платежного субагента информацию и документы (заверенные надлежащим образом копии первичных документов, подтверждающих прием денежных средств (контрольные ленты контрольно-кассовой техники, оригиналы заявлений о возврате денежных средств, изменений реквизитов плательщика), а также иную информацию и документы в целях подтверждения исполнения Банковским платежным субагентом обязанностей по настоящему Договору;

- направлять запросы в адрес Банковского платежного субагента для получения от него информации о всех специальных банковских счетах, предусмотренных частью 3 пункта 4 статьи 14 Федерального закона N 161-ФЗ, открытых Банковскому платежному субагенту для целей осуществления деятельности от имени оператора по переводу денежных средств согласно п. 2.1.2 настоящего Договора, выписок по указанным специальным банковским счетам, а также необходимых для осуществления контроля копий первичных учетных документов.

**2.4.3.** В случае возникновении технических неполадок и иных событий, препятствующих выполнению условий настоящего Договора, блокировать возможность осуществления Банковским платёжным субагентом приема денежных средств, уведомив Банковского платёжного субагента за 5 календарных дней по адресу электронной почты \_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_\_ с указанием причины блокировки.

**2.4.4.** При несоблюдении Банковским платежным субагентом указанных в настоящем Договоре условий его привлечения, требований статьи 14 Федерального закона № 161-ФЗ и законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, отказаться в одностороннем порядке от исполнения настоящего Договора.

**3. Вознаграждение Банковского платежного субагента**

**3.1.** Банковский платёжный агент уплачивает Банковскому платежному субагенту вознаграждение за осуществление деятельности банковского платежного агента согласно п.п.1.1., 1.2. настоящего Договора (за выполнение поручения, указанного в п.п.1.1., 1.2. Договора), размер которого определяется в соответствие с Приложением № 1 к настоящему Договору, кроме того НДС по ставке, подлежащей применению в соответствии с законодательством РФ. Приложение №1 к Договору может быть изменено по соглашению Сторон путем обмена официальными письмами, подписанными уполномоченными представителями Сторон.

**3.2.** Банковский платежный агент рассчитывает вознаграждение Банковскому платежному субагенту за приём денежных средств от суммы фактически принятых от плательщиков в отчетном календарном месяце денежных средств.

**3.4.** Вознаграждение выплачивается Банковским платёжным агентом на основании согласованного и подписанного Сторонами Акта об оказании услуг в соответствии с Приложением № 2 к Договору (далее - Акт), выставленного Банковским платежным субагентом счета на оплату и счета-фактуры.

**3.5.** Банковский платежный субагент не позднее 3 (трех) рабочих дней месяца, следующего за отчетным, предоставляет Банковскому платёжному субагенту на предварительное согласование Акт в электронном виде на адрес электронной почты \_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_\_, который согласовывается Банковским платёжным агентом в течение 5 (пяти) рабочих дней. В случае несогласия с данными, указанными в Акте, Банковский платёжный агент обязуется в тот же срок предоставить Банковскому платежному субагенту свои мотивированные возражения на адрес электронной почты \_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_. Если в течение указанного срока Банковский платёжный агент не представил возражений, Акт считается полностью одобренным и принятым Банковским платёжным агентом.

**3.6.** В письменном виде Акт, счет на оплату вознаграждения и счет-фактура направляется Банковским платежным субагентом Банковскому платёжному агенту по адресу, указанному в разделе 9 Договора. В течение 14 рабочих дней с даты получения Акта Банковский платёжный агент обязан подписать и направить один экземпляр Акта Банковскому платежному субагенту по адресу, указанному в разделе 9 Договора.

 **3.7.** Не позднее 14 (четырнадцати) рабочих дней с даты подписания Акта Банковским платёжным агентом последний перечисляет вознаграждение на счет Банковского платежного субагента, указанный в счете на оплату.

**4. Ответственность Сторон**

**4.1.** Банковский платежный субагент обязан возместить Банковскому платёжному агенту реальный ущерб, причиненный в результате неисполнения (ненадлежащего исполнения) обязательств по настоящему Договору, в том числе, суммы уплаченных Банком штрафов в случае привлечения Банка к административной ответственности в связи с допущенными Банковским платежным агентом нарушениями требований ФЗ «О персональных данных» при обработке персональных данных.

**4.2.** Банковский платежный субагент в полном объеме несет ответственность перед Банковским платёжным агентом по всем операциям, совершенным Банковским платежным субагентом.

**4.3.** В случае неисполнения/ненадлежащего исполнения обязательств Банковского платежного субагента при осуществлении расчетов в соответствии с п.2.1.1. настоящего Договора по соблюдению сроков поступления денежных средств на Специальный банковский счет, Банковский платежный субагент уплачивает Банковскому платёжному агенту неустойку в размере \_\_\_\_ % (\_\_\_\_\_\_\_\_\_\_\_\_\_\_) процентов от суммы неисполненного обязательства за каждый день неисполнения.

**4.4.** Банковский платёжный агент в рамках настоящего Договора не несет ответственности за неисполнение/ненадлежащее исполнение своих обязательств, если это явилось результатом предоставления со стороны Банковского платежного субагента неполной/недостоверной информации, используемой Банковским платёжным агентом для исполнения соответствующих обязательств по настоящему Договору. Банковский платёжный агент не несет ответственности по спорам и разногласиям, возникшим между Банковским платежным субагентом и плательщиками во всех случаях, когда споры и разногласия не относятся к предмету Договора.

**4.5.** Банковский платёжный агент не несет ответственности за убытки Банковского платежного субагента либо плательщика, возникшие вследствие злого умысла или ошибки со стороны сотрудников Банковского платежного субагента.

**4.6.** В качестве обеспечения надлежащего исполнения обязательств по настоящему Договору (обязательств по перечислению денежных средств и уплате неустойки), Банковский платёжный субагент перечисляет Банковскому платёжному агенту обеспечительный платеж (далее – Обеспечительный платёж) в размере, определяемом Сторонами (сумма Обеспечительного платежа НДС не облагается). Банковский платежный субагент вправе в любой момент увеличить Обеспечительный платеж путем перечисления дополнительных денежных средств. Банковский платежный субагент уведомляет Банковского платежного агента о перечислении/изменении суммы Обеспечительного платежа по адресу эл. почты \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_за 1 (Один) рабочий день до даты перечисления/изменения суммы Обеспечительного платежа.

**4.7.1.** В случае неисполнения Банковским платёжным субагентом в установленные сроки обязательств, предусмотренных настоящим Договором, Банковский платёжный агент удерживает из Обеспечительного платежа суммы, подлежащие зачислению Банковским платёжным субагентом на Специальный банковский счет, открытый в Банке в соответствии с условиями настоящего Договора.

**4.7.2.** В случае неисполнения Банковским платежным субагентом обязательства, предусмотренного п.4.6 настоящего Договора, Банковский платежный агент вправе в одностороннем порядке приостановить (прекратить) прием Банковским платежным субагентом денежных средств от плательщиков с последующим направлением Банковскому платежному субагенту уведомления по адресу электронной почты \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ вплоть до выполнения Банковским платежным субагентом обязательства, предусмотренного п.4.6. Договора. После предоставления Банковским платежным субагентом денежных средств в размере, необходимом для восстановления Обеспечительного платежа в размере, указанном в п.4.6. Договора, прием Банковским платежным субагентом денежных средств от плательщиков возобновляется.

**4.7.3.** В случае расторжения настоящего Договора, остаток Обеспечительного платежа подлежит возврату Банковским платёжным агентом Банковскому платёжному субагенту путем перечисления на счет Банковского платёжного субагента по реквизитам, указанным в настоящем Договоре, в течение 5 (Пяти) календарных дней с даты расторжения настоящего Договора.

**4.8.** Стороны обязуются соблюдать требования антикоррупционного законодательства и не предпринимать никаких действий, которые могут нарушить нормы антикоррупционного законодательства, в связи со своими правами или обязательствами согласно Договору, в том числе (не ограничиваясь) не совершать от своего имени предложение, санкционирование, обещание и осуществление незаконных платежей, включая (но не ограничиваясь) взятки в денежной или любой иной форме, каким-либо физическим или юридическим лицам, включая (но не ограничиваясь) коммерческие организации, органы власти и самоуправления, государственных служащих, частных компаний и их представителей.

4.9. В случае нарушения какой-либо из Сторон, указанных в настоящем разделе обязательств, другая сторона имеет право в одностороннем внесудебном порядке отказаться от исполнения Договора. Нарушившей стороне не возмещаются убытки в случае отказа другой стороны от исполнения Договора в соответствии с настоящим пунктом.

**5. Срок действия Договора**

**5.1.** Настоящий Договор вступает в силу с момента его подписания Сторонами и действует в течение неопределенного срока.

**5.2.** Досрочное расторжение Договора возможно в следующих случаях:

**5.2.1.** по соглашению Сторон, оформленному в письменном виде;

**5.2.2.** по инициативе любой из Сторон. Сторона, отказывающаяся от дальнейшего исполнения настоящего Договора, в письменной форме уведомляет другую сторону о своем намерении расторгнуть Договор не позднее, чем за 60 (шестьдесят) календарных дней до предполагаемой даты расторжения Договора. Уведомление должно быть сделано в письменной форме на бумажном носителе и содержать указание на причину расторжения Договора;

**5.2.3.** по инициативе Банковского платёжного агента при нарушении Банковским платежным субагентом любого из условий настоящего Договора;

**5.2.4.** в иных случаях, предусмотренных настоящим Договором и действующим законодательством Российской Федерации.

**5.3.** В случае несоблюдения Банковским платежным субагентом условий его привлечения, предусмотренных настоящим Договором, требований статьи 14 Федерального закона № 161-ФЗ, Банковский платёжный агент вправе в одностороннем порядке отказаться от Договора (исполнения Договора). Банковский платёжный агент уведомляет Банковского платежного субагента об одностороннем отказе от Договора (исполнения Договора) путем направления ему соответствующего письменного уведомления в электронной форме по адресу электронной почты \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_ и на бумажном носителе курьером либо заказным почтовым отправлением с уведомлением о вручении по адресу, указанному в разделе 9 настоящего Договора. Договор в этом случае прекращается с даты, указанной в уведомлении Банковского платёжного агента.

**5.4.** Обязательства Сторон по настоящему Договору, возникшие до расторжения/прекращения настоящего Договора, сохраняются вплоть до их полного исполнения.

**6. Конфиденциальность**

**6.1.** Банковский платёжный субагент обязуется соблюдать конфиденциальность персональных данных плательщиков и обеспечивать безопасность персональных данных при их обработке. При обработке персональных данных Банковский платёжный субагент должен руководствоваться требованиями к защите персональных данных, установленными законодательными актами РФ.

**6.2.** Стороны договорились сохранять в режиме конфиденциальности сведения, составляющие коммерческую тайну каждой из Сторон. Под сведениями, составляющими коммерческую тайну, понимаются не являющиеся общедоступными сведения о деятельности каждой из Сторон, разглашение которых может привести к возникновению убытков и/или негативно повлиять на деловую репутацию любой из Сторон, а также на информацию, которую любая из Сторон идентифицирует как конфиденциальную до или сразу после ее предоставления другой Стороне.

**6.3.** Стороны принимают на себя обязательства не разглашать полученные в ходе исполнения настоящего Договора сведения, составляющие банковскую или иную охраняемую законом тайну, включая, но не ограничиваясь, информацию об операциях, о персональных данных плательщиков.

**6.4.** Информация, составляющая банковскую или иную охраняемую законом тайну, может быть сообщена третьим лицам только при наличии письменного разрешения плательщика, за исключением случаев, предусмотренных действующим законодательством.

**6.5.** В целях обеспечения конфиденциальности при передаче информации между Сторонами, в том числе обрабатываемых персональных данных, Стороны обязуются организовать и использовать только защищенный канал связи.

**6.6.** Факт заключения настоящего Договора и предмет Договора не являются конфиденциальной информацией. К информации, признаваемой в соответствии с настоящим Договором конфиденциальной, не могут относиться сведения, являющиеся в соответствии с требованиями российского законодательства общедоступными.

**6.7.** Обязательства о конфиденциальности сохраняют силу в течение пяти лет после истечения срока действия или расторжения настоящего Договора.

1. **Антикоррупционная оговорка**
	1. В рамках исполнения настоящего Договора Стороны подтверждают, что в своей деятельности придерживаются высоких этических стандартов и обязуются соблюдать требования Применимого антикоррупционного законодательства, и не будут предпринимать никаких действий, которые могут нарушить нормы Применимого антикоррупционного законодательства или стать причиной такого нарушения другой Стороной, в том числе не требовать, не получать, не предлагать, не санкционировать, не обещать и не совершать незаконные платежи напрямую, через третьих лиц или в качестве посредника, включая (но не ограничиваясь) взятки в денежной или любой иной форме, каким-либо физическим или юридическим лицам, включая (но не ограничиваясь) органам власти и самоуправления, государственным служащим, частным компаниям и их представителям.
	2. Стороны обязуются не совершать действий (бездействий), создающих угрозу возникновения конфликта интересов, а также в разумные сроки сообщать другой Стороне о ставших известными ей обстоятельствах, способных вызвать конфликт интересов.
	3. Канал уведомления Банковского платежного агента для направления (раскрытия) сведений: \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_.
	4. Канал уведомления Банковского платежного субагента для направления (раскрытия) сведений: \_\_\_\_\_\_\_\_\_\_@\_\_\_\_\_\_\_\_\_.
	5. Канал уведомления ПАО «МТС-Банк» для направления (раскрытия) сведений: psmtsb@mtsbank.ru, compliance@mtsbank.ru.
	6. Стороны подтверждают, что любые третьи лица, привлеченные для исполнения настоящего Договора, не осуществляют свои действия с целью оказать незаконное влияние на Государственных должностных лиц либо с целью коммерческого подкупа и будут допущены к выполнению договорных обязательств после проведения достаточных проверочных мероприятий привлекающей их Стороной.
	7. Стороны обязуются надлежащим образом вести и хранить всю бухгалтерскую отчетность, и другие документы, подтверждающие расходы, осуществленные по настоящему Договору. Стороны обязуются в полной мере оказывать поддержку в отношении любого расследования и/или аудита, который может проводится в рамках исполнения настоящего Договора. Стороны обязуются охранять всю конфиденциальную информацию, которая может стать им известна в рамках аудита, в соответствии с законодательством РФ.
	8. В случае нарушения одной из Сторон изложенных в п. 7.1 - 7.2. антикоррупционных обязательств, другая Сторона вправе в одностороннем порядке приостановить исполнение своих обязательств по настоящему Договору до устранения причин такого нарушения или отказаться от исполнения Договора, направив об этом письменное уведомление.
	9. Под Применимым антикоррупционным законодательством понимается:

1) российское антикоррупционное законодательство (Федеральный закон от 25.12.2008 г. № 273-ФЗ «О противодействии коррупции», Уголовный Кодекс РФ, Гражданский Кодекс РФ, Кодекс РФ об административных правонарушениях, а также иные Федеральные законы и подзаконные нормативные правовые акты РФ, содержащие нормы, направленные на борьбу с коррупцией.),

2) иные законы по борьбе со взяточничеством и коррупцией, постановления, правила, политики, надзорные указания зарубежных стран, включая Закон США «О противодействии коррупции за рубежом», Закон Великобритании «О взяточничестве» 2010, в той мере, в какой указанные акты применимы к соответствующей Стороне.

* 1. Под Государственным Должностным Лицом понимается:

- любое российское или иностранное, назначаемое или избираемое лицо, занимающее какую-либо должность в законодательном, исполнительном, административном или судебном органе, или международной организации;

- любое лицо, выполняющее какую-либо публичную функцию для государства, в том числе для государственной организации;

- ведущие политические деятели, должностные лица политических партий, включая кандидатов на политические посты, послы, влиятельные функционеры в национализированных областях промышленности или естественных монополиях;

- руководители и сотрудники Государственных органов, учреждений и предприятий, включая врачей, военнослужащих, муниципальных служащих и т.п.;

- лица, о которых известно, что они связаны с государственным должностным лицом родственными, дружескими или деловыми отношениями и (или) действуют от имени и(или) в интересах государственного должностного лица.

1. **Дополнительные условия и заключительные положения**

**8.1.** Банковский платёжный агент и Банковский платежный субагент осуществляют информационное и технологическое взаимодействие в порядке, установленном Приложением №3 к настоящему Договору.

**8.2.** Банковский платёжный субагент не вправе привлекать других лиц к осуществлению операций банковского платёжного субагента.

**8.3.** Во всем остальном, что не предусмотрено настоящим Договором, Стороны руководствуются действующим законодательством Российской Федерации.

**8.4.** Договор составлен в двух экземплярах, по одному для каждой из Сторон.

1. **Реквизиты и подписи Сторон:**

|  |  |
| --- | --- |
| Общество с ограниченной ответственностью «\_\_\_\_\_»Место нахождения: \_\_\_\_\_\_\_\_\_\_\_ОГРН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, ИНН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, К/счет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_БИК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Бизнес-лидер Стрима «Система денежных переводов»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | Банковский платежный агент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Юридический адрес: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ИНН \_\_\_\_\_\_\_\_\_\_КПП \_\_\_\_\_\_\_\_\_р/с № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_БИК \_\_\_\_\_\_\_\_\_к/с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Должность \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_/мп |

**Приложение №1**

**к Договору о привлечении банковского платежного субагента**

**№ \_\_\_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_2016 г.**

**Перечень и условия совершения операций, подлежащих выполнению Банковским платёжным субагентом**

1. Проведение операций по приёму от физических лиц денежных средств в целях осуществления переводов без открытия банковского счета в пользу юридических лиц, перечисленных в п. 1.2 настоящего Приложения для оплаты работ/услуг, при условии, что такие переводы в соответствии с Федеральным законом № 115-ФЗ не требуют проведения идентификации, в том числе упрощенной идентификации:
	1. Перечень получателей переводов, размер вознаграждения:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Наименование получателя | Дополнительная комиссия (комиссия, взимаемая Банковским платежным субагентом с плательщика) | Размер вознаграждения Банковского платежного субагента, выплачиваемое Банковским платежным агентом, кроме того НДС по ставке, подлежащей применению в соответствии с законодательством РФ (в % от суммы принятых денежных средств плательщиков или в рублях) | Размер вознаграждения Банковского платежного агента, выплачиваемое плательщиком, кроме того НДС по ставке, подлежащей применению в соответствии с законодательством РФ (в % от суммы принятых денежных средств плательщиков или в рублях | Примечание | Минимальная сумма, руб. |
| 1 | 2  |  3 |  4 | 5 |  6 |
|  |  |  |  |  |   |
|  |  |  |  |  |   |
|  |  |  |  |  |   |
|  |  |  |  |  |  |
|  |  |  |  |  | 1 |

* 1. Условия совершения операций:

- Банковский платежный субагент обязан осуществить печать пречека или сообщать информацию иным способом, для ознакомления плательщика со стоимостью услуг и правильностью реквизитов операции,

- плательщик обязан проверить корректность реквизитов операции, суммы перевода, комиссий и подписать пречек.

**Подписи сторон:**

|  |  |
| --- | --- |
| **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_/мп | **Банковский платёжный субагент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/ мп |

**Приложение №2**

**к Договору о привлечении банковского платежного субагента**

**№ \_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_2016 г.**

**Акт об оказании услуг № \_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| г. Москва | «\_\_» \_\_\_\_\_\_201\_ года |

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем **«Банковский платежный агент»**, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, а также договора о привлечении банковского платёжного агента №\_\_\_\_ от \_\_\_\_\_\_\_\_г. (далее - Договор о привлечении банковского платёжного агента), заключённого с ПАО «МТС-Банк», генеральная лицензия Банка России №2268 от 17.12.2014г. (далее – «Банк»), с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем **«Банковский платежный субагент»**, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_, с другой стороны, совместно именуемые «Стороны», составили настоящий АКТ оказанных услуг по Договору № \_\_\_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2016 г. (далее – «Договор») о нижеследующем:

1. Отчетный период Банковским платежным субагентом оказаны услуги, предусмотренные п.1.1. Договора в следующем объеме:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование показателя | Значение показателя | Единица измерения |
| 1 | Дата и время начала Отчетного периода | дд.мм.гггг | 0:00:00 |
| 2 | Дата и время окончания Отчетного периода | дд.мм.гггг | 23:59:59 |
| 3 | Сумма наличных денежных средств, принятых от плательщиков Банковским платежным субагентом в Отчетном периоде |   | руб. |
| 4 | Сумма наличных денежных средств, принятых от плательщиков и зачисленных на Специальный банковский счет в Отчетном периоде |   | руб. |
| 5 | Сумма наличных денежных средств, принятых от плательщиков в Отчетном периоде, подлежащая зачислению Банковским платежным субагентом на Специальный банковский счет в следующем отчетном периоде |   | руб. |
| 6 | Сумма вознаграждения Банковского платежного субагента, подлежащая к перечислению Банковским платёжным агентом за Отчетный период*ОБРАЗЕЦ* |   | руб. |
| 7 | Сумма вознаграждения Банковского платежного субагента, перечисленная Банковским платёжным агентом в Отчетном периоде |   | руб. |
| 8 | Сумма вознаграждения Банковского платежного субагента, подлежащая к перечислению Банковским платёжным агентом в следующем Отчетном периоде |   | руб. |

1. Обязательства Банковского платежного субагента по оказанию услуг, предусмотренных Договором, выполнены в полном объеме, в соответствии с условиями Договора.
2. Банковский платёжный агент не имеет каких-либо претензий по оказанным Банковским платежным субагентом

 услугам за период, указанный в настоящем Акте.

1. Настоящий Акт составлен в двух экземплярах, по одному для каждой из Сторон.
2. Подписи сторон:

|  |  |
| --- | --- |
| **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/мп | **Банковский платежный субагент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_/мп |

**Образец Договора о привлечении банковского платежного субагента согласован Сторонами:**

|  |  |
| --- | --- |
| **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_/мп | **Банковский платёжный субагент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_/ мп |

**Приложение № 3**

**к Договору о привлечении банковского платежного агента**

**№ \_\_\_\_\_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.**

**Сведения о деятельности в качестве банковского платежного субагента**

Полное или сокращенное фирменное наименование Банковского платежного субагента \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Адрес (место нахождения) Банковского платежного субагента \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ИНН \_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование оператора по переводу денежных средств / поставщика[[5]](#footnote-6)  | Признак банковского платежного субагента[[6]](#footnote-7) | Номер договора, заключенного с другими операторами по переводу денежных средств / поставщиками | Дата заключенного договора | Срок действия договора |
| 1 | *ОБРАЗЕЦ* |  |  |  |  |
| 2 |  |  |  |  |  |

|  |  |
| --- | --- |
| **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_/мп | **Банковский платёжный субагент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_/ мп |

**Приложение № 4**

**к Договору о привлечении банковского платежного агента**

**№ \_\_\_\_\_\_\_\_\_\_ от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.**

**Уведомление Банковского платежного субагента об открытых специальных банковских счетах**

**на дату «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ г.**

Полное или сокращенное фирменное наименование Банковского платежного субагента\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Адрес (место нахождения) Банковского платежного субагента \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование кредитных организаций, в которых открыты специальные банковские счета банковскому платежному субагенту | БИК | № специального банковского счета |
| 1 | *ОБРАЗЕЦ* |  |  |
| 2 |  |  |  |

|  |  |
| --- | --- |
| **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_/мп | **Банковский платёжный субагент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_/ мп |

**Приложение №8**

**к Договору о привлечении банковского платежного агента**

**№\_\_\_\_\_\_\_\_\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.**

**Перечень принимаемых организационных и технических мер по защите информации[[7]](#footnote-8)**

Перечень мер разработан согласно в соответствии с требованиями Положения ЦБ РФ №719-П[[8]](#footnote-9).

1. Банковские платежные агенты (субагенты) должны обеспечивать защиту информации при участии в осуществлении переводов денежных средств в отношении следующих операций:
* принятие от физического лица наличных денежных средств, в том числе с применением платежных терминалов.
1. К защищаемой информации при совершении банковскими платежными агентами (субагентами) операций, указанных в п.3.1 Положения № 719-П, относится информация:
* Информация, содержащаяся в электронных сообщениях физических лиц;
* Информация, содержащаяся в электронных сообщениях, передаваемых при взаимодействии банковских платежных агентов (субагентов) и операторов по переводу денежных средств, в том числе в электронных сообщениях, составленных банковскими платежными агентами (субагентами) от имени операторов по переводу денежных средств;
* Информация, содержащаяся в реестрах, сформированных на основе электронных сообщений (далее - реестр электронных сообщений) физических лиц. Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между банковскими платежными агентами (субагентами) и операторами по переводу денежных средств;
* Ключевая информация СКЗИ, используемая при осуществлении обмена электронными сообщениями между банковскими платежными агентами (субагентами) и операторами по переводу денежных средств;

# Банковские платежные агенты (субагенты) должны обеспечить реализацию минимального уровня защиты информации для объектов информационной инфраструктуры в соответствии с ГОСТ Р 57580.1-2017.

1. Банковские платежные агенты (субагенты) должны обеспечить при осуществлении операций, указанных в пункте 1 настоящего Приложения, реализацию мер по обеспечению защиты информации приведенных в таблицах 1 и 2;
2. Информировать Банк об инцидентах нарушения защиты информационной безопасности, в результате которых были нарушены или могли быть нарушены конфиденциальность данных плательщика(ов) или могли быть выполнены неавторизованные платежи. Соответствующие сообщения должны направляться на адрес ib\_bpa@mtsbank.ru, psmtsb@mtsbank.ru. В части контроля выполнения требований 719-П БПА по запросу банка предоставляют Банку отчет, подготовленный проверяющей организацией по результатам оценки соответствия требованиям 719-П в части защиты информации по форме Приложения №9 к настоящему Договор.

АРМ - автоматизированное рабочее место;

АС – автоматизированные системы, в том числе программное обеспечение Банка

ПДн - персональные данные;

ИСПДн - информационные системы персональных данных;

МНИ - машинные носители информации;

НСД - несанкционированный доступ;

ПО - программное обеспечение;

СКЗИ - средства криптографической защиты информации;

СВТ - средство вычислительной техники;

СУБД - система управления базами данных.

Приведенные таблицы содержат меры защиты информации в соответствии с ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

Перечень мер, содержащихся в таблицах 1 и 2 являются обязательными к исполнению всеми Банковскими платежными агентами (субагентами)

Перечень мер, содержащихся в таблицах 3-7 вступает в действие с 01.01.2022 г. в соответствии с требованиями Положения ЦБ РФ №719-П.

# Банковский платежный агент (субагент) должен обеспечить выполнение следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
| 1 | **Обеспечение защиты информации при управлении доступом** |
| 1.2 | Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями |
| 1.3 | Исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа |
| 1.4 | Исключение возможного бесконтрольного изменения пользователями параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации |
| 1.5 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для банковского платежного агента (субагента) (субагента), клиентов и контрагентов. |
| 1.6 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению криптографическими ключами |
| 1.7 | [Идентификация](#sub_3016) и [однофакторная аутентификация](#sub_3028) пользователей |
| 1.8 | Идентификация и однофакторная аутентификация эксплуатационного персонала |
| 1.9 | Аутентификация программных сервисов, осуществляющих логический доступ с использованием [технических учетных записей](#sub_3020) |
| 1.10 | Сокрытие (неотображение) паролей при их вводе субъектами доступа |
| 1.11 | Временная блокировка учетной записи пользователей после выполнения ряда неуспешных последовательных попыток аутентификации на период времени не менее 30 мин. |
| 1.12 | Обеспечение возможности выполнения субъектом логического доступа - работниками банковского платежного агента (субагента) процедуры принудительного прерывания сессии логического доступа и (или) приостановки осуществления логического доступа (с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа) |
| 1.13 | Автоматическое прерывание сессии логического доступа (приостановка осуществления логического доступа) по истечении установленного времени бездействия (неактивности) субъекта логического доступа, не превышающего 15 мин., с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа |
| 1.14 | Выполнение процедуры повторной аутентификации для продолжения осуществления логического доступа после его принудительного или автоматического прерывания (приостановки осуществления логического доступа), предусмотренного мерами 1.12 и 1.13 настоящей таблицы |
| 1.15 | Использование на АРМ субъектов логического доступа встроенных механизмов контроля изменения базовой конфигурации оборудования (пароль на изменение параметров конфигурации системы, хранящихся в энергонезависимой памяти) |
| 1.16 | Запрет на использование технологии аутентификации с сохранением аутентификационных данных в открытом виде в СВТ |
| 1.17 | Запрет на передачу аутентификационных данных в открытом виде по каналам и линиям связи и их передачу куда-либо, кроме средств или систем аутентификации |
| 1.18 | Смена паролей пользователей не реже одного раза в год |
| 1.19 | Смена паролей эксплуатационного персонала не реже одного раза в квартал |
| 1.20 | Использование пользователями паролей длиной не менее восьми символов |
| 1.21 | Использование эксплуатационным персоналом паролей длиной не менее шестнадцати символов |
| 1.22 | Использование при формировании паролей субъектов логического доступа символов, включающих буквы (в верхнем и нижнем регистрах) и цифры |
| 1.23 | Обеспечение возможности самостоятельной смены субъектами логического доступа своих паролей |
| 1.24 | Авторизация логического доступа к ресурсам доступа, в том числе АС |
| 1.25 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа |
| 1.26 | Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа, в том числе АС |
| 1.27 | Запрет выполнения пользователями бизнес-процессов с использованием привилегированных прав логического доступа, в том числе работы пользователей с правами локального администратора АРМ |
| 1.28 | Регистрация осуществления субъектами логического доступа идентификации и аутентификации |
| 1.29 | Регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа, в том числе в АС |
|  | **Обеспечение защиты вычислительных сетей** |
| 1.30 | Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в [ГОСТ Р ИСО/МЭК 7498-1](http://mobileonline.garant.ru/document?id=70146072&sub=0), внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет |
| 1.31 | Межсетевое экранирование внутренних вычислительных сетей банковского платежного агента (субагента), включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в [ГОСТ Р ИСО/МЭК 7498-1](http://mobileonline.garant.ru/document?id=70146072&sub=0) |
| 1.32 | Реализация и контроль информационного взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет в соответствии с установленными правилами и протоколами сетевого взаимодействия |
| 1.33 | Сокрытие топологии внутренних вычислительных сетей банковского платежного агента (субагента) |
| 1.34 | Реализация сетевого взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет через ограниченное количество контролируемых точек доступа |
| 1.35 | Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей банковского платежного агента (субагента) |
| 1.36 | Контроль и обеспечение возможности блокировки нежелательных сообщений электронной почты (SPAM) |
| 1.37 | Применение сетевых протоколов, обеспечивающих защиту подлинности сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии [двухсторонней аутентификации](#sub_3030) при осуществлении логического доступа с использованием телекоммуникационных каналов и (или) линий связи, не контролируемых банковским платежным агентом |
| 1.38 | Реализация защиты информации от раскрытия и модификации, применение двухсторонней аутентификации при ее передаче с использованием сети Интернет, телекоммуникационных каналов и (или) линий связи, не контролируемых банковским платежным агентом |
|  | Защита беспроводных сетей |
| 1.39 | Аутентификация устройств доступа техническими средствами, реализующими функции беспроводного сетевого соединения (точками доступа по протоколу Wi-Fi) |
| 1.40 | Защита информации от раскрытия и модификации при ее передаче с использованием протоколов беспроводного доступа |
|  | **Защита от вредоносного кода** |
| 1.41 | Реализация защиты от вредоносного кода на уровне физических АРМ пользователей и эксплуатационного персонала |
| 1.42 | Реализация защиты от вредоносного кода на уровне виртуальной информационной инфраструктуры |
| 1.43 | Реализация защиты от вредоносного кода на уровне серверного оборудования |
| 1.44 | Реализация защиты от вредоносного кода на уровне контроля почтового трафика |
| 1.45 | Реализация защиты от вредоносного кода на уровне входного контроля устройств и переносных (отчуждаемых) носителей информации |
| 1.46 | Реализация защиты от вредоносного кода на уровне контроля общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) |
| 1.47 | Функционирование средств защиты от вредоносного кода в постоянном, автоматическом режиме, в том числе в части установки их обновлений и сигнатурных баз данных |
| 1.48 | Функционирование средств защиты от вредоносного кода на АРМ пользователей и эксплуатационного персонала в резидентном режиме (в режиме service - для операционной системы Windows, в режиме daemon - для операционной системы Unix), их автоматический запуск при загрузке операционной системы |
| 1.49 | Применение средств защиты от вредоносного кода, реализующих функцию контроля целостности их программных компонентов |
| 1.50 | Контроль отключения и своевременного обновления средств защиты от вредоносного кода |
| 1.51 | Выполнение еженедельных операций по проведению проверок на отсутствие вредоносного кода |
| 1.52 | Использование средств защиты от вредоносного кода различных производителей, как минимум для уровней:- физические АРМ пользователей и эксплуатационного персонала;- серверное оборудование |
| 1.53 | Входной контроль всех устройств и переносных (отчуждаемых) носителей информации (включая мобильные компьютеры и флеш-накопители) перед их использованием в вычислительных сетях банковского платежного агента (субагента) |
| 1.54 | Регистрация операций по проведению проверок на отсутствие вредоносного кода |
| 1.55 | Регистрация фактов выявления вредоносного кода |
| 1.56 | Регистрация сбоев в функционировании средств защиты от вредоносного кода |
| 1.57 | Регистрация сбоев в выполнении контроля (проверок) на отсутствие вредоносного кода |
| 1.58 | Регистрация отключения средств защиты от вредоносного кода |
| 1.59 | Регистрация нарушений целостности программных компонентов средств защиты от вредоносного кода |
|  | **Предотвращение утечек информации** |
| 1.60 | Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при осуществлении вывода МНИ из эксплуатации или вывода из эксплуатации СВТ, в состав которых входят указанные МНИ, а также при необходимости их передачи в сторонние организации |
| 1.61 | Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при передаче (перезакреплении) МНИ между работниками и (или) структурными подразделениями банковского платежного агента (субагента) |

# Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Обеспечение защиты информации при управлении доступом** |
| 2.1 | Контроль соответствия фактического состава разблокированных учетных записей фактическому составу [легальных субъектов](#sub_3024) логического доступа |
| 2.2 | Контроль отсутствия незаблокированных учетных записей:- уволенных работников;- работников, отсутствующих на рабочем месте более 90 календарных дней;- работников внешних (подрядных) организаций, прекративших свою деятельность в организации |
| 2.3 | Контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения |
| 2.4 | Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа) |
| 2.5 | Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа) |
| 2.6 | Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации |
| 2.7 | Контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа |
| 2.8 | Контроль необходимости отзыва прав субъектов логического доступа при изменении их должностных обязанностей |
| 2.9 | Контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа |
| 2.10 | Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 90 дней |
| 2.11 | Реализация контроля со стороны распорядителя логического доступа целесообразности дальнейшего предоставления прав логического доступа, не использованных субъектами на протяжении периода времени, указанного мерой 2.10 настоящей таблицы |
| 2.12 | Реализация возможности определения состава предоставленных прав логического доступа для конкретного ресурса доступа |
| 2.13 | Реализация возможности определения состава предоставленных прав логического доступа для конкретного субъекта логического доступа |
| 2.14 | Определение состава ролей, связанных с выполнением операции (транзакции) в АС, имеющих финансовые последствия для банковского платежного агента (субагента), клиентов и контрагентов, и ролей, связанных с контролем выполнения указанных операций (транзакций), запрет выполнения указанных ролей одним субъектом логического доступа |
| 2.15 | Реализация правил управления правами логического доступа, обеспечивающих запрет совмещения одним субъектом логического доступа ролей, предусмотренных мерой 2.14 настоящей таблицы |
| 2.16 | Запрет использования учетных записей субъектов логического доступа с незаданными аутентификационными данными или заданными по умолчанию разработчиком ресурса доступа, в том числе разработчиком АС |
| 2.17 | Запрет на использование групповых, общих и стандартных учетных записей и паролей, а также прочих подобных методов идентификации и аутентификации, не позволяющих определить конкретного субъекта доступа |
| 2.18 | Хранение копий аутентификационных данных эксплуатационного персонала на выделенных МНИ или на бумажных носителях |
| 2.19 | Реализация защиты копий аутентификационных данных эксплуатационного персонала от НСД при их хранении на МНИ или бумажных носителях |
| 2.20 | Регистрация персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации, реализующих многофакторную аутентификацию |
| 2.21 | Смена аутентификационных данных в случае их [компрометации](#sub_3026) |
| 2.22 | Запрет реализации пользователями бизнес-процессов и технологических процессов банковского платежного агента (субагента) с использованием учетных записей эксплуатационного персонала, в том числе в АС |
| 2.23 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
|  | Защита информации при осуществлении физического доступа |
| 2.24 | Контроль перечня лиц, которым предоставлено право самостоятельного физического доступа в помещения |
| 2.25 | Назначение для всех помещений распорядителя физического доступа |
| 2.26 | Предоставление права самостоятельного физического доступа в помещения по решению распорядителя физического доступа |
| 2.27 | Оборудование входных дверей помещения механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время |
| 2.28 | Контроль состояния общедоступных объектов доступа с целью выявлений несанкционированных изменений в их аппаратном обеспечении и (или) ПО |
| 2.29 | Приведение общедоступных объектов доступа, для которых были выявлены несанкционированные изменения в их аппаратном обеспечении и (или) ПО (до устранения указанных несанкционированных изменений), в состояние, при котором невозможно их использование для осуществления операции (транзакции), приводящей к финансовым последствиям для банковского платежного агента (субагента), клиентов и контрагентов |
| 2.30 | Учет созданных, используемых и (или) эксплуатируемых ресурсов доступа |
| 2.31 | Учет используемых и (или) эксплуатируемых объектов доступа |
| 2.32 | Учет эксплуатируемых общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) |
| 2.33 | Контроль фактического состава созданных, используемых и (или) эксплуатируемых ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) и их корректного размещения в сегментах вычислительных сетей банковского платежного агента (субагента) |
|  | **Контроль целостности и защищенности информационной инфраструктуры** |
| 2.34 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между внутренними вычислительными сетями банковского платежного агента (субагента) и сетью Интернет |
| 2.35 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет |
| 2.36 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный логический доступ к ресурсам доступа, размещенным в вычислительных сетях банковского платежного агента (субагента), подключенных к сети Интернет |
| 2.37 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный удаленный доступ |
| 2.38 | Контроль размещения и своевременного обновления на серверном и сетевом оборудовании ПО средств и систем защиты информации, прикладного ПО, ПО АС, системного ПО и сигнатурных баз средств защиты информации, в том числе с целью устранения выявленных уязвимостей защиты информации |
| 2.39 | Контроль размещения и своевременного обновления на АРМ пользователей и эксплуатационного персонала ПО средств и систем защиты информации, прикладного ПО, ПО АС и системного ПО, в том числе с целью устранения выявленных уязвимостей защиты информации |
| 2.40 | Контроль работоспособности (тестирование) и правильности функционирования АС после выполнения обновлений ПО, предусмотренного мерами [2.38](#sub_3317) и 2.39 настоящей таблицы, выполняемого в сегментах разработки и тестирования |
| 2.41 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации после выполнения обновлений ПО, предусмотренного мерой 2.38 настоящей таблицы |
| 2.42 | Обеспечение возможности восстановления эталонных копий ПО АС, ПО средств и систем защиты информации, системного ПО в случаях нештатных ситуаций |
| 2.43 | Наличие, учет и контроль целостности эталонных значений параметров настроек ПО АС, системного ПО, ПО средств и систем защиты информации, возможность восстановления указанных настроек в случаях нештатных ситуаций |
| 2.44 | Контроль целостности и достоверности источников получения при распространении и (или) обновлении ПО АС, ПО средств и систем защиты информации, системного ПО |
| 2.45 | Контроль состава разрешенного для использования ПО АРМ пользователей и эксплуатационного персонала |
| 2.46 | Исключение возможности установки и (или) запуска неразрешенного для использования ПО АРМ пользователей и эксплуатационного персонала |
|  | **Защита от вредоносного кода** |
| 2.47 | Запрет неконтролируемого открытия самораспаковывающихся архивов и исполняемых файлов, полученных из сети Интернет |
| 2.48 | **Предотвращение утечек информации** |
| 2.49 | Учет и контроль использования МНИ, предназначенных для хранения информации конфиденциального характера |
| 2.50 | Документарное определение порядка использования и доступа к МНИ, предназначенным для хранения информации конфиденциального характера |
| 2.51 | Маркирование учтенных МНИ |
| 2.52 | Регистрация действий по учету и снятию с учета МНИ, предназначенных для хранения информации конфиденциального характера |
| 2.53 | Регистрация фактов стирания информации с МНИ |

# При использовании среды виртуализации Банковский платежный агент (субагент) должен обеспечить выполнение следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Защита среды виртуализации** |
| 3.1 | Идентификация и аутентификация пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам |
| 3.2 | Обеспечение возможности принудительной блокировки (выключения) установленной сессии работы пользователя с виртуальной машиной |
| 3.3 | Регистрация операций, связанных с запуском (остановкой) виртуальных машин |
| 3.4 | Регистрация операций, связанных с созданием и удалением виртуальных машин |
| 3.5 | Регистрация операций, связанных с созданием, изменением, копированием, удалением базовых образов виртуальных машин |
| 3.6 | Регистрация операций, связанных с копированием текущих образов виртуальных машин |
| 3.7 | Регистрация операций, связанных с изменением прав логического доступа к серверным компонентам виртуализации |
| 3.8 | Регистрация операций, связанных с изменением параметров настроек серверных компонентов виртуализации |
| 3.9 | Регистрация операций, связанных с аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации |
| 3.10 | Регистрация операций, связанных с аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам |
| 3.11 | Регистрация операций, связанных с изменением параметров настроек технических мер защиты информации, используемых для реализации контроля доступа к серверным компонентам виртуализации |
| 3.12 | Регистрация операций, связанных с изменением настроек технических мер защиты информации, используемых для обеспечения защиты виртуальных машин |
| 3.13 | Аутентификация мобильных (переносных) устройств удаленного доступа |
| 3.14 | Реализация защиты информации от раскрытия и модификации, применение двухсторонней взаимной аутентификации участников информационного обмена при ее передаче при осуществлении удаленного логического доступа |
| 3.15 | Идентификация, двухфакторная аутентификация и авторизация субъектов доступа после установления защищенного сетевого взаимодействия, выполнения аутентификации |
| 3.16 | Реализация и контроль информационного взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и мобильных (переносных) устройств в соответствии с установленными правилами и протоколами сетевого взаимодействия |
| 3.17 | Обеспечение защиты мобильных (переносных) устройств от воздействий вредоносного кода |
| 3.18 | Стирание информации конфиденциального характера с мобильных (переносных) устройств средствами, обеспечивающими полную перезапись данных, при осуществлении вывода мобильных (переносных) устройств из эксплуатации, а также при необходимости их передачи в сторонние организации, между работниками и (или) структурными подразделениями банковского платежного агента (субагента) |

# При использовании среды виртуализации Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Защита среды виртуализации** |
| 4.1 | Запрет на копирование текущих образов виртуальных машин, использующих СКЗИ, с загруженными криптографическими ключами |
| 4.2 | Запрет на копирование текущих образов виртуальных машин, используемых для реализации технологии виртуализации АРМ пользователей |
| 4.3 | Определение правил удаленного доступа и перечня ресурсов доступа, к которым предоставляется [удаленный доступ](#sub_3045) |

# При использовании собственной разработки программного обеспечения Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Защита информации на этапах жизненного цикла автоматизированных систем и приложений** |
| 5.1 | Документарное определение перечня защищаемой информации, планируемой к обработке в АС |
| 5.2 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) |
| 5.3 | Документарное определение в проектной и эксплуатационной документации на систему защиты информации АС:- состава и порядка применения технических и (или) организационных мер системы защиты информации АС;- параметров настроек технических мер системы защиты информации АС и компонентов информационной инфраструктуры, предназначенных для размещения указанных технических мер |
| 5.4 | Контроль предоставления и обеспечение разграничения доступа в сегментах разработки и тестирования |
| 5.5 | Реализация запрета использования защищаемой информации в сегментах разработки и тестирования |
| 5.6 | Контроль (тестирование) полноты реализации мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) |
| 5.7 | Проведение модернизации АС при изменении требований к составу и содержанию мер системы защиты информации АС (функционально-технические требований к системе защиты информации АС) |
| 5.8 | Документарное определение в проектной и эксплуатационной документации на систему защиты информации АС:- состава и порядка применения клиентами банковского платежного агента (субагента) прикладного ПО и (или) технических и (или) организационных мер защиты информации (далее при совместном упоминании - клиентские компоненты);- параметров настроек клиентских компонентов и информационной инфраструктуры клиентов банковского платежного агента (субагента), предназначенной для размещения клиентских компонентов;- описания мер по обеспечению использования клиентом определенных доверенных версий (сборок) прикладного ПО |
| 5.9 | Размещение и настройка (конфигурирование) технических мер системы защиты информации АС в информационной инфраструктуре, используемой для непосредственной реализации бизнес-процессов или технологических процессов банковского платежного агента (субагента) (далее - промышленная среда), в соответствии с положениями проектной и эксплуатационной документации |
| 5.10 | Контроль (тестирование) полноты реализации мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) в промышленной среде |
| 5.11 | Реализация контроля эксплуатации технических мер системы защиты информации АС в соответствии с положениями проектной и эксплуатационной документации, включающего:- контроль фактического размещения технических мер защиты в промышленной среде;- контроль фактических параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенной для размещения технических мер защиты информации |
| 5.12 | Реализация контроля применения мер системы защиты информации АС |
| 5.13 | Назначение и реализация контроля деятельности лиц, ответственных за эксплуатацию (сопровождение) системы защиты информации АС |
| 5.14 | Обеспечение оперативного устранения выявленных уязвимостей защиты информации АС, включая уязвимости прикладного ПО |
| 5.15 | Регистрация операций по изменению параметров настроек технических мер системы защиты информации АС |
| 5.16 | Принятие мер по обеспечению защиты информации от несанкционированного копирования и распространения |

# Банковский платежный агент (субагент) должен обеспечить выполнение следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Обнаружение инцидентов защиты информации и реагирование на них** |
| 6.1 | Реализация защиты информации об инцидентах защиты информации от НСД, обеспечение целостности и доступности указанной информации |
| 6.2 | Обеспечение возможности доступа к информации об инцидентах защиты информации в течение трех лет |
|  | **Управление инцидентами защиты информации** |
| 6.3 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых техническими мерами, входящими в состав системы защиты информации |
| 6.4 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых АС и приложениями |
| 6.5 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых контроллерами доменов |
| 6.6 | Генерация временных меток для данных регистрации о событиях защиты информации и синхронизации системного времени объектов информатизации, используемых для формирования, сбора и анализа данных регистрации |
| 6.7 | Резервирование необходимого объема памяти для хранения данных регистрации о событиях защиты информации |
| 6.8 | Реализация защиты данных регистрации о событиях защиты информации от НСД при их хранении, обеспечение целостности и доступности хранимых данных регистрации |
| 6.9 | Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет |
| 6.10 | Обеспечение возможности выявления и анализа событий защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД |
| 6.11 | Обеспечение возможности определения состава действий и (или) операций конкретного субъекта доступа |
| 6.12 | Обеспечение возможности определения состава действий и (или) операций субъектов доступа при осуществлении логического доступа к конкретному ресурсу доступа |
| 6.13 | Регистрация доступа к хранимым данным о событиях защиты информации |
|  | **Требования к организации и управлению защитой информации** |
| 6.14 | Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса |

# Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |
| --- | --- |
| Номер меры | Содержание мер системы защиты информации |
|
|  | **Обнаружение инцидентов защиты информации и реагирование на них** |
| 7.1 | Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации |
| 7.2 | Регистрация информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, полученной от работников, клиентов и (или) контрагентов банковского платежного агента (субагента) |
| 7.3 | Классификация инцидентов защиты информации с учетом степени их влияния (критичности) на предоставление финансовых услуг, реализацию бизнес-процессов и (или) технологических процессов банковского платежного агента (субагента) |
| 7.4 | Установление и применение единых правил получения от работников, клиентов и (или) контрагентов банковского платежного агента (субагента) информации, потенциально связанной с инцидентами защиты информации |
| 7.5 | Установление и применение единых правил регистрации и классификации инцидентов защиты информации в части состава и содержания атрибутов, описывающих инцидент защиты информации, и их возможных значений |
| 7.6 | Установление и применение единых правил реагирования на инциденты защиты информации |
| 7.7 | Определение и назначение ролей, связанных с реагированием на инциденты защиты информации |
| 7.8 | Проведение реагирования на каждый обнаруженный инцидент защиты информации, включающего:- анализ инцидента;- определение источников и причин возникновения инцидента;- оценку последствий инцидента на предоставление финансовых услуг, реализацию бизнес-процессов или технологических процессов банковского платежного агента (субагента);- принятие мер по устранению последствий инцидента;- планирование и принятие мер по предотвращению повторного возникновения инцидента |
| 7.9 | Установление и применение единых правил сбора, фиксации и распространения информации об инцидентах защиты информации |
| 7.10 | Установление и применение единых правил закрытия инцидентов защиты информации |
|  | **Управление инцидентами защиты информации** |
| 7.11 | Контроль формирования данных регистрации о событиях защиты информации объектов информатизации |
|  | **Требования к организации и управлению защитой информации** |
| 7.12 | Документарное определение области применения процесса системы защиты информации для уровней информационной инфраструктуры |
| 7.13 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания организационных мер защиты информации, выбранных банковским платежным агентом и реализуемых в рамках процесса системы защиты информации |
| 7.14 | Документарное определение порядка применения организационных мер защиты информации, реализуемых в рамках процесса системы защиты информации |
| 7.15 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания технических мер защиты информации, выбранных финансовой организацией и реализуемых в рамках процесса системы защиты информации |
| 7.16 | Документарное определение порядка применения технических мер защиты информации, реализуемых в рамках процесса системы защиты информации, включающего:- правила размещения технических мер защиты информации в информационной инфраструктуре;- параметры настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации[\*\*](#sub_3340);- руководства по применению технических мер защиты информации (включающие руководства по эксплуатации, контролю эксплуатации и использованию по назначению технических мер защиты информации);- состав ролей и права субъектов доступа, необходимых для обеспечения применения технических мер защиты информации (включающего эксплуатацию, контроль эксплуатации и использование по назначению мер защиты информации) |
| 7.17 | Реализация учета объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, для уровней информационной инфраструктуры, в том числе объектов доступа, расположенных в публичных (общедоступных) местах (в том числе банкоматах, платежных терминалах) |
| 7.18 | Размещение и настройка (конфигурирование) технических мер защиты информации в информационной инфраструктуре банковского платежного агента (субагента) |
| 7.19 | Контроль (тестирование) полноты реализации технических мер защиты информации |
| 7.20 | Назначение работникам банковского платежного агента (субагента) ролей, связанных с применением мер защиты информации, и установление обязанности и ответственности за их выполнение |
| 7.21 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной инфраструктуры |
| 7.22 | Реализация эксплуатации, использования по назначению технических мер защиты информации |
| 7.23 | Реализация применения организационных мер защиты информации |
| 7.24 | Обучение, практическая подготовка (переподготовка) работников банковского платежного агента (субагента), ответственных за применение мер защиты информации в рамках процесса защиты информации |
| 7.25 | Повышение осведомленности (инструктаж) работников банковского платежного агента (субагента) в области реализации процесса защиты информации, применения организационных мер защиты информации, использования по назначению технических мер защиты информации |
| 7.26 | Контроль фактического состава объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, на соответствие учетным данным |
| 7.27 | Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий:- контроль фактического размещения технических мер защиты информации в информационной инфраструктуре банковского платежного агента (субагента);- контроль фактических параметров настроек технических мер защиты информации и компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации |
| 7.28 | Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий:- контроль назначения ролей, связанных с эксплуатацией и использованием по назначению технических мер защиты информации;- контроль выполнения руководств по эксплуатации и использованию по назначению технических мер защиты информации |
| 7.29 | Периодический контроль (тестирование) полноты реализации технических мер защиты информации |
| 7.30 | Контроль применения организационных мер защиты информации |
| 7.31 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование |
| 7.32 | Проведение проверок знаний работников банковского платежного агента (субагента) в части применения мер защиты информации в рамках процесса системы защиты информации |
| 7.33 | Фиксация результатов (свидетельств) проведения мероприятий по контролю реализации процесса системы защиты информации |
| 7.34 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях:- обнаружения инцидентов защиты информации;- обнаружения недостатков в рамках контроля системы защиты информации |
| 7.35 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях изменения политики банковского платежного агента (субагента) в отношении:- области применения процесса системы защиты информации;- основных принципов и приоритетов в реализации процесса системы защиты информации;- целевых показателей величины допустимого остаточного операционного риска (риск-аппетита), связанного с обеспечением безопасности информации |
| 7.36 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях:- изменений требований к защите информации, определенных правилами платежной системы;- изменений, внесенных в законодательство Российской Федерации, в том числе нормативные акты Банка России |
| 7.37 | Фиксация решений о проведении совершенствования процесса системы защиты информации в виде корректирующих или превентивных действий, например:- пересмотр области применения процесса системы защиты информации;- пересмотр состава и содержания организационных мер защиты информации, применяемых в рамках процесса системы защиты информации;- пересмотр состава технических мер защиты информации, применяемых в рамках процесса системы защиты информации |

|  |  |
| --- | --- |
| **Банк**Бизнес-лидер Стрима Система денежных переводов\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Пальчун К.В./мп | **Банковский платёжный агент**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_ /Мп |

**Приложение №9**

**к Договору о привлечении банковского платежного агента**

**№\_\_\_\_\_\_\_\_\_\_\_\_\_\_от «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_\_ г.**

**Анкета по Информационной безопасности**

|  |  |
| --- | --- |
| Наименование организации: |  |
| Сотрудник, заполнивший анкету:- Фамилия Имя Отчество:- должность:  |  |
| Дата заполнения:  |  |

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Вопрос**  | **Статус выполнения требования (да/нет)** |
|  | **Обеспечение защиты информации при управлении доступом** |  |
| 1.2 | Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями |  |
| 1.3 | Исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа |  |
| 1.4 | Исключение возможного бесконтрольного изменения пользователями параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации*ОБРАЗЕЦ* |  |
| 1.5 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала и пользователей, обладающих правами логического доступа, в том числе в АС, позволяющими осуществить операции (транзакции), приводящие к финансовым последствиям для банковского платежного агента (субагента) (субагента), клиентов и контрагентов. |  |
| 1.6 | Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по управлению криптографическими ключами |  |
| 1.7 | [Идентификация](#sub_3016) и [однофакторная аутентификация](#sub_3028) пользователей |  |
| 1.8 | Идентификация и однофакторная аутентификация эксплуатационного персонала |  |
| 1.9 | Аутентификация программных сервисов, осуществляющих логический доступ с использованием [технических учетных записей](#sub_3020) |  |
| 1.10 | Сокрытие (неотображение) паролей при их вводе субъектами доступа |  |
| 1.11 | Временная блокировка учетной записи пользователей после выполнения ряда неуспешных последовательных попыток аутентификации на период времени не менее 30 мин. |  |
| 1.12 | Обеспечение возможности выполнения субъектом логического доступа - работниками банковского платежного агента (субагента) процедуры принудительного прерывания сессии логического доступа и (или) приостановки осуществления логического доступа (с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа) |  |
| 1.13 | Автоматическое прерывание сессии логического доступа (приостановка осуществления логического доступа) по истечении установленного времени бездействия (неактивности) субъекта логического доступа, не превышающего 15 мин., с прекращением отображения на мониторе АРМ информации, доступ к которой получен в рамках сессии осуществления логического доступа |  |
| 1.14 | Выполнение процедуры повторной аутентификации для продолжения осуществления логического доступа после его принудительного или автоматического прерывания (приостановки осуществления логического доступа), предусмотренного мерами 1.12 и 1.13 настоящей таблицы |  |
| 1.15 | Использование на АРМ субъектов логического доступа встроенных механизмов контроля изменения базовой конфигурации оборудования (пароль на изменение параметров конфигурации системы, хранящихся в энергонезависимой памяти) |  |
| 1.16 | Запрет на использование технологии аутентификации с сохранением аутентификационных данных в открытом виде в СВТ |  |
| 1.17 | Запрет на передачу аутентификационных данных в открытом виде по каналам и линиям связи и их передачу куда-либо, кроме средств или систем аутентификации |  |
| 1.18 | Смена паролей пользователей не реже одного раза в год |  |
| 1.19 | Смена паролей эксплуатационного персонала не реже одного раза в квартал |  |
| 1.20 | Использование пользователями паролей длиной не менее восьми символов |  |
| 1.21 | Использование эксплуатационным персоналом паролей длиной не менее шестнадцати символов |  |
| 1.22 | Использование при формировании паролей субъектов логического доступа символов, включающих буквы (в верхнем и нижнем регистрах) и цифры |  |
| 1.23 | Обеспечение возможности самостоятельной смены субъектами логического доступа своих паролей |  |
| 1.24 | Авторизация логического доступа к ресурсам доступа, в том числе АС |  |
| 1.25 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа |  |
| 1.26 | Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа, в том числе АС |  |
| 1.27 | Запрет выполнения пользователями бизнес-процессов с использованием привилегированных прав логического доступа, в том числе работы пользователей с правами локального администратора АРМ |  |
| 1.28 | Регистрация осуществления субъектами логического доступа идентификации и аутентификации |  |
| 1.29 | Регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа, в том числе в АС |  |
|  | **Обеспечение защиты вычислительных сетей** |  |
| 1.30 | Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в [ГОСТ Р ИСО/МЭК 7498-1](http://mobileonline.garant.ru/document?id=70146072&sub=0), внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет |  |
| 1.31 | Межсетевое экранирование внутренних вычислительных сетей банковского платежного агента (субагента), включая фильтрацию данных на сетевом и прикладном уровнях семиуровневой стандартной модели взаимодействия открытых систем, определенной в [ГОСТ Р ИСО/МЭК 7498-1](http://mobileonline.garant.ru/document?id=70146072&sub=0) |  |
| 1.32 | Реализация и контроль информационного взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет в соответствии с установленными правилами и протоколами сетевого взаимодействия |  |
| 1.33 | Сокрытие топологии внутренних вычислительных сетей банковского платежного агента (субагента) |  |
| 1.34 | Реализация сетевого взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и сети Интернет через ограниченное количество контролируемых точек доступа |  |
| 1.35 | Регистрация изменений параметров настроек средств и систем защиты информации, обеспечивающих реализацию сегментации, межсетевого экранирования и защиты вычислительных сетей банковского платежного агента (субагента) |  |
| 1.36 | Контроль и обеспечение возможности блокировки нежелательных сообщений электронной почты (SPAM) |  |
| 1.37 | Применение сетевых протоколов, обеспечивающих защиту подлинности сетевого соединения, контроль целостности сетевого взаимодействия и реализацию технологии [двухсторонней аутентификации](#sub_3030) при осуществлении логического доступа с использованием телекоммуникационных каналов и (или) линий связи, не контролируемых банковским платежным агентом |  |
| 1.38 | Реализация защиты информации от раскрытия и модификации, применение двухсторонней аутентификации при ее передаче с использованием сети Интернет, телекоммуникационных каналов и (или) линий связи, не контролируемых банковским платежным агентом*ОБРАЗЕЦ* |  |
|  | Защита беспроводных сетей |  |
| 1.39 | Аутентификация устройств доступа техническими средствами, реализующими функции беспроводного сетевого соединения (точками доступа по протоколу Wi-Fi) |  |
| 1.40 | Защита информации от раскрытия и модификации при ее передаче с использованием протоколов беспроводного доступа |  |
|  | **Защита от вредоносного кода** |  |
| 1.41 | Реализация защиты от вредоносного кода на уровне физических АРМ пользователей и эксплуатационного персонала |  |
| 1.42 | Реализация защиты от вредоносного кода на уровне виртуальной информационной инфраструктуры |  |
| 1.43 | Реализация защиты от вредоносного кода на уровне серверного оборудования |  |
| 1.44 | Реализация защиты от вредоносного кода на уровне контроля почтового трафика |  |
| 1.45 | Реализация защиты от вредоносного кода на уровне входного контроля устройств и переносных (отчуждаемых) носителей информации |  |
| 1.46 | Реализация защиты от вредоносного кода на уровне контроля общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) |  |
| 1.47 | Функционирование средств защиты от вредоносного кода в постоянном, автоматическом режиме, в том числе в части установки их обновлений и сигнатурных баз данных |  |
| 1.48 | Функционирование средств защиты от вредоносного кода на АРМ пользователей и эксплуатационного персонала в резидентном режиме (в режиме service - для операционной системы Windows, в режиме daemon - для операционной системы Unix), их автоматический запуск при загрузке операционной системы |  |
| 1.49 | Применение средств защиты от вредоносного кода, реализующих функцию контроля целостности их программных компонентов |  |
| 1.50 | Контроль отключения и своевременного обновления средств защиты от вредоносного кода |  |
| 1.51 | Выполнение еженедельных операций по проведению проверок на отсутствие вредоносного кода |  |
| 1.52 | Использование средств защиты от вредоносного кода различных производителей, как минимум для уровней:- физические АРМ пользователей и эксплуатационного персонала;- серверное оборудование |  |
| 1.53 | Входной контроль всех устройств и переносных (отчуждаемых) носителей информации (включая мобильные компьютеры и флеш-накопители) перед их использованием в вычислительных сетях банковского платежного агента (субагента) |  |
| 1.54 | Регистрация операций по проведению проверок на отсутствие вредоносного кода |  |
| 1.55 | Регистрация фактов выявления вредоносного кода |  |
| 1.56 | Регистрация сбоев в функционировании средств защиты от вредоносного кода |  |
| 1.57 | Регистрация сбоев в выполнении контроля (проверок) на отсутствие вредоносного кода*ОБРАЗЕЦ* |  |
| 1.58 | Регистрация отключения средств защиты от вредоносного кода |  |
| 1.59 | Регистрация нарушений целостности программных компонентов средств защиты от вредоносного кода |  |
|  | **Предотвращение утечек информации** |  |
| 1.60 | Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при осуществлении вывода МНИ из эксплуатации или вывода из эксплуатации СВТ, в состав которых входят указанные МНИ, а также при необходимости их передачи в сторонние организации |  |
| 1.61 | Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при передаче (перезакреплении) МНИ между работниками и (или) структурными подразделениями банковского платежного агента (субагента) |  |

# 2.Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Обеспечение защиты информации при управлении доступом** |  |
| 2.1 | Контроль соответствия фактического состава разблокированных учетных записей фактическому составу [легальных субъектов](#sub_3024) логического доступа |  |
| 2.2 | Контроль отсутствия незаблокированных учетных записей:- уволенных работников;- работников, отсутствующих на рабочем месте более 90 календарных дней;- работников внешних (подрядных) организаций, прекративших свою деятельность в организации |  |
| 2.3 | Контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения |  |
| 2.4 | Назначение для всех ресурсов доступа распорядителя логического доступа (владельца ресурса доступа) |  |
| 2.5 | Предоставление прав логического доступа по решению распорядителя логического доступа (владельца ресурса доступа) |  |
| 2.6 | Хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности указанной информации |  |
| 2.7 | Контроль соответствия фактических прав логического доступа эталонной информации о предоставленных правах логического доступа |  |
| 2.8 | Контроль необходимости отзыва прав субъектов логического доступа при изменении их должностных обязанностей |  |
| 2.9 | Контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа |  |
| 2.10 | Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 90 дней |  |
| 2.11 | Реализация контроля со стороны распорядителя логического доступа целесообразности дальнейшего предоставления прав логического доступа, не использованных субъектами на протяжении периода времени, указанного мерой 2.10 настоящей таблицы |  |
| 2.12 | Реализация возможности определения состава предоставленных прав логического доступа для конкретного ресурса доступа |  |
| 2.13 | Реализация возможности определения состава предоставленных прав логического доступа для конкретного субъекта логического доступа |  |
| 2.14 | Определение состава ролей, связанных с выполнением операции (транзакции) в АС, имеющих финансовые последствия для банковского платежного агента (субагента), клиентов и контрагентов, и ролей, связанных с контролем выполнения указанных операций (транзакций), запрет выполнения указанных ролей одним субъектом логического доступа |  |
| 2.15 | Реализация правил управления правами логического доступа, обеспечивающих запрет совмещения одним субъектом логического доступа ролей, предусмотренных мерой 2.14 настоящей таблицы*ОБРАЗЕЦ* |  |
| 2.16 | Запрет использования учетных записей субъектов логического доступа с незаданными аутентификационными данными или заданными по умолчанию разработчиком ресурса доступа, в том числе разработчиком АС |  |
| 2.17 | Запрет на использование групповых, общих и стандартных учетных записей и паролей, а также прочих подобных методов идентификации и аутентификации, не позволяющих определить конкретного субъекта доступа |  |
| 2.18 | Хранение копий аутентификационных данных эксплуатационного персонала на выделенных МНИ или на бумажных носителях |  |
| 2.19 | Реализация защиты копий аутентификационных данных эксплуатационного персонала от НСД при их хранении на МНИ или бумажных носителях |  |
| 2.20 | Регистрация персонификации, выдачи (передачи) и уничтожения персональных технических устройств аутентификации, реализующих многофакторную аутентификацию |  |
| 2.21 | Смена аутентификационных данных в случае их [компрометации](#sub_3026) |  |
| 2.22 | Запрет реализации пользователями бизнес-процессов и технологических процессов банковского платежного агента (субагента) с использованием учетных записей эксплуатационного персонала, в том числе в АС |  |
| 2.23 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |  |
|  | Защита информации при осуществлении физического доступа |  |
| 2.24 | Контроль перечня лиц, которым предоставлено право самостоятельного физического доступа в помещения |  |
| 2.25 | Назначение для всех помещений распорядителя физического доступа |  |
| 2.26 | Предоставление права самостоятельного физического доступа в помещения по решению распорядителя физического доступа |  |
| 2.27 | Оборудование входных дверей помещения механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время |  |
| 2.28 | Контроль состояния общедоступных объектов доступа с целью выявлений несанкционированных изменений в их аппаратном обеспечении и (или) ПО |  |
| 2.29 | Приведение общедоступных объектов доступа, для которых были выявлены несанкционированные изменения в их аппаратном обеспечении и (или) ПО (до устранения указанных несанкционированных изменений), в состояние, при котором невозможно их использование для осуществления операции (транзакции), приводящей к финансовым последствиям для банковского платежного агента (субагента), клиентов и контрагентов |  |
| 2.30 | Учет созданных, используемых и (или) эксплуатируемых ресурсов доступа |  |
| 2.31 | Учет используемых и (или) эксплуатируемых объектов доступа |  |
| 2.32 | Учет эксплуатируемых общедоступных объектов доступа (в том числе банкоматов, платежных терминалов) |  |
| 2.33 | Контроль фактического состава созданных, используемых и (или) эксплуатируемых ресурсов доступа (баз данных, сетевых файловых ресурсов, виртуальных машин) и их корректного размещения в сегментах вычислительных сетей банковского платежного агента (субагента) |  |
|  | **Контроль целостности и защищенности информационной инфраструктуры** |  |
| 2.34 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между внутренними вычислительными сетями банковского платежного агента (субагента) и сетью Интернет |  |
| 2.35 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированное (неконтролируемое) информационное взаимодействие между сегментами, предназначенными для размещения общедоступных объектов доступа (в том числе банкоматов, платежных терминалов), и сетью Интернет |  |
| 2.36 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный логический доступ к ресурсам доступа, размещенным в вычислительных сетях банковского платежного агента (субагента), подключенных к сети Интернет*ОБРАЗЕЦ* |  |
| 2.37 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации, использование которых может позволить осуществить несанкционированный удаленный доступ |  |
| 2.38 | Контроль размещения и своевременного обновления на серверном и сетевом оборудовании ПО средств и систем защиты информации, прикладного ПО, ПО АС, системного ПО и сигнатурных баз средств защиты информации, в том числе с целью устранения выявленных уязвимостей защиты информации |  |
| 2.39 | Контроль размещения и своевременного обновления на АРМ пользователей и эксплуатационного персонала ПО средств и систем защиты информации, прикладного ПО, ПО АС и системного ПО, в том числе с целью устранения выявленных уязвимостей защиты информации |  |
| 2.40 | Контроль работоспособности (тестирование) и правильности функционирования АС после выполнения обновлений ПО, предусмотренного мерами [2.38](#sub_3317) и 2.39 настоящей таблицы, выполняемого в сегментах разработки и тестирования |  |
| 2.41 | Контроль отсутствия и обеспечение оперативного устранения известных (описанных) уязвимостей защиты информации после выполнения обновлений ПО, предусмотренного мерой 2.38 настоящей таблицы |  |
| 2.42 | Обеспечение возможности восстановления эталонных копий ПО АС, ПО средств и систем защиты информации, системного ПО в случаях нештатных ситуаций |  |
| 2.43 | Наличие, учет и контроль целостности эталонных значений параметров настроек ПО АС, системного ПО, ПО средств и систем защиты информации, возможность восстановления указанных настроек в случаях нештатных ситуаций |  |
| 2.44 | Контроль целостности и достоверности источников получения при распространении и (или) обновлении ПО АС, ПО средств и систем защиты информации, системного ПО |  |
| 2.45 | Контроль состава разрешенного для использования ПО АРМ пользователей и эксплуатационного персонала |  |
| 2.46 | Исключение возможности установки и (или) запуска неразрешенного для использования ПО АРМ пользователей и эксплуатационного персонала |  |
|  | **Защита от вредоносного кода** |  |
| 2.47 | Запрет неконтролируемого открытия самораспаковывающихся архивов и исполняемых файлов, полученных из сети Интернет |  |
| 2.48 | **Предотвращение утечек информации** |  |
| 2.49 | Учет и контроль использования МНИ, предназначенных для хранения информации конфиденциального характера |  |
| 2.50 | Документарное определение порядка использования и доступа к МНИ, предназначенным для хранения информации конфиденциального характера |  |
| 2.51 | Маркирование учтенных МНИ |  |
| 2.52 | Регистрация действий по учету и снятию с учета МНИ, предназначенных для хранения информации конфиденциального характера |  |
| 2.53 | Регистрация фактов стирания информации с МНИ |  |

# При использовании среды виртуализации Банковский платежный агент (субагент) должен обеспечить выполнение следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Защита среды виртуализации** |  |
| 3.1 | Идентификация и аутентификация пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам |  |
| 3.2 | Обеспечение возможности принудительной блокировки (выключения) установленной сессии работы пользователя с виртуальной машиной |  |
| 3.3 | Регистрация операций, связанных с запуском (остановкой) виртуальных машин |  |
| 3.4 | Регистрация операций, связанных с созданием и удалением виртуальных машин |  |
| 3.5 | Регистрация операций, связанных с созданием, изменением, копированием, удалением базовых образов виртуальных машин |  |
| 3.6 | Регистрация операций, связанных с копированием текущих образов виртуальных машин |  |
| 3.7 | Регистрация операций, связанных с изменением прав логического доступа к серверным компонентам виртуализации |  |
| 3.8 | Регистрация операций, связанных с изменением параметров настроек серверных компонентов виртуализации*ОБРАЗЕЦ* |  |
| 3.9 | Регистрация операций, связанных с аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации |  |
| 3.10 | Регистрация операций, связанных с аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам |  |
| 3.11 | Регистрация операций, связанных с изменением параметров настроек технических мер защиты информации, используемых для реализации контроля доступа к серверным компонентам виртуализации |  |
| 3.12 | Регистрация операций, связанных с изменением настроек технических мер защиты информации, используемых для обеспечения защиты виртуальных машин |  |
| 3.13 | Аутентификация мобильных (переносных) устройств удаленного доступа |  |
| 3.14 | Реализация защиты информации от раскрытия и модификации, применение двухсторонней взаимной аутентификации участников информационного обмена при ее передаче при осуществлении удаленного логического доступа |  |
| 3.15 | Идентификация, двухфакторная аутентификация и авторизация субъектов доступа после установления защищенного сетевого взаимодействия, выполнения аутентификации |  |
| 3.16 | Реализация и контроль информационного взаимодействия внутренних вычислительных сетей банковского платежного агента (субагента) и мобильных (переносных) устройств в соответствии с установленными правилами и протоколами сетевого взаимодействия |  |
| 3.17 | Обеспечение защиты мобильных (переносных) устройств от воздействий вредоносного кода |  |
| 3.18 | Стирание информации конфиденциального характера с мобильных (переносных) устройств средствами, обеспечивающими полную перезапись данных, при осуществлении вывода мобильных (переносных) устройств из эксплуатации, а также при необходимости их передачи в сторонние организации, между работниками и (или) структурными подразделениями банковского платежного агента (субагента) |  |

# 4.При использовании среды виртуализации Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Защита среды виртуализации** |  |
| 4.1 | Запрет на копирование текущих образов виртуальных машин, использующих СКЗИ, с загруженными криптографическими ключами |  |
| 4.2 | Запрет на копирование текущих образов виртуальных машин, используемых для реализации технологии виртуализации АРМ пользователей |  |
| 4.3 | Определение правил удаленного доступа и перечня ресурсов доступа, к которым предоставляется [удаленный доступ](#sub_3045)*ОБРАЗЕЦ* |  |

# При использовании собственной разработки программного обеспечения Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Защита информации на этапах жизненного цикла автоматизированных систем и приложений** |  |
| 5.1 | Документарное определение перечня защищаемой информации, планируемой к обработке в АС |  |
| 5.2 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) |  |
| 5.3 | Документарное определение в проектной и эксплуатационной документации на систему защиты информации АС:- состава и порядка применения технических и (или) организационных мер системы защиты информации АС;- параметров настроек технических мер системы защиты информации АС и компонентов информационной инфраструктуры, предназначенных для размещения указанных технических мер |  |
| 5.4 | Контроль предоставления и обеспечение разграничения доступа в сегментах разработки и тестирования |  |
| 5.5 | Реализация запрета использования защищаемой информации в сегментах разработки и тестирования |  |
| 5.6 | Контроль (тестирование) полноты реализации мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) |  |
| 5.7 | Проведение модернизации АС при изменении требований к составу и содержанию мер системы защиты информации АС (функционально-технические требований к системе защиты информации АС) |  |
| 5.8 | Документарное определение в проектной и эксплуатационной документации на систему защиты информации АС:- состава и порядка применения клиентами банковского платежного агента (субагента) прикладного ПО и (или) технических и (или) организационных мер защиты информации (далее при совместном упоминании - клиентские компоненты);- параметров настроек клиентских компонентов и информационной инфраструктуры клиентов банковского платежного агента (субагента), предназначенной для размещения клиентских компонентов;- описания мер по обеспечению использования клиентом определенных доверенных версий (сборок) прикладного ПО |  |
| 5.9 | Размещение и настройка (конфигурирование) технических мер системы защиты информации АС в информационной инфраструктуре, используемой для непосредственной реализации бизнес-процессов или технологических процессов банковского платежного агента (субагента) (далее - промышленная среда), в соответствии с положениями проектной и эксплуатационной документации |  |
| 5.10 | Контроль (тестирование) полноты реализации мер системы защиты информации АС (функционально-технических требований к системе защиты информации АС) в промышленной среде |  |
| 5.11 | Реализация контроля эксплуатации технических мер системы защиты информации АС в соответствии с положениями проектной и эксплуатационной документации, включающего:*ОБРАЗЕЦ*- контроль фактического размещения технических мер защиты в промышленной среде;- контроль фактических параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенной для размещения технических мер защиты информации |  |
| 5.12 | Реализация контроля применения мер системы защиты информации АС |  |
| 5.13 | Назначение и реализация контроля деятельности лиц, ответственных за эксплуатацию (сопровождение) системы защиты информации АС |  |
| 5.14 | Обеспечение оперативного устранения выявленных уязвимостей защиты информации АС, включая уязвимости прикладного ПО |  |
| 5.15 | Регистрация операций по изменению параметров настроек технических мер системы защиты информации АС |  |
| 5.16 | Принятие мер по обеспечению защиты информации от несанкционированного копирования и распространения |  |

# Банковский платежный агент (субагент) должен обеспечить выполнение следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Обнаружение инцидентов защиты информации и реагирование на них** |  |
| 6.1 | Реализация защиты информации об инцидентах защиты информации от НСД, обеспечение целостности и доступности указанной информации |  |
| 6.2 | Обеспечение возможности доступа к информации об инцидентах защиты информации в течение трех лет |  |
|  | **Управление инцидентами защиты информации** |  |
| 6.3 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых техническими мерами, входящими в состав системы защиты информации |  |
| 6.4 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых АС и приложениями |  |
| 6.5 | Организация мониторинга данных регистрации о событиях защиты информации, формируемых контроллерами доменов |  |
| 6.6 | Генерация временных меток для данных регистрации о событиях защиты информации и синхронизации системного времени объектов информатизации, используемых для формирования, сбора и анализа данных регистрации |  |
| 6.7 | Резервирование необходимого объема памяти для хранения данных регистрации о событиях защиты информации |  |
| 6.8 | Реализация защиты данных регистрации о событиях защиты информации от НСД при их хранении, обеспечение целостности и доступности хранимых данных регистрации |  |
| 6.9 | Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет |  |
| 6.10 | Обеспечение возможности выявления и анализа событий защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД |  |
| 6.11 | Обеспечение возможности определения состава действий и (или) операций конкретного субъекта доступа |  |
| 6.12 | Обеспечение возможности определения состава действий и (или) операций субъектов доступа при осуществлении логического доступа к конкретному ресурсу доступа |  |
| 6.13 | Регистрация доступа к хранимым данным о событиях защиты информации |  |
|  | **Требования к организации и управлению защитой информации** |  |
| 6.14 | Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса*ОБРАЗЕЦ* |  |

# Банковский платежный агент (субагент) должен разработать и внедрить внутренние нормативные документы (приказы, регламенты и пр.) для выполнения следующих мер по защите информации

|  |  |  |
| --- | --- | --- |
|  | **Обнаружение инцидентов защиты информации и реагирование на них** |  |
| 7.1 | Регистрация информации о событиях защиты информации, потенциально связанных с инцидентами защиты информации, в том числе НСД, выявленными в рамках мониторинга и анализа событий защиты информации |  |
| 7.2 | Регистрация информации, потенциально связанной с инцидентами защиты информации, в том числе НСД, полученной от работников, клиентов и (или) контрагентов банковского платежного агента (субагента) |  |
| 7.3 | Классификация инцидентов защиты информации с учетом степени их влияния (критичности) на предоставление финансовых услуг, реализацию бизнес-процессов и (или) технологических процессов банковского платежного агента (субагента) |  |
| 7.4 | Установление и применение единых правил получения от работников, клиентов и (или) контрагентов банковского платежного агента (субагента) информации, потенциально связанной с инцидентами защиты информации |  |
| 7.5 | Установление и применение единых правил регистрации и классификации инцидентов защиты информации в части состава и содержания атрибутов, описывающих инцидент защиты информации, и их возможных значений |  |
| 7.6 | Установление и применение единых правил реагирования на инциденты защиты информации |  |
| 7.7 | Определение и назначение ролей, связанных с реагированием на инциденты защиты информации |  |
| 7.8 | Проведение реагирования на каждый обнаруженный инцидент защиты информации, включающего:- анализ инцидента;- определение источников и причин возникновения инцидента;- оценку последствий инцидента на предоставление финансовых услуг, реализацию бизнес-процессов или технологических процессов банковского платежного агента (субагента);- принятие мер по устранению последствий инцидента;- планирование и принятие мер по предотвращению повторного возникновения инцидента |  |
| 7.9 | Установление и применение единых правил сбора, фиксации и распространения информации об инцидентах защиты информации |  |
| 7.10 | Установление и применение единых правил закрытия инцидентов защиты информации |  |
|  | **Управление инцидентами защиты информации** |  |
| 7.11 | Контроль формирования данных регистрации о событиях защиты информации объектов информатизации |  |
|  | **Требования к организации и управлению защитой информации** |  |
| 7.12 | Документарное определение области применения процесса системы защиты информации для уровней информационной инфраструктуры |  |
| 7.13 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания организационных мер защиты информации, выбранных банковским платежным агентом и реализуемых в рамках процесса системы защиты информации |  |
| 7.14 | Документарное определение порядка применения организационных мер защиты информации, реализуемых в рамках процесса системы защиты информации |  |
| 7.15 | Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания технических мер защиты информации, выбранных финансовой организацией и реализуемых в рамках процесса системы защиты информации |  |
| 7.16 | Документарное определение порядка применения технических мер защиты информации, реализуемых в рамках процесса системы защиты информации, включающего:- правила размещения технических мер защиты информации в информационной инфраструктуре;*ОБРАЗЕЦ*- параметры настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации[\*\*](#sub_3340);- руководства по применению технических мер защиты информации (включающие руководства по эксплуатации, контролю эксплуатации и использованию по назначению технических мер защиты информации);- состав ролей и права субъектов доступа, необходимых для обеспечения применения технических мер защиты информации (включающего эксплуатацию, контроль эксплуатации и использование по назначению мер защиты информации) |  |
| 7.17 | Реализация учета объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, для уровней информационной инфраструктуры, в том числе объектов доступа, расположенных в публичных (общедоступных) местах (в том числе банкоматах, платежных терминалах) |  |
| 7.18 | Размещение и настройка (конфигурирование) технических мер защиты информации в информационной инфраструктуре банковского платежного агента (субагента) |  |
| 7.19 | Контроль (тестирование) полноты реализации технических мер защиты информации |  |
| 7.20 | Назначение работникам банковского платежного агента (субагента) ролей, связанных с применением мер защиты информации, и установление обязанности и ответственности за их выполнение |  |
| 7.21 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной инфраструктуры |  |
| 7.22 | Реализация эксплуатации, использования по назначению технических мер защиты информации |  |
| 7.23 | Реализация применения организационных мер защиты информации |  |
| 7.24 | Обучение, практическая подготовка (переподготовка) работников банковского платежного агента (субагента), ответственных за применение мер защиты информации в рамках процесса защиты информации |  |
| 7.25 | Повышение осведомленности (инструктаж) работников банковского платежного агента (субагента) в области реализации процесса защиты информации, применения организационных мер защиты информации, использования по назначению технических мер защиты информации |  |
| 7.26 | Контроль фактического состава объектов и ресурсов доступа, входящих в область применения процесса системы защиты информации, на соответствие учетным данным |  |
| 7.27 | Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий:- контроль фактического размещения технических мер защиты информации в информационной инфраструктуре банковского платежного агента (субагента);- контроль фактических параметров настроек технических мер защиты информации и компонентов информационной инфраструктуры, предназначенных для размещения технических мер защиты информации |  |
| 7.28 | Контроль эксплуатации и использования по назначению технических мер защиты информации, включающий:- контроль назначения ролей, связанных с эксплуатацией и использованием по назначению технических мер защиты информации;- контроль выполнения руководств по эксплуатации и использованию по назначению технических мер защиты информации |  |
| 7.29 | Периодический контроль (тестирование) полноты реализации технических мер защиты информации |  |
| 7.30 | Контроль применения организационных мер защиты информации |  |
| 7.31 | Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование*ОБРАЗЕЦ* |  |
| 7.32 | Проведение проверок знаний работников банковского платежного агента (субагента) в части применения мер защиты информации в рамках процесса системы защиты информации |  |
| 7.33 | Фиксация результатов (свидетельств) проведения мероприятий по контролю реализации процесса системы защиты информации |  |
| 7.34 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях:- обнаружения инцидентов защиты информации;- обнаружения недостатков в рамках контроля системы защиты информации |  |
| 7.35 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях изменения политики банковского платежного агента (субагента) в отношении:- области применения процесса системы защиты информации;- основных принципов и приоритетов в реализации процесса системы защиты информации;- целевых показателей величины допустимого остаточного операционного риска (риск-аппетита), связанного с обеспечением безопасности информации |  |
| 7.36 | Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы защиты информации в случаях:- изменений требований к защите информации, определенных правилами платежной системы;- изменений, внесенных в законодательство Российской Федерации, в том числе нормативные акты Банка России |  |
| 7.37 | Фиксация решений о проведении совершенствования процесса системы защиты информации в виде корректирующих или превентивных действий, например:- пересмотр области применения процесса системы защиты информации;- пересмотр состава и содержания организационных мер защиты информации, применяемых в рамках процесса системы защиты информации;- пересмотр состава технических мер защиты информации, применяемых в рамках процесса системы защиты информации*ОБРАЗЕЦ* |  |

1. Указывается либо наименование оператора по переводу денежных средств, либо наименование поставщика (если БПА по данному договору является оператором по приему платежей), либо наименование поставщика и оператора по переводу денежных средств (если БПА по данному договору является платежным субагентом) [↑](#footnote-ref-2)
2. банковский платежный агент / оператор по приему платежей/ платежный субагент [↑](#footnote-ref-3)
3. Требования настоящего Приложения распространяются на БПА только в части деятельности БПА, предусмотренной п.1.1. Договора. [↑](#footnote-ref-4)
4. Положение Банка России от 04.06.2020 N 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». [↑](#footnote-ref-5)
5. Указывается либо наименование оператора по переводу денежных средств, либо наименование поставщика (если Банковский платежный субагент по данному договору является оператором по приему платежей), либо наименование поставщика и оператора по переводу денежных средств (если Банковский платежный субагент по данному договору является платежным агентом) [↑](#footnote-ref-6)
6. банковский платежный агент / оператор по приему платежей/ банковский платежный субагент / платежный агент [↑](#footnote-ref-7)
7. Требования настоящего Приложения распространяются на БПА только в части деятельности БПА, предусмотренной п.1.1. Договора. [↑](#footnote-ref-8)
8. Положение Банка России от 04.06.2020 N 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств». [↑](#footnote-ref-9)