Приложение 1

к Договору об оказании услуг сервис-бюро Системы передачи финансовых сообщений Банка России

**ПРАВИЛА ОКАЗАНИЯ УСЛУГ СЕРВИС-БЮРО СИСТЕМЫ ПЕРЕДАЧИ ФИНАНСОВЫХ СООБЩЕНИЙ БАНКА РОССИИ**

**Оглавление**:

[1. Термины и определения 3](#_Toc60062652)

[2. Основные положения 4](#_Toc60062653)

[3. Порядок заключения Договора 4](#_Toc60062654)

[4. Порядок взаимодействия Сторон 5](#_Toc60062655)

[5. Порядок оплаты услуг 6](#_Toc60062656)

[6. Ответственность Сторон 7](#_Toc60062657)

[7. Обстоятельства непреодолимой силы (форс-мажор) 8](#_Toc60062658)

[8. Антикоррупционная оговорка 8](#_Toc60062659)

[9. Персональные данные 8](#_Toc60062660)

[10. Конфиденциальность 8](#_Toc60062661)

[11. Срок действия и расторжение Договора 9](#_Toc60062662)

[12. Порядок разрешения споров 9](#_Toc60062663)

[13. Заключительные условия 9](#_Toc60062664)

[Приложение 1 10](#_Toc60062665)

[Приложение 2 11](#_Toc60062666)

[Приложение 3 12](#_Toc60062667)

[Приложение 4 17](#_Toc60062668)

[Приложение 5 25](#_Toc60062669)

[Приложение 6 28](#_Toc60062670)

[Приложение 7 33](#_Toc60062671)

## Термины и определения

* 1. **Акт готовности** – Акт готовности передачи электронных сообщений через
	Сервис-бюро по форме Приложения 2 к Правилам.
	2. **Акт соблюдения требований ИБ** – Акт о соблюдении Клиентом требований по информационной безопасности по форме Приложения 4 к Правилам.
	3. **Анкета** – Анкета пользователя Системы передачи финансовых сообщений Банка России по форме Приложения 1 к Правилам.
	4. **Договор** – Договор об оказании услуг сервис-бюро Системы передачи финансовых сообщений Банка России.
	5. **Договор ЭДО** – Договор об обмене электронными документами, заключенный между НРД и Клиентом.
	6. **Клиент** – юридическое лицо, заключившее с Сервис-бюро Договор.
	7. **Лицензионный договор** – лицензионный договор, в соответствии с которым НРД предоставляет лицензиату право использования программного обеспечения «Терминал транзита» или программного обеспечения «Терминал транзита. Модуль мультибанк».
	8. **НРД** – Небанковая кредитная организация акционерное общество «Национальный расчетный депозитарий» (НКО АО НРД).
	9. **Пользователь СПФС** – участник обмена, чьи реквизиты включены в Справочник пользователей СПФС.
	10. **Правила** – настоящие Правила оказания услуг сервис-бюро Системы передачи финансовых сообщений Банка России, являющиеся Приложением 1 к Договору.
	11. **Правила ЭДО** – Правила электронного документооборота НКО АО НРД.
	12. **Сервис-бюро** – НРД, являющийся Пользователем СПФС и имеющий на основании договора, заключенного с Банком России, право передачи финансовой информации третьих лиц с использованием СПФС.
	13. **СПФС** – Система передачи финансовых сообщений Банка России.
	14. **Список уполномоченных представителей Клиента** – Список уполномоченных представителей Клиента, являющийся Приложением 3 к Договору, по форме Приложения 7 к Правилам.
	15. **Сайт НРД** – официальный сайт НРД в сети «Интернет» по адресу: www.nsd.ru.
	16. **Справочник пользователей СПФС** – справочник, содержащий реквизиты пользователей СПФС, которые используются при проведении контроля при обмене через СПФС.
	17. **Тарифы НРД** – Тарифы на услуги сервис-бюро Системы передачи финансовых сообщений Банка России, являющиеся Приложением 2 к Договору.
	18. **УИС** – уникальный идентификатор составителя, присваиваемый Банком России.
	19. **Учетные документы** – первичные учетные документы (счета, документы об оказанных услугах, иные документы, предусмотренные законодательством Российской Федерации или Договором), формы и документы налогового учета при наличии (счета-фактуры, корректировочные счета-фактуры)
	20. Иные термины используются в значениях, установленных законодательством Российской Федерации, нормативными правовыми актами, нормативными актами Банка России, Договором ЭДО.

## Основные положения

* 1. Правила определяют порядок и условия оказания услуг Сервис-бюро.
	2. Услуги Сервис-бюро включают в себя обеспечение обмена электронными сообщения, между Клиентом и Пользователями СПФС, заключающееся в:
		1. приеме от Клиента Пакетов транзитных электронных документов;
		2. передаче Электронных сообщений, содержащихся в Пакетах транзитных электронных документов, полученных от Клиента, Пользователям СПФС через СПФС в соответствии с нормативными актами Банка России и договором об обмене электронными сообщениями, заключенными между Сервис-бюро и Банком России;
		3. приеме из СПФС Электронных сообщений, получателем которых является Клиент;
		4. передачу полученных из СПФС Электронных сообщений Клиенту.
	3. В рамках оказания услуг Сервис-бюро также обеспечивает:
		1. внесения сведений в Справочник пользователей СПФС;
		2. ведение архивов сообщений, переданных/полученных через СПФС.

## Порядок заключения Договора

* 1. Сервис-бюро заключает Договор с юридическими лицами:
		1. в отношении которых от Банка России получено уведомление о возможности включения в Справочник пользователей СПФС в качестве клиента сервис-бюро;
		2. заключившими с Сервис-бюро Договор ЭДО;
		3. заключившими с Сервис-бюро Лицензионный договор.
		4. предоставившими документы в соответствии с [Перечнем документов, предоставляемых Клиентами-юридическими лицами в НКО АО НРД](https://www.nsd.ru/ru/documents/docs_in/), размещенном на Сайте НРД, а также Список уполномоченных представителей Клиента. Если юридическое лицо ранее предоставило комплект документов в соответствии с Перечнем документов, юридическому лицу необходимо предоставить только те документы и (или) изменения к ним, которые не были предоставлены ранее.
	2. Для получения уведомления Банка России о возможности включения юридического лица в Справочник пользователей СПФС, юридическое лицо предоставляет в НРД:
		1. Анкету;
		2. копии документов, запрашиваемых Банком России.
	3. Предоставляя НРД Анкету, юридическое лицо подтверждает, что информация, указанная в Анкете, является достоверной и может быть использована для включения в Справочник пользователей СПФС в случае заключения Договора.
	4. НРД в течение 5 (пяти) рабочих дней, исчисляемых с даты получения полного комплекта документов, указанного в подпунктах пункта 3.2 Правил, передает полученные сведения и документы на рассмотрение в Банк России. Срок рассмотрения устанавливается Банком России.
	5. При получении от Банка России уведомления НРД уведомляет о нем представителя юридического лица, сведения о котором содержатся в Анкете.
	6. В случае получения уведомления о возможности включения юридического лица в Справочник пользователей СПФС в качестве клиента сервис-бюро Стороны приступают к переговорам о заключении Договоров ЭДО, Лицензионного договора и Договора.

## Порядок взаимодействия Сторон

* 1. В течение 14 (четырнадцати) рабочих дней с даты заключения Договора Сервис-бюро обеспечивает внесение сведений о Клиенте в Справочник пользователей СПФС. Срок может быть увеличен в случае получения дополнительных запросов и (или) рекомендаций Банка России.
	2. В течение 14 (четырнадцати) рабочих дней с даты заключения Договора Стороны осуществляют проверку соблюдения Клиентом Требований по информационной безопасности, являющихся Приложением 3 к Правилам, и тестовые испытания с целью подтверждения отладки электронного взаимодействия между Сторонами.
	3. По результатам прохождения проверки соблюдения требований по информационной безопасности и тестовых испытаний Сторонами составляются Акт готовности и Акт соблюдения требований ИБ. Сервис-бюро обеспечивает сохранения указанных актов в течение 5 (пяти) лет.
	4. В последующем проверка требований по информационной безопасности проводится Клиентом самостоятельно ежегодно. Результат проверки оформляется Актом проведения контроля выполнения требований к обеспечению информационной безопасности при обмене сообщениями с Сервис-бюро СПФС по форме Приложения 6 к Правилам, либо Отчетом о результатах оценки соответствия ЗИ участка СПФС в соответствии с Национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2018).
	5. Клиент обязан хранить результаты ежегодной проверки не менее 5 (пяти) лет и предоставлять их Сервис-бюро по соответствующему запросу.
	6. Сервис-бюро СПФС оставляет за собой право на проведение проверки соблюдения Клиентом Требований по информационной безопасности путем документарной или выездной проверки в течение всего срока действия Договора.
	7. Передача Электронных сообщений в промышленной среде (контуре):
		1. возможна только при условии включения Клиента в Справочник пользователей СПФС, присвоения Клиенту УИС, подписания Сторонами актов, указанных в пункте 4.3 Правил и соблюдения Клиентом Правил,
		2. начинается не ранее даты, указанной в Акте готовности.
	8. Обмен Пакетами транзитных электронных сообщений, содержащих Электронные сообщения для передачи через/поступивших из СПФС, осуществляется Сторонами в порядке Транзита электронных документов через СЭД НРД, установленном Договором ЭДО (Приложением 4 к Правилам ЭДО), с учетом особенностей, предусмотренных Приложением 5 к Правилам.
	9. Конфиденциальность и неизменность Электронных сообщений, содержащихся в Пакете транзитных электронных сообщений, обеспечивается Клиентом их шифрованием с использованием СКПЭП получателя-Пользователя СПФС.
	10. Особенности формирования и (или) обмена Электронными сообщения могут устанавливаться эксплуатационно-технической документацией, предоставляемой Сервис-бюро.
	11. Клиент обязан:
		1. уведомлять Сервис-бюро о случаях невозможности обмена Пакетами транзитных электронных документов/Электронных сообщений (передачи и (или) получения), возникновении ошибок при обработке Пакетов транзитных электронных документов/Электронных сообщений по следующему адресу электронной почты: soed@nsd.ru.
		2. уведомлять Сервис-бюро о выявленных инцидентах, связанных с нарушениями требований по информационной безопасности, путем направления сообщения на адрес электронной почты: soed@nsd.ru. По результатам уведомления уполномоченные представители Сторон принимают решения о действиях Сторон для устранения и (или) минимизации негативных последствий возникшего инцидента.
		3. назначить лиц, уполномоченных направлять в Сервис-бюро уведомления, указанные в подпунктах 4.11.1, 4.11.2 Правил, и предоставить сведения о них в Сервис-бюро в Списке уполномоченных представителей Клиента одновременно с заключением Договора. В случае изменения уполномоченных лиц и (или) сведений о них, Клиент обязан предоставить Сервис-бюро обновленный Список уполномоченных представителей Клиента в порядке, определенном пунктом 13.2 Правил.
		4. контролировать передаваемые и получаемые Электронные сообщения на отсутствие вредоносного кода.
	12. Клиент вправе приостановить информационный обмен путем направления соответствующего заявления в Сервис-бюро на следующий адрес электронной почты: soed@nsd.ru. Сервис-бюро обрабатывает поступившие заявление и обеспечивает приостановку информационного обмена с рабочего дня, следующего за днем получения заявления.
	13. Сервис-бюро обязано уведомлять Клиента о возникновении/прекращении обстоятельств, препятствующих обмену путем публикации сведений об этом на Сайте НРД. Сервис-бюро обязано принимать меры по обеспечению оперативного восстановления обмена.
	14. Сервис-бюро вправе приостанавливать оказание услуг Клиенту на время проведения профилактических, тестовых и других регламентных работ. О дате и времени начала и окончания планируемых работ Сервис-бюро уведомляет Клиента не позднее, чем за 2 (два) рабочих дня до начала их проведения путем публикации сведений об этом на Сайте НРД. При этом приостановка предоставления услуг, связанная с выполнением таких работ, не считается перерывами в предоставлении услуг.

## Порядок оплаты услуг

* 1. Клиент обязан оплачивать услуги Сервис-бюро в порядке, установленном Договором, и в размере, установленном Тарифами НРД.
	2. Оплата услуг Сервис-бюро производится ежемесячно в соответствии с Тарифами НРД, действующими на дату оказания услуг, начиная с даты начала обмена, указанной Сторонами в Акте готовности.
	3. В стоимость Услуг не включен налог на добавленную стоимость, который оплачивается Клиентом сверх стоимости Услуг в размере, установленном законодательством Российской Федерации.
	4. Сервис-бюро выставляет счет и предоставляет иные Учетные документы не позднее 5 (пятого) рабочего дня месяца, следующего за расчетным.
	5. Учетные документы предоставляются Клиенту:
		1. в виде электронных документов по Каналам информационного взаимодействия, предусмотренным Договором ЭДО и предназначенным для указанных целей. При этом оригиналы Учетных документов на бумажном носителе предоставляются в офисе НРД. При необходимости Сервис-бюро вправе направить оригиналы Учетных документов по почтовому адресу;
		2. при отсутствии электронного документооборота между Сторонами – в виде документов на бумажном носителе в офисе НРД. При необходимости Сервис-бюро вправе направить оригиналы Учетных документов по почтовому адресу;
		3. в случае подключения обмена Учетными документами через информационную систему, оператор которой соответствует требованиям ФНС России, - в порядке, предусмотренном Договором ЭДО.
	6. В случае подключения обмена, предусмотренного пунктом 5.5.3 Правил, Стороны осуществляют его на условиях, предусмотренных Договором ЭДО. При этом иные способы направления Учетных документов больше не применяются.
	7. Клиент обязан оплатить счет путем перечисления денежных средств по банковским реквизитам НРД, указанным в счете, не позднее 20 (двадцатого) числа месяца, следующего за расчетным.
	8. При несоблюдении срока оплаты, Сервис-бюро вправе потребовать уплаты неустойки в размере 1 (одного) процента от несвоевременно оплаченной суммы за каждый день просрочки, но не более 10 (десяти) процентов от указанной суммы.
	9. В случае нарушения срока оплаты более чем на один календарный месяц Сервис-бюро вправе:
		1. приостановить оказание услуг;
		2. потребовать оплаты путем внесения авансовых платежей и не оказывать услуги, если внесенный авансовый платеж не достаточен.

## Ответственность Сторон

* 1. Стороны несут ответственность за неисполнение или ненадлежащее исполнение возложенных на них обязательств в соответствии с законодательством Российской Федерации.
	2. Сервис-бюро не несет ответственности за невозможность обеспечение обмена электронными сообщения между Клиентом и Пользователями СПФС, возникшую из-за сбоев в СПФС или нарушения Клиентом установленных Правилами требований.
	3. Клиент несет ответственность:
		1. за содержание любого передаваемого им через Сервис-бюро Электронного сообщения, в том числе за реквизиты получателей-Пользователей СПФС;
		2. за обеспечение соблюдения требований по информационной безопасности, предусмотренных Правилами.
	4. Если Договор будет признан незаключенным или недействительным в связи с отсутствием у Стороны необходимых для его заключения разрешений и согласований (если они необходимы), такая Сторона обязана возместить понесенные другой Стороной убытки.

## Обстоятельства непреодолимой силы (форс-мажор)

* 1. Стороны освобождаются от ответственности за неисполнение своих обязательств по Договору, если это неисполнение явилось следствием обстоятельств непреодолимой силы: сбоев, неисправностей и отказов оборудования, контроль над которыми не осуществляют Стороны; сбоев, неисправностей и отказов систем связи, энергоснабжения и других систем жизнеобеспечения, которые Стороны не могли предвидеть или предотвратить, и иных чрезвычайных обстоятельств.
	2. Сторона, для которой стало невозможным исполнение своих обязательств из-за обстоятельств непреодолимой силы обязана сообщить другой Стороне об их возникновении/прекращении.

## Антикоррупционная оговорка

* 1. Сторонами в соответствии с законодательством Российской Федерации разработаны и применяются меры по предупреждению и противодействию коррупции. Стороны не осуществляют действия, квалифицируемые законодательством Российской Федерации как дача и (или) получение взятки, коммерческий подкуп, не выплачивают и не предлагают выплатить какие-либо денежные средства или ценности, прямо или косвенно, любым лицам для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества или для достижения иных неправомерных целей, а также не предпринимают иные действия, нарушающие требования законодательства Российской Федерации о противодействии коррупции.

## Персональные данные

* 1. В случае передачи одной Стороной другой Стороне персональных данных при заключении и исполнении Договора передающая Сторона обязана обладать правом на их передачу другой Стороне, а принимающая Сторона обязана обеспечить их конфиденциальность и осуществлять их обработку в соответствии с принципами и условиями, предусмотренными законодательством Российской Федерации. При получении мотивированного запроса Стороны другая Сторона обязана предоставить в течение 3 (трех) рабочих дней со дня его получения письменное подтверждение:
		1. права обработки персональных данных;
		2. права на их передачу другой Стороне (в том числе подтверждение уведомления субъекта об обработке его персональных данных);
		3. обеспечения их конфиденциальности.

## Конфиденциальность

* 1. Сторона не вправе раскрывать третьим лицам информацию, которой Стороны обмениваются при заключении Договора и (или) которая стала известна Стороне в процессе исполнения Договора, без предварительного письменного согласия другой Стороны, за исключением случаев, предусмотренных законодательством Российской Федерации или Правилами, а также предпринимать меры для охраны такой информации.
	2. Сторона вправе раскрывать третьим лицам, привлекаемым для исполнения обязанностей по Договору, информацию, которой Стороны обмениваются при заключении и исполнении Договора, без предварительного письменного согласия другой Стороны. Раскрытие Стороной конфиденциальной информации третьему лицу возможно только на условиях, аналогичных изложенным в настоящем разделе Правил.

## Срок действия и расторжение Договора

* 1. Договор считается заключенным с даты его подписания и действует до 31 декабря года (включительно), в котором он был заключен. Договор считается продленным на каждый последующий календарный год, если ни одна из Сторон за 1 (один) месяц до истечения каждого календарного года не предоставит другой Стороне письменное уведомление об отказе от продления Договора.
	2. Договор может быть расторгнут по соглашению Сторон, а также в одностороннем внесудебном порядке по инициативе любой Стороны.
	3. При расторжении Договора по инициативе одной из Сторон Договор считается расторгнутым по истечении 10 (десяти) календарных дней с даты направления/получения НРД уведомления о расторжении Договора.
	4. Уведомление об отказе от продления Договора или о расторжении Договора вручается представителю Стороны или направляется регистрируемым почтовым отправлением по почтовому адресу Стороны. Почтовый адрес НРД размещен на официальном Сайте НРД.
	5. Прекращение (расторжение) Договора не освобождает Стороны от исполнения обязательств, которые возникли до даты прекращения (расторжения) Договора.

## Порядок разрешения споров

* 1. Все противоречия, возникающие при исполнении Договора или связанные с ним, Стороны разрешают с соблюдением претензионного порядка. Сторона, которой заявлена претензия, обязана в течение 5 (пяти) рабочих дней со дня получения ее оригинала представить ответ на претензию путем вручения представителю другой Стороны или направления регистрируемого почтового отправления по адресу места нахождения другой Стороны, указанному в едином государственном реестре юридических лиц (указанном в ином официальном источниках, если Сторонами договора – нерезидент Российской Федерации). Непредставление ответа на претензию в указанный срок рассматривается как отказ в ее удовлетворении.

## Заключительные условия

* 1. Правом, подлежащим применению к отношениям Сторон, является российское право.
	2. Передача информационных писем, уведомлений, предусмотренных настоящими Правилами, осуществляется Клиентом с адресов электронной почты, сведения о которых содержатся в Списке уполномоченных представителей.
	3. Сторона обязана уведомлять другую Сторону об изменении адреса места нахождения, почтового адреса и банковских реквизитов в срок не позднее 3 (трех) рабочих дней с даты таких изменений. Сервис-бюро уведомляет Клиента о таких изменениях путем размещения изменений на Сайте НРД.

## Приложение 1

к Правилам оказания услуг сервис-бюро
Системы передачи финансовых сообщений Банка России

**Анкета пользователя
Системы передачи финансовых сообщений Банка России**

|  |
| --- |
| 1. **Сведения об организации**
 |
| Полное фирменное наименование |  |
| Сокращенное фирменное наименование |  |
| Страна регистрации |  |
| Дата регистрации |  |
| SWIFT BIC |  |

|  |
| --- |
| 1. **Сведения о счетах организации в российских банках**
 |
| Наличие счета | *да/нет* |
| Тип счета | *при наличии* |
| Сведения о банке, в котором открыт счет | *при наличии* |
|  |  |
| 1. **Контактная информация представителя**
 |
| ФИО |  |
| Должность |  |
| Адрес электронной почты |  |
| Номер телефона |  |

|  |
| --- |
| 1. **Иная информация**
 |
| Предпочтительный язык общения |  |

*Подписанием настоящей анкеты я соглашаюсь с предоставлением НКО АО НРД
(ОГРН 1027739132563) права на обработку моих персональных данных, указанных в анкете; подтверждаю наличие у меня права на предоставление НРД согласия на обработку персональных данных, указанных в анкете, в том числе на их передачу в Центральный Банк Российской Федерации, в целях получения уведомления о возможности включения организации в состав пользователей Системы передачи финансовых сообщений Банка России в качестве клиента сервис-бюро.*

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(должность* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(подпись)* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(ФИО)* |

## Приложение 2

к Правилам оказания услуг сервис-бюро Системы передачи финансовых сообщений Банка России

ФОРМА

**Акт готовности
передачи электронных сообщений через Сервис-бюро**

Москва «\_\_\_\_»\_\_\_\_\_\_\_20\_\_г.

Небанковская кредитная организация акционерное общество «Национальный расчетный депозитарий», именуемая в дальнейшем «Сервис-бюро», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Клиент» в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,, действующей на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, именуемые вместе «Стороны», а по отдельности «Сторона», подписали настоящий Акт готовности передачи электронных сообщений через Сервис-бюро о нижеследующем:

1. Программное обеспечение «Терминал Транзита», переданное Клиенту по лицензионному договору № \_\_\_ от \_\_.\_\_\_\_.\_\_\_\_ г., для осуществления обмена электронными сообщениями через Сервис-бюро установлено.
2. Сторонами проведены тестовые испытания, свидетельствующие о возможности начала обмена Пакетами транзитных электронных сообщений/Электронными сообщениями в промышленной среде (контуре).
3. Обмен в промышленной среде (контуре) может быть начат Сторонами с \_\_\_\_\_\_\_\_\_\_\_.
4. Акт составлен в 2 (двух) экземплярах, имеющих равную юридическую силу, по одному экземпляру для каждой из Сторон.

|  |  |
| --- | --- |
| **Сервис-бюро** | **Клиент**  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |
| М.П. | М.П. |

## Приложение 3

к Правилам оказания услуг сервис-бюро Системы передачи финансовых сообщений Банка России

|  |  |
| --- | --- |
| **№** | **Требования по информационной безопасности** |
| **1.**  | Объекты информационной инфраструктуры, используемые при передаче электронных сообщений, размещаются Клиентом в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей (далее - объекты информационной инфраструктуры). |
| Для объектов информационной инфраструктуры в пределах указанного сегмента (группы сегментов) вычислительных сетей Клиентом реализуются меры защиты информации по следующим направлениям[[1]](#footnote-2): |
| **1.1.** | обеспечение защиты информации при управлении доступом | организация и контроль использования учетных записей субъектов логического доступа; |
| организация и контроль предоставления (отзыва) и блокирования логического доступа; |
| регистрация событий защиты информации, связанных с операциями с учетными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа; |
| идентификация и аутентификация субъектов логического доступа; |
| организация управления и организация защиты идентификационных и аутентификационных данных; |
| авторизация (разграничение доступа) при осуществлении логического доступа; |
| регистрация событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа; |
| организация и контроль физического доступа в помещения, в которых расположены объекты информационной инфраструктуры; |
| регистрация событий, связанных с физическим доступом; |
| организация учета и контроль состава ресурсов и объектов информационной инфраструктуры; |
| регистрация событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов информационной инфраструктуры. |
| **1.2.** |   | сегментация и межсетевое экранирование внутренних вычислительных сетей; |
| защита внутренних вычислительных сетей при взаимодействии с информационно-телекоммуникационной сетью «Интернет»; |
| регистрация событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей; |
| мониторинг и контроль содержимого сетевого трафика; |
| регистрация событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика; |
| защита информации от раскрытия и модификации при использовании беспроводных сетей; |
| защита внутренних вычислительных сетей при использовании беспроводных сетей; |
| регистрация событий защиты информации, связанных с использованием беспроводных сетей. |
| **1.3.** | контроль целостности и защищенности информационной инфраструктуры | контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информационной инфраструктуры; |
| организация и контроль размещения, хранения и обновления программного обеспечения информационной инфраструктуры; |
| контроль состава и целостности программного обеспечения информационной инфраструктуры; |
| регистрация событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры. |
| **1.4.** | защита от вредоносного кода | организация эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры; |
| организация и контроль применения средств защиты от вредоносного кода; |
| регистрация событий защиты информации, связанных с реализацией защиты от вредоносного кода. |
| **1.5.** | предотвращение утечек информации | блокирование неразрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации; |
|  контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации; |
| организация защиты машинных носителей информации; |
|  регистрация событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации. |
| **1.6.** | управление инцидентами защиты информации | организация мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информационной инфраструктуры; |
| сбор, защита и хранение данных регистрации о событиях защиты информации; |
| анализ данных регистрации о событиях защиты информации; |
| регистрация событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации; |
| обнаружение и регистрация инцидентов защиты информации; |
| организация реагирования на инциденты защиты информации; |
| организация хранения и защита информации об инцидентах защиты информации; |
|  регистрация событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них. |
| **1.7.** | защита среды виртуализации | идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа; |
| сегментация и межсетевое экранирование вычислительныхсетей |
| **1.8.** | защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств. |
| **2** | В документах, разрабатываемых Клиентом сервис-бюро, в целях обеспечения защиты информации при передаче электронных сообщений, указываются, в том числе | технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры; |
| состав и правила применения технологических мер защиты информации, используемых для контроля целостности и подтверждения подлинности электронных сообщений на этапах их формирования (подготовки), обработки, передачи и хранения, в том числе порядок применения средств криптографической защиты информации (далее - СКЗИ) и управления ключевой информацией СКЗИ; |
| план действий, направленных на обеспечение непрерывности и (или) восстановление деятельности, связанной с обменом электронными сообщениями; |
| лица, допущенные к работе со СКЗИ; |
| лица, ответственные за обеспечение функционирования и безопасности СКЗИ (ответственный пользователь СКЗИ); |
| лица, обладающие правами по управлению криптографическими ключами, в том числе ответственные за формирование криптографических ключей и обеспечение безопасности криптографических ключей; |
| лица, уполномоченные направлять заявления о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении обмена электронными сообщениями. |
| **3** | Сведения о лицах, уполномоченных направлять заявления о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении обмена электронными сообщениями, направляются Клиентом в Сервис-бюро не позднее следующего дня после дня их назначения или изменения. |
| **4** | Передача и прием электронных сообщений между Сервис-бюро и Клиентом осуществляется с использованием автоматизированного рабочего места обмена электронными сообщениями. |
| **5** | Хранение входящих и исходящих электронных сообщений осуществляется Клиентом не менее пяти лет с даты отправки/получения. |
| **6** | Защита создаваемых электронных сообщений при их передаче Сервис-бюро посредством формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре, обеспечиваемая Клиентом, реализуется с учетом следующего: |
| **6.1.** | Контур формирования электронных сообщений и контур контроля реквизитов электронных сообщений в информационной инфраструктуре Клиента реализованы с использованием разных рабочих мест и с привлечением отдельных работников для каждого из контуров. |
| **6.2.** | Объекты информационной инфраструктуры контура формирования электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре Клиента размещаются в разных сегментах вычислительных сетей, в том числе реализованных с использованием технологии виртуализации. Способ допустимого информационного взаимодействия между указанными сегментами вычислительных сетей оформляется документально и согласовывается со службой информационной безопасности Клиента. |
| **6.3.** | В контуре формирования электронных сообщений на основе первичного документа в бумажной или электронной форме или входящего электронного сообщения осуществляются | формирование исходящего электронного сообщения, предназначенного для направления Сервис-бюро; |
| контроль реквизитов исходящего электронного сообщения, предназначенного для направления Сервис-бюро |
| подписание исходящего электронного сообщения, предназначенного для направления Сервис-бюро, электронной подписью, применяемой в контуре формирования электронных сообщений, при положительном результате контроля реквизитов; |
| направление исходящего электронного сообщения, предназначенного для направления Сервис-бюро, в контур контроля реквизитов электронных сообщений; |
| **6.4.** | В контуре контроля реквизитов электронных сообщений осуществляется | контроль реквизитов исходящего электронного сообщения, предназначенного для направления Сервис-бюро, на соответствие реквизитам первичного документа в бумажной или электронной форме или входящего электронного сообщения; |
| контроль на отсутствие дублирования исходящих электронных сообщений; |
| передача исходящего электронного сообщения, при положительном результате контроля реквизитов, на автоматизированное рабочее место обмена электронными сообщениями с последующим шифрованием электронных сообщений на прикладном уровне в соответствии с семиуровневой стандартной моделью взаимодействия открытых систем, определенной международным стандартом ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model. |
| **7.** | При обмене электронными сообщениями с Сервис-бюро с обеспечивается защита электронных сообщений с учетом следующего: |
| **7.1.** | Применяются средства защиты информации, реализующие двухстороннюю аутентификацию и шифрование информации на сеансовом уровне (5 уровень) и ниже, в соответствии с эталонной моделью взаимосвязи открытых систем, определенной международным стандартом ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model. |
| **7.2.** | При осуществлении взаимодействия с Сервис-бюро рекомендуется обеспечить взаимодействие с применением технических средств, имеющих заранее оговоренные индивидуальные дистанционно распознаваемые идентификационные признаки (1Р-адреса, DNS-имена и т.д.) с запретом возможности подключения с другими признаками. |
| **8** | Для целей анализа обеспечения защиты информации при осуществлении обмена Клиентом (уполномоченным лицом Клиента) осуществляется уведомление Сервис-бюро о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении обмена электронными сообщениями в течение восьми рабочих часов с момента фиксации инцидента путем направления информационного сообщения доступными способами. |

## Приложение 4

к Правилам оказания услуг сервис-бюро Системы передачи финансовых сообщений Банка России

ФОРМА

**Акт о соблюдении Клиентом
требований по информационной безопасности**

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ |
|  | *(должность)* |
|  | *(подпись)* |  *(Фамилия И.О.)* |
| Мп |
|  | "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ |

Настоящий акт составлен по результатам проверки готовности к обмену электронными сообщениями (ЭС) с использованием\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(наименование и серийные номера применяемых программных и программно-аппаратных средств)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Комиссия \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(наименование Клиента*)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, созданная на основании Приказа № \_\_\_ от \_\_\_\_\_\_\_\_\_\_\_, в составе:

|  |  |  |
| --- | --- | --- |
|  | Руководитель Комиссии: |  |
|  | Члены Комиссии: |  |
|  |  |  |
|  |  |  |
|  |  |  |

провела проверку готовности к обмену ЭС с Сервис-бюро СПФС.

Комиссия установила следующее:

1. Размещение и техническое состояние аппаратных, системных, сетевых и телекоммуникационных средств, а также состояние программного обеспечения автоматизированных рабочих мест соответствует рекомендациям Сервис-бюро СПФС, а именно:
	1. Определен и документально зафиксирован участок платежной системы Банка России в зоне ответственности *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(наименование Клиента)\_\_\_\_\_\_\_\_\_\_\_\_* приказом № \_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_.
	2. Аппаратные, системные, сетевые и телекоммуникационные средства АРМ обмена установлены в помещениях \_\_\_\_\_ по адресу \_\_\_\_\_\_\_\_\_\_, удовлетворяющих требованиям безопасности (оборудованы охранной сигнализацией, сдаются под охрану, располагаются в зоне действия системы видеонаблюдения и контроля доступа), находятся в исправном состоянии и готовы к работе.
	3. Необходимые программные средства обеспечения электронного документооборота, включая программно-аппаратные средства защиты от НСД \_\_\_\_\_\_\_, средства защиты от ВВК \_\_\_\_\_\_\_\_\_\_\_, средства криптографической защиты информации \_\_\_\_\_\_\_\_\_\_\_\_\_ (далее - СКЗИ) на АРМ обмена установлены, их настройка произведена в соответствии с требованиями эксплуатационной документации.
	4. Резервные программные и аппаратные средства имеются и готовы к использованию.
	5. Для телекоммуникационного взаимодействия с Сервис-бюро СПФС обеспечена связь по \_\_\_\_\_\_\_\_\_\_\_\_ от провайдеров \_\_\_\_\_\_\_\_\_\_\_ (основной канал) и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (резервный канал).
2. Используется следующий вариант взаимодействия АС Клиента с АРМ обмена: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
3. Информационная безопасность обмена ЭС обеспечивается путем применения мер и средств установленных:
	1. Объекты информационной инфраструктуры Клиента Сервис-бюро, используемые при передаче электронных сообщений, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей (далее – объекты информационной инфраструктуры).
	2. Для объектов информационной инфраструктуры в пределах указанного сегмента (группы сегментов) вычислительных сетей Клиентом Сервис-бюро реализованы меры защиты информации по следующим направлениям согласно национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2017):
* обеспечение защиты информации при управлении доступом;
* обеспечение защиты вычислительных сетей;
* контроль целостности и защищенности информационной инфраструктуры;
* защита от вредоносного кода;
* предотвращение утечек информации;
* управление инцидентами защиты информации;
* защита среды виртуализации;
* защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.
	1. В части обеспечения защиты информации при управлении доступом Клиентом Сервис-бюро реализованы следующие меры защиты информации:
* организация и контроль использования учетных записей субъектов логического доступа;
* организация и контроль предоставления (отзыва) и блокирования логического доступа;
* регистрация событий защиты информации, связанных с операциями с учетными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа;
* идентификация и аутентификация субъектов логического доступа;
* организация управления и организация защиты идентификационных и аутентификационных данных;
* авторизация (разграничение доступа) при осуществлении логического доступа;
* регистрация событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа;
* организация и контроль физического доступа в помещения, в которых расположены объекты информационной инфраструктуры;
* регистрацию событий, связанных с физическим доступом;
* организация учета и контроль состава ресурсов и объектов информационной инфраструктуры;
* регистрация событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов информационной инфраструктуры.
	1. В части обеспечения защиты вычислительных сетей Клиентом Сервис-бюро реализованы следующие меры защиты информации:
* сегментация и межсетевое экранирование внутренних вычислительных сетей;
* защита внутренних вычислительных сетей при взаимодействии с сетью «Интернет»;
* регистрация событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей;
* мониторинг и контроль содержимого сетевого трафика;
* регистрация событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика;
* защита информации от раскрытия и модификации при использовании беспроводных сетей;
* защита внутренних вычислительных сетей при использовании беспроводных сетей;
* регистрация событий защиты информации, связанных с использованием беспроводных сетей.
	1. В части контроля целостности и защищенности информационной инфраструктуры Клиентом Сервис-бюро реализованы следующие меры защиты информации:
* контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информационной инфраструктуры;
* организация и контроль размещения, хранения и обновления программного обеспечения информационной инфраструктуры;
* контроль состава и целостности ПО информационной инфраструктуры;
* регистрация событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры.
	1. В части защиты от вредоносного кода Клиентом Сервис-бюро реализованы следующие меры защиты информации:
* организация эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры;
* организация и контроль применения средств защиты от вредоносного кода;
* регистрация событий защиты информации, связанных с реализацией защиты от вредоносного кода.
	1. В части предотвращения утечек информации Клиентом Сервис-бюро реализованы следующие меры защиты информации:
* блокирование неразрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации;
* контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации;
* организация защиты машинных носителей информации;
* регистрация событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации.
	1. В части управления инцидентами защиты информации Клиентом сервис-бюро реализованы следующие меры защиты информации:
* организация мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информационной инфраструктуры;
* сбор, защита и хранение данных регистрации о событиях защиты информации;
* анализ данных регистрации о событиях защиты информации;
* регистрация событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации;
* обнаружение и регистрация инцидентов защиты информации;
* организация реагирования на инциденты защиты информации;
* организация хранения и защиту информации об инцидентах защиты информации;
* регистрация событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них.
	1. В части защиты среды виртуализации Клиентом Сервис-бюро реализованы следующие меры защиты информации:
* идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;
* сегментация и межсетевое экранирование вычислительных сетей;
* организация идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации;
* организация и контроль информационного взаимодействия и изоляции виртуальных машин;
* организация защиты образов виртуальных машин;
* регистрация событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации.
	1. В части защиты информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств защиты среды виртуализации Клиентом Сервис-бюро реализованы следующие меры защиты информации:
* защита информации от раскрытия и модификации при осуществлении удаленного доступа;
* защита внутренних вычислительных сетей при осуществлении удаленного доступа;
* защита информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах.
	1. Для реализации требований к защите информации Клиентом Сервис-бюро применяются/не применяются положения международного стандарта ISO/IEC 27002:2013 Information technology. Security techniques. Codes of practice for information security controls.
1. Клиентом Сервис-бюро разрабатаны документы, определяющие порядок обеспечения защиты информации при передаче электронных сообщений:
* технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры определены в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* состав и правила применения технологических мер защиты информации, используемых для контроля целостности и подтверждения подлинности электронных сообщений на этапах их формирования (подготовки), обработки, передачи и хранения, в том числе порядок применения средств криптографической защиты информации (далее – СКЗИ) и управления ключевой информацией СКЗИ определены в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;
* план действий, направленных на обеспечение непрерывности и (или) восстановление деятельности, связанной с обменом электронными сообщениями определен в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
1. Клиентом Сервис-бюро обеспечена защита создаваемых электронных сообщений при их передаче Сервис-бюро посредством формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре с учетом следующего:
	1. Контур формирования электронных сообщений и контур контроля реквизитов электронных сообщений в информационной инфраструктуре Клиента Сервис-бюро реализованы с использованием разных рабочих мест и с привлечением отдельных работников для каждого из контуров.
	2. Объекты информационной инфраструктуры контура формирования электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре Клиента Сервис-бюро размещаются в разных сегментах вычислительных сетей, в том числе реализованных с использованием технологии виртуализации. Способ допустимого информационного взаимодействия между указанными сегментами вычислительных сетей оформлен документально и согласован со службой информационной безопасности Клиента Сервис-бюро.
	3. В контуре формирования электронных сообщений на основе первичного документа в бумажной или электронной форме, или входящего электронного сообщения осуществляются:
* формирование исходящего электронного сообщения, предназначенного для направления Сервис-бюро;
* контроль реквизитов исходящего электронного сообщения, предназначенного для направления Сервис-бюро;
* подписание исходящего электронного сообщения, предназначенного для направления Сервис-бюро, электронной подписью, применяемой в контуре формирования электронных сообщений, при положительном результате контроля реквизитов;
* направление исходящего электронного сообщения, предназначенного для направления Сервис-бюро, в контур контроля реквизитов электронных сообщений.
	1. В контуре контроля реквизитов электронных сообщений осуществляется:
* контроль реквизитов исходящего электронного сообщения, предназначенного для направления Сервис-бюро, на соответствие реквизитам первичного документа в бумажной или электронной форме, или входящего электронного сообщения;
* контроль на отсутствие дублирования исходящих электронных сообщений;
* передача исходящего электронного сообщения, при положительном результате контроля реквизитов, на автоматизированное рабочее место обмена электронными сообщениями с последующим шифрованием электронных сообщений на прикладном уровне в соответствии с семиуровневой стандартной моделью взаимодействия открытых систем, определенной международным стандартом ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model;
1. При обмене электронными сообщениями с Сервис-бюро Клиентом Сервис-бюро обеспечена защита электронных сообщений с учетом следующего:
	1. Применяются средства защиты информации, реализующие двухстороннюю аутентификацию и шифрование информации на сеансовом уровне (5 уровень) и ниже, в соответствии с эталонной моделью взаимосвязи открытых систем, определенной международным стандартом ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model.
	2. При осуществлении взаимодействия с Сервис-бюро обеспечено/не обеспечено взаимодействие с применением технических средств, имеющих заранее оговоренные индивидуальные дистанционно распознаваемые идентификационные признаки: *\_\_\_\_\_\_\_\_\_\_(IP-адреса, DNS-имена и т.д.)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* с запретом возможности подключения с другими признаками.
2. Процедура тестирования успешно проведена при использовании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ в период с \_\_\_\_\_\_\_\_\_ по \_\_\_\_\_\_\_\_\_\_\_.
3. Назначены следующие ответственные лица (функции ответственных лиц могут совмещаться):
	1. лица, допущенные к работе со СКЗИ:

|  |  |  |  |
| --- | --- | --- | --- |
| Ф.И.О. | Должность | Телефон | Приказ о назначении |
|  |  |  |  |

* 1. лица, ответственные за обеспечение функционирования и безопасности СКЗИ:

|  |  |  |  |
| --- | --- | --- | --- |
| Ф.И.О. | Должность | Телефон | Приказ о назначении |
|  |  |  |  |

* 1. лица, обладающие правами по управлению криптографическими ключами, в том числе ответственные за формирование криптографических ключей и обеспечение безопасности криптографических ключей:

|  |  |  |  |
| --- | --- | --- | --- |
| Ф.И.О. | Должность | Телефон | Приказ о назначении |
|  |  |  |  |

* 1. лица, уполномоченные направлять заявления о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении обмена финансовыми сообщениями:

|  |  |  |  |
| --- | --- | --- | --- |
| Ф.И.О. | Должность | Телефон | Приказ о назначении |
|  |  |  |  |

**Заключение**

Комиссия считает, что *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Наименование Клиента)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* готов к осуществлению обмена ЭС при переводе денежных средств в рамках взаимодействия с Сервис-бюро СПФС.

|  |  |
| --- | --- |
| Руководитель Комиссии: |  |
| Члены Комиссии: |  |
|  |  |
|  |  |

Приложения: Уведомления о назначении лиц, согласно пункту 8 Акта

## Приложение 5

к Правилам оказания услуг сервис-бюро Системы передачи финансовых сообщений Банка России

**Особенности обмена Пакетами транзитных электронных документов**

1. **Особенности применения Приложения 4 к Правилам ЭДО к обмену Электронными сообщениями между Сторонами**
	1. Правила Транзита электронных документов через СЭД НРД применяются к обмену Электронными сообщения между Клиентом и Сервис-бюро в части условий, связанных с:
		1. формированием и передачей Транзитных электронных документов;
		2. обработкой Пакетов транзитных электронных документов.
2. **Особенности формирования и передачи Пакетов транзитных электронных документов Клиентом**
	1. Для формирования Электронных сообщений, а также для передачи и приема Пакетов транзитных электронных документов Клиент, являющийся кредитной организацией, обязан использовать программное обеспечение «Терминал транзита», а Клиент, не являющийся кредитной организацией, - ПО «Терминал транзита. Модуль мультибанк», право использования которого предоставляет Сервис-бюро по лицензионному договору.
	2. Электронные сообщения, передаваемые в Сервис-бюро, формируются с использованием форматов электронных сообщений в соответствии с Альбомом унифицированных форматов электронных банковских сообщений "Унифицированные форматы электронных банковских сообщений для безналичных расчетов. Обмен с кредитными организациями и другими клиентами Банка России с учетом взаимодействия пользователей системы передачи финансовых сообщений Банка России", размещенным в информационно-телекоммуникационной сети "Интернет" ([www.cbr.ru)](http://www.cbr.ru))"
	3. Описание Пакета транзитных электронных документов (winf.xml), спецификация которого определена Приложением 3 к Правилам ЭДО, формируется в соответствии с нижеуказанными особенностями:
		1. формальное описание (DTD):

<!ELEMENT COVERING\_LE

TTER (ORIGINATOR, RECIPIENT, DEPOSITARY?, SERVICE\_MARKS, DOC+)>

<!ELEMENT RECIPIENT (CONTRAGENT)>

<!ELEMENT CONTRAGENT (CONTRAGENT\_CODE, CONTRAGENT\_NAME?, MAIL?)>

<!ELEMENT CONTRAGENT\_CODE (#PCDATA)>

<!ELEMENT SERVICE\_MARKS (SUBJECT?, COMMENT?, LETTER\_ID, CONTR\_LETTER\_ID, LETTER\_TYPE, CONVERSATION\_ID?, CREATE\_TIME, NDC\_RECEPT\_TIME?, NDC\_LETTER\_ID?, ORIG\_CONF\_SEND\_TIME?, NDC\_CHECKING?, RECIPIENT\_CHECKING?, RECIPIENT\_DELIV\_TIME?, RECIPIENT\_LETTER\_ID?, NDC\_RECIPIENT\_CONF\_DELIV\_TIME?, ORIG\_FINAL\_DELIV\_CONF\_SEND\_TIME?)>

<!ELEMENT SUBJECT (#PCDATA)>

<!ELEMENT DOC (FILE\_NAME, MAX\_DELIVERY\_TIME?, DOC\_TYPE, ORIGINAL\_FILE\_NAME?, IDENT\_CODE?, NDC\_STORAGE\_DOC\_ID?, NDC\_CHECKING?, RECIPIENT\_CHECKING?, RECIPIENT\_DOC\_ID?)>

<!ELEMENT DOC\_TYPE (#PCDATA)>

<!ELEMENT ORIGINAL\_FILE\_NAME (#PCDATA)>

* + 1. описание используемых элементов и атрибутов:

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Название элемента** | **Название атрибута элемента** | **Комментарий** |
|  | COVERING\_LETTER |  | Корневой элемент, содержит всю необходимую информацию о пакете документов.Содержит вложенные элементы ORIGINATOR, RECIPIENT, DEPOSITARY, SERVICE\_MARKS и повторяющийся элемент DOC |
|  | RECIPIENT |  | Получатель пакета транзитных электронных документов. Содержит вложенный элемент CONTRAGENT |
|  | CONTRAGENT |  | Структура, содержащая информацию об отправителе и получателе пакета транзитных электронных документов. Содержит вложенный элемент CONTRAGENT\_CODE |
|  | CONTRAGENT\_CODE |  | Депозитарный код Получателя  |
|  | SERVICE\_MARKS |  | Пустой элемент, содержащий вложенные элементы.Обязательные: SUBJECT. |
|  | SUBJECT |  | Тема сообщения, содержит наименование типа финансового сообщения в соответствии с УФЭБС Банка России «SPFS.ED.\_тип\_» |
|  | DOC |  | Структура, содержащая информацию об одном электронном документе. Повторяется по одному разу для каждого документа из пакета.Содержит обязательные элементы: DOC\_TYPE, ORIGINAL\_FILE\_NAME |
|  | DOC\_TYPE |  | Признак транзитного пакета. Указывается «TRZT» |
|  | DOC | ENCRYPTED | Признак шифрования документа в пакете.Указывается «YES» если пакет зашифрован, «NO» в противном случае |
| 1. 9
 | ORIGINAL\_FILE\_NAME |  | Исходное имя файла для документа |

* 1. В одном Пакете транзитных электронных документов передается одно Электронное сообщение, содержащее финансовую информацию, подлежащее передачи Пользователю СПФС.
	2. Клиент обязан Зашифровать Электронное сообщение (использовать схему «с закрытым конвертом»).
1. **Особенности обработки Пакетов транзитных электронных документов, полученных Сервис-бюро от Клиента**
	1. В случае успешного прохождения первичных и дополнительных проверок, определенных Приложением 4 к Правилам ЭДО, Сервис-бюро осуществляет передачу Электронных сообщений в СПФС в соответствии с требованиями и правилами, предусмотренными нормативными актами Банка России и договором об обмене электронными документами, заключенным между Сервис-бюро и с Банком России.

## Приложение 6

к Правилам оказания услуг сервис-бюро Системы передачи финансовых сообщений Банка России

ФОРМА

**Акт**

**проведения контроля выполнения требований**

**к обеспечению информационной безопасности на участке обмена СПФС**

**за \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ год.**

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

| **№**  | **Описание контроля** | ***Результат контроля*** *(комментарий)* |
| --- | --- | --- |
| **1.** | **Защита информации при управлении доступом**  |
|  | организация и контроль использования учетных записей субъектов логического доступа | *Выполняется/Выявленные недостатки* |
|  | организация и контроль предоставления (отзыва) и блокирования логического доступа | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с операциями с учетными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа | *Выполняется/Выявленные недостатки* |
|  | идентификация и аутентификация субъектов логического доступа | *Выполняется/Выявленные недостатки* |
|  | организация управления и организация защиты идентификационных и аутентификационных данных | *Выполняется/Выявленные недостатки* |
|  | авторизация (разграничение доступа) при осуществлении логического доступа | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа | *Выполняется/Выявленные недостатки* |
|  | организация и контроль физического доступа в помещения, в которых расположены объекты информационной инфраструктуры | *Выполняется/Выявленные недостатки* |
|  | регистрация событий, связанных с физическим доступом | *Выполняется/Выявленные недостатки* |
|  | организация учета и контроль состава ресурсов и объектов информационной инфраструктуры; | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов информационной инфраструктуры | *Выполняется/Выявленные недостатки* |
| **2.** | **Защита вычислительных сетей** |
|  | сегментация и межсетевое экранирование внутренних вычислительных сетей | *Выполняется/Выявленные недостатки* |
|  | защита внутренних вычислительных сетей при взаимодействии с сетью «Интернет» | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей | *Выполняется/Выявленные недостатки* |
|  | мониторинг и контроль содержимого сетевого трафика | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика | *Выполняется/Выявленные недостатки* |
|  | защита информации от раскрытия и модификации при использовании беспроводных сетей | *Выполняется/Выявленные недостатки* |
|  | защита внутренних вычислительных сетей при использовании беспроводных сетей | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с использованием беспроводных сетей | *Выполняется/Выявленные недостатки* |
| **3** | **Контроль целостности и защищенности информационной инфраструктуры** |
|  | контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информационной инфраструктуры | *Выполняется/Выявленные недостатки* |
|  | организация и контроль размещения, хранения и обновления программного обеспечения информационной инфраструктуры | *Выполняется/Выявленные недостатки* |
|  | контроль состава и целостности ПО информационной инфраструктуры | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры | *Выполняется/Выявленные недостатки* |
| **4** | **Защита от вредоносного кода** |
|  | организация эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры | *Антивирус \_\_\_\_\_\_\_\_\_ функционирует, дополнительно используется \_\_\_\_\_\_\_\_/Выявленные недостатки* |
|  | организация и контроль применения средств защиты от вредоносного кода | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с реализацией защиты от вредоносного кода | *Выполняется/Выявленные недостатки* |
| **5** | **Предотвращения утечек информации** |
|  | блокирование неразрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации | *Выполняется/Выявленные недостатки* |
|  | контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации | *Выполняется/Выявленные недостатки* |
|  | организация защиты машинных носителей информации | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации | *Выполняется/Выявленные недостатки* |
| **6** | **Управление инцидентами защиты информации** |
|  | организация мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информационной инфраструктуры | *Выполняется/Выявленные недостатки* |
|  | сбор, защита и хранение данных регистрации о событиях защиты информации | *Выполняется/Выявленные недостатки* |
|  | анализ данных регистрации о событиях защиты информации | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации | *Выполняется/Выявленные недостатки* |
|  | обнаружение и регистрация инцидентов защиты информации | *Выполняется/Выявленные недостатки* |
|  | организация реагирования на инциденты защиты информации; | *Выполняется/Выявленные недостатки* |
|  | организация хранения и защита информации об инцидентах защиты информации | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирование на них | *Выполняется/Выявленные недостатки* |
| **7** | **Защита среды виртуализации** |
|  | идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа | *Выполняется/Выявленные недостатки* |
|  | сегментация и межсетевое экранирование вычислительных сетей | *Выполняется/Выявленные недостатки* |
|  | организация идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации | *Выполняется/Выявленные недостатки* |
|  | организация и контроль информационного взаимодействия и изоляции виртуальных машин | *Выполняется/Выявленные недостатки* |
|  | организация защиты образов виртуальных машин | *Выполняется/Выявленные недостатки* |
|  | регистрация событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации | *Выполняется/Выявленные недостатки* |
| **9** | **Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств** |
|  | защита информации от раскрытия и модификации при осуществлении удаленного доступа | *Выполняется/Удаленный доступ не используется/Выявленные недостатки* |
|  | защита внутренних вычислительных сетей при осуществлении удаленного доступа | *Выполняется/Удаленный доступ не используется/Выявленные недостатки* |
|  | защита информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах | *Выполняется/Удаленный доступ не используется/Выявленные недостатки* |
| **10** | **Документы, определяющие порядок обеспечения защиты информации при передаче электронных сообщений**  |
|  | технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры | *Выполняется, определено в \_\_\_\_ (наименование документа) /Требуется актуализация, Выявленные недостатки* |
|  | состав и правила применения технологических мер защиты информации, используемых для контроля целостности и подтверждения подлинности электронных сообщений на этапах их формирования (подготовки), обработки, передачи и хранения, в том числе порядок применения средств криптографической защиты информации (далее – СКЗИ) и управления ключевой информацией СКЗИ | *Выполняется, определено в \_\_\_\_ (наименование документа) /Требуется актуализация, Выявленные недостатки* |
|  | план действий, направленных на обеспечение непрерывности и (или) восстановление деятельности, связанной с обменом электронными сообщениями; | *Выполняется, определено в \_\_\_\_ (наименование документа) /Требуется актуализация, Выявленные недостатки* |
|  | перечень лиц, допущенных к работе со СКЗИ | *Выполняется, определено в \_\_\_\_ (наименование документа) /Требуется актуализация, Выявленные недостатки* |
|  | перечень лиц, ответственных за обеспечение функционирования и безопасности СКЗИ (ответственный пользователь СКЗИ) | *Выполняется, определено в \_\_\_\_ (наименование документа) /Требуется актуализация, Выявленные недостатки* |
|  | перечень лиц, обладающих правами по управлению криптографическими ключами, в том числе ответственных за формирование криптографических ключей и обеспечение безопасности криптографических ключей | *Выполняется, определено в \_\_\_\_ (наименование документа) /Требуется актуализация, Выявленные недостатки* |
|  | перечень лиц, уполномоченных направлять заявления о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении обмена финансовыми сообщениями | *Выполняется, определено в \_\_\_\_ (наименование документа) /Требуется актуализация, Выявленные недостатки* |
|  | Сведения о лицах, уполномоченных направлять заявления о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении обмена финансовыми сообщениями направляются в Сервис-бюро СПФС не позднее следующего дня после дня их назначения или изменения | *Выполняется/В отчетный период изменений не было/Выявленные недостатки* |
|  | Передача и прием электронных сообщений Клиента Сервис-бюро осуществляется с использованием автоматизированного рабочего места обмена электронными сообщениями | *Выполняется/Выявленные недостатки* |
|  | Обеспечение хранения входящих и исходящих электронных сообщений не менее 5 (пяти) лет | *Выполняется/Выявленные недостатки* |
| **11** | **Защита создаваемых электронных сообщений при их передаче Сервис-бюро посредством формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре** |
|  | Контур формирования электронных сообщений и контур контроля реквизитов электронных сообщений в информационной инфраструктуре Клиента Сервис-бюро реализованы с использованием разных рабочих мест и с привлечением отдельных работников для каждого из контуров | *Выполняется/Выявленные недостатки* |
|  | Объекты информационной инфраструктуры контура формирования электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре Клиента Сервис-бюро размещаются в разных сегментах вычислительных сетей, в том числе реализованных с использованием технологии виртуализации. Способ допустимого информационного взаимодействия между указанными сегментами вычислительных сетей оформлен документально и согласован со службой информационной безопасности Клиента Сервис-бюро. | *Выполняется/Выявленные недостатки* |
| **12** | **В контуре формирования электронных сообщений на основе первичного документа в бумажной или электронной форме или входящего электронного сообщения осуществляются:** |
|  | формирование исходящего электронного сообщения, предназначенного для направления Сервис-бюро | *Выполняется/Выявленные недостатки* |
|  | контроль реквизитов исходящего электронного сообщения, предназначенного для направления Сервис-бюро | *Выполняется/Выявленные недостатки* |
|  | подписание исходящего электронного сообщения, предназначенного для направления Сервис-бюро, электронной подписью, применяемой в контуре формирования электронных сообщений, при положительном результате контроля реквизитов | *Выполняется/Выявленные недостатки* |
|  | направление исходящего электронного сообщения, предназначенного для направления Сервис-бюро, в контур контроля реквизитов электронных сообщений | *Выполняется/Выявленные недостатки* |
| **13** | **В контуре контроля реквизитов электронных сообщений осуществляется:** |
|  | контроль реквизитов исходящего электронного сообщения, предназначенного для направления Сервис-бюро, на соответствие реквизитам первичного документа в бумажной или электронной форме или входящего электронного сообщения | *Выполняется/Выявленные недостатки* |
|  | контроль на отсутствие дублирования исходящих электронных сообщений | *Выполняется/Выявленные недостатки* |
|  | передача исходящего электронного сообщения, при положительном результате контроля реквизитов, на автоматизированное рабочее место обмена электронными сообщениями с последующим шифрованием электронных сообщений на прикладном уровне в соответствии с семиуровневой стандартной моделью взаимодействия открытых систем, определенной международным стандартом ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model | ***Выполняется/Выявленные недостатки*** |
| **14** | **Защита электронных сообщений при обмене электронными сообщениями с Сервис-бюро** |
|  | Применяются средства защиты информации, реализующие двухстороннюю аутентификацию и шифрование информации на сеансовом уровне (5 уровень) и ниже, в соответствии с эталонной моделью взаимосвязи открытых систем, определенной международным стандартом ISO/IEC 7498-1:1994 Information technology. Open Systems Interconnection. Basic Reference Model. The Basic Model. | *Выполняется/Выявленные недостатки* |
|  | При осуществлении взаимодействия с Сервис-бюро обеспечено взаимодействие с применением технических средств, имеющих заранее оговоренные индивидуальные дистанционно распознаваемые идентификационные признаки (IP-адреса, DNS-имена и т.д.) с запретом возможности подключения с другими признаками | *Выполняется/Выявленные недостатки* |
|  | Для целей анализа обеспечения защиты информации при осуществлении обмена Клиент Сервис-бюро (уполномоченное лицо Клиента Сервис-бюро) информирует Сервис-бюро о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении обмена финансовыми сообщениями в течение восьми рабочих часов с момента фиксации инцидента путем направления информационного сообщения доступными способами | *Выполняется/В отчетный период инцидентов не было/Выявленные недостатки* |

По выявленным в ходе проверки недостаткам необходимы следующие корректирующие мероприятия:

| **№ п.п.** | **Описание корректирующего мероприятия** | **Плановый срок исполнения, ответственный** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Контроль выполнения требований к обеспечению ИБ на участке СПФС выполнен:

*Сотрудник от подразделения ИБ,
Должность, ФИО \_\_\_*\_\_\_\_\_\_\_\_\_\_\_\_

*Сотрудник от подразделения ИТ-сопровождения,
Должность, ФИО \_\_\_*\_\_\_\_\_\_\_\_\_\_\_\_

*Сотрудник от подразделения физической безопасности,
Должность, ФИО \_\_\_*\_\_\_\_\_\_\_\_\_\_\_\_

## Приложение 7

к Правилам оказания услуг сервис-бюро Системы передачи финансовых сообщений Банка России

**Список уполномоченных представителей Клиента**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | ФИО  | Должность | Рабочий телефон | Адрес электронной почты | Область ответственности |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(должность)**М.П,* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(подпись)* | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*(ФИО)* |

1. Рекомендуется использовать национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 *«Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»*, утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст «*Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ*», 2017). [↑](#footnote-ref-2)