Оговорка по кибербезопасности

1. Общие положения

1.1. Настоящий документ (далее – Оговорка) определяет обязательные требования в области информационной безопасности (далее – ИБ), которые Контрагент обязуется соблюдать в течение всего срока действия Договора [в соответствии с формой документа: Соглашение, Договор, Дополнительное соглашение и т.п.] с ПАО «МТС-Банк» (далее – Банк).

1.2. Контрагент подтверждает, что его организационные и технические меры по обеспечению информационной безопасности соответствуют настоящим Требованиям и применимому законодательству РФ.

1.3. Требования распространяются на всех представителей Контрагента.

1.4 Требования по ИБ при предоставлении облачных услуг приведены в разделе 5.

1.5 Дополнительные требования к разработчикам программного обеспечения (автоматизированные банковские системы, процессинг, дистанционное банковское обслуживание) приведены в разделе 6.

1.6 Настоящие требования имеют приоритет над требованиями, изложенными в Договоре, в котором указана ссылка на настоящую Оговорку.

2. Конфиденциальность

2.1. В отношении информации ограниченного доступа[1], полученной Контрагентом в связи с исполнением Договора с Банком, Контрагент обязуется:

- обрабатывать информацию ограниченного доступа исключительно в целях исполнения Договора с Банком;
- применять меры по охране конфиденциальности информации ограниченного доступа, включая, но не ограничиваясь, меры из настоящих Требований;
- не разглашать[2] информацию ограниченного доступа, а также факт ее получения третьим лицам;
- сообщить Банку о допущенном Контрагентом либо ставшем известном Контрагенту факте разглашения, незаконном получении или незаконном использовании информации ограниченного доступа третьими лицами;
- не копировать и не воспроизводить другими способами информацию ограниченного доступа, за исключением случаев, когда это необходимо в целях исполнения Договора с Банком.
- обеспечить конфиденциальность копий информации ограниченного доступа;
- обеспечить прекращение обработки, возврат или уничтожение информации ограниченного доступа, в соответствии с требованием Банка и сроками, указанными в требовании.
- подтверждать уничтожение информации ограниченного доступа предоставлением акта уничтожения Банку;
- незамедлительно уведомлять Банк о получении требований (запросов) о предоставлении информации ограниченного доступа, о фактах изъятия или выемки, о фактах утраты[3] носителей информации ограниченного доступа, о наличии обоснованной необходимости передачи информации ограниченного доступа третьим лицам.

3. Меры по информационной безопасности

3.1 Контрагент обязуется реализовать и поддерживать как минимум следующие меры ИБ:

- регулярно обучать работников, имеющих доступ к информации Банка, основам ИБ;
- разработать, утвердить и контролировать соблюдение Политики ИБ;
- защищать рабочие станции, серверы, виртуальную инфраструктуру (при наличии) от вредоносного программного обеспечения, регулярно обновлять сигнатуры;
- реализовать разграничение доступа к полученной от Банка информации, регулярно пересматривать правила разграничения доступа;
- выявлять и проводить анализ угроз безопасности информации;
- контролировать содержание информации, передаваемой из инфраструктуры Контрагента или записываемой на отчуждаемые носители информации;
- выявлять уязвимости и регулярно устанавливать актуальные обновления безопасности, тестировать обновления безопасности перед установкой;
- использовать пароли, соответствующие требованиям[4] к сложности и сроку действия;
- обеспечить физическую защиту помещений и оборудования, где обрабатывается информация, полученная от Банка, от несанкционированного доступа;
- не позднее 24 (двадцати четырех) часов с момента обнаружения, уведомить Банк о любом инциденте ИБ[5], способном оказать негативное влияние на исполнение Договора или на безопасность информации, полученной от Банка:

---

[1] Информация ограниченного доступа – коммерческая тайна, персональные данные, иная информация, доступ к которой ограничен в соответствии с законодательством РФ.

[2] Разглашение информации ограниченного доступа - действие или бездействие Контрагента, в результате которых информация ограниченного доступа в любой возможной форме становится известной третьим лицам без согласия Банка

[3] Включая хищение и повреждение носителя

[4] Длина пароля должна быть не менее 8 символов. Пароль должен содержать буквы верхнего и нижнего регистра (А-Я, A-Z, а-я, a-z), специальные символы. Пароль не должен содержать персонифицированной информации (имена, адреса, дата рождения, номер телефона), последовательности символов и знаков (111, qwerty, qwerty123113), срок действия пароля не более 90 календарных дней. Новый пароль должен отличаться минимум на 4 символа и не совпадать с тремя предыдущими паролями.

[5] Инцидент ИБ – это непредвиденное или нежелательное событие (или группа событий), которое привело или может привести к нарушению или прекращению функционирования объекта информационной инфраструктуры, возникновению угроз безопасности информации, нарушению безопасности обрабатываемой информации и/или нарушению установленных требований по защите информации, в том числе произошедшее в результате компьютерной атаки

- уведомление должно содержать следующую информацию: характер инцидента, объем и категории затронутых данных, предполагаемые последствия и принятые меры;
- уведомление направляется на электронный адрес soc@mtsbank.ru;
- Контрагент обязуется предпринять меры для минимизации последствий инцидента ИБ.

3.2. Контрагент обязан оказывать поддержку в отношении любого расследования и/или проверки, аудита, который может проводиться в случае возникновения разумно обоснованных подозрений того, что произошло или может произойти нарушение каких-либо положений настоящих Требований.

3.3. Контрагент по запросу Банка предоставляет подтверждение соблюдения Требований.

3.4 В отношении персональных данных, полученных Контрагентом в рамках Договора с Банком, Контрагент обязуется применять правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов.

3.4.1. До осуществления трансграничной передачи персональных данных в адрес Контрагента, Контрагент предоставляет Банку на официальном бланке:

- сведения о принимаемых Контрагентом мерах по защите передаваемых персональных данных и об условиях прекращения их обработки;
- информацию о правовом регулировании в области персональных данных иностранного государства, под юрисдикцией которого находятся Контрагент[6]
- сведения о Контрагенте (наименование, номера контактных телефонов, почтовые адреса и адреса электронной почты).

3.4. При удалённом доступе к информационным системам Банка применяются дополнительные требования по ИБ, указанные в разделе 4.

4. Требования по ИБ при удаленном доступе к информационным системам Банка

4.1. Настоящий раздел определяет требования к организации удаленного доступа для работников Контрагента в рамках технологических процессов создания, сопровождения (модернизации), использования или поддержки информационных систем (иных компонентов информационной инфраструктуры) Банка.

4.2. Предоставление удаленного доступа для работников Контрагента осуществляется при наличии:

- подписанного Договора с Банком, содержащего ссылку на настоящие Требования;
- официального информационного письма на бланке Контрагента с указанием трудоустроенных в штат работников Контрагента задействованных в оказании услуг по Договору (по пилотному проекту).

4.3. Удаленный доступ Контрагенту может быть приостановлен в случае:

- выявления Банком нарушений требований по ИБ, установленных настоящим Разделом, при предоставлении удаленного доступа работникам Контрагента;
- инцидента ИБ (или подозрения на компьютерной инцидент) в информационной инфраструктуре Контрагента;
- подозрения на инцидент ИБ, связанный с действием или бездействием Контрагента.

4.4 Контрагент обязан:

- уведомлять Банк в течение 1 (одного) рабочего дня об изменении состава работников Контрагентов, задействованных в оказании услуг по Договору:
- исключить передачу между работниками Контрагента учетных записей, выданных Банком, и ключевой информации для удаленного доступа;
- по запросу Банка предоставлять журналы событий безопасности и аудита с автоматизированного рабочего места, подключенного к информационным системам Банка (далее – удаленное рабочее место);
- обеспечить хранение событий безопасности с удаленного рабочего места не менее 1 (одного) года.

4.5. Требования по ИБ

4.5.1 В инфраструктуре, связанной с оказанием услуг по Договору Контрагентом, должны быть реализованы:

- двухфакторная аутентификация;
- защищенное удаленное подключение с использованием средств криптографической защиты информации;
- защита почтовых сервисов от фишинга и вредоносного программного обеспечения;
- исключение применения программного обеспечения для удаленного управления (например, R-Admin, TeamViewer, Mikogo, DameWare, Ammyy Admin и другие аналоги).

4.5.2. На удаленном рабочем месте должны быть реализованы:

- персональный межсетевой экран;
- включена автоматическая блокировка экрана (при неактивности пользователя более 10 минут);
- исключено применение программного обеспечения для мгновенного обмена сообщениями (например, Google-Talk, Miranda, Telegram, WhatsApp и др.);
- пароли от учетной записи в инфраструктуре Контрагента и учетной записи, предоставленной Банком, должны отличаться;
- средства вычислительной техники, реализующее функции удаленного рабочего места, должны принадлежать Контрагенту и на них должны распространяться политики безопасности.

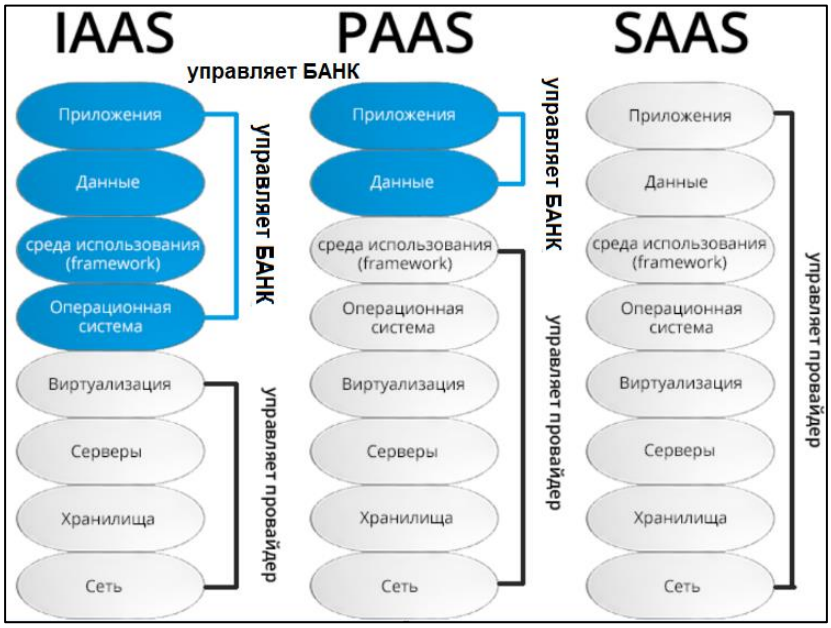
---

[6] Информация предоставляется в случае, если предполагается осуществление трансграничной передачи персональных данных иностранным юридическим лицам, находящимся под юрисдикцией иностранного государства, не являющегося стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и не включенного в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных

5. Требования по информационной безопасности при предоставлении облачных услуг Банку

5.1. Общие положения при предоставлении облачных услуг Банку

5.1.1. Границы ответственности Контрагента за обеспечение информационной безопасности определяется моделью предоставления услуг, указанной в Договоре: IaaS, PaaS, SaaS:



5.1.2. При наличии обязательных требований по ИБ к Банку, между Банком и Контрагентом согласовывается матрица ответственности за реализуемые меры ИБ.

5.1.3. Контрагент не вправе привлекать третьих лиц для обработки информации Банка и (или) размещать такую информацию вне своей инфраструктуры без письменного согласования с Банком. Контрагент обязан заранее уведомить Банк о пределах своего контроля над инфраструктурой третьих лиц, которая может быть использована. На всех привлекаемых третьих лиц распространяется действие настоящих Требований.

5.1.4. Между Контрагентом и Банком должно быть заключено соглашение о конфиденциальности в редакции Банка.

5.1.5. В случае, когда предоставление сервиса подразумевает обработку персональных данных клиентов или работников Банка, между Контрагентом и Банком должно быть подписано поручение на обработку персональных данных.

5.1.6. Контрагент обязан сообщать о планируемых перерывах в работе предоставляемого сервиса не менее чем за 7 (семь) календарных дней по согласованным в Договоре каналам уведомления.

5.1.7. Центры обработки данных (далее – ЦОД), в которых размещается сервис Контрагента, должны располагаться на территории РФ.

5.1.8. Контрагент предоставляет круглосуточную техническую поддержку на весь срок предоставления сервиса.

5.1.9. Контрагент уведомляет Банк о сбоях в работе предоставляемого сервиса (срок уведомления устанавливается в SLA).

5.2. Общие требования по информационной безопасности при предоставлении облачных услуг Банку

5.2.1. Конфиденциальность и защита данных

Контрагент обязуется:

- обеспечить конфиденциальность обрабатываемых данных Банка. Не использовать данные Банка в каких-либо целях, кроме целей исполнения Договора;
- уведомлять Банк о любом запросе уполномоченных государственных органов, связанном с предоставлением данных Банка;
- при выявлении попыток несанкционированного доступа к данным Банка – незамедлительно сообщать Банку;
- предоставить защищенные интерфейсы и использовать средства защиты информации (шифрование канала связи, межсетевое экранирование, антивирусную защиту и т.д.) для обеспечения безопасного обращения Банка к своим данным и (или) информационными системам, размещенным в инфраструктуре Контрагента.
- обеспечить изоляцию данных Банка от данных других клиентов.

5.2.2. Управление доступом.

Контрагент обязуется:

- исключить несанкционированный доступ к данным Банка для своих работников. Доступ работникам Контрагента предоставляется исключительно в рамках их служебных обязанностей для оказания услуг по Договору на основе ролевой модели и принципа наименьших привилегий;
- обеспечить регистрацию, анализ и предоставление по запросу Банка информации о доступе работников Контрагента к инфраструктуре Банка;
- выполнять все административные действия под персонифицированными учетными записями;
- обеспечить многофакторную аутентификацию с возможностью блокировки при подозрительной активности.
- предоставить возможность интеграции с IDM и SSO Банка;
- обеспечить реализацию ролевой модели доступа.

5.2.3. Защита инфраструктуры

Контрагент обязуется:

- реализовать и поддерживать систему защиты от DDoS-атак;
- реализовать и поддерживать систему защиты от несанкционированного доступа;
- проводить на регулярной основе инструментальную оценку состояния защищенности инфраструктуры, используемой для предоставления услуг Банку. Для проведения оценки может привлекаться вешний исполнитель;
- обеспечить на регулярной основе обновление и устранение уязвимостей предоставляемого сервиса. Процедуры обновления и устранения уязвимостей не должны приводить к приостановке или прекращению предоставления услуги. По запросу Банка предоставлять отчет о выявленных и устраненных уязвимостях, установленных обновлениях;
- предоставить Банку до начала оказания услуг описание принятых в облачной инфраструктуре мер защиты, включая описание механизмов разграничения доступа, в т.ч. (для IaaS) на физическом уровне, выписку из модели угроз безопасности информации.

5.2.4. Физическая безопасность

Контрагент обязуется обеспечивать физическую безопасность средств вычислительной техники, с применением которых обрабатывается информация Банка.

5.2.5. Шифрование данных

Контрагент обязуется:

- применять средства криптографической защиты информации для защиты данных Банка при передаче по открытым каналам связи.
- по запросу Банка предоставить возможность использования средств шифрования данных при хранении.

5.2.6. Регистрация событий и реагирование на инциденты

Контрагент обязуется:

- обеспечить регистрацию событий безопасности в инфраструктуре или в выделенном для оказания услуг сегменте;
- предоставить Банку доступ к журналам безопасности и аудита;
- обеспечить хранение событий безопасности не менее 1 (одного) года в защищённом виде с контролем их целостности;
- уведомлять об инцидентах ИБ в сроки, установленные SLA.
- принимать меры для устранения последствий инцидентов ИБ, предоставлять отчет по запросу Банка (в согласованные сроки), сотрудничать с Банком или уполномоченным им третьим лицом при расследовании.

5.2.7. Аудит и соответствие

Контрагент обязуется:

- не реже 1 раза в год проводить внешние и внутренние аудиты безопасности;
- предоставлять по запросу Банка актуальные отчеты независимых аудиторов или иные документы, подтверждающие соответствие применяемых мер по информационной безопасности требованиям нормативно-правовых актов РФ, отраслевым или международным стандартам.

5.2.8. Лицензирование и сертификация (в случае размещения персональных данных или инфраструктуры ОКИИ)

Контрагент обязуется:

- на момент оказания услуг обладать действующей лицензией ФСТЭК России на техническую защиту конфиденциальной информации;
- на момент оказания услуг обладать действующей лицензией ФСБ России на криптосредства.
- применять средства защиты информации, имеющие действующий сертификат ФСТЭК России, соответствующие 4 классу защиты и 4 уровню доверия;
- применяемые средства виртуализации должны иметь действующий сертификат ФСТЭК России, соответствующие 4 классу защиты и 4 уровню доверия.

5.2.9. Резервное копирование и восстановление

Контрагент обязуется:

- обеспечивать восстановление работы предоставляемого сервиса в соответствии с согласованным SLA;
- обеспечить хранение резервных копий Банка в географически распределенных ЦОД на территории РФ. Срок хранения резервных копий должен составлять не менее 30 (тридцати) календарных дней;
- обеспечить защиту резервных копий Банка от несанкционированного доступа при хранении и передаче;
- предоставлять Банку возможность тестирования процедуры восстановления из резервных копий.

5.2.10. Уничтожение информации

Контрагент обязуется:

- с применением средств гарантированного уничтожения информации уничтожать всю информацию Банка с оборудования:
  - подлежащего выводу из эксплуатации;
  - при прекращении отношений с Банком;
  - по требованию Банка.
- предоставлять Банку акты уничтожения информации.

5.3. Дополнительные требования по ИБ при предоставлении облачных услуг

5.3.1. При оказании услуг по модели IaaS Контрагент обязуется:

- предоставить доступ в выделенную консоль управления тенантом;
- обеспечивать безопасность виртуальной сетевой инфраструктуры;
- для защиты каналов управления и передачи пользовательских данных применять сертифицированные ФСБ России средства криптографической защиты информации;
- обеспечить Банку возможность хранения данных в зашифрованном виде с использованием криптографических ключей, принадлежащих Банку;
- обеспечить защиту от:
  - выключения тенанта;
  - несанкционированного удаления или модификации ресурсов тенанта;
  - несанкционированного изменения прав и состава пользователей, управляющих тенантом;
  - несанкционированного изменения архитектуры или способа доступа к тенанту;
- настроить правила на межсетевых экранах, включая ограничение входящих и исходящих соединений, по принципу: «все запрещено, что не разрешено в явном виде».
- обеспечить физическую охрану ЦОД с использованием систем контроля доступа, видеонаблюдения и круглосуточной охраны. Срок хранения записей видеонаблюдения должен составлять не менее 90 (девяносто) дней;
- предоставить Банку возможность удаленного доступа к сегменту системы видеонаблюдения и архиву видеонаблюдения (в зоне размещения предоставляемой инфраструктуры);
- обеспечить возможность организации собственной системы охраны Банка в зоне арендуемых площадей ЦОД;
- оформлять пропуска для посещения ЦОД представителям Банка, обеспечить сопровождение работниками Контрагента в зону размещения инфраструктуры Банка;
- обеспечить передачу событий ИБ в централизованную систему мониторинга Банка для анализа в режиме реального времени;
- обеспечить мониторинг работоспособности оборудования и оповещать Банк о сбоях в его работе (срок оповещения устанавливается в SLA);
- обеспечить бесперебойное электропитание ЦОД;
- обеспечить соответствие требованиям пожарной безопасности;
- обеспечить ЦОД системами климат-контроля.

5.3.2. При оказании услуг по модели PaaS Контрагент обязуется:

- предоставить Банку доступ ко встроенным средствам защиты платформы;
- обеспечить Банку возможность хранения данных в зашифрованном виде с использованием криптографических ключей, принадлежащих Банку;
- обеспечить передачу события ИБ в централизованную систему мониторинга Банка для анализа в режиме реального времени.

5.3.3 При оказании услуг по модели SaaS Контрагент обязуется:

- обеспечить безопасность предоставляемого приложения: безопасность кода, API и др.;
- предоставить инструменты для управления доступом, ролями и сессиями пользователей.

6. Дополнительные требования при разработке/модернизации программного обеспечения для Банка

6.1. При разработке/модификации программного обеспечения (автоматизированные банковские системы, процессинг, дистанционное банковское обслуживание) Контрагент обязуется:

- разработать, утвердить и применять руководство по безопасной разработке программного обеспечения (или совокупный набор регламентов);
- проводить анализ угроз, разрабатываемого/модернизируемого программного обеспечения;
- проводить статический анализ кода, разрабатываемого/модернизируемого программного обеспечения;
- проводить фаззинг-тестирование, разрабатываемого/модернизируемого программного обеспечения;
- отслеживать и исправлять обнаруженные ошибки и уязвимости, разрабатываемого/модернизируемого программного обеспечения;
- определить способы и сроки информирования об уязвимостях программного обеспечения, о компенсирующих мерах по защите информации или ограничениях по применению программного обеспечения, способов получения Банком программного обеспечения его обновлений, проверки их целостности и подлинности.

6.2. По запросу Банка Контрагент предоставляет документальное подтверждение выполнения требований, указанных в п. 6.1.

6.3. При разработке/модификации программного обеспечения для осуществления банковских операций Контрагент обязуется предоставить комплект документации для оценки соответствия по ОУД4[7].

[7] Оценочный уровень доверия. п. 6.7.2. ГОСТ Р ИСО/МЭК 15408-3 2013