

ОГОВОРКА ПО КИБЕРБЕЗОПАСНОСТИ ПАО «МТС-Банк»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ (далее - Оговорка) определяет обязательные требования в области информационной безопасности, 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 применяемые им организационные и технические меры по обеспечению информационной безопасности соответствуют настоящей Оговорке и законодательству РФ.

1.3. Положения Оговорки имеют приоритет перед требованиями по информационной безопасности, изложенными в Договоре.

2. ПРЕДМЕТ ОГОВОРКИ

2.1. Обязательство Контрагента по исполнению требований по кибербезопасности, применению защитных мер, проведению мероприятий и иных условий, установленных Оговоркой, является обстоятельством, имеющим существенное значение для Банка для заключения, исполнения и расторжения Договора.

2.2. Контрагент обязуется безоговорочно соблюдать требования по кибербезопасности, применять защитные меры и проводить иные мероприятия, перечисленные в разделе 3 Оговорки.

2.3. Стороны обязуются обеспечить наличие между ними, к моменту заключения Оговорки, действующего соглашения о неразглашении конфиденциальной информации, заключенного по предложенной Банком и согласованной Сторонами форме.

2.4. Контрагент обязан передавать Банку всю необходимую информацию для выполнения Банком своих обязательств перед Банком России и уполномоченными органами исполнительной власти в рамках выполнения ими надзорных (контрольных) мероприятий.

3. ТРЕБОВАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ

3.1. При обработке данных Банка Контрагентом должны использоваться технические средства, расположенные на территории Российской Федерации.

3.2. Правила предоставления доступа к информационным активам Банка приведены в Приложении №1.

3.3. *В случае, если предмет договора предполагает оказание услуг Контрагентом по разработке/модернизации программного обеспечения для Банка, Контрагент гарантирует, что в разрабатываемом в рамках договора ПО будут отсутствовать не декларированные возможности и вредоносная функциональность и дополнительно к мерам, указанным в п.3.2. (применимом в зависимости от условий Договора удаленный доступ к инфраструктуре Банка или разработка ПО в инфраструктуре Контрагента):*

3.3.1. разработать, утвердить и применять руководство по безопасной разработке программного обеспечения (или совокупный набор регламентов);

3.3.2. проводить анализ угроз разрабатываемого/модернизируемого программного обеспечения;

3.3.3. проводить статический анализ кода, разрабатываемого/модернизируемого программного обеспечения;

3.3.4. проводить выявление уязвимостей, содержащихся в OWASP TOP 10;

3.3.5. отслеживать и исправлять обнаруженные ошибки и уязвимости, разрабатываемого/модернизируемого программного обеспечения;

3.3.6. проводить анализ состава зависимостей (SCA);

3.3.7. 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;

3.3.8. предоставлять комплект документации для оценки соответствия по ОУД4 (при разработке/модификации программного обеспечения для осуществления банковских операций);

3.3.9. предоставлять по запросу Банка документальное подтверждение выполнения требований, указанных в п. 3.3.

3.4. *В случае, если предмет договора предполагает оказание услуг Контрагентом посредством удаленного доступа с пользовательскими правами (посредством VDI) к информационным системам Банка, то дополнительно к мерам, указанным в п.3.2., Контрагентом должны быть реализованы следующие меры по обеспечению безопасности информации в своей ИТ-инфраструктуре:*

3.4.1. двухфакторная аутентификация;

3.4.2. защита почтовых сервисов (включая, но не ограничиваясь функционалом песочницы (sandbox), антивирусной и анти-спам программами);

3.4.3. ограничение и фильтрация сетевого трафика, включая трафик сети Интернет.

На рабочем месте Контрагента, с которого осуществляется удаленный доступ с пользовательскими правами (посредством VDI) к информационным системам Банка, должны выполняться следующие требования:

3.4.4. исключено использование специализированного ПО для записи экрана;

3.4.5. средства вычислительной техники, реализующие функции удаленного рабочего места, должны принадлежать Контрагенту и на них должны распространяться политики безопасности, утвержденные Контрагентом.

3.5. *В случае, если предмет договора предполагает оказание услуг Контрагентом посредством удаленного доступа с правами администратора (посредством VDI) к информационным системам Банка, то дополнительно к мерам, указанным в п.3.4., Контрагентом должны применяться следующие меры по обеспечению безопасности информации в своей ИТ-инфраструктуре:*

3.5.1. применение систем обнаружения и предотвращения вторжений уровня сети или межсетевого экрана типа NGFW (многофункциональный межсетевой экран, реализующим фильтрацию, контроль доступа в информационную систему, контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы, и обеспечивающим защиту информационной системы от угроз безопасности информации, связанных с подключением к сетям связи общего пользования);

3.5.2. регистрация событий безопасности, обеспечивающая сбор, запись, хранение и защиту информации о событиях безопасности в информационной инфраструктуре Контрагента, а также возможность просмотра и анализа информации о таких событиях и реагирование на них;

3.5.3. использование специализированного ПО для безопасного хранения паролей и управления ими;

3.5.4. регулярное (не реже 1 раза в месяц) сканирование на уязвимости и их устранение в сроки с момента выявления:

критический уровень уязвимости: до 24 часов;

высокий уровень уязвимости: до 7 дней;

средний уровень уязвимости: до 4 недель;

низкий уровень уязвимости: до 4 месяцев.

3.5.5. исключено использование специализированного ПО для удаленного администрирования;

3.5.6. использование на рабочих станциях и серверах EDR с регулярным обновлением сигнатур.

3.6. *В случае, если предмет договора предполагает интеграцию информационных систем Контрагента с информационными системами Банка, то дополнительно к мерам, указанным в п.3.2., Контрагентом должны применяться следующие меры по обеспечению безопасности информации в сегменте своей ИТ-инфраструктуры:*

3.6.1. двухфакторная аутентификация (для административного доступа к системам интеграции);

3.6.2. использование средств криптографической защиты информации для интеграции с ИС Банка;

3.6.3. реализация разграничения доступа к среде функционирования СКЗИ;

3.6.4. применение систем обнаружения и предотвращения вторжений уровня сети или межсетевого экрана типа NGFW (многофункциональный межсетевой экран, реализующим фильтрацию, контроль доступа в информационную систему, контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы, и обеспечивающим защиту информационной системы от угроз безопасности информации, связанных с подключением к сетям связи общего пользования)

3.6.5. выделение отдельного сетевого сегмента для взаимодействия с Банком;

3.6.6. реализовать сбор, запись, хранение событий безопасности и защиту информации о событиях безопасности, а также оперативное реагирование на них;

3.6.7. проведение на регулярной основе (не реже 1 раза в месяц) выявление (поиск), анализ и устранение уязвимостей (в том числе выявление, анализ и устранение уязвимостей API) в сроки с момента выявления:

критический уровень уязвимости: до 24 часов;

высокий уровень уязвимости: до 7 дней;

средний уровень уязвимости: до 4 недель;

низкий уровень уязвимости: до 4 месяцев.

3.6.8. защита почтовых сервисов (включая, но не ограничиваясь функционалом песочницы (sandbox), антивирусной и анти-спам программами);

3.6.9. исключено использование специализированного ПО для записи экрана;

3.6.10. использование специализированного ПО для безопасного хранения паролей и управления ими;

3.6.11. использование в инфраструктуре Контрагента EDR регулярным обновлением сигнатур.

3.7. Способ организации защищенного удаленного доступа к информационным ресурсам Банка, технические параметры подключения, тип и настройки оборудования, используемого для удаленного доступа, определяются Банком.

4. ОБМЕН ИНФОРМАЦИЕЙ ОБ ИНЦИДЕНТАХ КИБЕРБЕЗОПАСНОСТИ

4.1. При возникновении в ИТ-инфраструктуре Контрагента значимого инцидента компьютерной безопасности, последствия которого могут затронуть интересы Банка в том числе клиентов или партнеров Банка), Контрагент обязана известить об этом Банк в максимально возможный короткий срок, но не позднее 3-х (трех) часов с момента обнаружения такого инцидента (подозрения на инцидент).

4.2. Значимым считается инцидент компьютерной безопасности, удовлетворяющий одному из следующих критериев:

4.2.1. разглашение аутентификационных данных или конфиденциальной информации Банка (коммерческая тайна, банковская тайна, персональные данные);

4.2.2. воздействие вредоносного программного обеспечения, массовые блокировки учетных записей, создание несанкционированных учетных записей;

4.2.3. выявленные признаки несанкционированного доступа или неудачного получения несанкционированного доступа, а также злоупотребление привилегиями доступа;

4.2.4. DDOS-атака на информационную инфраструктуру Контрагента.

4.3. Контрагент направляет сведения о значимых инцидентах (подозрениях на инциденты) компьютерной безопасности на e-mail: soc@mtsbank.ru.

4.4. В случае устранения значимого инцидента компьютерной безопасности Контрагент обязан не позднее 24 часов после устранения инцидента уведомить Банк о мерах, принятых для управления инцидентом. Для повышения оперативности при передаче технической информации Стороны вправе использовать телефонную связь и иные каналы передачи информации.

4.5. В случае появления новых типов инцидентов компьютерной безопасности, способов и механизмов их выявления, а также при необходимости оптимизации взаимодействия или изменения форматов передаваемых файлов.

5. КОНФИДЕНЦИАЛЬНОСТЬ И ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. За исключением случаев, явно указанных в Договоре или применимом законодательстве, Стороны обязуются:

5.1.1. без предварительного письменного согласия передающей стороны не раскрывать и/или не передавать, и/или не предоставлять каким-либо третьим лицам, за исключением своих работников и подрядчиков, принявших на себя обязательства конфиденциальности не менее строгие, чем предусмотренные настоящим разделом Оговорки, никакой конфиденциальной информации (информация, касающаяся предмета договора, хода его исполнения и результатов), при этом получающая сторона несет ответственность за действия таких работников и подрядчиков с конфиденциальной информацией, как за свои собственные;

5.1.2. не использовать конфиденциальную информацию передающей стороны в каких-либо целях, кроме цели заключения и исполнения Договора;

5.1.3. принимать все необходимые меры предосторожности для охраны конфиденциальной информации передающей стороны, и как минимум такие же строгие меры предосторожности, какие получающая сторона разумно принимала бы в отношении своей собственной конфиденциальной информации.

5.2. Не будет считаться нарушением обязательств, установленных разделом 5 Оговорки, передача конфиденциальной информации, если такая информация передана по письменному запросу органов государственной власти в целях исполнения ими предписанных функций, установленных применимым законодательством. Конфиденциальная информация должна передаваться в минимальном допустимом объеме. При этом получающая сторона обязана письменно известить передающую сторону о поступившем запросе в течение трех рабочих дней с момента получения такого запроса.

5.3. Обязательство по сохранению в тайне конфиденциальной информации возникает у получающей стороны с момента подписания Договора или Соглашения о конфиденциальности и остается в силе в течение 5 (пяти) лет после прекращения Договора или Соглашения о конфиденциальности.

5.4. В случае нарушения обязательств по сохранению конфиденциальности конфиденциальной информации, Контрагент несет ответственность в соответствии с применимым законодательством и обязан возместить Банку все причинённые таким нарушением документально подтвержденные убытки.

5.5. В случае, если по условиям договора, заключаемого между Банком и Контрагентом, одна из Сторон осуществляет обработку персональных данных по поручению другой Стороны, в содержание соответствующего договора должно быть включено поручение обработки персональных данных, либо Стороны должны заключить отдельный договор поручения обработки персональных данных.

5.6. Стороны принимают на себя обязательства осуществлять обработку персональных данных, ставших известными Сторонам или полученных Сторонами в ходе исполнения Договора, а также обеспечить конфиденциальность и защиту персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

5.7. Стороны обязуются осуществлять передачу (предоставление, доступ) персональных данных одной из Сторон только при наличии правовых оснований на такую передачу.

5.8. Передача персональных данных между Сторонами может осуществляться по электронным каналам связи с использованием средств криптографической защиты информации, на машинном носителе информации или на бумажном носителе. Передача персональных данных на машинном носителе информации осуществляется по Акту приема-передачи (сопроводительным письмом).

6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Контрагент обязуется ознакомить своих работников, участвующих в предоставлении услуг Банку, с требованиями Оговорки.

6.2. В случае нарушения Контрагентом требований Оговорки, как существенного условия Договора, Банк вправе отказать Контрагенту в предоставлении доступа к своей ИТ-инфраструктуре, а также расторгнуть Договор в любое время без возмещения убытков Контрагенту посредством направления Контрагенту соответствующего уведомления не менее чем за 5 (пять) рабочих дней до момента расторжения Договора.

6.3. В случае нарушения Контрагентом принятых на себя обязательств по Оговорке, Контрагент обязуется возместить Банку убытки, причиненные таким нарушением. Убытки возмещаются в соответствии с законодательством Российской Федерации. Кроме того, в

случае если к Банку будут предъявлены претензии (требования, иски) со стороны третьих лиц и/или государственных органов, вследствие реализованных рисков кибербезопасности, в рамках Оговорки, Контрагент по получении извещения от Банка обязуется:

6.3.1. выступить на стороне Банка;

6.3.2. оказать всемерное содействие Банку при урегулировании таких претензий;

6.3.3. взять на себя обязанность по подготовке и проведению досудебных переговоров и переписки с такими третьими лицами или государственными органами, а впоследствии (в том случае, если Банк будет вынужден в силу вступившего в силу решения суда или если по согласованию с Контрагентом будет признано приемлемым возместить ущерб третьих лиц во внесудебном порядке);

6.3.4. возместить Банку в полном объеме выплаченные Банком третьим лицам или государственным органам денежные средства, связанные с нарушением прав третьих лиц судебные издержки Банка и иные расходы. Возмещение производится Контрагентом не позднее 10 (десяти) рабочих дней со дня получения соответствующего письменного требования и счета от Банка.

6.4. Банк вправе пересмотреть условия Оговорки по своей инициативе в следующих случаях:

6.4.1. наличие у Банка необходимости сохранить надлежащий уровень контроля и управления в отношении риска нарушения требований Оговорки Контрагентом;

6.4.1. наличие у Банка необходимости принять соответствующие меры для выполнения своих обязательств перед клиентами и контрагентами, а также уполномоченными государственными органами.

6.5. Банк имеет право на инициировать внешний независимый аудит состояния информационной безопасности Контрагента (включая, но не ограничиваясь, тестирование на проникновение). Контрагент обязуется не препятствовать проведению аудита и предоставить необходимые разрешения и доступы в согласованные с обеих сторон сроки (не более 5 рабочих дней с момента поступления запроса).

6.6. Все споры, разногласия и требования, возникающие из Оговорки или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или недействительности, будут разрешаться путем переговоров.

Правила предоставления доступа к информационным активам Банка (далее - Правила)

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Банк предоставляет Контрагенту доступ к информационным активам Банка, а Контрагент обязуется пользоваться доступом на условиях, предусмотренных настоящими Правилами.

1.2. Банк предоставляет Контрагенту доступы к информационным активам только для целей исполнения обязанностей Контрагента в рамках Договора между Банком и Контрагентом. Контрагент обязуется использовать предоставленные доступы исключительно в интересах Банка.

2. ТРЕБОВАНИЯ ПО СОБЛЮДЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На средствах вычислительной техники, на которых обрабатываются информационные активы Банка, должны быть:

- 2.1. установлены средства защиты от вредоносного ПО с регулярно обновляемыми антивирусными базами данных;
- 2.2. обеспечено применение мер по ограничению и фильтрации сетевого трафика, включая трафик сети Интернет;
- 2.3. регулярно устанавливаться обновления операционной системы;
- 2.4. исключен доступ неуполномоченных работников Контрагента или третьих лиц к конфиденциальной информации или информационным системам Банка;
- 2.5. включена автоматическая блокировка экрана (при неактивности работника Контрагента более 10 минут);
- 2.6. исключена работа с сервисами обмена мгновенными сообщениями;
- 2.7. исключено использование специализированного ПО для удаленного администрирования

3. ТРЕБОВАНИЯ ПО ПРИМЕНЕНИЮ ПАРОЛЕЙ

3.1. Все применяемые работниками Контрагента пароли доступа к средствам вычислительной техники, на которых обрабатываются информационные активы Банка, должны отвечать приведенным ниже требованиям:

- 3.1.1. содержать не менее 8 символов для пользовательских паролей, не менее 16 символов для административных паролей;
- 3.1.2. содержать: буквы различных регистров, цифры, спецсимволы;
- 3.1.3. не являться словом из словаря, сленга, диалекта, жаргона;
- 3.1.4. не являться личной информацией (к примеру, для создания паролей не должны применяться имена членов семьи, адреса, телефоны, даты рождения);
- 3.1.5. не состоять из последовательностей символов раскладок клавиатуры (к примеру, 123456qwerty, 1qaz2wsx3456);
- 3.1.6. пароли от учетной записи в инфраструктуре Контрагента и учетной записи, предоставленной Банком, должны отличаться;
- 3.1.7. исключено хранение паролей в браузере.

3.2. Работники Контрагента обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.

3.3. Запрещается:

- 3.3.1. сообщать или разглашать свой пароль кому-либо, включая коллег, руководителей и работников службы технической поддержки, любыми средствами и способами;
- 3.3.2. записывать, хранить пароли учетных записей пользователей в доступной для чтения форме в любом виде;
- 3.3.3. использовать автоматическое сохранение пароля;

3.3.4. использовать общие пароли доступа к персональным компьютерам совместно с другими работниками.

3.4. Пароль должен быть немедленно изменен, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого работника Контрагента.

3.5. Все текущие операции с паролем работники Контрагента должны осуществлять лично, не допуская возможности рассмотреть состав вводимого пароля и порядок введения символов другими работниками или третьими лицами.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН ПРИ ИНТЕГРАЦИИ ИЛИ УДАЛЕННОМ ДОСТУПЕ К ИТ-ИНФРАСТРУКТУРЕ БАНКА

4.1. Банк обязан обеспечить предоставление доступа Контрагента к информационным активам Банка в целях исполнения обязанностей по Договору на условиях настоящих Правил.

4.2. Банк имеет право:

4.2.1. осуществлять контроль за использованием Контрагентом предоставленных доступов к информационным активам Банка;

4.2.2. в любой момент приостановить, ограничить и полностью закрыть доступ Контрагента к информационным активам Банка, в том числе в случае нарушения настоящих Правил со стороны работников Контрагента.

4.3. Контрагент обязан:

4.3.1. предоставить необходимую информацию по запросу Банка, в том числе перечень лиц Контрагента, которые будут или уже имеют доступ к информационным активам Банка для целей исполнения обязательств по Договору;

4.3.2. осуществлять замену своих работников, имеющих доступ к информационным активам Банка, на иных, только по письменному согласованию с Банком;

4.3.3. извещать Банк не менее чем за 5 (пять) рабочих дней до даты увольнения работника Контрагента или его отстранения от осуществления действий, связанных с использованием обязательств по Договору (если предмет Договора подразумевает интеграцию информационных систем Банка и Контрагента или предоставление Контрагенту удаленного доступа к ИТ-инфраструктуре Банка);

4.3.4. не препятствовать контролю со стороны Банка за соблюдением правил доступа к информационным активам Банка;

4.3.5. в случае попадания к работникам Контрагента паролей доступа, прав, полномочий и привилегий (умышленного или случайного), отличных от согласованных и выданных Банком, Контрагент не вправе их использовать и обязан незамедлительно сообщить Банку об их получении;

4.3.6. использовать предоставленные доступы, в том числе программное обеспечение, только для исполнения Контрагентом обязательств по Договору.

5. ОТВЕТСТВЕННОСТЬ КОНТРАГЕНТА И ВОЗМЕЩЕНИЕ ПОТЕРЬ

5.1. При обнаружении фактов нарушения настоящих Правил, уполномоченный работник Банка уведомляет Контрагента о факте нарушения и имеет право требовать сведения о причинах нарушения, а также о принятых Контрагентом мерах по недопущению подобного нарушения. В случае не предоставления объяснений Контрагентом в течение 3 (трех) дней с момента сообщения о факте нарушения без уважительной причины, все предоставленные Контрагенту доступы к информационным активам Банка могут быть отозваны.