Приложение о безопасности Услуг Cloud Software Group

Версия 3.0

Дата вступления в силу: 30 сентября 2022 г.

Содержание

Это Приложение о безопасности услуг Cloud Software Group, Inc. (далее — Cloud Software Group, «Мы» и все другие местоимения 1-го лица множественного числа) (далее — Приложение») описывает элементы управления безопасностью, реализованные в рамках предоставления Облачных услуг, услуг технической поддержки или консультационных услуг (далее — «Услуги») клиентам (далее — «Клиент», «Вы» и все местоимения 2-го лица множественного числа) по соответствующей лицензии Cloud Services Group и (или) соглашению об использовании услуг и применимому заказу на Услуги (все вместе — Соглашение»). Бета-версии или предварительные версии лабораторных/технических услуг (в том числе Cloud Labs) и наши внутренние ИТ-системы, не используемые в предоставлении Услуг, не входят в область действия этого Приложения.

Термины, написанные с заглавной буквы, имеют значение, указанное в Соглашении или определенное в настоящем документе. «Клиентское содержимое» означает любые данные, к которым Мы имеем доступ или которые Мы получаем, или которые Вы отправляете или загружаете для хранения или обработки с целью предоставления Нами Услуг. Оно также включает в себя запатентованную техническую информацию, связанную с Вашей средой, такую как выбираемые Вами конфигурации системы или сети и элементы управления. «Журналы» означает данные о работе, стабильности, использовании, безопасности, поддержке, устройствах, программном обеспечении, службах или периферийных устройствах, относящиеся к использованию Наших продуктов или Услуг.

1. Область действия

В настоящем Приложении описываются административные, физические и технические элементы управления безопасностью, которые Мы используем для обеспечения конфиденциальности, целостности и доступности Наших Услуг. Эти элементы управления относятся к Нашим операционным средам, а также системам и средам Наших Услуг. Компания Cloud Software Group применяет в качестве основы программы по безопасности Услуг стандарт ISO/IEC 27002 и прошла отраслевые сертификации и процедуры оценки для конкретных Услуг. Дополнительные сведения см. в разделе «Конфиденциальность и соответствие требованиям» Нашего центра управления безопасностью.

Мы стремимся постоянно дорабатывать и улучшать свои методы обеспечения безопасности, поэтому оставляем за собой право изменять элементы управления, описанные в настоящем документе. Независимо от изменений уровень безопасности не будет снижен в течение соответствующего срока предоставления Услуг.

2. Инфраструктура программы и политики обеспечения безопасности

В Cloud Software Group есть инфраструктура программы и политики обеспечения безопасности, установленная и одобренная руководителями

подразделений, относящихся к различным сферам деятельности.

2.1 Курирование угроз безопасности

Комитет по курированию угроз кибербезопасности (Cyber Risk Oversight Committee, CROC) управляет действиями по контролю угроз безопасности. Комитет CROC состоит из руководителей различных подразделений. Руководство высшего звена ежегодно проверяет состав комитета и следит за тем, чтобы различные бизнес- и операционные сферы были представлены в равной степени.

Комитет CROC собирается не реже чем раз в квартал и предоставляет аналитические данные, указания и инструкции в отношении идентификации, оценки и устранения угроз безопасности в корпоративной деятельности и в инфраструктуре предоставления услуг.

2.2 Управление угрозами безопасности

Cloud Software Group использует программу контроля угроз безопасности (security risk management, SRM), которая определяет потенциальные угрозы для Наших продуктов, услуг и Нашей инфраструктуры, оценивает значимость рисков, связанных с этими угрозами, разрабатывает стратегии снижения рисков и помогает Нашим отделам разработки продуктов и проектирования реализовать эти стратегии.

2.3 Информационная безопасность

Компания Cloud Software Group назначила Руководителя по информационной безопасности (Chief Information Security Officer, CISO), который несет ответственность за курирование безопасности, стратегию политики безопасности, обеспечение соответствия требованиям и контроль за исполнением. Директор по мониторингу безопасности и реагированию руководит процессами реагирования на инциденты, в том числе изучением, сдерживанием и устранением.

2.4 Физическая безопасность и безопасность окружающей среды

Отдел безопасности Cloud Software Group контролирует физический доступ на Наши объекты.

3. Управление доступом

Мы требуем использовать меры по контролю доступа, предполагающие предоставление и сохранение необходимых прав для доступа к системам, ресурсам, данным и объектам компании с целью защиты от потенциального повреждения, раскрытия или потери. Мы используем принцип минимальных прав (безопасность на основе ролей), предоставляя пользователям доступ только к тому содержимому, которое им необходимо для выполнения должностных функций или ролей.

Менеджеры разрабатывают роли для обеспечения надлежащего разделения обязанностей, распределяя задачи и права между несколькими людьми с целью обеспечения защиты от мошеннических действий и ошибок.

3.1 Новые учетные записи, роли и запросы на доступ

Cloud Software Group требует формальный запрос для доступа к системам или данным компании. Для каждого запроса на доступ требуется минимальное утверждение менеджера пользователя, гарантирующее, что пользователь обладает необходимыми ролью и правами доступа. Администраторы доступа подтверждают получение необходимых утверждений, прежде чем предоставить доступ к системам или данным. Применяется принцип минимальных прав.

3.2 Проверка учетных записей

Мы выполняем проверку учетных записей и предоставленных прав в отношении основных систем не реже двух раз в год. Любые изменения, которые необходимо внести в результате проверки, проходят формальный процесс запроса на доступ для подтверждения того, что пользователю и его роли требуется доступ к соответствующим системам.

3.3 Удаление учетной записи, роли и отмена доступа

Мы требуем, чтобы доступ учетной записи пользователя был отключен, отозван или отменен сразу после уведомления об изменении (если

применимо), увольнении или аннулировании роли пользователя, завершении взаимодействия с пользователем или его уходе из компании.

Запросы на отмену доступа документируются и отслеживаются.

3.4 Учетные данные

Cloud Software Group требует наличия многофакторной проверки подлинности для удаленного доступа сотрудников к Нашим системам и в обязательном порядке требует применения следующих способов работы с паролями и управления ими.

- Согласно установленным Нами системным требованиям, регулярно проводится ротация паролей.

- Пароли должны быть определенной длины и сложности, включать сочетание цифр, специальных символов и букв в верхнем и нижнем регистре, а также минимальное количество символов; обычные или редкие слова в качестве пароля не принимаются.
- Деактивированные или недействительные идентификаторы пользователей не назначаются другим лицам.
- Мы следим за порядком деактивации паролей, которые были непреднамеренно раскрыты.
- Мы отслеживаем повторные попытки получить доступ к Услугам с помощью недействительного пароля и применяем автоматические действия для блокировки таких попыток.

Cloud Software Group предпринимает специальные меры для сохранения конфиденциальности и целостности паролей во время их назначения, распределения и хранения, например:

- требует хеширования паролей в течение всего срока их действия;
- запрещает раскрытие паролей.

4. Разработка и обслуживание систем

Мы применяем процесс безопасного проектирования, который включает в себя стандарты и процедуры изменения элементов управления, позволяющие обеспечить соответствие требованиям к безопасности информационных систем, проверку и тестирование кода, а также безопасность в отношении использования данных тестирования. Управляет этим процессом и отслеживает его специальный отдел безопасности, который также несет ответственность за проверку разработок, моделирование угроз, ручную проверку кода, выборочные проверки и тестирование на проникновение.

4.1 Принципы безопасного проектирования

Компания Cloud Software Group внедрила формальную методику жизненного цикла разработки систем (systems development life cycle, SDLC), которая управляет требованиями в отношении разработки, комплектования, реализации и обслуживания компьютеризированных информационных систем и соответствующих технологий.

Мы используем программную систему для управления проверкой и утверждением открытого кода, в том числе для периодических проверок и аудитов собственных программных продуктов. У нас есть задокументированные политики, доступные всем сотрудникам, в отношении использования открытых источников информации, а также обучения разработчиков и использования ими рекомендаций по работе с открытыми источниками.

4.2 Управление изменениями

Наш процесс управления изменениями в инфраструктуре и программном обеспечении определяет требования к безопасности и требует, чтобы изменения программного обеспечения и инфраструктуры были авторизованны, формально задокументированы, протестированы (если применимо), проверены и утверждены перед развертыванием в рабочей среде. Отслеживание изменений программного обеспечения и инфраструктуры и управление ими осуществляется с помощью систем управления работой.

Процесс управления изменениями надлежащим образом разделен, и доступ

к переносу изменений в производственную среду имеет только авторизованный персонал.

5. Управление активами

5.1 Управление физическими и виртуальными активами

Cloud Software Group ведет динамический учет управляемых нами физических и виртуальных систем, используемых для предоставления Услуг (далее — «Активы услуг»). Владельцы систем несут ответственность за обслуживание и обновление своих Активов услуг в соответствии с Нашими стандартами безопасности.

Разработаны формальные процедуры уничтожения, содержащие инструкции о безопасном уничтожении данных Cloud Software Group и Клиентов. Мы уничтожаем все данные, которые больше не требуются, с учетом классификации и процедур удаления, предотвращающих воссоздание и чтение данных.

Наши технологические активы очищаются и удаляются, когда больше не требуются в соответствующей области. Технологические активы включают, в частности, отдельные вычислительные устройства, многофункциональные вычислительные устройства, устройства хранения данных, устройства обработки изображений и сетевые устройства. Уничтожение координируется глобальными службами управления угрозами безопасности и системой информационной безопасности.

5.2 Управление приложениями и системами

Владельцы приложений и систем несут ответственность за проверку и классификацию данных, которые они хранят, уничтожают, передают или к которым они получают доступ. Помимо других элементов управления сотрудники и подрядчики обязаны выполнять следующее.

- Отнесение Клиентского содержимого к одной из двух наивысших категорий конфиденциальной информации Citrix и применение надлежащих ограничений доступа.
- Ограничение печати Клиентского содержимого и уничтожение печатных материалов в безопасных контейнерах.
- Отказ от хранения корпоративной или Конфиденциальной информации на любом оборудовании или устройстве, которое не соответствует требованиям политик и стандартов безопасности Citrix.
- Защита компьютеров и данных, оставленных без присмотра.

5.3 Удержание данных

Клиентское содержимое, хранящееся в рамках предоставления Наших Облачных услуг, доступно Клиенту в течение ограниченного периода времени после окончания предоставления Услуг, а затем удаляется (за исключением резервных копий) после отправки подтверждения Клиенту об удалении. Дополнительные сведения см. в документации к конкретным услугам. Клиентское содержимое также может храниться после окончания предоставления услуг, если это требуется по закону. Компания Citrix будет соблюдать требования настоящего Приложения, пока такое Клиентское содержимое не будет навсегда удалено.

6. Безопасность управления персоналом

Обеспечение безопасности Клиентского содержимого является одним из основных требований для всех сотрудников и подрядчиков. Наш Кодекс делового поведения требует, чтобы все сотрудники и подрядчики придерживались Наших политик и стандартов безопасности, и отдельно рассматривает вопрос защиты конфиденциальной информации, а также личной информации Клиентов, партнеров, поставщиков и сотрудников.

Все сотрудники и подрядчики должны соблюдать соглашения о конфиденциальности, распространяющиеся на такую информацию Клиентов. Кроме того, отдел безопасности Cloud Software Group регулярно информирует сотрудников по вопросам, касающимся информационной и физической безопасности, в целях обеспечения осведомленности по конкретным вопросам в области безопасности.

6.1 Проверка данных

В настоящее время мы пользуемся услугами поставщиков проверки биографических данных в каждом случае приема на работу новых сотрудников по всему миру и требуем того же для персонала сторонних поставщиков, кроме тех случаев, когда это ограничено местным законом или трудовым законодательством.

6.2 Обучение

Все сотрудники должны пройти обучение по защите данных и политикам компании, разработанным для защиты Нашей Конфиденциальной информации, которая включает в себя Конфиденциальную информацию Клиентов, партнеров, поставщиков и сотрудников. В обучении рассматриваются методики и принципы обеспечения конфиденциальности, которые применяются к обработке персональных данных сотрудниками, в том числе необходимость ограничений использования, хранения персональных данных, доступа и предоставления доступа к ним. Сотрудники инженерных подразделений проходят специальное обучение, в котором рассматриваются вопросы безопасной разработки, построения архитектуры и написания кода.

6.3 Обеспечение соблюдения

Все сотрудники обязаны соблюдать Наши политики и стандарты безопасности и конфиденциальности. Их несоблюдение повлечет применение мер дисциплинарного воздействия вплоть до увольнения.

7. Безопасность операций

7.1 Безопасность сети и системы

В Cloud Software Group есть задокументированные стандарты усиления защиты сети и системы, созданные для обеспечения безопасной конфигурации сетей и систем. В частности, в соответствии с этими стандартами обязательными являются следующие процедуры:

- изменение или отключение настроек и (или) учетных записей по умолчанию;
- контроль административного доступа;
- использование служебных учетных записей только в целях, для которых они были созданы;
- настройка параметров входа и оповещения, подходящих для аудита.

Мы требуем установки антивредоносного программного обеспечения на серверах и рабочих станциях и проверок сети на вредоносное

программное обеспечение.

Элементы управления сети контролируют доступ к Клиентскому содержимому. К ним относятся, если применимо: настройка промежуточной недоверенной зоны между Интернетом и внутренней сетью, которая включает защитный механизм для ограничения доступа и несанкционированного трафика; сегментация сети для предотвращения несанкционированного доступа к Клиентскому содержимому; отделение веб-серверов и серверов приложений от соответствующих серверов баз данных в многоуровневой структуре, ограничивающей трафик между уровнями.

7.2 Ведение журналов

Мы собираем Журналы для подтверждения правильного функционирования наших Услуг, чтобы помочь в устранении системных проблем и защитить сети и Клиентское содержимое. Журналы могут содержать идентификатор доступа, время, предоставленную или отклоненную авторизацию, диагностические данные, например файлы трассировки и сбоев, и другие важные сведения.

Мы собираем и используем Журналы (i) для предоставления и улучшения Услуг, обеспечения их защиты, управления ими и определения их параметров, (ii) по запросу Клиента или его конечных пользователей, (iii) в целях ведения бухгалтерского учета, управления учетными записями, внутренней отчетности и разработки стратегии в отношении продуктов и (или) (iv) для соответствия требованиям соглашений, политик, применимого законодательства, нормативов или запросов государственных служб. Для этого может выполняться мониторинг работы, стабильности, использования и безопасности Услуг и соответствующих компонентов. Журналы могут содержать идентификатор доступа, время, предоставленную или отклоненную авторизацию, диагностические данные, например файлы трассировки и сбоев, и другие важные сведения. Клиенты не могут блокировать такой мониторинг или вмешиваться в него.

Дополнительную информацию об обращении с Клиентским содержимым и Журналами см. в Нашем центре управления безопасностьюCloud Assurance Data Protection & Security section, где содержатся несколько технических документов в отношении ведения журналов для Облачных услуг Citrix.

7.3 Управление сертификатами, учетными данными и секретными ключами

В компании Cloud Software Group применяются политики, регулирующие срок действия сертификатов, учетных данных и секретных ключей для обеспечения их защиты, доступности и конфиденциальности. Хранители секретных ключей должны быть указаны в документации и официально подтвердить, что они принимают на себя ответственность за управление секретными ключами.

Их обязанности включают в том числе соблюдение следующих условий.

- Сертификаты должны выдаваться утвержденным центром сертификации.
- Криптографические ключи не могут храниться или передаваться в виде простого текста и должны использовать надежные одобренные криптографические протоколы.
- Учетные данные и секретные ключи должны меняться не реже одного раза в год и храниться в утвержденном инструменте управления аутентификацией.

7.4 Управление уязвимостями

Мы регулярно отслеживаем приложения и системы на предмет уязвимостей с помощью автоматизированного сканирования уязвимостей и портов.

Выявленные уязвимости необходимо устранять в сроки, зависящие от уровня опасности и рекомендаций поставщиков. Если исправления, обновления или постоянные решения для смягчения последствий не доступны, будут использоваться соответствующие контрмеры для снижения риска эксплуатации уязвимости.

8. Шифрование

8.1 Защита данных во время передачи

Компания Cloud Software Group развернула протоколы безопасной передачи данных в отношении передачи информации в общедоступных сетях, которые являются частью Услуг. Услуги защищены шифрованием, а доступ через Интернет защищен с помощью TLS-соединений.

8.2 Защита данных в состоянии покоя

Мы требуем, чтобы все рабочие станции, используемые для обеспечения предоставления Услуг, были зашифрованы как минимум 128-битным полным шифрованием диска. Клиентское содержимое не может храниться на каких-либо незашифрованных переносных устройствах.

Некоторые Облачные услуги по умолчанию шифруют определенные элементы данных, а также могут предоставлять клиентам другие функции шифрования. Дополнительные сведения см. в применимой документации по работе Облачных услуг.

9. Физическая безопасность

9.1 Объекты

Мы используем следующие элементы управления, разработанные для предотвращения несанкционированного доступа на объекты.

- Доступ на объекты предоставляется только лицам, обладающим соответствующим разрешением.
- Посетителям необходимо зарегистрироваться в цифровом журнале посетителей; их будут сопровождать и за ними будут наблюдать в течение всего визита.
- Сотрудники, подрядчики и гости должны носить значки с идентификаторами, которые должны быть видны в течение всего времени пребывания на объекте.
- Доступ на объекты в нерабочее время контролирует служба безопасности.
- Охранники, система обнаружения проникновения и (или) камеры видеонаблюдения следят за пунктами входа в здания, платформами отгрузки и разгрузки и зонами общего доступа (механизмы отслеживания доступа могут различаться в зависимости от объекта и его расположения).

Кроме того, на объектах Cloud Software Group имеются следующие средства обеспечения безопасности:

- системы и устройства подавления и обнаружения огня;
- системы и устройства управления климатом (температурой, влажностью и т. д.);

- запорная арматура или изолирующие клапаны в легкой доступности;
- аварийные выходы и пути эвакуации.

Защита коммуникационных шкафов, расположенных в офисах, осуществляется посредством доступа по значкам и мониторинга.

9.2 Центры данных

Кроме элементов управления объектами, описанных выше, для объектов, которыми управляет и владеет Cloud Software Group, в центрах обработки данных, используемых для предоставления Услуг, реализованы дополнительные элементы управления.

Мы используем системы, созданные для защиты от потери данных из-за прекращения подачи питания или сетевых помех, в том числе глобальную избыточную инфраструктуру служб с настроенными узлами аварийного восстановления. Центры обработки данных и поставщики услуг Интернета оцениваются с целью оптимизации пропускной способности, задержек и аварийного восстановления.

Центры обработки данных располагаются в объектах, не связанных с поставщиками услуг Интернета. В них обеспечена физическая защита, резервный источник питания, избыточность инфраструктуры и уровень непрерывной работы в рамках соглашений с ключевыми поставщиками.

Когда Мы используем сторонние центры обработки данных или облачные службы для предоставления Услуг, Мы заключаем договоры с поставщиками, которые соответствуют минимальным требованиям к физической и экологической безопасности Наших объектов.

10. Непрерывность бизнес-процессов и аварийное восстановление

10.1 Непрерывность бизнес-процессов

Cloud Software Group стратегически планирует непрерывность бизнес-операций во время неблагоприятных или аварийных ситуаций и разрабатывает системы для обеспечения предоставления услуг при возникновении таких событий.

Мы выполняем анализ последствий для деятельности (Business Impact Analysis, BIA) на уровне подразделений не менее одного раза в два года и осуществляем ежегодные проверки. Результаты такого анализа используются для создания плана непрерывности деятельности для каждого подразделения, в котором определены и задокументированы требования к ресурсам, параметры и методы восстановления, потребности перемещения и меры безопасности, необходимые на каждом этапе процесса, чтобы избежать сбоев и простоев. Руководящий состав каждого подразделения проверяет и утверждает план непрерывности деятельности каждый год или в случае серьезных организационных изменений.

У нас есть аварийные планы и планы экстренных мероприятий для всех Наших объектов. Если объекты недоступны, сотрудники могут работать удаленно на других объектах Cloud Software Group или в другом месте по своему выбору. Дополнительные стратегии восстановления задокументированы в планах непрерывности деятельности, если применимо.

10.2 Аварийное восстановление

Мы стремимся свести к минимуму влияние от прерывания

обслуживания или выполнения операций, реализуя процессы и элементы управления, созданные для обеспечения стабильного и организованного восстановления Наших бизнес-систем и данных. Cloud Software Group реализует избыточность для всех критически важных систем, данных и инфраструктуры. В плане аварийного восстановления используется оценка, выполненная в рамках анализа последствий для деятельности (см. выше), для определения и документации параметров времени восстановления, методов, приоритетов и мер безопасности, необходимых на каждом этапе процесса, чтобы избежать сбоев и простоев.

В плане указывается общая структура и подход к восстановлению критически важных систем и данных, в том числе следующее:

- роли и обязанности сотрудников или команд;
- контактные данные важного персонала или сторонних компаний;
- требования к обучению и планы для важного персонала;
- цели и приоритеты восстановления и показатели успеха;
- схема полного восстановления.

Руководящий состав проверяет и утверждает план аварийного восстановления каждый год или в случае серьезных организационных изменений.

11. Реагирование на инциденты

Компания Cloud Software Group имеет план реагирования на инциденты кибербезопасности, где подробно описаны процессы обнаружения, идентификации, анализа Инцидентов безопасности, влияющих на управляемые Нами сети и (или) системы или Клиентское содержимое, сообщения о них и реагирования на них. Обучение реагированию на Инциденты безопасности и соответствующие проверки проводятся не реже раза в год.

«Инцидент безопасности» означает несанкционированный доступ к Клиентскому содержимому, ставший причиной нарушения конфиденциальности, целостности или доступности. Если Мы определяем, что Клиентское содержимое, которое находится под Нашим управлением, подверглось воздействию в результате Инцидента безопасности, Клиент будет уведомлен об этом в срок, требуемый по закону. В своем уведомлении Мы опишем, если известно, характер инцидента, период времени и возможные последствия для Клиента.

Мы ведем записи обо всех Инцидентах безопасности.

12. Управление поставщиками

Для предоставления Услуг Cloud Software Group может пользоваться услугами субподрядчиков и агентов. Всем субподрядчикам и агентам доступ к Клиентскому содержимому должен предоставляться, только если это необходимо для предоставления Услуг. Субподрядчики и агенты должны заключать письменные соглашения, по которым от них требуется обеспечение уровня защиты данных не меньше установленного в настоящем Приложении, если применимо. Мы постоянно несем ответственность за соответствие своих субподрядчиков и агентов условиям Соглашения, если применимо. Список дополнительных обработчиков данных Cloud Software Group, у которых может быть доступ к Клиентскому содержимому, можно найти в Нашем центре управления безопасностью.

12.1 Начало работы с подрядчиками

В Нашей программе контроля угроз сторонних организаций представлен системный подход к управлению угрозами безопасности, которые возникают при работе со сторонними поставщиками. Мы работаем над определением, анализом и сведением к минимуму угроз безопасности, прежде чем приступить к закупкам у таких сторонних компаний.

Cloud Software Group заключает соглашения с поставщиками для документации надлежащих мер безопасности и обязательств, соответствующих тем, что указаны в настоящем Приложении.

12.2 Непрерывная оценка

Мы периодически осуществляем оценку угроз безопасности, чтобы меры безопасности постоянно применялись в ходе взаимодействия с поставщиками. В случае изменения предоставляемых услуг или существующих договоров требуется провести оценку угроз безопасности, чтобы убедиться, что изменения не несут дополнительные или чрезмерные угрозы.

12.3 Окончание работы с подрядчиками

Мы стремимся уведомлять отдел компании, занимающийся материально-техническим обеспечением, как минимум за 90 дней до планируемой даты завершения сотрудничества или завершения срока действия договора с поставщиком (если прекратить отношения с ним не требуется ранее). Организация, занимающаяся материально-техническим обеспечением, координирует окончание сотрудничества, чтобы убедиться в том, что Наши корпоративные данные и активы в безопасности и обрабатываются надлежащим образом.

13. Соответствие требованиям

13.1 Обращение с персональными данными

Персональные данные — это информация, относящаяся к идентифицированному или идентифицируемому лицу. Вы определяете персональные данные, которые входят в Клиентское содержимое. Во время предоставления Услуг Мы выступаем в качестве обработчика данных, а Вы остаетесь контролером всех персональных данных, входящих в Клиентское содержимое. Мы будем действовать в соответствии с Вашими инструкциями в отношении обработки таких персональных данных, как указано в Соглашении.

Дальнейшие сведения об обработке персональных данных в соответствии с Общим регламентом по защите данных, в том числе о механизмах, используемых для международной передачи таких данных, представлены в Дополнительном Соглашении об обработке данных Cloud Software Group.

13.2 Расположение услуг

Клиенты Облачных услуг могут выбирать географическое расположение среды Облачных услуг. В ходе действия подписки на Облачные услуги Мы не будем менять географическое расположение среды, выбранное Вами, без Вашего согласия. Обратите внимание: для некоторых Облачных услуг выбор определенных географических расположений может не предоставляться, и в рамках общего предоставления Услуг Клиентское содержимое может передаваться в США или другие страны, где работает компания Citrix и (или) ее поставщики услуг, если это необходимо для

предоставления Услуг.

13.3 Раскрытие Клиентского содержимого

Мы можем раскрывать Клиентское содержимое в объеме, предусмотренном законом, в том числе в ответ на судебный запрос, судебное решение, административное постановление или иной нормативный акт, имеющий обязательную силу (далее каждый из вариантов — «Требование»). За исключением случаев, когда это запрещено законом, Мы незамедлительно уведомим Вас о любом Требовании и предоставим Вам помощь, обоснованно необходимую для своевременного ответа на Требование.

13.4 Безопасность клиентов и нормативные требования

Услуги предназначены для использования в более крупной ИТ-среде Клиентов, поэтому Клиенты несут полную ответственность за все аспекты безопасности, которые не контролируются компанией Citrix явным образом, в частности за техническую интеграцию с Услугами, за управление доступом пользователей и предназначенные для этого элементы и за все приложения и сети, которые Клиенты могут использовать вместе с Услугами.

Вы обязаны сами определить, распространяются ли на использование Вами Услуг, в том числе на предоставление Нам доступа к Клиентскому содержимому в рамках Услуг, какие-либо нормативные требования или требования к безопасности помимо тех, что указаны в Соглашении, в том числе в настоящем Приложении. В связи с этим Клиенты не должны отправлять или хранить какое-либо Клиентское содержимое, подпадающее под действие законов, которые предусматривают конкретные элементы управления, не указанные в настоящем Приложении (к таким законам могут относиться, например, Международные правила торговли оружием США или аналогичные нормативные требования любой страны, которая запрещает импорт или экспорт предметов военного снабжения или услуг в сфере обороны), защищенную медицинскую информацию, информацию о платежных картах или данные с контролируемым распространением в соответствии с постановлениями правительства, если иное не указано в Соглашении и применимом Описании Услуг и стороны заранее не заключили дополнительные соглашения (например, Соглашение с деловым партнером HIPAA), дающие право компании Citrix обрабатывать такие данные.

14. Аудит и запросы Клиентов

Cloud Software Group будет не чаще одного раза в год отвечать на запросы аудита. Таким ответом будет считаться ответ на оценки угроз Клиента. Клиенты также могут в любое время получить доступ к Нашему пакету комплексной проверки для ознакомления с актуальным пакетом безопасности и анкетой. Наш пакет комплексной проверки был создан для запросов клиентов, связанных с безопасностью. В нем можно легко найти необходимую информацию по безопасности, включая заполненную анкету для сбора стандартизированной информации для общих оценок (Shared Assessments' Standardized Information Gathering, SIG), версия Lite, для Наших Облачных услуг. Пакет комплексной проверки можно загрузить из Нашего центра управления безопасностью, раздел «Защита и безопасность данных Cloud Assurance».

15. Контакты

Функция	Контактные данные
Служба поддержки	https://www.citrix.com/contact/technical-support.html
Сообщение об Инциденте безопасности Подозрение на уязвимость в Наших Услугах	secure@citrix.com https://www.citrix.com/about/trust-center/ (нажмите на кнопку «Сообщить об Инциденте безопасности»).

Корпоративные продажи
Северная Америка | 800-424-8749 Другие страны | +1 408-790-8000

Местонахождение
Штаб-квартира корпорации | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States (США) Силиконовая долина | 4988 Great America Parkway Santa Clara, CA 95054, United States (США)