Последняя редакция: 1 марта 2018 г.

Приложение о безопасности служб Citrix

В этом Приложении о безопасности служб Citrix (далее — «Приложение») описаны технические и организационные меры по контролю безопасности, применяемые в связи с использованием служб Citrix Cloud, услуг по технической поддержке или консультационных услуг компании Citrix по ее лицензии, подписке или заключенному с ней соглашению об обслуживании. Это Приложение включается в подобные соглашения об обслуживании (далее — «Соглашения») посредством ссылки. Приложение не применяется к службам бета-версии или версий Lab и Tech Preview, включая Citrix Cloud Labs.
Терминам, написанным с заглавной буквы, присваивается значение, указанное в Соглашении или этом документе, в том числе в приведенной ниже статье 7 «Определения».

Статья 1. Меры Citrix по контролю безопасности

В этой статье описаны физические, логические и административные меры по контролю, которые Citrix применяет для обеспечения безопасности Служб и выполнения связанных с ними обязательств Заказчика в отношении безопасности. Основа действующей в Citrix программы безопасности Служб — стандарт ISO/IEC 27002.

Меры по контролю, указанные в статье 1.А, применяются ко всем Службам. Дополнительные меры по контролю, указанные в разделе 1.Б, применяются ко всем общедоступным службам Citrix Cloud Service (в совокупности — «Облачные службы»).

Citrix оставляет за собой право изменять меры по контролю, указанные в статье 1, при условии, что меры, применяемые во время срока обслуживания, оплаченного Заказчиком, обеспечивают по крайней мере такой же уровень безопасности Содержимого заказчика, как меры, указанные в статье 1 на момент начала такого срока.

1.А. Корпоративные меры по контролю безопасности: все Службы

Область	Меры по контролю
Управление программой безопасности	**Ответственность за безопасность**. Компания Citrix назначила одного или нескольких сотрудников по вопросам безопасности, которые отвечают за координацию и мониторинг мер по контролю безопасности Служб. **Роли и обязанности в сфере безопасности**. Персонал Citrix, обладающий доступом к Содержимому заказчика, должен соблюдать обязательства по конфиденциальности.

Область	Меры по контролю
	Политики безопасности служб. В компании Citrix действует всеобъемлющая Концепция глобальной безопасности (Global Security Framework, GSF). Она содержит общие принципы безопасности и предосторожности, которые ввело и утвердило исполнительное руководство Citrix. В политиках четко и лаконично изложены требования к безопасности. Процесс или методологию выполнения требований политик определяют стандарты. Программа безопасности GSF регулярно проверяется и анализируется. Citrix постоянно составляет по программе GSF сводку, которую предоставляет заказчикам по их запросу. **Управление рисками, связанными с продуктами.** Citrix оценивает ключевые сферы риска, связанного со Службами, в частности определяет риски для конфиденциальности, проверяет открытый код и анализирует экспортный контроль (эти меры, применяемые в конкретных случаях, приведены только в качестве примера).
Управление активами	**Список активов**. Компания Citrix ведет список находящегося под своим управлением оборудования, с помощью которого обеспечивается работа Служб (далее — «Активы»). За то, чтобы по мере необходимости вести и обновлять этот список, отвечают установленные владельцы систем. **Обращение с активами и данными** Чтобы надлежащим образом ограничить доступ, Citrix определяет и классифицирует Содержимое заказчика. Citrix накладывает ограничения на печать Содержимого заказчика и утилизацию печатных материалов, в которых есть такое содержимое. Прежде чем сохранять Содержимое заказчика на портативных устройствах, получать к нему удаленный доступ или обрабатывать такое содержимое вне объектов, находящихся под управлением компании Citrix или ее поставщиков услуг, персонал Citrix должен получать разрешение.
Управление доступом	**Политика доступа.** Citrix ведет учет прав в сфере безопасности, выдаваемых лицам, у которых есть доступ к Содержимому заказчика, и следует принципу минимальных прав. **Авторизация доступа** Citrix ведет учет персонала, которому разрешено получать доступ к системам Citrix с Содержимым заказчика, и обновляет соответствующую информацию. Прежде чем предоставлять доступ к системам новым пользователям, руководство должно проверять и утверждать их. Citrix регулярно проверяет учетные записи пользователей и назначенные разрешения

Область	Меры по контролю
	для ключевых систем. Citrix определяет сотрудников, которые могут предоставлять, изменять или отменять авторизованный доступ к данным и ресурсам. Citrix гарантирует, что в ситуациях, в которых доступ к системам с Содержимым заказчика должны получать несколько лиц, им выдаются отдельные идентификаторы и данные для входа. **Принцип минимальных прав** Citrix предоставляет доступ к Содержимому заказчика только тем лицам, которым это необходимо для выполнения должностных обязанностей. **Целостность и конфиденциальность** Citrix требует, чтобы пользователи защищали компьютеры и данные, когда оставляют их без присмотра. Citrix требует, чтобы пароли оставались неразборчивыми на протяжении всего их жизненного цикла. **Проверка подлинности** Чтобы определять пользователей, получающих доступ к информационным системам, и проверять подлинность этих пользователей, Citrix применяет стандартные в отрасли методы. Если механизмы проверки подлинности основаны на паролях, Citrix применяет стандартные в отрасли методы по обращению с паролями и управлению ими, в том числе следующие: пароли регулярно обновляются в соответствии с требованиями систем и стандартами Citrix; пароли должны отвечать требованиям к длине и сложности, в том числе содержать минимум 8 символов; сотрудникам запрещено передавать пароли другим лицам; деактивированные или просроченные идентификаторы не предоставляются другим лицам.

Область	Меры по контролю
	В Citrix действуют процедуры по деактивации искаженных или непреднамеренно разглашенных паролей. Citrix отслеживает многократные попытки получить доступ к Службам с помощью недопустимого пароля. Citrix использует методы по поддержанию конфиденциальности и целостности паролей во время их назначения, распространения и хранения.
Предотвращение потери	**Вредоносные программы**. Чтобы не давать вредоносным программам, в том числе тем из них, которые происходят из общедоступных сетей, получать несанкционированный доступ к Содержимому заказчика, Citrix использует антивирусное ПО. **Утилизация носителей.** Citrix утилизирует носители, когда они становятся ненужными. Это делается на основе классификации и с помощью процедур безопасного удаления.
Физическая безопасность и безопасность сред (управление доступом и доступностью)	**Физический доступ к объектам Citrix**. Citrix допускает на объекты только лиц с соответствующим разрешением. Когда сотрудники, подрядчики и гости находятся на объекте, они обязаны носить идентификационные карточки, которые должны быть всегда видны. Citrix наблюдает за точками входа на объекты с помощью различных методов, включая службу охраны, средства обнаружения вторжений и камеры видеонаблюдения. **Защита от прерывания работы**. Citrix использует системы защиты от потери данных, которая может произойти из-за сбоя источника питания или помех на линиях, в том числе глобальную избыточную инфраструктуру обслуживания, предусматривающую наличие площадок для аварийного восстановления; оценивает центры обработки данных и поставщиков услуг Интернета, чтобы оптимизировать производительность с точки зрения пропускной способности, задержки и изоляции при аварийном восстановлении; размещает центры обработки данных на безопасных объектах, которые не зависят от поставщиков услуг Интернета и обеспечивают физическую безопасность, избыточное питание и избыточность инфраструктуры; заключает соглашения о времени доступности с ключевыми поставщиками. **Центры обработки данных, размещенные у третьих лиц.** Если компания Citrix предоставляет Службы с помощью совместно размещенных сторонних центров обработки данных, она требует от поставщика услуг, чтобы у него действовали такие же или более строгие требования к физической безопасности и безопасности сред, как на объектах, находящихся под управлением Citrix. Вот некоторые минимальные требования к безопасности: • наличие средств ограничения физического доступа и соответствующих

Область	Меры по контролю
	предупредительных мер (проверка подлинности, журналы, мониторинг и т. д.); • надлежащее разделение сред; • наличие механизмов подавления, обнаружения и предотвращения пожаров; • наличие систем климат-контроля (температуры, влажности и т. д.). **Облачные вычисления.** Если компания Citrix предоставляет Службы с помощью подхода «Все как услуга» (Anything as a Service, Xaas), включающего в себя модели «Инфраструктура как услуга» (Infrastructure as a Service, IaaS), «Платформа как услуга» (Platform as a Service, PaaS) и «Программное обеспечение как услуга» (Software as a Service, SaaS), она заключает контракты с поставщиками XaaS, которые обеспечивают в значительной степени аналогичный контроль физического доступа к размещенным у них центрам обработки данных.
Безопасность приложений и разработки	**Разработка и обслуживание систем.** В Citrix применяется процесс, основанный на подходе Secure by Design («Безопасность заложена в проект»). Он включает в себя стандарты и процедуры управления изменениями, призванные помочь выполнить требования к безопасности, которые охватывают информационные системы, проверку и тестирование кода, а также использование данных тестирования. Управлением этим процессом и наблюдением за ним занимается специализированная команда инженеров в области безопасности, которая также отвечает за анализ проектов, моделирование угроз, ручную и выборочную проверку кода, выполнение тестов на проникновение. **Управление открытым кодом**. Чтобы управлять проверками и утверждениями открытого кода, Citrix использует программную систему. В дополнение к этому Citrix периодически подвергает свое программное обеспечение проверкам и аудитам, в ходе которых выясняется, насколько оно соответствует требованиям в области открытого кода. **Управление изменениями.** В Citrix применяются процедуры управления изменениями, призванные помочь выполнить требования к безопасности, которые охватывают информационные системы, тестирование, приемку его результатов и использование его данных. Citrix управляет изменениями в программном обеспечении и конфигурации, а также отслеживает их с помощью стандартных систем тикетинга.
Безопасные операции	**Архитектура сетей**. В Citrix внедрены механизмы, с помощью которых по отношению ко всем Службам принудительно применяются политики и стандарты управления доступом, в том числе элементы управления сетями, контролирующие доступ к Содержимому заказчика. В зависимости от обстоятельств к таким механизмам относятся настройка между Интернетом и внутренней сетью промежуточной недоверенной зоны,

Область	Меры по контролю
	содержащей механизм безопасности для ограничения доступа и несанкционированного трафика, и отделение веб-серверов и серверов приложений от соответствующих серверов баз данных в многоуровневой структуре, ограничивающей трафик между уровнями.
Управление инцидентами	**Реагирование на инциденты**. В Citrix действует программа реагирования на инциденты, цель которой — сдерживать, анализировать и устранять инциденты в области безопасности, затрагивающие находящиеся под управлением Citrix сети и (или) системы либо Содержимое заказчика, а также сообщать о таких инцидентах. **Уведомление об инцидентах**. Если компания Citrix установит, что находящееся в ее ведении Содержимое заказчика затронул Инцидент в области безопасности, Заказчик будет уведомлен об этом в течение срока, установленного применимым правом. **Учет инцидентов**. Citrix ведет учет известных Инцидентов в области безопасности с фиксацией описания, срока и последствий инцидента, имен сообщившего о нем лица и лица, которому поступило сообщение об инциденте, а также процедуры восстановления данных и Служб в зависимости от обстоятельств.
Управление поставщиками	**Допуск к обработке содержимого**. Citrix оценивает надежность поставщиков услуг, которые будут иметь доступ к Содержимому заказчика и (или) обрабатывающим его компонентам Служб. Citrix требует от поставщиков услуг, связанных со Службами, соблюдать описанный в этом разделе уровень безопасности применительно к услугам, которые они предоставляют. Поставщики услуг с правом доступа к Содержимому заказчика, на которое распространяется законодательство Европейского Союза, обязаны самостоятельно проходить сертификацию на соответствие требованиям программ Privacy Shield, действующих в отношениях ЕС-США и ЕС-Швейцария, или подписывать Стандартные договорные условия. **Текущее обслуживание.** Поставщики услуг периодически оцениваются в зависимости от степени конфиденциальности и риска, связанной с их услугами. **Отмена допуска к обработке содержимого.** После прекращения отношений с поставщиком услуг он обязан вернуть все находившееся в его владении Содержимое заказчика или подтвердить безопасное уничтожение всего такого содержимого.
Непрерывность бизнес-процессов и аварийное восстановление	**Непрерывность бизнес-процессов.** В компании Citrix для объектов, на которых расположены ее информационные системы, обрабатывающие Содержимое заказчика, предусмотрены планы на случай чрезвычайных и непредвиденных обстоятельств.

Область	Меры по контролю
	Аварийное восстановление. Избыточное хранилище Citrix и его процедуры восстановления данных спроектированы так, чтобы пытаться воссоздать Содержимое заказчика в его исходном состоянии или состоянии, актуальном на момент последней репликации.
Обязательства Заказчика в области безопасности	Заказчик отвечает за управление аспектами безопасности, которые не включены явным образом в Службы. В частности, в сферу ответственности Заказчика входит следующее: • предоставлять Citrix доступ только к тому Содержимому заказчика, без которого Заказчик не сможет получать Службы; • защищать свою сеть и компоненты служб от вмешательства, в том числе отслеживать и свои сети и вычислительное оборудование и обеспечивать их безопасность; • загружать при необходимости Содержимое заказчика как во время получения Служб, так и после завершения этого срока. • Citrix либо шифрует передаваемые данные по умолчанию, либо предлагает заказчикам предназначенные для этого средства. Подробную информацию можно найти в документации по Службам. Заказчик отвечает за то, чтобы во время передачи данные были защищены надлежащим образом.

1.Б. Дополнительные меры по контролю безопасности облачных служб

Область	Меры по контролю
Защита данных (управление доступностью и передачей, удаление данных)	**Процедуры обработки отказа**. В Citrix внедрены механизмы, предотвращающие утрату доступности Содержимого заказчика. В частности, копии Содержимого заказчика хранятся не в том же месте, в котором расположено основное компьютерное оборудование, обрабатывающее это содержимое. **Данные, передаваемые за пределами внутренних сетей**. Citrix шифрует Содержимое заказчика, передаваемое по общедоступным сетям, которые входят в Службу, или предоставляет Заказчику средства для такого шифрования. **Удержание.** Если это требуется в юридических целях, Citrix может удерживать Содержимое заказчика после срока предоставления Служб, помещая это содержимое в архив, к которому у Заказчика есть доступ. Citrix будет выполнять требования этого Приложения до тех пор, пока такое Содержимое заказчика не будет окончательно удалено. С учетом следующего пункта «Возврат» компания Citrix не обязана удерживать Содержимое заказчика после прекращения предоставления Служб. **Возврат.** С учетом доступности и соответствующего Описания служб Заказчику предоставляется 30 (тридцать) дней для загрузки Содержимого заказчика после

Область	Меры по контролю
	прекращения предоставления Служб. **Удаление данных**. Citrix безопасно удалит Содержимое заказчика, если оно больше не будет нужно для законной цели.
Безопасные операции	**Ведение журналов событий**. В определенных Службах Citrix собирает Журналы. Журналы могут содержать идентификатор и время доступа, информацию о предоставлении полномочий или отказе в этом, диагностические данные, такие как файлы трассировки и аварийного завершения работы, и сведения о других соответствующих действиях. Журналы используются (**i**) для предоставления, защиты и улучшения Служб и связанных с ними аналитических данных, а также для управления Службами и связанными с ними аналитическими данными и измерения соответствующих показателей, (**ii**) согласно указаниям Заказчика и (или) его Пользователей, (**iii**) для соблюдения политик Citrix, применимого права, нормативно-правового акта или запроса государственных органов. Это может включать в себя мониторинг производительности, стабильности, использования и безопасности Служб и связанных с ними компонентов. Заказчик не должен блокировать эти мероприятия по мониторингу или вмешиваться в них. В указанных выше целях Citrix может дополнять Журналы информацией, собранной у сторонних производителей. Журналы могут использоваться в целях, не указанных в этом Приложении, только в совокупной форме.
Непрерывность бизнес-процессов и аварийное восстановление	**Резервные копии.** Если в соответствующем Описании служб не указано иное, Службы содержатся в активно-активных кластерах с высоким уровнем доступности, распределенных по нескольким физическим объектам. Для систем, не находящихся в активно-активной конфигурации, в соответствии с Целями уровней обслуживания конкретной Службы создаются резервные копии.

Статья 2. **<u>Обращение с персональными данными</u>**

Персональные данные — это информация о человеке, личность которого уже установлена или может быть установлена. Заказчик определяет персональные данные, которые включает в свое Содержимое. Когда обеспечивается работа Служб, в отношении персональных данных, содержащихся в Содержимом заказчика, Citrix действует как обработчик, а Заказчик остается управляющим. В том, что касается обработки таких персональных данных, Citrix будет действовать по указаниям Заказчика согласно условиям Соглашения.

Подробная информация об обращении с персональными данными, на которые распространяется Общий регламент по защите данных, в том числе о механизмах, применяемых для международной передачи таких данных, приведена в Приложении I «Условия Общего регламента по защите данных».

Статья 3. **Расположение Служб**

Содержимое заказчика может передаваться в Соединенные Штаты, храниться и (или) обрабатываться в них. Также в это могут быть вовлечены другие страны, в которых компания Citrix и (или) ее поставщики услуг ведут деятельность. Требования этого Приложения продолжают применяться, где бы компания Citrix ни хранила или ни обрабатывала Содержимое заказчика.

Стороны могут в духе доброй воли вести переговоры о заключении дополнительных соглашений об обработке или передаче данных, если такие соглашения нужны для облегчения законной международной передачи данных в связи с предоставлением Служб со стороны Citrix.

Статья 4. **Разглашение Содержимого заказчика**

Заказчик соглашается, что Citrix будет разглашать его Содержимое согласно условиям этого раздела. Чтобы обеспечивать работу Служб, Citrix может привлекать субподрядчиков и агентов. Сообразно обстоятельствам любые субподрядчики и агенты получают право на доступ к Содержимому только в той мере, в которой он необходим для обеспечения работы Служб, и должны нести обязательства по письменным соглашениям, предписывающим защищать данные минимум на уровне, который требуется от Citrix в этом Приложении. Компания Citrix продолжает всегда отвечать за то, чтобы ее субподрядчики и агенты соблюдали условия Соглашения в установленном порядке.

Компания Citrix также может разглашать Содержимое заказчика (а) аффилированным организациям в целях, не противоречащих Соглашению; (б) в связи с такими ожидаемыми или фактическими событиями, как слияние, приобретение, продажа, банкротство или другая частичная либо полная реорганизация своего бизнеса, причем в ходе этого компания Citrix обязана защищать Содержимое заказчика согласно условиям Соглашения; (в) в юридических целях, в том числе для принудительной реализации своих прав, обнаружения и предотвращения мошенничества, защиты от ущерба правам или имуществу Citrix, Заказчиков, Пользователей или общественности; (в) в соответствии с требованиями законов, в частности в ответ на повестку с вызовом в суд, судебное или административное постановление либо другое предписание с юридической силой (каждое из них — «Требование»). Если того не запрещает законодательство, Citrix будет оперативно уведомлять Заказчика о каких-либо Требованиях и оказывать ему необходимую в разумных пределах помощь, чтобы Заказчик своевременно отреагировал на Требование.

Статья 5. **Обязательства Заказчика**

1. Общие. Заказчик может использовать Службы и получать к ним доступ только в порядке, разрешенном в Соглашении. Заказчик должен соблюдать все законы, применимые к нему в связи с использованием им Служб.

2. Разрешения. Заказчик отвечает за получение всех разрешений, которые нужны компании Citrix для обеспечения работы Служб, в том числе за предоставление всех уведомлений и обретение подтверждений согласия или лицензий, необходимых компании Citrix для осуществления доступа к Содержимому заказчика и его обработки согласно условиям этого Приложения.

3. Нормативно-правовое соответствие. Заказчик отвечает за определение того, распространяются ли на какое-либо его Содержимое дополнительные требования в области нормативно-правого соответствия или безопасности, кроме тех, что указаны в Соглашении, в том числе в этом Приложении. Заказчик обязуется не

отправлять и не хранить в каких-либо Службах какое бы то ни было свое Содержимое, порядок использования которого регулируют руководство по международной торговле оружием правительства США (US International Traffic in Arms Regulations, ITAR) или аналогичные правила какой-либо другой страны, ограничивающей импорт либо экспорт предметов военного снабжения или оборонных услуг. Кроме того, Заказчик не должен предоставлять или хранить какое-либо свое Содержимое, на которое распространяются дополнительные нормативно-правовые требования, в частности защищенную медицинскую информацию (Protected Health Information, PHI), информацию о платежных картах (Payment Card Information, PCI) или данные, распространение которых контролируют нормативно-правовые акты государственных органов, если это не указано в Заказе Заказчика и применимом Описании службы и стороны не заключают заранее дополнительных соглашений (таких как Соглашение с деловым партнером (Business Associate Agreement, BAA)), которые могут требоваться для того, чтобы компания Citrix обрабатывала такие данные. Чтобы запросить соглашение BAA, Заказчики службы ShareFile могут обратиться в Citrix, воспользовавшись адресом privacy@sharefile.com.

4. Среда безопасности Заказчика. Службы рассчитаны на предоставление исключительно в рамках более обширной среды безопасности Заказчика. Заказчик должен обеспечивать наличие надлежащих функций безопасности для всех компонентов, которыми прямо не управляет компания Citrix, включая, помимо прочего, средства управления доступом, брандмауэры, приложения и сети, используемые в сочетании со Службами. См. пункт «Обязательства Заказчика в области безопасности» раздела 1.A. выше.

5. Уведомление по вопросам безопасности. Заказчик отвечает за оперативное уведомление компании Citrix о любых инцидентах в области безопасности, в которые вовлечены Службы и (или) его Содержимое, в соответствии с приведенной ниже статьей VI «Контакты Citrix».

6. Соблюдение условий Пользователями. Заказчик отвечает за то, чтобы его Пользователи соблюдали условия Заказа и Соглашения.

Статья 6. Контакты Citrix

ФУНКЦИЯ	КОНТАКТ
Служба поддержки	https://www.citrix.com/contact/technical-support.html
Сообщение об инциденте	secure@citrix.com
Подозрение о наличии в продуктах Citrix уязвимостей	secure@citrix.com

Статья 7. Определения терминов

Значение терминов, написанных в этом Приложении с заглавной буквы, указано в Соглашении или ниже. Если между оставшимися терминами Соглашения и любым из приведенных ниже определений есть противоречие, к этому Приложению применяется приведенное ниже определение.

Содержимое заказчика — любые данные, отправленные в учетную запись Заказчика для хранения, или данные в вычислительной среде Заказчика, к которой компании Citrix предоставляется доступ для обеспечения работы Служб.

Журнал — записанные данные о событиях, связанных со Службами, в том числе записи с измеренными показателями производительности, стабильности, использования, безопасности и поддержки.

Инцидент в области безопасности — несанкционированный доступ к Содержимому заказчика, влекущий за собой утерю конфиденциальности, целостности или доступности.