K2 CLOUD

Матрица разделения ответственности

за защиту персональных данных, согласно требованиям Приказа ФСТЭК № 21 от 18 февраля 2013 г, между облачной платформой K2 Cloud и пользователями

2025

Оглавление

1 Назначение документа

Настоящий документ является приложением к договору об оказании услуг между K2 Cloud и пользователями, обрабатывающими персональные данные в информационных системах персональных данных (ИСПДн) в соответствии с №152-ФЗ «О персональных данных» от 27 июля 2006 г (152-ФЗ).

В отношении данной категории пользователей данная Матрица действует по умолчанию, если сторонами не было проведено уточнение документа, согласно разделу 3 настоящего документа. K2 Cloud и пользователи, упоминаемые далее вместе или по отдельности, именуются «стороны» («сторона»).

Матрица устанавливает разделение зон ответственности за выполнение мер по защите персональных данных, предусмотренных Приказом ФСТЭК России от 18 февраля 2013 г. № 21 (Приказ ФСТЭК №21).

2 Статус соответствия K2 Cloud

K2 Cloud, включая: облачную платформу, сетевую инфраструктуру и платформенные сервисы, а также поддерживающие указанные объекты информатизации:

- процессы защиты информации;
- систему организации и управления защитой;

Соответствуют требованиям к первому уровню защищенности (УЗ-1) обрабатываемых персональных данных, согласно требованиям Приказа ФСТЭК №21. Аттестат соответствия публикуется на официальном сайте K2 Cloud: https://k2.cloud/.

3 Принципы внесения изменений в документ

Содержимое документа может уточняться, если в процессе заключения договора стороны, на основании моделирования угроз, инициированного пользователем и проводимого в соответствии с действующими методиками ФСТЭК России, произвели адаптацию (уточнение), исключение и/или дополнение базового набора мер защиты с учетом:

- актуальных нарушителей безопасности персональных данных;
- структурно-функциональных характеристик объектов информатизации (в том числе автоматизированных систем и приложений);
- используемых информационных технологий;
- иных требований, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации.

После внесения соответствующих изменений и согласования сторон актуальная форма Матрицы должна быть зафиксирована в измененном документе, в качестве приложения к договору между конкретным пользователем, ответственным за проведенное моделирование угроз, и K2 Cloud.

4 Общие принципы разделения зон ответственности

Состав требований, реализуемых K2 Cloud и описание разделения зон ответственности зафиксированы в Приложении 1 к настоящему документу. Общие принципы разделения зон ответственности включают в себя

Со стороны K2 Cloud:

- прохождение процедуры подтверждения соответствия требованиям 152-ФЗ не реже одного раза в два года;
- обеспечение выбора необходимых защитных мер, включенных в систему защиты информации K2 Cloud на основании базового набора мер защиты первого уровня защищенности, согласно Приказу ФСТЭК №21;
- обеспечение полноты и качества реализации мер системы защиты персональных данных на основании базового набора мер защиты первого уровня защищенности, согласно Приказу ФСТЭК №21.

Со стороны Пользователя:

- корректное включение сегментов облака, объектов информатизации и иных сервисов облака, выделенных пользователю на основании договора с K2 Cloud в контур безопасности организации (или принятие решения о выделении облачной инфраструктуры, размещенной в K2 Cloud, в отдельный контур безопасности организации);
- выполнение всех применимых требований регуляторов, включая требования 152-ФЗ, в том числе о прохождении аттестации соответствия требованиям Приказа ФСТЭК №21;
- обеспечение выбора необходимых защитных мер, включенных в систему защиты информации пользователя, на основании базового набора мер защиты, в соответствии с установленным для пользователя уровнем защищенности (определяется Постановлением Правительства РФ от 1 ноября 2012 г. № 1119);
- обеспечение полноты и качества реализации мер системы защиты персональных данных на основании базового набора мер защиты Приказа ФСТЭК №21, в соответствии с установленным для пользователя уровнем защищенности (определяется Постановлением Правительства РФ от 1 ноября 2012 г. № 1119).

До внесения изменений в Матрицу по инициативе конкретного пользователя между сторонами действует схема разделения зон ответственности по модели «инфраструктура как услуга», согласно методическому документу ФСТЭК России «Методика оценки угроз безопасности информации» от 05.02.2021. Пользователь отвечает за уровни «Оператора», K2 Cloud за уровни «Поставщика услуг».

Рис. 1 – Схема разделения зон ответственности

5 Аутсорсинг информационной безопасности K2 Cloud

По согласованию сторон конкретные меры защиты, находящиеся в зоне ответственности пользователя (например, связанные с мониторингом событий и реагированием на инциденты защиты информации на уровне виртуальных машин пользователя в его контуре безопасности) могут быть реализованы с привлечением K2 Cloud. В этом случае в Матрицу вносятся изменения, согласно принципам, зафиксированным в разделе 3 настоящего документа. Дополнительно в Приложение 1 может быть отдельной таблицей включен перечень требований, в отношении которых было проведено изменение зон ответственности, в связи с их передачей на аутсорсинг K2 Cloud.

6 Дополнительная информация

Некоторые защитные меры пользователь может реализовать с помощью сервисов K2 Cloud, актуальные сведения по которым описаны в документации: https://docs.k2.cloud. Наиболее востребованными такими сервисами являются:

- шаблоны запуска;
- Auto Scaling;
- виртуальные частные облака (VPC);
- подсети;
- группы безопасности;
- ACL;
- резервное копирование;
- внешние сети;
- VPN-соединения;
- мониторинг;
- журнал действий;
- IAM.

При обращении пользователя на портале поддержки https://support.k2.cloud или по электронной почте support@k2.cloud возможно включить дополнительные политики безопасности. На момент публикации данного документа к ним относятся:

- требование смены пароля для учетной записи пользователя K2 Cloud не реже чем каждые 60 дней;
- автоматическая блокировка учетной записи пользователя K2 Cloud при его неактивности в течение 45 дней.

Приложение 1.

Состав мер по обеспечению безопасности персональных данных, реализуемых K2 Cloud и описание разделения зон ответственности [1]

Мера	Содержание меры	Ответственность K2 Cloud	Ответственность Пользователя
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора.	На уровне: • физического оборудования K2 Cloud; • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств; • сервисов K2 Cloud.	На уровне клиентских виртуальных машин.
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных.	На уровне физического оборудования K2 Cloud.	Не применимо.
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов.	На уровне: • физического оборудования K2 Cloud; • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств; • сервисов K2 Cloud.	На уровне клиентских виртуальных машин.
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.		
ИАФ.5	Защита обратной связи при вводе аутентификационной информации.		
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).	На уровне доступа к сервисам K2 Cloud, предоставляемым клиентам.	На уровне клиентских виртуальных машин.

1 Состав мер по обеспечению безопасности персональных данных (в соответствии с требованиями Приказа ФСТЭК №21) и распределение зон ответственности, указанные в приложении, являются типовыми и применяются по умолчанию. При необходимости они могут быть изменены в соответствии с принципами, изложенными в разделе 3 Матрицы разделения ответственности между облачной платформой K2 Cloud и пользователями.

Мера	Содержание меры	Ответственность K2 Cloud	Ответственность Пользователя
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей.	На уровне: • физического оборудования K2 Cloud; • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств; • сервисов K2 Cloud.	На уровне клиентских виртуальных машин.
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа.		
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами.	Управление сетевым доступом на уровне: • физического оборудования K2 Cloud; • сервисных/служебных сетей K2 Cloud; • ограничение доступа между сегментами сетей различных клиентов K2 Cloud; • ограничение доступа из клиентских сетей в сервисную/служебную сеть.	Управление сетевым доступом: • между сегментами клиентской виртуальной сети; • сетевого доступа к клиентской виртуальной сети из-за ее пределов.
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.	На уровне: • физического оборудования K2 Cloud; • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств; • сервисов K2 Cloud.	На уровне клиентских виртуальных машин.
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.		
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).		
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу.		

Мера	Содержание меры	Ответственность K2 Cloud	Ответственность Пользователя
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации.	На уровне: • физического оборудования K2 Cloud; • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств; • сервисов K2 Cloud.	На уровне клиентских виртуальных машин.
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.	На уровне доступа: • пользователей к сервисам K2 Cloud; • административного доступа к физическим и виртуальным сервисным/служебным системным компонентам.	На уровне удаленного доступа к клиентским виртуальным серверам.
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа.	Не применяется.	Не применимо.
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств.	Не применяется.	Применимо при использовании в составе ИСПДн клиента мобильных технических средств.
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).	На уровне сервисных/служебных системных компонентов.	При организации такого взаимодействия с клиентскими виртуальными машинами.
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники.	На уровне сервисных/служебных системных компонентов.	Не применимо.
III. Ограничение программной среды (ОПС)			
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения.	На уровне: • физического оборудования K2 Cloud; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств.	На уровне клиентских виртуальных машин.

Мера	Содержание меры	Ответственность K2 Cloud	Ответственность Пользователя
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.	На уровне: • физического оборудования K2 Cloud; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств.	На уровне клиентских виртуальных машин.
IV. Защита машинных носителей персональных данных (ЗНИ)			
ЗНИ.1	Учет машинных носителей персональных данных.	На уровне физических носителей информации, применяемых в инфраструктуре K2 Cloud.	Не применимо.
ЗНИ.2	Управление доступом к машинным носителям персональных данных.		
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания.		
V. Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения.	На уровне: • сервисных/служебных системных компонентов; • сервисов K2 Cloud, в том числе клиентских действий по использованию сервисов.	На уровне клиентских виртуальных серверов и используемого на них программного обеспечения и средств защиты информации.
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.		
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.		
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.		
РСБ.7	Защита информации о событиях безопасности.		
VI. Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты.	На уровне: • сервисных/служебных серверов K2 Cloud. • АРМ эксплуатационного персонала.	На уровне клиентских виртуальных машин.

Мера	Содержание меры	Ответственность K2 Cloud	Ответственность Пользователя
АВ3.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов).	На уровне: • сервисных/служебных серверов K2 Cloud. • АРМ эксплуатационного персонала.	На уровне клиентских виртуальных машин.
VII. Обнаружение вторжений (СОВ)			
СОВ.1	Обнаружение вторжений.	На уровне: • физического оборудования K2 Cloud; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств.	На уровне клиентских сегментов сети.
СОВ.2	Обновление базы решающих правил.		
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)			
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей.	На уровне сервисных/служебных виртуальных и физических системных компонентов K2 Cloud.	На уровне клиентских виртуальных машин.
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации.		
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.		
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации.		
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе.		

Мера	Содержание меры	Ответственность K2 Cloud	Ответственность Пользователя
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)			
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.	На уровне: • физического оборудования K2 Cloud; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств.	На уровне клиентских виртуальных машин.
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).	Не применимо, так как в состав K2 Cloud не входит функционал по приему электронной почты.	На уровне клиентских почтовых серверов.
X. Обеспечение доступности персональных данных (ОДТ)			
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.	На уровне: • физического оборудования K2 Cloud; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств. • выполняется автоматизированная репликация данных в платформенном хранилище.	На уровне ИСПДн клиента резервное копирование и восстановление персональных данных осуществляется клиентом.
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных.		
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала.		

Мера	Содержание меры	Ответственность K2 Cloud	Ответственность Пользователя
XI. Защита среды виртуализации (ЗСВ)			
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.	На уровне: • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств; • сервисов K2 Cloud.	Не применимо.
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин.		На уровне клиентских виртуальных машин.
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре.		
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.	На уровне: • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств.	Реализовано на уровне архитектуры K2 Cloud.
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций.	На уровне: • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств.	На уровне клиентских виртуальных машин.
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры.		
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре.		
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей.	Управление сетевым доступом на уровне: • сервисных/служебных сетей K2 Cloud; • ограничения доступа между сегментами сетей различных клиентов K2 Cloud.	На уровне сегментов сети клиента.

Мера	Содержание меры	Ответственность K2 Cloud	Ответственность Пользователя
XII. Защита технических средств (ЗТС)			
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены.	На уровне обеспечения физической безопасности ЦОД.	Не применимо.
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.	На уровне АРМ эксплуатационного персонала.	На уровне АРМ эксплуатационного персонала ИСПДн клиента, в случае их использования.
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы.	На уровне: • физического оборудования K2 Cloud; • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств; • сервисов K2 Cloud.	На уровне клиентских виртуальных машин.
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.	На уровне каналов: • используемых для доступа администраторов к системным компонентам K2 Cloud; • используемых для доступа пользователей и администраторов к консоли управления средой виртуализации; • между ЦОД.	На уровне каналов связи, установленных клиентом для доступа к его виртуальным машинам.

Мера	Содержание меры	Ответственность K2 Cloud	Ответственность Пользователя
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов.	На уровне каналов: • используемых для доступа администраторов к системным компонентам K2 Cloud; • используемых для доступа пользователей и администраторов к консоли управления средой виртуализации; • между ЦОД.	На уровне сегментов сети клиента.
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных.	На уровне: • физического оборудования K2 Cloud; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств.	На уровне клиентских виртуальных машин.
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы.	На уровне сервисных/служебных сегментов сети.	На уровне сегментов виртуальной сети клиента.
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе.	Не применимо.	Не применимо.
XIV. Выявление инцидентов и реагирование на них (ИНЦ)			
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них.	Из числа сотрудников K2 Cloud или его подрядчиков.	Из числа сотрудников клиентской организации или ее подрядчиков.
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов.	На уровне: • физического оборудования K2 Cloud; • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств; • сервисов K2 Cloud.	На уровне клиентских виртуальных машин.
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами.		

Мера	Содержание меры	Ответственность K2 Cloud	Ответственность Пользователя
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий.	На уровне: • физического оборудования K2 Cloud; • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств; • сервисов K2 Cloud.	На уровне клиентских виртуальных машин.
ИНЦ.5	Принятие мер по устранению последствий инцидентов.		
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов.		
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)			
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных.	На уровне: • физического оборудования K2 Cloud; • средств управления средой виртуализации; • сервисных/служебных серверов K2 Cloud и прочих виртуальных устройств; • программного обеспечения K2 Cloud.	На уровне клиентской виртуальной инфраструктуры.
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных.		
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных.		
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных.		