K2 CLOUD

Матрица разделения ответственности

за информационную безопасность, согласно требованиям ГОСТ Р 57580.1-2017, 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, для которых актуальны требования ГОСТ Р 57580.1-2017. 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 требований базового набора мер защиты для усиленного уровня защиты (уровень 1), согласно ГОСТ Р 57580.1-2017, обязательному для выполнения финансовыми организациями, включая кредитные организации, некредитные финансовые организации и субъекты национальной платежной системы, на основании нормативно-правовых актов Банка России в области защиты информации.

2 Статус соответствия K2 Cloud

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

- процессы защиты информации (раздел 7 ГОСТ Р 57580.1-2017);
- систему организации и управления защитой информации (раздел 8 ГОСТ Р 57580.1-2017);
- жизненный цикл разрабатываемых автоматизированных систем и приложений (раздел 9 ГОСТ Р 57580.1-2017)

Соответствуют требованиям к усиленному уровню защиты (уровень 1), согласно ГОСТ Р 57580.2-2018. Подробные результаты оценки соответствия фиксируются в актуальном заключении по результатам оценки соответствия, публикуемом 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 информации финансовой организации;
- 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 ежегодной оценки соответствия выделенного контура безопасности K2 Cloud, в соответствии с ГОСТ Р 57580.2-2018 для поддержания соответствия требованиям к усиленному уровню защиты (1 уровень);
- обеспечение выбора необходимых защитных мер, включенных в систему защиты информации K2 Cloud на основании базового набора мер защиты усиленного уровня, согласно ГОСТ Р 57580.1-2017;
- обеспечение полноты и качества реализации процессов системы защиты и направлений системы организации и управления защитой информации, а также безопасности жизненного цикла, автоматизированной системы K2 Cloud, на основании базового набора мер защиты усиленного уровня, согласно ГОСТ Р 57580.1-2017.

Со стороны Пользователя:

- корректное включение сегментов облака, объектов информатизации и иных сервисов облака, выделенных пользователю на основании договора с K2 Cloud в контур безопасности финансовой организации (или принятие решения о выделении облачной инфраструктуры, размещенной в K2 Cloud, в отдельный контур безопасности финансовой организации);
- выполнение всех применимых требований регуляторов, включая требования Банка России к защите информации, в том числе о прохождении независимой оценки соответствия, согласно ГОСТ Р 57580.2-2018;
- обеспечение выбора необходимых защитных мер, включенных в систему защиты информации пользователя, на основании базового набора мер защиты, согласно установленного для пользователя уровня защиты (определяется согласно нормативно-правовым актам Банка России в области защиты информации);
- обеспечение полноты и качества реализации процессов системы защиты и направлений системы организации и управления защитой информации, а также безопасности жизненного цикла, автоматизированной системы пользователя, согласно установленного для пользователя уровня защиты (определяется согласно нормативно-правовым актам Банка России в области защиты информации).

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».

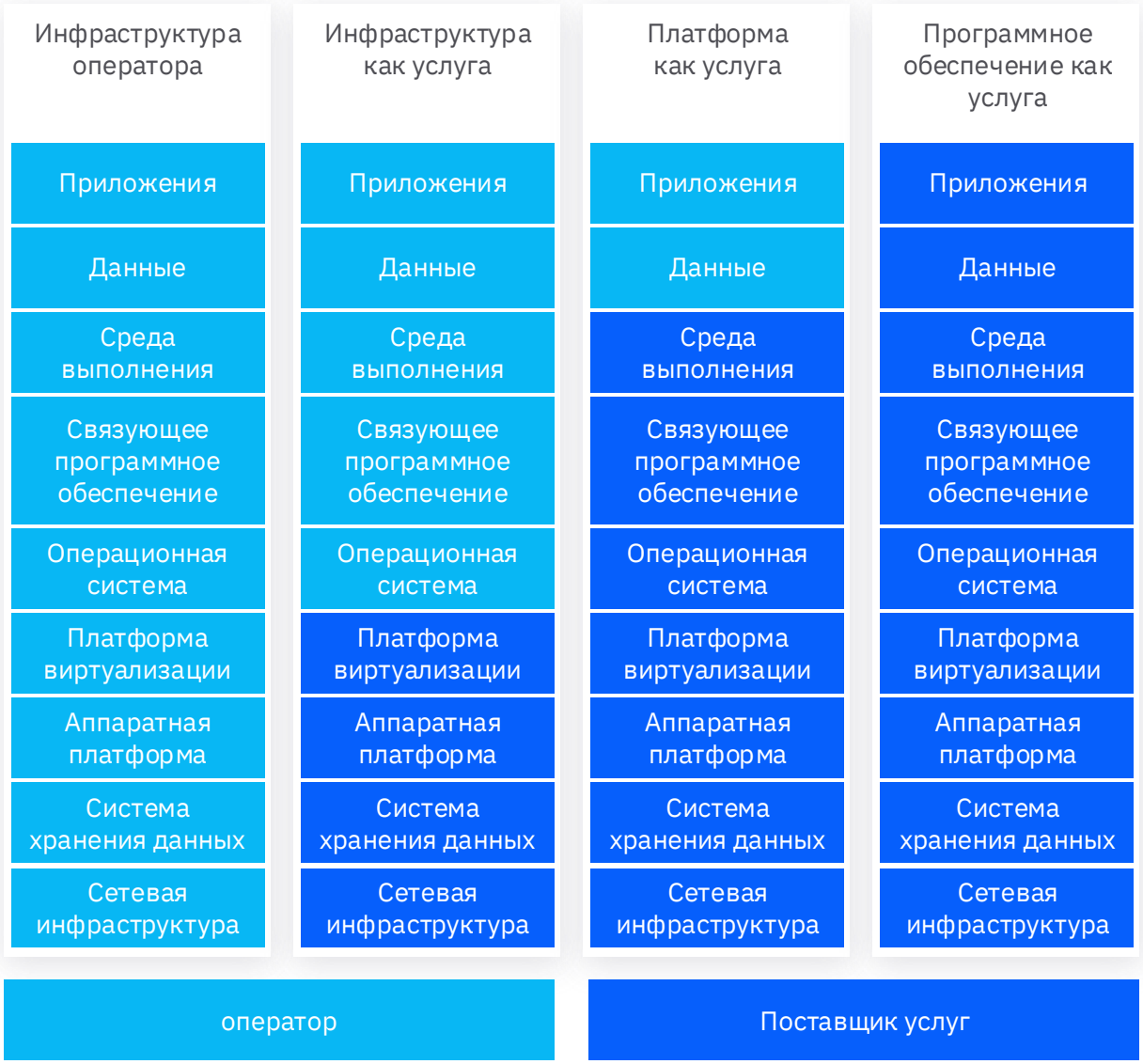

Рис. 1 – Схема разделения зон ответственности

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 требований, реализуемых K2 Cloud и описание разделения зон ответственности [1]

Процесс 1 «Обеспечение защиты информации при управлении доступом»
Подпроцесс «Управление учетными записями и правами субъектов логического доступа»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
УЗП.1 УЗП.2 УЗП.3 УЗП.4 УЗП.5 УЗП.6 УЗП.7 УЗП.8 УЗП.9 УЗП.10 УЗП.11 УЗП.12 УЗП.13 УЗП.14 УЗП.15 УЗП.16 УЗП.17 УЗП.18 УЗП.19 УЗП.20 УЗП.21 УЗП.22 УЗП.23 УЗП.24 УЗП.25 УЗП.26 УЗП.27 УЗП.28 УЗП.29	K2 Cloud, для объектов информатизации[2], относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.2.1.1 ГОСТ Р 57580.1-2017, включая: • организацию и контроль использования учетных записей субъектов логического доступа; • организацию и контроль предоставления (отзыва) и блокирования логического доступа; • регистрацию событий защиты информации, связанных с операциями с учетными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.2.1.1 ГОСТ Р 57580.1-2017, включая: • организацию и контроль использования учетных записей субъектов логического доступа; • организацию и контроль предоставления (отзыва) и блокирования логического доступа; • регистрацию событий защиты информации, связанных с операциями с учетными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа.

1 Указанный в приложении состав требований и разделение зон ответственности является типовым, реализуемым по умолчанию, и может изменяться, на основании принципов, изложенных в разделе 3 Матрицы разделения ответственности за информационную безопасность, согласно требованиям ГОСТ Р 57580.1-2017, между Облачной платформой и пользователями

2 Под объектом информатизации понимаются объекты и/или ресурсы доступа, определяемые согласно ГОСТ Р 57580.1-2017 (п. 3.6, 3.8 и 3.9 стандарта).

Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
РД.1 РД.2 РД.3 РД.4 РД.5 РД.6 РД.7 РД.8 РД.9 РД.10 РД.11 РД.12 РД.13 РД.14 РД.15 РД.16 РД.17 РД.18 РД.19 РД.20 РД.21 РД.22 РД.23 РД.24 РД.25 РД.26 РД.27 РД.28 РД.29 РД.30 РД.31 РД.32 РД.33 РД.34 РД.35 РД.36 РД.37 РД.38 РД.39 РД.40 РД.41 РД.42 РД.43 РД.44	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.2.2.1 ГОСТ Р 57580.1-2017, включая: идентификацию и аутентификацию субъектов логического доступа; • организацию управления и организацию защиты идентификационных и аутентификационных данных; • авторизацию (разграничение доступа) при осуществлении логического доступа; • регистрацию событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.2.2.1 ГОСТ Р 57580.1-2017, включая: идентификацию и аутентификацию субъектов логического доступа; • организацию управления и организацию защиты идентификационных и аутентификационных данных; • авторизацию (разграничение доступа) при осуществлении логического доступа; • регистрацию событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа.

Подпроцесс «Защита информации при осуществлении физического доступа»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ФД.1	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.2.3.1 ГОСТ Р 57580.1-2017, включая: • организацию и контроль физического доступа в помещения, в которых расположены объекты доступа; • организацию и контроль физического доступа к объектам доступа, расположенным в публичных (общедоступных) местах; • регистрацию событий, связанных с физическим доступом.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.2.3.1 ГОСТ Р 57580.1-2017, включая: • организацию и контроль физического доступа в помещения, в которых расположены объекты доступа; • организацию и контроль физического доступа к объектам доступа, расположенным в публичных (общедоступных) местах; • регистрацию событий, связанных с физическим доступом.
ФД.2		
ФД.3		
ФД.4		
ФД.5		
ФД.6		
ФД.7		
ФД.8		
ФД.9		
ФД.10		
ФД.11		
ФД.12		
ФД.13		
ФД.14		
ФД.15		
ФД.16		
ФД.17		
ФД.18		
ФД.19		
ФД.20		
ФД.21		

Подпроцесс «Идентификация и учет ресурсов и объектов доступа»

<table>
<tr><td></td><td colspan="2">Зоны ответственности</td></tr>
<tr><td>Мера защиты</td><td>K2 Cloud</td><td>Пользователь</td></tr>
<tr><td>ИУ.1</td><td rowspan="8">K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.2.4.1 ГОСТ Р 57580.1-2017, включая:
организацию учета и контроль состава ресурсов и объектов доступа;
регистрацию событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа.</td><td rowspan="8">Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.2.4.1 ГОСТ Р 57580.1-2017, включая:
организацию учета и контроль состава ресурсов и объектов доступа;
регистрацию событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа.</td></tr>
<tr><td>ИУ.2</td></tr>
<tr><td>ИУ.3</td></tr>
<tr><td>ИУ.4</td></tr>
<tr><td>ИУ.5</td></tr>
<tr><td>ИУ.6</td></tr>
<tr><td>ИУ.7</td></tr>
<tr><td>ИУ.8</td></tr>
</table>

Процесс 2 «Обеспечение защиты вычислительных сетей»
Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
СМЭ.1	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.3.1.1 ГОСТ Р 57580.1-2017, включая: • сегментацию и межсетевое экранирование внутренних вычислительных сетей; • защиту внутренних вычислительных сетей при взаимодействии с сетью Интернет; • регистрацию событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.3.1.1 ГОСТ Р 57580.1-2017, включая: • сегментацию и межсетевое экранирование внутренних вычислительных сетей; • защиту внутренних вычислительных сетей при взаимодействии с сетью Интернет; • регистрацию событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей.
СМЭ.2		
СМЭ.3		
СМЭ.4		
СМЭ.5		
СМЭ.6		
СМЭ.7		
СМЭ.8		
СМЭ.9		
СМЭ.10		
СМЭ.11		
СМЭ.12		
СМЭ.13		
СМЭ.14		
СМЭ.15		
СМЭ.16		
СМЭ.17		
СМЭ.18		
СМЭ.19		
СМЭ.20		
СМЭ.21		

Подпроцесс «Выявление вторжений и сетевых атак»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ВСА.1	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.3.2.1 ГОСТ Р 57580.1-2017, включая: • мониторинг и контроль содержимого сетевого трафика; • регистрацию событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.3.2.1 ГОСТ Р 57580.1-2017, включая: • мониторинг и контроль содержимого сетевого трафика; • регистрацию событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика.
ВСА.2		
ВСА.3		
ВСА.4		
ВСА.5		
ВСА.6		
ВСА.7		
ВСА.8		
ВСА.9		
ВСА.10		
ВСА.11		
ВСА.12		
ВСА.13		
ВСА.14		

Подпроцесс «Защита информации, передаваемой по вычислительным сетям»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ЗВС.1	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.3.3.1 ГОСТ Р 57580.1-2017, включая: • меры по защите информации, передаваемой по вычислительным сетям.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.3.3.1 ГОСТ Р 57580.1-2017, включая: • меры по защите информации, передаваемой по вычислительным сетям.
ЗВС.2		

Подпроцесс «Защита беспроводных сетей»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ЗБС.1	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.3.4.1 ГОСТ Р 57580.1-2017, включая: • защиту информации от раскрытия и модификации при использовании беспроводных сетей; • защиту внутренних вычислительных сетей при использовании беспроводных сетей; • регистрацию событий защиты информации, связанных с использованием беспроводных сетей.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.3.4.1 ГОСТ Р 57580.1-2017, включая: • защиту информации от раскрытия и модификации при использовании беспроводных сетей; • защиту внутренних вычислительных сетей при использовании беспроводных сетей; • регистрацию событий защиты информации, связанных с использованием беспроводных сетей.
ЗБС. 2		
ЗБС.3		
ЗБС.4		
ЗБС.5		
ЗБС.6		
ЗБС.7		
ЗБС.8		
ЗБС.9		
ЗБС.10		

Процесс 3 «Контроль целостности и защищенности информационной инфраструктуры»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ЦЗИ.1 ЦЗИ.2 ЦЗИ.3 ЦЗИ.4 ЦЗИ.5 ЦЗИ.6 ЦЗИ.7 ЦЗИ.8 ЦЗИ.9 ЦЗИ.10 ЦЗИ.11 ЦЗИ.12 ЦЗИ.13 ЦЗИ.14 ЦЗИ.15 ЦЗИ.16 ЦЗИ.17 ЦЗИ.18 ЦЗИ.19 ЦЗИ.20 ЦЗИ.21 ЦЗИ.22 ЦЗИ.23 ЦЗИ.24 ЦЗИ.25 ЦЗИ.26 ЦЗИ.27 ЦЗИ.28 ЦЗИ.29 ЦЗИ.30 ЦЗИ.31 ЦЗИ.32 ЦЗИ.33 ЦЗИ.34 ЦЗИ.35 ЦЗИ.36	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.4.1 ГОСТ Р 57580.1-2017, включая: • контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации; • организацию и контроль размещения, хранения и обновления ПО информационной инфраструктуры; • контроль состава и целостности ПО информационной инфраструктуры; • регистрацию событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.4.1 ГОСТ Р 57580.1-2017, включая: • контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации; • организацию и контроль размещения, хранения и обновления ПО информационной инфраструктуры; • контроль состава и целостности ПО информационной инфраструктуры; • регистрацию событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры.

Процесс 4 «Защита от вредоносного кода»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ЗВК.1 ЗВК.2 ЗВК.3 ЗВК.4 ЗВК.5 ЗВК.6 ЗВК.7 ЗВК.8 ЗВК.9 ЗВК.10 ЗВК.11 ЗВК.12 ЗВК.13 ЗВК.14 ЗВК.15 ЗВК.16 ЗВК.17 ЗВК.18 ЗВК.19 ЗВК.20 ЗВК.21 ЗВК.22 ЗВК.23 ЗВК.24 ЗВК.25 ЗВК.26 ЗВК.27 ЗВК.28	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.5.1 ГОСТ Р 57580.1-2017, включая: • организацию эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры; • организацию и контроль применения средств защиты от вредоносного кода; • регистрацию событий защиты информации, связанных с реализацией защиты от вредоносного кода.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.5.1 ГОСТ Р 57580.1-2017, включая: • организацию эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры; • организацию и контроль применения средств защиты от вредоносного кода; • регистрацию событий защиты информации, связанных с реализацией защиты от вредоносного кода.

Процесс 5 «Предотвращение утечек информации»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ПУИ.1 ПУИ.2 ПУИ.3 ПУИ.4 ПУИ.5 ПУИ.6 ПУИ.7 ПУИ.8 ПУИ.9 ПУИ.10 ПУИ.11 ПУИ.12 ПУИ.13 ПУИ.14 ПУИ.15 ПУИ.16 ПУИ.17 ПУИ.18 ПУИ.19 ПУИ.20 ПУИ.21 ПУИ.22 ПУИ.23 ПУИ.24 ПУИ.25 ПУИ.26 ПУИ.27 ПУИ.28 ПУИ.29 ПУИ.30 ПУИ.31 ПУИ.32 ПУИ.33	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.6.1 ГОСТ Р 57580.1-2017, включая: • блокирование неразрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации; • контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации; • организацию защиты машинных носителей информации (МНИ); • регистрацию событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.6.1 ГОСТ Р 57580.1-2017, включая: • блокирование неразрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации; • контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации; • организацию защиты машинных носителей информации (МНИ); • регистрацию событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации.

Процесс 6 «Управление инцидентами защиты информации»
Подпроцесс «Мониторинг и анализ событий защиты информации»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
МАС.1	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.7.1.1 ГОСТ Р 57580.1-2017, включая: • организацию мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информатизации, в том числе в соответствии с требованиями к содержанию базового состава мер защиты информации настоящего стандарта; • сбор, защиту и хранение данных регистрации о событиях защиты информации; • анализ данных регистрации о событиях защиты информации; • регистрацию событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с 7.7.1.1 ГОСТ Р 57580.1-2017, включая: • организацию мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информатизации, в том числе в соответствии с требованиями к содержанию базового состава мер защиты информации настоящего стандарта; • сбор, защиту и хранение данных регистрации о событиях защиты информации; • анализ данных регистрации о событиях защиты информации; • регистрацию событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации.
МАС.2		
МАС.3		
МАС.4		
МАС.5		
МАС.6		
МАС.7		
МАС.8		
МАС.9		
МАС.10		
МАС.11		
МАС.12		
МАС.13		
МАС.14		
МАС.15		
МАС.16		
МАС.17		
МАС.18		
МАС.19		
МАС.20		
МАС.21		
МАС.22		
МАС.23		

Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
РИ.1	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.7.2.1 ГОСТ Р 57580.1-2017, включая: • обнаружение и регистрацию инцидентов защиты информации; • организацию реагирования на инциденты защиты информации; • организацию хранения и защиту информации об инцидентах защиты информации; • регистрацию событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.7.2.1 ГОСТ Р 57580.1-2017, включая: • обнаружение и регистрацию инцидентов защиты информации; • организацию реагирования на инциденты защиты информации; • организацию хранения и защиту информации об инцидентах защиты информации; • регистрацию событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них.
РИ.2		
РИ.3		
РИ.4		
РИ.5		
РИ.6		
РИ.7		
РИ.8		
РИ.9		
РИ.10		
РИ.11		
РИ.12		
РИ.13		
РИ.14		
РИ.15		
РИ.16		
РИ.17		
РИ.18		
РИ.19		

Процесс 7 «Защита среды виртуализации»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ЗСВ.1 ЗСВ.2 ЗСВ.3 ЗСВ.4 ЗСВ.5 ЗСВ.6 ЗСВ.7 ЗСВ.8 ЗСВ.9 ЗСВ.10 ЗСВ.11 ЗСВ.12 ЗСВ.13 ЗСВ.14 ЗСВ.15 ЗСВ.16 ЗСВ.17 ЗСВ.18 ЗСВ.19 ЗСВ.20 ЗСВ.21 ЗСВ.22 ЗСВ.23 ЗСВ.24 ЗСВ.25 ЗСВ.26 ЗСВ.27 ЗСВ.28 ЗСВ.29 ЗСВ.30 ЗСВ.31 ЗСВ.32 ЗСВ.33 ЗСВ.34 ЗСВ.35 ЗСВ.36 ЗСВ.37 ЗСВ.38 ЗСВ.39 ЗСВ.40 ЗСВ.41 ЗСВ.42 ЗСВ.43	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.8.2 ГОСТ Р 57580.1-2017, включая[3]: • организацию идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации; • организацию и контроль информационного взаимодействия и изоляции виртуальных машин; • организацию защиты образов виртуальных машин; • регистрацию событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.8.2 ГОСТ Р 57580.1-2017, включая: • организацию идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации; • организацию и контроль информационного взаимодействия и изоляции виртуальных машин; • организацию защиты образов виртуальных машин; • регистрацию событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации.

[3] Дополнительно, на основании п. 7.8.1 ГОСТ Р 57580.1-2017 применяются дополнительные меры защиты для среды виртуализации, согласно п. 7.1.1 указанного выше стандарта.

Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ЗУД.1 ЗУД.2 ЗУД.3 ЗУД.4 ЗУД.5 ЗУД.6 ЗУД.7 ЗУД.8 ЗУД.9 ЗУД.10 ЗУД.11 ЗУД.12	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.9.1 ГОСТ Р 57580.1-2017, включая: • защиту информации от раскрытия и модификации при осуществлении удаленного доступа; • защиту внутренних вычислительных сетей при осуществлении удаленного доступа; • защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 7.9.1 ГОСТ Р 57580.1-2017, включая: • защиту информации от раскрытия и модификации при осуществлении удаленного доступа; • защиту внутренних вычислительных сетей при осуществлении удаленного доступа; • защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах.

Требования к организации и управлению защитой информации
Направление 1 «Планирование процесса системы защиты информации»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ПЗИ.1	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 8.2.1 ГОСТ Р 57580.1-2017, включая определение (пересмотр): • области применения процесса системы защиты информации; • состава применяемых (а также не применяемых) мер защиты информации из числа мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580.1-2017 (актуальные меры, с учетом уровня защиты K2 Cloud, зафиксированы в настоящем документе); • состава и содержания мер защиты информации, являющихся дополнительными к базовому составу мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580.1-2017, определяемых на основе актуальных угроз защиты информации, требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации (при наличии таковых[4]); • порядка применения мер защиты информации в рамках процесса системы защиты информации.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 8.2.1 ГОСТ Р 57580.1-2017, включая определение (пересмотр): • области применения процесса системы защиты информации; • состава применяемых (а также не применяемых) мер защиты информации из числа мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580.1-2017 (актуальные меры, с учетом уровня защиты конкретного пользователя, фиксируются в его ведомости применимости и/или аналогичном документе, например модели угроз и нарушителя или приложениях к ней); • состава и содержания мер защиты информации, являющихся дополнительными к базовому составу мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580.1-2017, определяемых на основе актуальных угроз защиты информации, требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации (при наличии таковых); • порядка применения мер защиты информации в рамках процесса системы защиты информации.
ПЗИ.2		
ПЗИ.3		
ПЗИ.4		
ПЗИ.5		

4 Принципы актуализации настоящего документа изложены в разделе 3 Матрицы разделения ответственности.

Направление 2 «Реализация процесса системы защиты информации»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
РЗИ.1	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 8.3.1 ГОСТ Р 57580.1-2017 и обеспечивает: • должное применение мер защиты информации; • определение ролей защиты информации, связанных с применением мер защиты информации; • назначение ответственных лиц за выполнение ролей защиты информации; • доступность реализации технических мер защиты информации; • применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия [в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности], в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации K2 Cloud; • обучение, практическую подготовку (переподготовку) работников K2 Cloud, ответственных за применение мер защиты информации; • повышение осведомленности (инструктаж) работников K2 Cloud в области защиты информации.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 8.3.1 ГОСТ Р 57580.1-2017 и обеспечивает: • должное применение мер защиты информации; • определение ролей защиты информации, связанных с применением мер защиты информации; • назначение ответственных лиц за выполнение ролей защиты информации; • доступность реализации технических мер защиты информации; • применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия [в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности], в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации пользователя; • обучение, практическую подготовку (переподготовку) работников пользователя, ответственных за применение мер защиты информации; • повышение осведомленности (инструктаж) работников пользователя в области защиты информации.
РЗИ.2		
РЗИ.3		
РЗИ.4		
РЗИ.5		
РЗИ.6		
РЗИ.7		
РЗИ.8		
РЗИ.9		
РЗИ.10		
РЗИ.11		
РЗИ.12		
РЗИ.13		
РЗИ.14		
РЗИ.15		
РЗИ.16		

Направление 3 «Контроль процесса системы защиты информации»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
КЗИ.1 КЗИ.2 КЗИ.3 КЗИ.4 КЗИ.5 КЗИ.6 КЗИ.7 КЗИ.8 КЗИ.9 КЗИ.10 КЗИ.11 КЗИ.12	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 8.4.1 ГОСТ Р 57580.1-2017, включая: • области применения процесса системы защиты информации; • должного применения мер защиты информации в рамках процесса системы защиты информации; • знаний работников K2 Cloud в части применения мер защиты информации.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с 8.4.1 ГОСТ Р 57580.1-2017, включая: • области применения процесса системы защиты информации; • должного применения мер защиты информации в рамках процесса системы защиты информации; • знаний работников пользователя в части применения мер защиты информации.

Направление 4 «Совершенствование процесса системы защиты информации»

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
СЗИ.1 СЗИ.2 СЗИ.3 СЗИ.4	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 8.5.1 ГОСТ Р 57580.1-2017, включая обеспечение формирования и фиксацию решений о необходимости корректирующих или превентивных действий, в частности пересмотр применяемых мер защиты информации.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 8.5.1 ГОСТ Р 57580.1-2017, включая обеспечение формирования и фиксацию решений о необходимости корректирующих или превентивных действий, в частности пересмотр применяемых мер защиты информации.

Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений

	Зоны ответственности	
Мера защиты	K2 Cloud	Пользователь
ЖЦ.1 ЖЦ.2 ЖЦ.3 ЖЦ.4 ЖЦ.5 ЖЦ.6 ЖЦ.7 ЖЦ.8 ЖЦ.9 ЖЦ.10 ЖЦ.11 ЖЦ.12 ЖЦ.13 ЖЦ.14 ЖЦ.15 ЖЦ.16 ЖЦ.17 ЖЦ.18 ЖЦ.19 ЖЦ.20 ЖЦ.21 ЖЦ.22 ЖЦ.23 ЖЦ.24 ЖЦ.25 ЖЦ.26 ЖЦ.27 ЖЦ.28	K2 Cloud, для объектов информатизации, относящихся к её зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 9.2 и 9.3 ГОСТ Р 57580.1-2017, включая: • соблюдение требований к стадиям жизненного цикла автоматизированных систем, разрабатываемых в рамках K2 Cloud (с целью функционирования сервисов самого облака); • применение необходимых мер защиты информации к соответствующим автоматизированным системам.	Пользователь K2 Cloud, для объектов информатизации, относящихся к его зоне ответственности, определяемой на основании раздела 4 Матрицы разделения ответственности, обеспечивает реализацию требований, установленных в соответствии с п. 9.2 и 9.3 ГОСТ Р 57580.1-2017, включая: • соблюдение требований к стадиям жизненного цикла автоматизированных систем, разрабатываемых в рамках технологических и бизнес-процессов пользователя (для их автоматизации); • применение необходимых мер защиты информации к соответствующим автоматизированным системам (например, АБС, ДБО, учетным системам страховых и пенсионных организаций).