

УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ОТДЕЛЬНЫХ СЕРВИСОВ: АТТЕСТОВАННЫЙ СЕГМЕНТ ЦОД

Версия от 29 августа 2022 г.,
вступает в силу с 13 сентября 2022 г.

Настоящие условия использования отдельных сервисов («Условия») являются неотъемлемой частью Пользовательского соглашения («Соглашение»). Термины с прописной буквы, которые используются, но не определены в настоящих Условиях, имеют значение, присвоенное им в Соглашении.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аттестованный сегмент ЦОД - объект информатизации «Аттестованный сегмент ЦОД», размещенный в Дата-центрах «Цветочная-2», «Берзарина-1», «Дубровка-2» Исполнителя. Состоит из набора аттестованных информационных систем (далее - ИС), соответствующих требованиям безопасности информации согласно Условиям:

- **ИС. Инфраструктура** - внутренняя ИС, которая служит для размещения серверного и сетевого оборудования, предоставляемого Исполнителем в рамках Основных услуг.
- **ИС. Управляемые сервисы безопасности** - внутренняя ИС, которая предназначена для управления средствами защиты информации. Позволяет Заказчику выполнять требования приказов ФСТЭК России № 21 и № 17 и требования международных стандартов, используя сервисы безопасности.
- **ИС. Администрирование** - внутренняя ИС, которая состоит из выделенных рабочих мест сотрудников Исполнителя с необходимыми мерами безопасности. Данная ИС позволяет Исполнителю проводить в рамках оказания Услуги как разовые работы, так и полное сопровождение систем Заказчика, включая реагирование на инциденты информационной безопасности.
- **ИС. Мониторинг информационной безопасности** - внутренняя ИС, предназначенная для мониторинга событий информационной безопасности, регистрации и реагирования на инциденты информационной безопасности.

Дополнительное оборудование - средства защиты информации и сетевое оборудование, необходимое для организации локальной сети и обеспечения сетевой изоляции выделенных серверов.

Юнит - монтажная единица юнит (от англ. unit), единица измерения высоты оборудования. 1 юнит равен 44,45 мм.

1. ПРЕДМЕТ

- 1.1. Исполнитель предоставляет Заказчику в Аттестованном сегменте ЦОД вычислительные мощности Выделенного сервера произвольной конфигурации (далее - «Выделенный сервер») в соответствии с Условиями использования отдельных сервисов - «Предоставление Выделенного сервера и Выделенного сервера произвольной конфигурации» и настоящими Условиями, а также устанавливает Дополнительное оборудование, обеспечивающее возможность сетевой изоляции Выделенных серверов (далее - «Услуга»).

- 1.2. Размещение Выделенного сервера и Дополнительного оборудования осуществляется в ИС.Инфраструктура Услуги “Аттестованный сегмент ЦОД” в рамках соответствующей типовой схемы подключения в соответствии с Приложением №1 к Условиям (далее - “Типовая схема подключения”) или по индивидуальной схеме подключения, согласованной Исполнителем и Заказчиком.
- 1.3. Пользование Услугой осуществляется удаленно. Заказчик принимает и оплачивает Услугу Исполнителю.
- 1.4. В качестве дополнительных возможностей для Заказчика могут предоставляться дополнительные услуги - Администрирование систем и сервисов информационной безопасности. Порядок предоставления дополнительных услуг по администрированию средств защиты информации регламентируется в соответствии с дополнительным соглашением, оформляемым к Соглашению.

2. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГИ

- 2.1. Заказчик заказывает Выделенный сервер. При заказе Выделенного сервера или в процессе пользования услугой “Предоставление Выделенного сервера и Выделенного сервера произвольной конфигурации” указывает на необходимость его размещения в Аттестованном сегменте ЦОД. Услуга заказывается в количестве, соответствующем количеству Юнитов, занимаемых Выделенным сервером и Дополнительным оборудованием.
- 2.2. Перед подключением Услуги Заказчик согласует с Исполнителем индивидуальную схему подключения Выделенного сервера и Дополнительного оборудования. Согласование происходит способом, предусмотренным в Соглашении. В случае, если Заказчик не заявил о необходимости согласования индивидуальной схемы, Исполнителем используется Типовая схема подключения.
- 2.3. Начало оказания Услуги:
 - при использовании для подключения Услуги Типовой схемы подключения для Выделенного сервера и Дополнительного оборудования Исполнитель в течение 10 (десяти) рабочих дней с момента заказа Услуги обязуется подключить Услугу и уведомить об этом Заказчика по Тикет-системе.
 - при использовании для подключения Услуги индивидуальной схемы подключения Выделенного сервера и Дополнительного оборудования Исполнитель в течение 20 (двадцати) рабочих дней с момента заказа всех Услуг и согласования индивидуальной схемы обязуется подключить Услугу и уведомить об этом Заказчика в Тикет-системе.
- 2.4. Исполнитель размещает Выделенный сервер и Дополнительное оборудование в соответствии с согласованной схемой подключения в ИС.Инфраструктура Услуги “Аттестованный сегмент ЦОД” и подключает Услугу. В момент подключения Услуги Исполнитель передает Заказчику информацию, необходимую для доступа к Выделенным серверам и Дополнительному оборудованию.
- 2.5. Исполнитель обеспечивает физическую безопасность Выделенного сервера и Дополнительного оборудования в соответствии с Приложением 2 “Перечень мер, реализуемых Исполнителем в зоне своей ответственности в Аттестованном сегменте ЦОД

в соответствии с Приказом ФСТЭК России от 18.02.2013 г. № 21 и Приказом ФСТЭК России от 11.02.2013 г. № 17” . Заказчик самостоятельно обеспечивает логическую безопасность Выделенного сервера и Дополнительного оборудования, в том числе Заказчик самостоятельно осуществляет установку необходимого программного обеспечения, разработку настроек и их применение, установление и согласование политик обеспечения безопасности, организацию удаленного и защищенного доступа для администрирования.

2.6. Физический доступ к Выделенному серверу и Дополнительному оборудованию в рамках настоящих Условий Заказчику не предоставляется.

3. ОПЛАТА УСЛУГИ

3.1. Если иное не установлено настоящими Условиями, Услуга оплачивается в порядке, сроки и форме, установленные Соглашением.

3.2. Оплата Услуги осуществляется за каждый Юнит, занимаемый Выделенным сервером и Дополнительным оборудованием. Учет количества Юнитов, подлежащих оплате, ведется отдельно для Выделенного сервера и Дополнительного оборудования.

3.3. Заказчик может выбрать период оплаты Услуги при заказе из доступных периодов оплаты. Дальнейшее продление Услуги осуществляется на ежемесячной основе. При необходимости Заказчик может изменить период оплаты Услуги, а также отключить функцию автопродления (автоплатежа) в Панели управления.

4. ОКОНЧАНИЕ ПРЕДОСТАВЛЕНИЯ УСЛУГИ

4.1. Окончание предоставления Услуги происходит одновременно с окончанием предоставления услуги “Предоставление Выделенного сервера и Выделенного сервера произвольной конфигурации” и регламентируется Условиями использования отдельных сервисов - “Предоставление Выделенного сервера и Выделенного сервера произвольной конфигурации”.

5. УРОВЕНЬ ОКАЗАНИЯ УСЛУГИ (SLA)

5.1.

Компенсированный простой	Некомпенсированный простой
Недоступность Выделенного сервера из-за сбоя инфраструктуры Исполнителя.	Недоступность сервера из-за аппаратного сбоя в Дополнительном оборудовании (например, межсетевом экране) в том случае, если в Услуге используется Дополнительное оборудование без резервирования (не используется отказоустойчивая схема - не применяется кластер межсетевых экранов и т.п.).
Недоступность Выделенного сервера из-за аппаратного сбоя в предоставляемом Заказчику Дополнительном оборудовании (например межсетевой экран), в случае, если при оказании Услуги используется резервирование Дополнительного оборудования (используется отказоустойчивая схема - кластер межсетевых экранов	Недоступность сервера из Интернет из-за программного сбоя в Дополнительном оборудовании.

и т.п.).	
Данный вид даунтайма компенсируется согласно стоимости Выделенного сервера, Дополнительного оборудования, а также соответствующей им услуги Размещение в аттестованном сегменте ЦОД.	

5.2. Размер и условия компенсации устанавливается в соответствии с Условиями использования отдельных сервисов - "Предоставление Выделенного сервера и Выделенного сервера произвольной конфигурации".

6. ИНЫЕ УСЛОВИЯ

6.1. **Аттестованный сегмент ЦОД включает в себя ИС, которые соответствуют требованиям безопасности информации, а именно:**

6.1.1. **ИС.Инфраструктура согласно аттестату № 3479.00001.2022 от 10 марта 2022 г., предъявляемым к:**

- информационным системам персональных данных первого уровня защищенности (У31) персональных данных в соответствии с Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных» и Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- государственным информационным системам первого класса (К1) защищенности в соответствии с Приказом ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- информационно-телекоммуникационным инфраструктурам центров обработки данных, обеспечивающим техническую и организационную возможность размещения в своей инфраструктуре сторонних информационных систем, предъявляющих требования к классу защищенности информации до первого класса (К1) защищенности включительно в соответствии с Приказом ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- объектам информатизации, обеспечивающим техническую и организационную возможность размещения в своей инфраструктуре сторонних информационных систем, предъявляющих требования к уровню защищенности персональных данных до первого (У31) включительно в соответствии с Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- 6.1.2. Исполнитель обязуется поддерживать Аттестованный сегмент ЦОД в аттестованном состоянии в соответствии с действующим законодательством.
- 6.1.3. **согласно сертификату PCI DSS (для Аттестованного сегмента ЦОД, размещенного в Дата-центрах «Цветочная-2» и «Берзарина-1»):**
- Стандарта безопасности данных индустрии платежных карт - PCI DSS в части ограничения физического доступа к системам (требования 9.1, 9.1.1, 9.1.2, 9.1.3, 9.2, 9.3, 9.4, 9.4.1, 9.4.2, 9.4.3, 9.4.4, 9.10) и регулярного мониторинга и тестирования сети (беспроводных точек доступа) (требования 11.1, 11.1.1, 11.1.2).
- 6.1.4. **Согласно отчету SOC2 тип-1 Аттестованный сегмент ЦОД соответствует критериям надежности сервисов относящихся к критериям безопасности и доступности, изложенных в разделе TSP 100, 2017.**
- 6.2. Перечень мер для обеспечения физической безопасности, принимаемый Исполнителем, приведен в Приложении 2 к Условиям.
- 6.3. Во всём, что не отражено настоящими Условиями, применяются положения Соглашения и Условий использования отдельных сервисов - "Предоставление Выделенного сервера и Выделенного сервера произвольной конфигурации".
- 7. ПРИЛОЖЕНИЯ:**
- 7.1. Приложение 1 - Типовые схемы подключения, на 3 л.
- 7.2. Приложение 2 - Перечень мер, реализуемых Исполнителем в зоне своей ответственности, в Аттестованном сегменте ЦОД в соответствии с Приказом ФСТЭК России от 18.02.2013 г. № 21 и Приказом ФСТЭК России от 11.02.2013 г. № 17, на 4 л.

ПРИЛОЖЕНИЕ 1 - ТИПОВЫЕ СХЕМЫ ПОДКЛЮЧЕНИЯ ОБОРУДОВАНИЯ В ИС. Инфраструктура Услуги “Аттестованный сегмент ЦОД”

Схема 1. При заказе от 1 до 8 Выделенных серверов произвольной конфигурации, с управлением через IPMI и арендой межсетевого экрана Fortinet FG-100E.

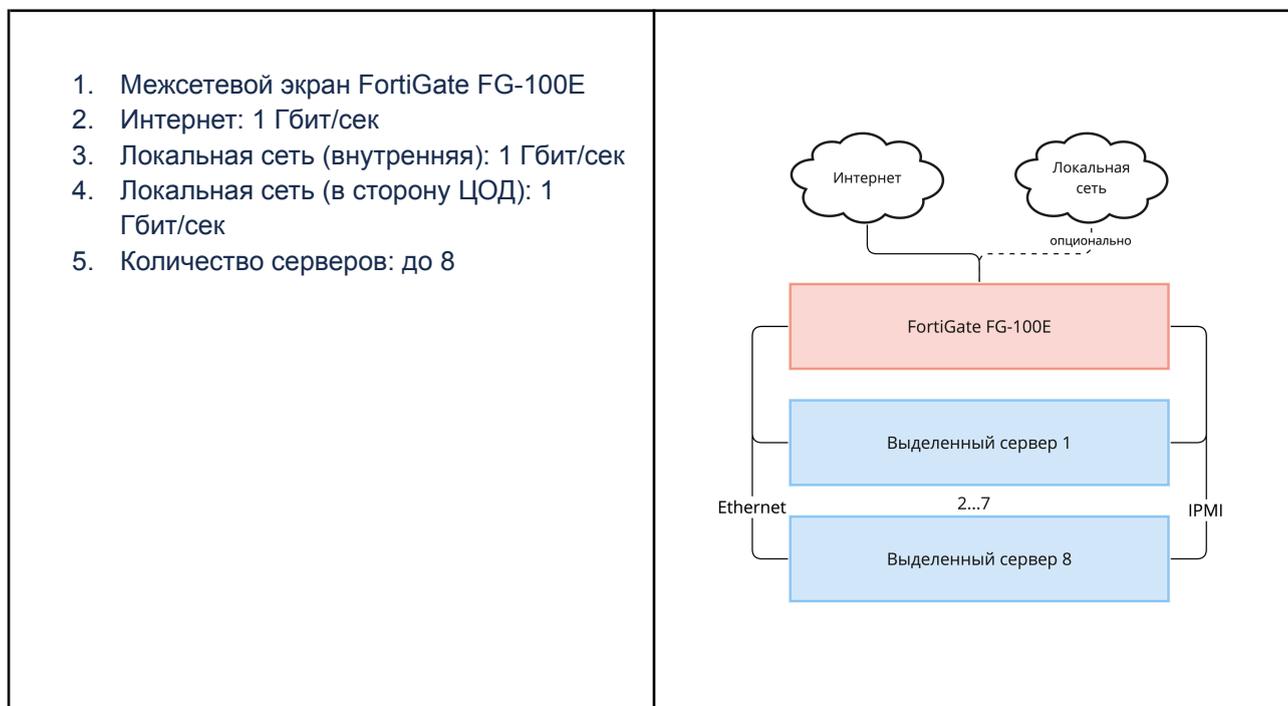


Схема 2. При заказе от 1 до 2 Выделенных серверов произвольной конфигурации, с управлением через IPMI и арендой сертифицированного межсетевого экрана UserGate D200.

1. Межсетевой экран UserGate D200
2. Интернет: 1 Гбит/сек
3. Локальная сеть (внутренняя): 1 Гбит/сек
4. Локальная сеть (в сторону ЦОД): 1 Гбит/сек
5. Количество серверов: до 2

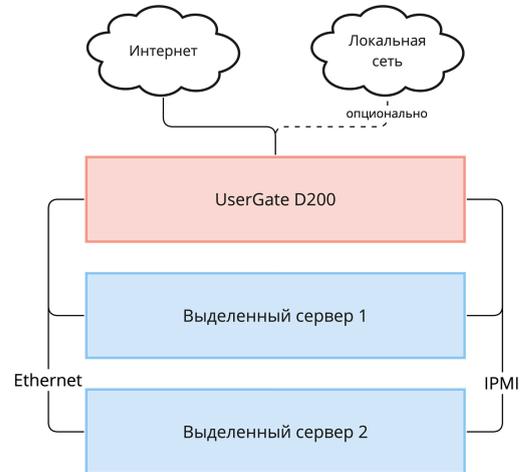
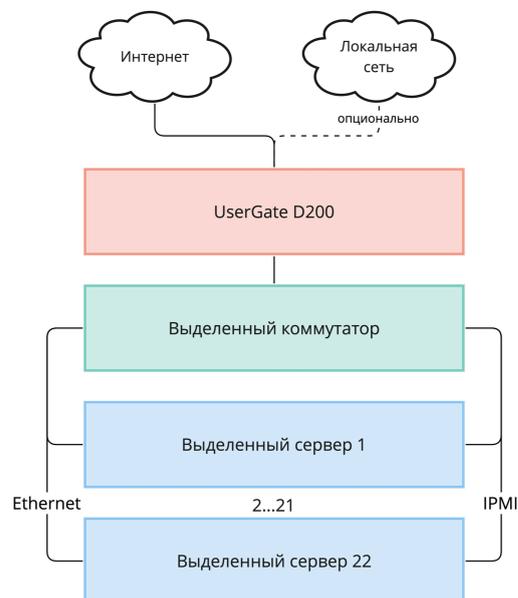


Схема 3. При заказе от 1 до 22 Выделенных серверов произвольной конфигурации, с управлением через IPMI и арендой сертифицированного межсетевого экрана UserGate D200 и коммутатора H3C S5560

1. Межсетевой экран UserGate D200 и коммутатор H3C S5560
2. Интернет: 1 Гбит/сек
3. Локальная сеть (внутренняя): 1 Гбит/сек
4. Локальная сеть (в сторону ЦОД): 1 Гбит/сек
5. Количество серверов: до 22



Исключения из применения Типовой схемы подключения - необходимость в индивидуальной схеме подключения. Индивидуальная схема согласуется Заказчиком и Исполнителем отдельно в соответствии с Условиями. Индивидуальная схема применяется в А-ЦОД в следующих случаях:

-
- использование кластера межсетевых экранов,
- использование 10GE интерфейсов,
- размещение информационной системы на нескольких площадках А-ЦОД одновременно,
- другие требования для реализации которых не подходит Типовая схема подключения.

Сетевое оборудование Заказчика (например, средства криптографической защиты информации, СКЗИ) размещается по согласованию и подключается в арендованный и выделенный под Заказчика межсетевой экран или коммутатор.

Приложение 2 – Перечень мер, реализуемых Исполнителем в зоне своей ответственности, в ИС. Инфраструктура Услуги “Аттестованный сегмент ЦОД” в соответствии с Приказом ФСТЭК России от 18.02.2013 г. № 21 и Приказом ФСТЭК России от 11.02.2013 г. № 17

Мера	Расшифровка	Реализация
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	Организована контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования
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	Обеспечивается 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. Определены лица, допущенные к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены. Производится учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения. Правила и процедуры управления физическим доступом регламентированы.
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Отсутствуют устройства вывода (отображения) информации.
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)	Дата-центры, в которых располагаются аттестованные сегменты ЦОД, соответствуют требованиям Tier III. Реализованы мероприятия, позволяющие обеспечить оперативное восстановление электроснабжения и/или системы кондиционирования. Реализованы меры пожарной безопасности, условия эксплуатации оборудования и условий окружающей среды, которые соответствуют установленным требованиям.
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	Условия предоставления услуги предполагают схему подключения сервера за выделенным межсетевым экраном, что позволяет выполнить требование по управлению информационными потоками.
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц,	Обеспечено разделение ролей администраторов информационной безопасности и лиц,

	обеспечивающих функционирование информационной системы	обеспечивающих функционирование. Роли документированы.
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Назначены минимально необходимые права и привилегии в соответствии с должностными обязанностями. Роли и должностные обязанности документированы.
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы	Схема подключения сервера предусматривает его обязательное размещение за межсетевым экраном, что позволяет выполнить требование по разбиению информационной системы на сегменты и обеспечить защиту периметра сегмента.
ЗНИ.1	Учет машинных носителей информации	Производится учет машинных носителей информации (жестких дисков) серверов.
ЗНИ.2	Управление доступом к машинным носителям информации	Обеспечивается управление доступом к машинным носителям информации, а именно определены должностные лица, имеющие физический доступ. Правила и процедуры доступа документированы.
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	Обеспечивается уничтожение (стирание) информации на машинных носителях при отказе от услуги, при выводе носителя из эксплуатации. Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации документированы.
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Определены события безопасности, подлежащие регистрации, и сроки их хранения, в части физической безопасности.
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	Определены и документированы состав и содержание информации о событиях безопасности, подлежащих регистрации, в части физической безопасности.
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	Осуществляется сбор, запись и хранение информации о событиях физической безопасности в течение установленного времени. Обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях физической безопасности.
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Осуществляется мониторинг (просмотр, анализ) результатов регистрации событий физической безопасности и реагирование на них. Правила и процедуры мониторинга результатов регистрации событий физической безопасности и реагирования на них документированы.
РСБ.7	Защита информации о событиях безопасности	Обеспечивается защита информации о событиях физической безопасности. Доступ к

		записям аудита и функциям управления предоставляется только уполномоченным должностным лицам. Обеспечивается резервное копирование записей аудита.
ОДТ.1	Использование отказоустойчивых технических средств	В инфраструктуре дата-центра используются отказоустойчивые технические средства. Определены предельные значения характеристик готовности и надежности и зафиксированы в условиях использования. Производится контроль за значениями характеристик готовности и надежности, замена средств, которые достигли предельного значения.
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы	Инфраструктура дата-центра полностью зарезервирована. Применяются резервные технические средства, каналы передачи информации и средства обеспечения функционирования. Правила и процедуры резервирования документированы.
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Осуществляется контроль безотказного функционирования инфраструктуры дата-центра, обнаружение и локализация отказов, принятие мер по восстановлению отказавших средств и их тестирование.
ОДТ.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации	Пользовательское соглашение, условия использования отдельных сервисов и поручение на обработку персональных данных позволяют осуществлять контроль состояния и качества предоставления ресурсов.
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	Определены лица, ответственные за выявление инцидентов физической безопасности и реагирование на них.
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	Осуществляется обнаружение, идентификация и регистрация инцидентов физической безопасности.
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами	Осуществляется своевременное информирование лиц, ответственных за выявление инцидентов физической безопасности и реагирование на них.
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	В случае возникновения инцидента физической безопасности проводится анализ источников и причин возникновения, оценка последствий.
ИНЦ.5	Принятие мер по устранению последствий инцидентов	В случае возникновения инцидента физической безопасности принимаются меры по устранению последствий.
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	В случае возникновения инцидента физической безопасности проводится планирование и принятие мер по предотвращению повторного возникновения.

УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты информации	Определены лица, которым разрешены действия по внесению изменений в конфигурацию.
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты информации	Процесс управления изменениями конфигурации документирован.
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты информации на обеспечение защиты информации и согласование изменений в конфигурации информационной системы с должностным лицом, ответственным за обеспечение безопасности информации	Проводится анализ потенциального воздействия планируемых изменений в конфигурации на обеспечение защиты информации и согласование изменений в конфигурации с должностным лицом (работником), ответственным за обеспечение безопасности.
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты информации	Осуществляется документирование информации об изменениях в конфигурации: схема подключения, схема размещения сервера, конфигурация сервера.