Selectel

УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ОТДЕЛЬНЫХ СЕРВИСОВ:
АТТЕСТОВАННЫЙ СЕГМЕНТ ЦОД

Версия от 30 сентября 2024 г.,
вступает в силу с 15 октября 2024 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 инженерной инфраструктуры центров обработки данных (далее - ЦОД) и набора аттестованных информационных систем (далее - ИС), соответствующих требованиям безопасности информации согласно Условиям, а именно:

- **Инженерная инфраструктура ЦОД (далее -Инфраструктура)** - комплекс систем и их оборудования, обеспечивающих бесперебойное функционирование систем и оборудования ИТ-инфраструктуры которые служат для размещения Выделенных серверов и Дополнительного оборудования.

- **ИС. Управляемые сервисы безопасности** - ИС, предназначенная для управления средствами защиты информации, а также оказания услуг и сервисов информационной 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,

CONDITIONS FOR USAGE OF INDIVIDUAL SERVICES:
CERTIFIED DC SEGMENT

Revision dated September 30, 2024,
shall enter into force from October 15, 2024

These conditions for usage of individual services ("Conditions") are the integral part of the User Agreement ("Agreement"). Capitalized terms (used but not defined in these Conditions) shall have the meanings assigned to them in the Agreement.

TERMS AND DEFINITIONS

Certified DC segment shall mean an informatization object "Attested Data Center Segment" placed in the Contractor's Data Centers "Tsvetochnaya-2", "Berzarina-1", "Dubrovka-2". It consists of the engineering infrastructure of data centers (hereinafter referred to as DC) and a set of certified information systems (hereinafter referred to as IS) that meet the information security requirements under the Terms and Conditions, namely:

- **DC Engineering Infrastructure (hereinafter referred to as the Infrastructure)** is a set of systems and their equipment ensuring continuous operation of IT infrastructure systems and equipment which serve to accommodate Dedicated Servers and Additional Equipment.

- **IS. Managed** security services shall mean an IS intended for managing information protection means and providing information security services and facilities.

- **IS. Administration** shall mean an internal IS which consists of dedicated workplaces of the Contractor's employees with required security measures. This IS allows the Contractor to carry out both once-only works and full support of the Customer's systems, including response to information security breaches, within the framework of the Service provision.

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.

- **IS. Information security monitoring** shall mean an internal IS designed to monitor information security events, register and respond to information security breaches.

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

Additional equipment includes information protection tools and network equipment required for arrangement of the local area network and ensuring network isolation of dedicated servers.

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

Unit means an assembly unit used to designate the height of equipment. 1 unit is equal to 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. Использование Услуги позволяет Заказчику выполнить требования информационной безопасности согласно разделу 6 Условий в рамках реализуемых Исполнителем мер в соответствии с Приложением № 2.

Реализацию иных мер информационной безопасности Заказчик выполняет самостоятельно, в том числе:

1. SUBJECT

1.1. The Contractor shall provide to the Customer computing capacity of a Dedicated Server with an arbitrary configuration (hereinafter referred to as the "Dedicated Server") in the Certified Data Center Segment in accordance with the Conditions for Usage of Individual Services ("Provision of a Dedicated Server and Dedicated Server with Arbitrary Configuration") and these Conditions, and also shall install Additional equipment providing the possibility of network isolation of Dedicated Servers (hereinafter referred to as the "Service").

1.2. The Service allows the Customer to fulfill the information security requirements under Section 6 of the Terms and Conditions within the framework of measures implemented by the Contractor under Appendix No. 2.

The Customer shall implement other information security measures independently, including:

- обеспечивает логическую безопасность Выделенного сервера и Дополнительного оборудования,
- providing logical security of the Dedicated Server and Additional Equipment,

- осуществляет установку необходимого программного обеспечения, разработку настроек и их применение, установление и согласование политик обеспечения безопасности, организацию удаленного и защищенного доступа для администрирования,
- installing necessary software, developing settings and applying them, establishing and coordinating security policies, organizing remote and secure access for administration,

или вправе заказать реализацию иных мер информационной безопасности у Исполнителя в качестве дополнительных услуг.

or being entitled to order the implementation of other information security measures from the Contractor as additional services.

1.3. В соответствии с п.2.11. Методического документа «Методика оценки угроз безопасности информации», утвержденного ФСТЭК России 5 февраля 2021 г., по запросу Заказчика в Тикет-системе Исполнитель предоставляет результаты оценки угроз безопасности информации для инженерной инфраструктуры ЦОД, а также перечень выполняемых мер в зоне ответственности Исполнителя.

1.3. Under Clause 2.11. of the Guideline "Information Security Threat Assessment Methodology" approved by FSTEC of Russia on February 5, 2021, upon the Customer's request in the Ticket System the Contractor shall provide the results of information security threat assessment for the DC engineering infrastructure and the list of measures implemented in the Contractor's area of liability.

1.4. Размещение Выделенного сервера и Дополнительного оборудования осуществляется в Инфраструктуре 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.

1.4. The Dedicated Server and Additional Equipment shall be installed in the Certified DC segment Service Infrastructure under the standard connection pattern subject to Appendix No. 1 to the Terms and Conditions (hereinafter referred to as the Standard Connection Pattern) or in accordance with an individual connection pattern agreed by the Contractor and the Customer.

1.5. Пользование Услугой осуществляется удаленно. Заказчик принимает и оплачивает Услугу Исполнителю.

1.5. The Service shall be used remotely. The Customer shall accept and pay for the Service to the Contractor.

1.6. В качестве дополнительных возможностей для Заказчика могут предоставляться дополнительные услуги - Администрирование систем и сервисов информационной безопасности. Порядок

1.6. As additional options for the Customer, additional services may be provided such as Administration of information security systems and services. The procedure for providing these additional services shall be

предоставления указанных дополнительных услуг регламентируется в соответствии с дополнительным соглашением, оформляемым к Соглашению.

regulated by an additional agreement to the Agreement.

2. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УСЛУГИ

2. PROCEDURE FOR SERVICE PROVISION

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.

2.1. The Customer orders the Dedicated Server. When ordering the Dedicated Server or in the process of using the service "Provision of a Dedicated Server and Dedicated Server with Arbitrary Configuration", the Customer shall indicate the need for its installation in the Certified Data Center Segment. The scope of the Service ordered shall correspond to the number of Units occupied by the Dedicated Server and Additional Equipment.

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.

2.2. Before connecting the Service, the Customer shall agree with the Contractor on the individual connection scheme for the Dedicated Server and Additional Equipment. Such agreement shall be reached in the form provided for by the Agreement. If the Customer has not indicated the need to agree on the individual connection scheme, the Contractor shall follow the Standard Connection Scheme.

2.3. Начало оказания Услуги:

2.3. Commencement of the Service provision:

- 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.

- In cases where the typical connection diagram for the Dedicated Server and Additional Equipment is used to connect the Service, the Contractor shall connect the Service and notify the Customer about it via the Ticket System within 10 (ten) working days from the moment of ordering the Service.

- 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

- In cases where the customized connection diagram for the Dedicated Server and Additional Equipment is used to connect the Service, the Contractor shall connect the Service and notify the Customer about it via the Ticket System within 20 (twenty) working

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 Инфраструктуре 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. 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

days from the moment of ordering the Service.

2.4. The Contractor shall install the Dedicated Server and Additional Equipment under the agreed connection pattern in the Certified DC segment Service Infrastructure and shall connect the Service. At the moment of the Service connection, the Contractor shall transfer to the Customer the information required for access to the Dedicated Servers and Additional Equipment.

2.5. These Conditions do not provide for granting the Customer physical access to the Dedicated Server and Additional Equipment.

3. SERVICE PAYMENT

3.1. Unless otherwise established by these Conditions, the Service shall be paid for in the manner, time and form established by the Agreement.

3.2. Payment for the Service shall be affected for each Unit occupied by the Dedicated Server and Additional Equipment. The number of units subject to payment shall be accounted separately for the Dedicated Server and Additional Equipment.

3.3. The customer may select the payment period for the Service at the moment of ordering from the available payment periods. Further extension of the Service provision period shall be performed on a monthly basis. If necessary, the Customer may change the period of payment for the Service, as well as disable the auto-renewal (auto-payment) function in the Control Panel.

4. END OF SERVICE PROVISION

4.1. The Service provision shall be terminated simultaneously with the termination of the provision of the service "Provision Dedicated

предоставления услуги “Предоставление Выделенного сервера и Выделенного сервера произвольной конфигурации” и регламентируется Условиями использования отдельных сервисов - “Предоставление Выделенного сервера и Выделенного сервера произвольной конфигурации”.

Server and Dedicated Server of Custom configuration" and shall be regulated by the Conditions for Usage of Individual Services - "Provision Dedicated Server and Dedicated Server of Custom configuration".

5. УРОВЕНЬ ОКАЗАНИЯ УСЛУГИ (SLA)

5. SERVICE LEVEL ACCOMPLISHMENT (SLA)

5.1.

Компенсируемый простой ***Compensable downtime***	**Некомпенсируемый простой** ***Non-compensable downtime***
Недоступность Выделенного сервера из-за сбоя инфраструктуры Исполнителя. / *Server unavailability due to a failure of the Contractor's infrastructure.* 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 и т.п.). / *Unavailability of the Dedicated Server due to a hardware failure of the Additional Equipment provided to the Customer (for example, a firewall failure), if the Service is provided with Additional Equipment redundancy (a fault-tolerant scheme is used such as a firewall cluster, etc.).* Данный вид даунтайма компенсируется согласно стоимости Выделенного сервера, Дополнительного оборудования, а также соответствующей им услуги Размещение в аттестованном сегменте ЦОД. / *A downtime of this type shall be compensated according to the cost of the Dedicated Server, Additional Equipment, and the corresponding service "Installation in the Certified Data Center Segment".*	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.). / *Server unavailability due to a hardware failure of the Additional Equipment (for example, a firewall failure) if the Service is provided without Additional Equipment redundancy (no fault-tolerant scheme such as a firewall cluster is used).* Недоступность сервера из Интернет из-за программного сбоя в Дополнительном оборудовании. / *Server unavailability from the Internet due to a software failure in the Additional Equipment.*

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

5.2. The amount and terms of compensation shall be determined in accordance with the Conditions for Usage of Individual Services ("Provision Dedicated Server and Dedicated Server of Custom configuration").

6. ИНЫЕ УСЛОВИЯ

6. OTHER CONDITIONS

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

6.1. **The Certified DC segment includes the Infrastructure and the IS that meet information security requirements, namely:**

6.1.1. Инфраструктура обеспечивает техническую и организационную возможность размещения информационных систем Заказчика, предъявляющих требования:

6.1.1. Infrastructure: provides technical and organizational capability to accommodate the Customer's information systems that have requirements:

- к классу защищенности информации до первого класса (К1) защищенности включительно в соответствии с приказом ФСТЭК России No 17 от 11.02.2013 г. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», а также

- to the information security class up to the first class (K1) of security inclusive in accordance with the order of FSTEC of Russia No. 17 dated February 11, 2013, "On Approval of the Requirements for the Protection of Information Not Constituting a State Secret Contained in State Information Systems", and

- к уровню защищенности персональных данных до первого (У31) уровня защищенности включительно в соответствии с Постановлением Правительства No 1119 и приказом ФСТЭК России No 21 от 18.02.2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

- to the level of protection of personal data up to the first protection level (PL1) inclusive under Government Decree No. 1119 and the order of the FSTEC of Russia No. 21 dated February 18, 2013, "On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Personal Data Security in Their Processing in Personal Data Information Systems".

6.1.2. Исполнитель обязуется поддерживать ИС в рамках Услуги в аттестованном состоянии в соответствии с действующим законодательством.

6.1.2. The Contractor shall maintain the IS within the Service in an attested state pursuant to the applicable law.

6.1.3. Услуга соответствует требованиям стандарта PCI DSS. Подробная

6.1.3. The Service complies with the requirements of the PCI DSS standard. The detailed

информация о реализуемых требованиях, содержащаяся в Attestation of Compliance, и разграничении зон ответственности предоставляет по запросу в Тикет-системе.

information on implemented requirements contained in the Attestation of Compliance and division of areas of liability is available upon request in the Ticket System.

6.1.4. Услуга соответствует стандарту SSAE 18. Подробная информация о реализуемых требованиях, содержащаяся в отчете SOC 2 Type I, предоставляется по запросу в Тикет-системе.

6.1.4. The Service complies with SSAE 18 standard. The detailed information on implemented requirements contained in the SOC 2 Type I report is available upon request in the Ticket System.

6.1.5. Услуга соответствует стандарту ISO/IEC 27001:2022, а также стандартам для облачных провайдеров ISO/IEC 27017:2015 и защите персональных данных в облаке ISO/IEC 27018:2019.

6.1.5. The Service complies with ISO/IEC 27001:2022 and ISO/IEC 27017:2015 standards for cloud providers and ISO/IEC 27018:2019 standard for the cloud protection of personal data.

6.2. Перечень мер для обеспечения физической безопасности, принимаемый Исполнителем, приведен в Приложении 2 к Условиям.

6.2. The list of measures to ensure physical security to be taken by the Contractor is presented in Appendix 2 to the Conditions.

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”.

6.3. All other issues not reflected in these Conditions shall be governed by the provisions of the Agreement and the the Conditions for Usage of Individual Services (""Provision Dedicated Server and Dedicated Server of Custom configuration").

7. ПРИЛОЖЕНИЯ:

7. APPENDICES:

7.1. Приложение 1 - Типовые схемы подключения, на 2 л.

7.1. Appendix 1 - Typical connection diagrams, 2 sheets.

7.2. Приложение 2 - Перечень мер, реализуемых Исполнителем в зоне своей ответственности,в инженерной инфраструктуре ЦОД в рамках Услуги на 4 л.

7.2. Appendix 2 - List of measures implemented by the Contractor within its area of liability, in the DC engineering infrastructure within the framework of the Service

ПРИЛОЖЕНИЕ 1 - ТИПОВЫЕ СХЕМЫ ПОДКЛЮЧЕНИЯ ОБОРУДОВАНИЯ В РАМКАХ УСЛУГИ

APPENDIX 1 - Typical connection diagrams, 2 sheets

Схема подключения, вариант 1. При подключении Выделенных серверов произвольной конфигурации в арендуемый межсетевой экран. Количество Выделенных серверов зависит от количества сетевых портов в выбранной модели межсетевого экрана.

Connection pattern, option 1. When connecting Dedicated Servers of arbitrary configuration to a leased firewall. The number of Dedicated Servers depends on the number of internet ports in the selected firewall model.

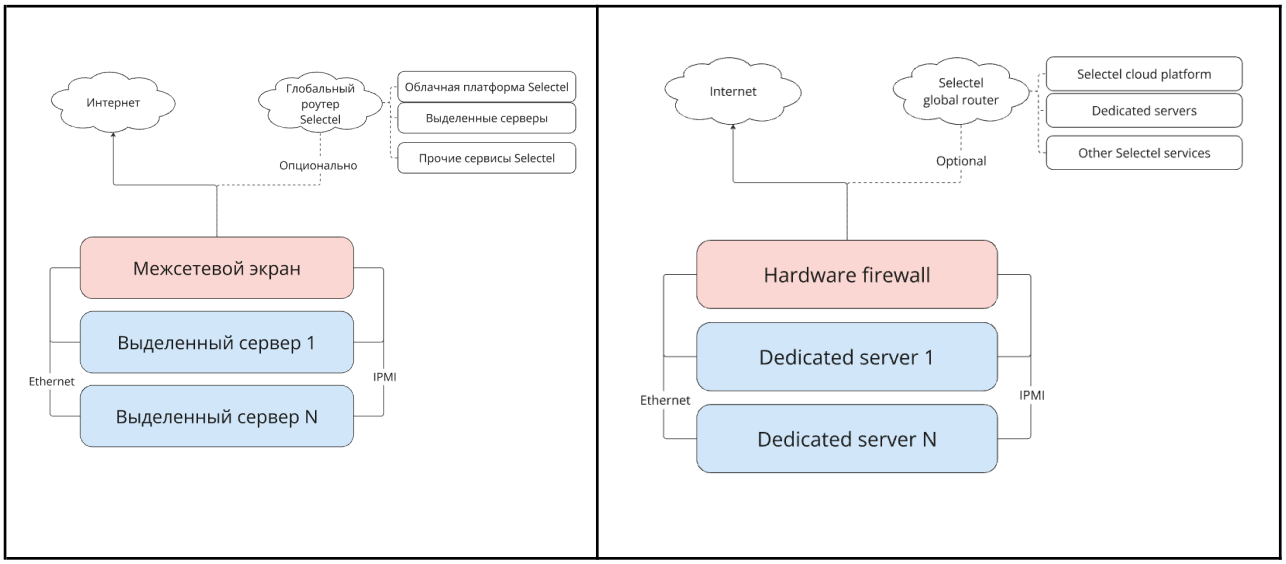
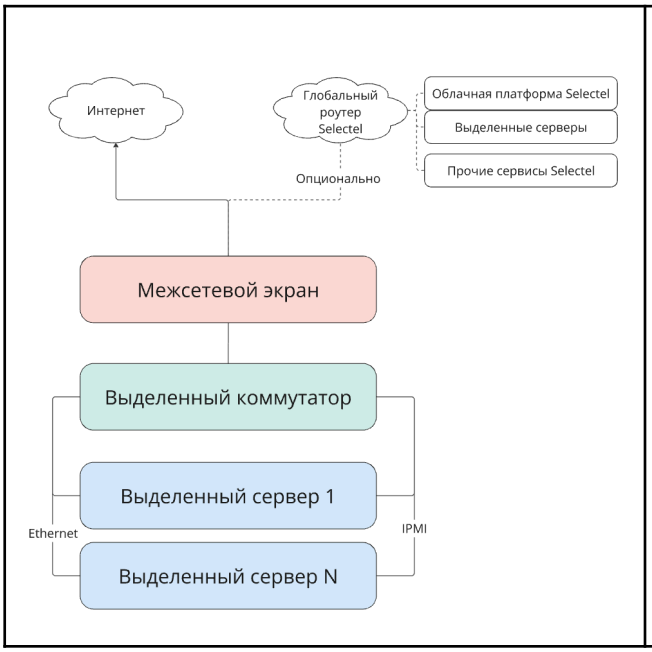
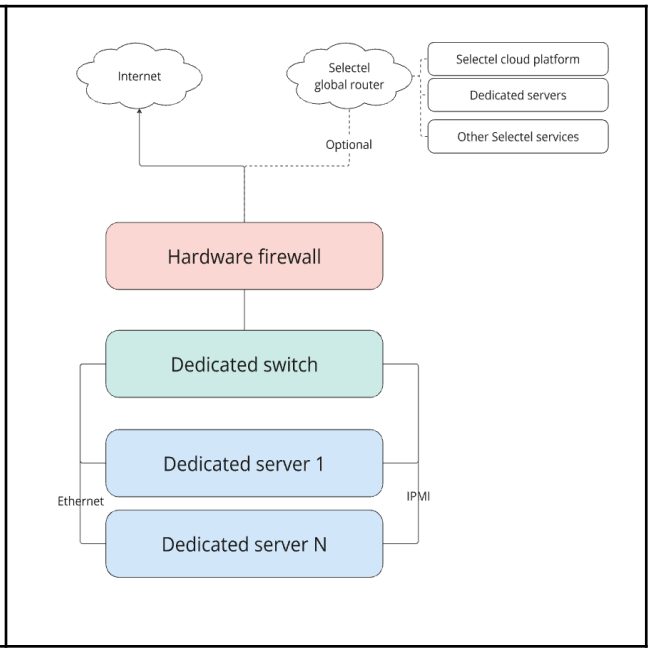


Схема подключения, вариант 2. При подключении Выделенных серверов произвольной конфигурации в арендуемый коммутатор и межсетевой экран. Количество Выделенных серверов зависит от количества сетевых портов в выбранной модели коммутатора.

Connection pattern, option 2. When connecting Dedicated Servers of arbitrary configuration to a leased switch and firewall. The number of Dedicated Servers depends on the number of internet ports in the selected switch model.





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:

Typical connection diagrams are not used when the customized connection diagram is required. The customized connection diagram shall be separately agreed by the Customer and the Contractor in accordance with the Terms and Conditions. The customized connection diagram shall be used in the certified data center when:

- 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.

- the cluster of firewalls is used,
- 10GE interfaces are used,
- the information system is placed simultaneously in several certified data center areas,
- there are other implementation requirements where typical connection diagrams are not applicable.

Сетевое оборудование Заказчика (например, средства криптографической защиты информации, СКЗИ) размещается по согласованию и подключается в арендованный

The Customer's network equipment (for example, data encryption tools) shall be placed as agreed and shall be connected to the rented firewall or switch dedicated for the Customer.

и выделенный под Заказчика межсетевой экран или коммутатор.

ПРИЛОЖЕНИЕ 2 - Перечень мер, реализуемых Исполнителем в зоне своей ответственности, в инженерной инфраструктуре ЦОД в рамках Услуги

APPENDIX 2 - List of measures implemented by the Contractor within its area of liability, in the DC engineering infrastructure within the framework of the Service

Мера / Measure	Расшифровка / Description	Реализация / Implementation
ЗТС.2 / ZTS.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования / Arrangement of the controlled zone within which stationary information processing technical means, information protection hardware, as well as means for ensuring operation thereof will be permanently placed	Организована контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования / The controlled zone (within which stationary information processing hardware, information protection hardware, as well as means for ensuring operation thereof are permanently placed) will be arranged
ЗТС.3 / ZTS.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 / Control and monitoring of physical access to technical means, information protection hardware and means for ensuring operation thereof as well as to premises and structures wherein they are installed so to prevent unauthorized physical access to information processing means, information protection hardware, as well as means for ensuring operation of the information system, and also to premises and structures wherein they are installed	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. / Control and monitoring of physical access to technical means, information protection hardware and means for ensuring operation thereof as well as to premises and structures wherein they are installed so to prevent unauthorized physical access will be provided. Persons authorized to have access to technical means, information protection hardware and means for ensuring operation thereof as well as to premises and structures wherein they are installed will be assigned. Physical access to technical means, information

		protection hardware and means for ensuring operation thereof as well as to premises and structures wherein they are installed will be logged. Physical access control rules and procedures are regulated.
ЗТС.4 / ZTS.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр / Placement of information output (display) devices so to prevent its unauthorized viewing	Отсутствуют устройства вывода (отображения) информации. / No information output (display) devices are used.
ЗТС.5 / ZTS.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов) / Protection against external impacts (environmental impacts, power supply fluctuations, air conditioning and other external factors)	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. / Data centers where the certified data center segments are located comply with Tier III requirements. Measures to ensure the prompt power supply and/or air conditioning systems restoration have been implemented. Fire safety measures, equipment operating conditions and environmental conditions that meet the established requirements have been arranged.
УПД.3 / UPD.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами / Management (filtering, routing, connection control, unidirectional transmission and other management methods) of data streams between devices, information system segments, as well as between information systems	Условия предоставления услуги предполагают схему подключения сервера за выделенным межсетевым экраном, что позволяет выполнить требование по управлению информационными потоками. / Service provision terms envisage arrangement of the server connection diagram downstream of the dedicated firewall so to meet requirements for managing data streams.
УПД.4 / UPD.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы / Delimitation of powers (roles) for users, administrators and persons ensuring operation of the information system	Обеспечено разделение ролей администраторов информационной безопасности и лиц, обеспечивающих функционирование. Роли документированы. / Delimitation of roles for information security administrators and persons ensuring operation of the information system will be provided. Roles will be documented.
УПД.	Назначение минимально необходимых прав	Назначены минимально необходимые права

5 / UPD. 5	и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы / Assignment of the minimum required rights and privileges to users, administrators and persons ensuring operation of the information system	и привилегии в соответствии с должностными обязанностями. Роли и должностные обязанности документированы. / The minimum required rights and privileges will be assigned in accordance with job responsibilities. Roles and job responsibilities will be documented.
ЗИС. 17 / ZIS.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы / Splitting the information system into segments (information system segmentation) and ensuring protection of information system segment perimeters	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. / The server connection diagram provides for its mandatory placement downstream of the firewall so to meet requirements for splitting the information system into segments and ensuring protection of the segment perimeter.
ЗНИ. 1 / ZNI. 1	Учет машинных носителей информации / Registration of machine-readable media	Производится учет машинных носителей информации (жестких дисков) серверов. / Registration of servers` machine-readable media (hard disks) will be carried out.
ЗНИ. 2 / ZNI. 2	Управление доступом к машинным носителям информации / Machine-readable media access control	Обеспечивается управление доступом к машинным носителям информации, а именно определены должностные лица, имеющие физический доступ. Правила и процедуры доступа документированы. / Machine-readable media access control will be provided by assigning officials having physical access thereto. Access control rules and procedures will be documented.
ЗНИ. 8 / ZNI. 8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) / Destruction (deletion) of the data contained on machine-readable media when these are transferred between users, or to third-parties for repair or disposal as well as checking if data destruction (deletion) has been carried out properly	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. / Destruction (deletion) of the data contained on machine-readable media will be ensured in case of service cancellation and/or when machine-readable media are decommissioned. Procedures for destruction deletion) of the data contained on machine-readable media will be documented.
РСБ. 1 / RSB.	Определение событий безопасности, подлежащих регистрации, и сроков	Определены события безопасности, подлежащие регистрации, и сроки их хранения, в части

1	их хранения / Defining security events to be logged and its storage periods	физической безопасности. / Physical security events to be logged and their storage period will be defined.
РСБ. 2 / RSB. 2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации / Defining composition and content of information about security events to be logged	Определены и документированы состав и содержание информации о событиях безопасности, подлежащих регистрации, в части физической безопасности. / The composition and content of information about physical security events to be logged will be defined and documented.
РСБ. 3 / RSB. 3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения / Collection, recording and storage of information about security events for the specified storage period	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. / Information about physical security events will be collected, recorded and stored for the specified time period. Centralized automated management of collection, recording and storage of information related to physical security events will be provided.
РСБ. 5 / RSB. 5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них / Monitoring (viewing, analysis) of security event registration results and response thereto	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. / Monitoring (viewing, analysis) of security event registration results and responses thereto will be carried out. Rules and procedures for monitoring of physical security event registration results and responses thereto will be documented.
РСБ. 7 / RSB. 7	Защита информации о событиях безопасности / Protection of information about security events	Обеспечивается защита информации о событиях физической безопасности. Доступ к записям аудита и функциям управления предоставляется только уполномоченным должностным лицам. Обеспечивается резервное копирование записей аудита. / Information about physical security events will be protected. Access to audit records and management functions will be provided only to authorized officials. Audit record back-up will be ensured.
ОДТ. 1 / ODT. 1	Использование отказоустойчивых технических средств / Use of fail-safe hardware	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. / Fail-safe hardware are used in the data center infrastructure. Availability and reliability characteristic limit values will be determined and documented in the conditions of use. Availability and reliability characteristic limit values will be monitored. Hardware items that have reached the limit value will be replaced.
ОДТ.2 / ODT.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы / Redundancy of hardware, software, data transmission channels, means for ensuring operation of the information system	Инфраструктура дата-центра полностью зарезервирована. Применяются резервные технические средства, каналы передачи информации и средства обеспечения функционирования. Правила и процедуры резервирования документированы. / The data center infrastructure is fully redundant. Backup hardware, data transmission channels and means for ensuring operation of the information system will be used. Redundancy rules and procedures will be documented.
ОДТ.3 / ODT.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование / Monitoring of trouble-free operation of hardware, detection and localization of operation failures, taking measures to restore failed hardware and testing thereof	Осуществляется контроль безотказного функционирования инфраструктуры дата-центра, обнаружение и локализация отказов, принятие мер по восстановлению отказавших средств и их тестирование. / Monitoring of trouble-free operation of the data center infrastructure, detection and localization of operation failures, taking measures to restore failed hardware and testing thereof
ОДТ.7 / ODT.7	Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации / Control of the status and quality of computing resources (capacities) provided by the authorized person including those for data transmission	Пользовательское соглашение, условия использования отдельных сервисов и поручение на обработку персональных данных позволяют осуществлять контроль состояния и качества предоставления ресурсов. / User agreement, terms of the use for separate services, and the assignment for personal data processing make it possible to monitor the status and quality of provided resources.
ИНЦ.1 / INTs.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них / Assignment of persons to be responsible for detection of incidents and responding thereto	Определены лица, ответственные за выявление инцидентов физической безопасности и реагирование на них. / Persons responsible for detecting and responding to physical security incidents will be assigned.
ИНЦ.2 / INTs.	Обнаружение, идентификация и регистрация инцидентов /	Осуществляется обнаружение, идентификация и регистрация инцидентов физической

2	Detection, identification and logging of incidents	безопасности. / Physical security incidents will be detected, identified and logged.
ИНЦ .3 / INTs. 3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами / Users and administrators shall timely inform the persons responsible for detection of incidents and responding thereto, about the occurrence of incidents in the information system	Осуществляется своевременное информирование лиц, ответственных за выявление инцидентов физической безопасности и реагирование на них. / Persons responsible for identifying physical security incidents and responding thereto will be timely informed about relevant incidents.
ИНЦ .4 / INTs. 4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий / Incident analysis, including identifying sources and causes of incidents, as well as assessment of their consequences	В случае возникновения инцидента физической безопасности проводится анализ источников и причин возникновения, оценка последствий. / In case where a physical security incident occurs, sources and causes of incident occurrence will be identified and consequences thereof will be assessed.
ИНЦ .5 / INTs. 5	Принятие мер по устранению последствий инцидентов / Taking measures to eliminate consequences of incidents	В случае возникновения инцидента физической безопасности принимаются меры по устранению последствий. / In case where a physical security incident occurs, appropriate measures will be taken to eliminate consequences thereof.
ИНЦ .6 / INTs. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов / Planning and taking measures to prevent the recurrence of incidents	В случае возникновения инцидента физической безопасности проводится планирование и принятие мер по предотвращению повторного возникновения. / In case where a physical security incident occurs, appropriate measures to prevent its recurrence will be planned and taken.
УКФ. 1 / UKF. 1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты информации / Assignment of persons authorized to make changes in information system and information security system configurations	Определены лица, которым разрешены действия по внесению изменений в конфигурацию. / Persons authorized to make changes in the configuration of above mentioned systems will be assigned.
УКФ. 2 / UKF. 2	Управление изменениями конфигурации информационной системы и системы защиты информации / Managing changes in information system and information security system configurations	Процесс управления изменениями конфигурации документирован. / The process for managing configuration changes will be documented.
УКФ. 3 /	Анализ потенциального воздействия планируемых изменений в конфигурации	Проводится анализ потенциального воздействия планируемых изменений в конфигурации на

UKF.3	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 / Analysis of the potential impact of planned changes in information system and information security system configurations on ensuring the information security and coordination of changes in the information system configuration with the official responsible for ensuring information security	обеспечение защиты информации и согласование изменений в конфигурации с должностным лицом (работником), ответственным за обеспечение безопасности. / Potential impact of planned changes in information system and information security system configurations on ensuring the information security and coordination of changes in the relevant system configuration with the official responsible for ensuring information security will be analyzed.
УКФ.4 / UKF.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты информации / Documenting information (data) regarding changes made in the information system and information security system configurations	Осуществляется документирование информации об изменениях в конфигурации: схема подключения, схема размещения сервера, конфигурация сервера. / Information about changes made in the connection diagram configuration, server layout, and the server configuration will be documented.