Yandex.Cloud.

Матрица разделения ответственности PCI DSS

Contents

Введение

Клиенты, которые строят свое соответствие Стандарту безопасности данных индустрии платежных карт (PCI DSS) на базе компонентов Yandex.Cloud, должны использовать настоящий документ.

Документ описывает разделение ответственности за выполнение требований PCI DSS. Часть требований выполняет платформа Yandex.Cloud, часть должен выполнить Клиент, часть требований является обоюдной ответственностью сторон.

Разделение ответственности за выполнение большинства требований каждого раздела PCI DSS в зависимости от используемой модели облачных сервисов показано в таблице.

Набор требований PCI DSS		**Разделение ответственности**		
		IaaS	**PaaS**	**SaaS**
1	Install and maintain a firewall configuration to protect cardholder data	Обоюдная	Обоюдная	Yandex.Cloud
2	Do not use vendor-supplied defaults for system passwords and other security parameters	Обоюдная	Обоюдная	Yandex.Cloud
3	Protect stored cardholder data	Обоюдная	Обоюдная	Yandex.Cloud
4	Encrypt transmission of cardholder data across open, public networks	Клиент	Обоюдная	Yandex.Cloud
5	Protect all systems against malware and regularly update anti-virus software or programs	Клиент	Обоюдная	Yandex.Cloud
6	Develop and maintain secure systems and applications	Обоюдная	Обоюдная	Обоюдная
7	Restrict access to cardholder data by business need to know	Обоюдная	Обоюдная	Обоюдная
8	Identify and authenticate access to system components	Обоюдная	Обоюдная	Обоюдная
9	Restrict physical access to cardholder data	Yandex.Cloud	Yandex.Cloud	Yandex.Cloud
10	Track and monitor all access to network resources and cardholder data	Обоюдная	Обоюдная	Yandex.Cloud
11	Regularly test security systems and processes	Обоюдная	Обоюдная	Yandex.Cloud
12	Maintain a policy that addresses information security for all personnel	Обоюдная	Обоюдная	Обоюдная

	Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers	Yandex.Cloud	Yandex.Cloud	Yandex.Cloud
	Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS	Клиент	Клиент	Клиент

Документ подготовлен с учетом следующих документов:

- PCI DSS v3.2.1 — May 2018: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
- Information Supplement: PCI SSC Cloud Computing Guidelines: https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf

Последовательность действий для достижения соответствия требованиям PCI DSS

- Изучить настоящий документ
- Построить инфраструктуру, обрабатывающую данные платежных карт (CDE) на платформе Yandex.Cloud. Ссылка на гайд по построению PCI DSS контура.
- Выполнить требования PCI DSS в зоне ответственности Клиента
- Выбрать QSA-аудитора и провести аудит инфраструктуры, развернутой на платформе Yandex.Cloud, на соответствие требованиям PCI DSS

Область оценки PCI DSS

Платформа Yandex.Cloud соответствует всем требованиям PCI DSS 3.2.1 как Level 1 Service Provider. Клиенты могут использовать сервисы платформы Yandex.Cloud для построения инфраструктуры, отвечающей требованиям PCI DSS.

В область оценки входят базовая инфраструктура платформы Yandex.Cloud, а также сервисы на ее основе:

Infrastructure & Network

- Yandex Compute Cloud (https://cloud.yandex.ru/services/compute)
- Yandex Object Storage (https://cloud.yandex.ru/services/storage)
- Yandex Virtual Private Cloud (https://cloud.yandex.ru/services/vpc)
- Yandex Network Load Balancer (https://cloud.yandex.ru/services/load-balancer)
- Yandex Cloud Interconnect (https://cloud.yandex.ru/services/interconnect)
- Yandex Instance Groups (https://cloud.yandex.ru/services/instance-groups)
- Yandex API Gateway (https://cloud.yandex.ru/services/api-gateway)

Containers

- Yandex Container Registry (https://cloud.yandex.ru/services/container-registry)
- Yandex Managed Service for Kubernetes® (https://cloud.yandex.ru/services/managed-kubernetes)

Security

- Yandex Identity and Access Management (https://cloud.yandex.ru/services/iam)
- Yandex Certificate Manager (https://cloud.yandex.ru/services/certificate-manager)
- Yandex Key Management Service (https://cloud.yandex.ru/services/kms)

Data Platform

- Yandex Managed Service for PostgreSQL (https://cloud.yandex.ru/services/managed-postgresql)
- Yandex Managed Service for ClickHouse (https://cloud.yandex.ru/services/managed-clickhouse)
- Yandex Managed Service for MongoDB (https://cloud.yandex.ru/services/managed-mongodb)
- Yandex Managed Service for MySQL® (https://cloud.yandex.ru/services/managed-mysql)

- Yandex Managed Service for Redis™ (https://cloud.yandex.ru/services/managed-redis)
- Yandex Data Proc (https://cloud.yandex.ru/services/data-proc)
- Yandex Managed Service for Apache Kafka® (https://cloud.yandex.ru/services/managed-kafka)
- Yandex Managed Service for Elasticsearch (https://cloud.yandex.ru/services/managed-elasticsearch)
- Yandex Database (https://cloud.yandex.ru/services/ydb)

Serverless

- Yandex Message Queue (https://cloud.yandex.ru/services/message-queue)
- Yandex Cloud Functions (https://cloud.yandex.ru/services/functions)
- Yandex API Gateway (https://cloud.yandex.ru/services/api-gateway)
- Yandex Database (https://cloud.yandex.ru/services/ydb)
- Yandex Object Storage (https://cloud.yandex.ru/services/storage)

Operations

- Yandex Resource Manager (https://cloud.yandex.ru/services/resource-manager)

Полезные ссылки

- Создание группы безопасности
- Шифрование секретов в Yandex Managed Service for Kubernetes
- Шифрование по схеме envelope encryption
- Рекомендации по управлению доступом к Yandex.Cloud
- Использование SAML-совместимых федераций удостоверений

Матрица разделения ответственности PCI DSS

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

<table>
<tr><th>PCI DSS Requirements</th><th>Yandex.Cloud</th><th>Клиент</th></tr>
<tr><td>1.1 Establish and implement firewall and router configuration standards that include the following:</td><td rowspan="3">Платформа Yandex.Cloud отвечает за обеспечение безопасности согласно требованиям PCI DSS для сервисов в области оценки.
Платформа Yandex.Cloud обеспечивает реализацию опорной и SDN-сетей, а также процедур управления ими в соответствии с требованиями PCI DSS.
В инфраструктуре платформы Yandex.Cloud используется межсетевое экранирование (МЭ) на разных уровнях.</td><td rowspan="5">Клиент отвечает за реализацию процессов и процедур в соответствии с требованиями PCI DSS для компонентов, развернутых на платформе Yandex.Cloud, а именно:
подготовку необходимой внутренней документации в части управления межсетевыми экранами (МЭ) и сетевым оборудованием;
конфигурацию настроек сетевых компонентов Yandex.Cloud;
управление клиентскими виртуальными сетями;
управление МЭ и маршрутизаторами;
управление группами безопасности.
Для системного управления правилами МЭ рекомендуется использовать группы безопасности.</td></tr>
<tr><td>1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.</td></tr>
<tr><td>1.1.2 Current diagram that identifies all networks, network devices, and system components, with all connections between the CDE and other networks, including any wireless networks.</td></tr>
<tr><td>1.1.3 Current network diagram that shows all cardholder data flows across systems and networks.</td></tr>
<tr><td>1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.</td><td>Платформа Yandex.Cloud обеспечивает для сервисов в области оценки межсетевое экранирование и процессы управления им в соответствии с требованиями PCI DSS.
В инфраструктуре платформы Yandex.Cloud все соединения с сетями вне области оценки проходят фильтрацию через МЭ.</td></tr>
<tr><td>1.1.5 Description of groups, roles, and responsibilities for management of network components</td><td></td></tr>
</table>

1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	Платформа Yandex.Cloud отвечает за обеспечение безопасности согласно требованиям PCI DSS для сервисов в области оценки. Платформа Yandex.Cloud обеспечивает реализацию опорной и SDN-сетей, а также процедур управления ими в соответствии с требованиями PCI DSS.	
1.1.7 Requirement to review firewall and router rule sets at least every six months		
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки межсетевое экранирование и процессы управления им в соответствии с требованиями PCI DSS. В инфраструктуре платформы Yandex.Cloud контроль исходящего и входящего трафика реализован средствами МЭ с контролем состояния соединений.	Клиент отвечает за реализацию процессов и процедур в соответствии с требованиями PCI DSS для компонентов, развернутых на платформе Yandex.Cloud: • архитектуру проекта и конфигурацию настроек сетевых компонентов Yandex.Cloud; • управление клиентскими виртуальными сетями; • управление МЭ и маршрутизаторами; • используемый набор сервисов, протоколов и портов.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.		
1.2.2 Secure and synchronize router configuration files.		
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.		
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.		
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.		
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.		

1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.		
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.		
1.3.5 Permit only “established” connections into the network.		
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.		Клиент отвечает за конфигурирование клиентских сетей таким образом, чтобы серверы баз данных, в которых могут храниться данные платежных карт, размещались во внутренних сегментах виртуальных сред, недоступных напрямую из недоверенных сетей.
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: • Network Address Translation (NAT), • Placing servers containing cardholder data behind proxy servers/firewalls, • Removal or filtering of route advertisements for private networks that employ registered addressing, • Internal use of RFC1918 address space instead of registered addresses.	Платформа Yandex.Cloud отвечает за реализацию опорной и SDN-сетей, а также процедур управления ими в соответствии с требованиями PCI DSS.	Клиент отвечает за реализацию процессов и процедур в соответствии с требованиями PCI DSS: • архитектуру проекта и конфигурацию настроек сетевых компонентов Yandex.Cloud; • управление клиентскими виртуальными сетями; • управление МЭ и маршрутизаторами.
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or	Платформа Yandex.Cloud отвечает за безопасность рабочих станций	Клиент отвечает за установку и управление персональных МЭ и/или

employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running. • Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	пользователей, имеющих доступ к компонентам платформы Yandex.Cloud.	других средств защиты информации для всех рабочих мест пользователей, которые имеют доступ к компонентам платформы Yandex.Cloud, задействованным в обработке данных платежных карт.
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение всех необходимых документов и процедур согласно требованиям PCI DSS.	Клиент отвечает за документирование и выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Requirements	**Yandex.Cloud**	**Клиент**
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network.	Платформа Yandex.Cloud отвечает за выполнение требований PCI DSS в части настроек безопасности для всех компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за изменение параметров по умолчанию для компонентов, развернутых на платформе Yandex.Cloud: • операционных систем; • баз данных (за исключением PAAS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database); • прикладного ПО; • других компонентов и сервисов, включенных Клиентом в область оценки.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Требование неприменимо. Платформа Yandex.Cloud не использует беспроводные сети для передачи данных пользователей.	Клиент отвечает за настройку параметров безопасности используемых беспроводных сред.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Платформа Yandex.Cloud отвечает за выполнение группы требований 2.2 PCI DSS для компонентов,	Клиент отвечает за имплементацию настроек безопасности для

Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST)	обеспечивающих функционирование сервисов в области оценки.	компонентов, развернутых на платформе Yandex.Cloud: • операционных систем; • баз данных (за исключением PAAS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database); • прикладного ПО; • других компонентов и сервисов, включенных Клиентом в область оценки. Клиент отвечает за разделение ресурсов, реализующих функции различных уровней защиты, для компонентов, развернутых на платформе Yandex.Cloud. Документация по настройке отдельных сервисов: • Yandex Managed Service for PostgreSQL (Сервис Управления для PostgreSQL). • Yandex Managed Service for ClickHouse (Сервис Управления для ClickHouse).
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)		
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.		
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure		
2.2.4 Configure system security parameters to prevent misuse.		
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.		

		• Yandex Managed Service for MongoDB (Сервис Управления для MongoDB). • Yandex Managed Service for MySQL® (Сервис Управления для MySQL). • Yandex Managed Service for Redis™ (Сервис Управления для Redis). • Yandex Data Proc (Сервис Управления данными Data Proc). • Yandex Managed Service for Apache Kafka® (Сервис управления для Apache Kafka®) • Yandex Managed Service for Elasticsearch (Сервис для управления кластерами Elasticsearch и Kibana) • Yandex Managed Service for Kubernetes® (Сервис Управления для Kubernetes) • Yandex Database (Сервис Yandex Database)
2.3 Encrypt all non-console administrative access using strong cryptography.	Платформа Yandex.Cloud обеспечивает шифрование любого неконсольного административного доступа для компонентов,	Клиент отвечает за имплементацию безопасных протоколов и стойкой криптографии для доступа к

	обеспечивающих функционирование сервисов в области оценки.	компонентам, развернутым на платформе Yandex.Cloud.
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	Платформа Yandex.Cloud обеспечивает выполнение процедур учета для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за ведение журнала учета компонентов, развернутых на платформе Yandex.Cloud и входящих в область оценки соответствия стандарту PCI DSS.
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение всех необходимых документов и процедур.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.*	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение требований приложения A1 стандарта PCI DSS.	Требование неприменимо. *требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов

Requirement 3: Protect stored cardholder data

PCI DSS Requirements	Yandex.Cloud	Клиент
3.1 Keep cardholder data storage to a minimum by implementing data-retention and disposal policies, procedures and processes that include at least the following for all CHD storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed. A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	Требование неприменимо. Платформа Yandex.Cloud самостоятельно не обрабатывает данные платежных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе данных платежных карт.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.	Требование неприменимо. Платформа Yandex.Cloud самостоятельно не обрабатывает данные платежных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе SAD.
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	Требование неприменимо. Платформа Yandex.Cloud самостоятельно не обрабатывает данные платежных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе track.
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions after authorization.	Требование неприменимо. Платформа Yandex.Cloud самостоятельно не обрабатывает данные платежных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе CVC/CVV.
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	Требование неприменимо. Платформа Yandex.Cloud самостоятельно не обрабатывает данные платежных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе PIN.

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN.	Требование неприменимо. Платформа Yandex.Cloud самостоятельно не обрабатывает данные платежных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе PAN.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN). • Truncation (hashing cannot be used to replace the truncated segment of PAN). • Index tokens and pads (pads must be securely stored). • Strong cryptography with associated key-management processes and procedures.		
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	Требование неприменимо. Платформа Yandex.Cloud самостоятельно не обрабатывает данные платежных карт. Платформа Yandex.Cloud предоставляет Клиентам сервис Yandex Key Management Service для шифрования данных. Сервис KMS выполняет требования PCI DSS.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе использование шифрования. Клиент отвечает за процедуры управления ключами шифрования данных. Клиент может использовать сервис Yandex Key Management Service для защиты данных платежных карт при хранении.
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:	Требование неприменимо. Платформа Yandex.Cloud	-

	самостоятельно не обрабатывает данные платежных карт. Платформа Yandex.Cloud предоставляет Клиентам сервис Yandex Key Management Service для шифрования данных. Сервис KMS выполняет требования PCI DSS.	
3.5.1 ***Additional requirement for service providers only:*** Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and other SCDs used for key management		Требование неприменимо. *требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.		Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе использование шифрования. Клиент отвечает за процедуры управления ключами шифрования данных. Клиент может использовать сервис Yandex Key Management Service для защиты данных платежных карт при хранении.
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device). • As at least two full-length key components or key shares, in accordance with an industry-accepted method.		
3.5.4 Store cryptographic keys in the fewest possible locations.		
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	Требование неприменимо. Платформа Yandex.Cloud самостоятельно не обрабатывает данные платежных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе использование шифрования.
3.6.1 Generation of strong cryptographic keys.		

3.6.2 Secure cryptographic key distribution.	Платформа Yandex.Cloud предоставляет Клиентам сервис Yandex Key Management Service для шифрования данных. Сервис KMS выполняет требования PCI DSS.	Клиент отвечает за процедуры управления ключами шифрования данных. Клиент может использовать сервис Yandex Key Management Service для защиты данных платежных карт при хранении.
3.6.3 Secure cryptographic key storage.		
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).		
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.		

3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.		
3.6.7 Prevention of unauthorized substitution of cryptographic keys.		
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.		
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение всех необходимых документов и процедур.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirements	Yandex.Cloud	Клиент
4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.	Платформа Yandex.Cloud использует безопасные криптографические протоколы, обеспечивающие защиту данных при передаче.	Клиент отвечает за процессы безопасной передачи данных платежных карт, включая использование безопасных протоколов и шифрования. Клиент должен использовать компоненты, поддерживающие протоколы TLS 1.2 и выше. Yandex.Cloud рекомендует использовать шифрование данных платежных карт во всех случаях, включая передачу внутри клиентских сетей и передачу в общедоступных сетях.
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	Требование неприменимо. Платформа Yandex.Cloud не использует беспроводные сети для передачи данных пользователей.	Клиент отвечает за настройку параметров шифрования при аутентификации в случае использования беспроводных сетей для связи с компонентами платформы Yandex.Cloud, которые обрабатывают данные платежных карт.
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	Требование неприменимо. Платформа Yandex.Cloud самостоятельно не обрабатывает данные платежных карт и не передает данные пользователей в открытом виде.	Клиент отвечает за приведение PAN в нечитаемый вид в случае использования технологий обмена мгновенными сообщениями.

4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение всех необходимых документов и процедур.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

<table>
<tr><th>PCI DSS Requirements</th><th>Yandex.Cloud</th><th>Клиент</th></tr>
<tr><td>5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).</td><td rowspan="4">Платформа Yandex.Cloud отвечает за функционирование антивирусного программного обеспечения для компонентов, обеспечивающих функционирование сервисов в области оценки.</td><td rowspan="4">Клиент отвечает за процессы защиты от вредоносного ПО для компонентов, развернутых на платформе Yandex.Cloud и подверженных вирусному заражению.</td></tr>
<tr><td>5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.</td></tr>
<tr><td>5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.</td></tr>
<tr><td>5.2 Ensure that all anti-virus mechanisms are maintained as follows:
Are kept current.
Perform periodic scans.
Generate audit logs which are retained per PCI DSS Requirement 10.7.</td></tr>
<tr><td>5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.</td><td></td><td></td></tr>
<tr><td>5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.</td><td>Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение всех необходимых документов и процедур.</td><td>Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.</td></tr>
</table>

Requirement 6:Develop and maintain secure systems and applications

PCI DSS Requirements	**Yandex.Cloud**	**Клиент**
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.	Платформа Yandex.Cloud отвечает за процессы управления уязвимостями для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы управления уязвимостями для компонентов, развернутых на платформе Yandex.Cloud: • операционных систем; • баз данных (за исключением PAAS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database); • прикладного ПО; • других компонентов и сервисов, включенных Клиентом в область оценки.
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	Платформа Yandex.Cloud отвечает за процессы установки обновлений безопасности для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за установку обновлений для компонентов, развернутых на платформе Yandex.Cloud: • операционных систем; • баз данных (за исключением PAAS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL,

		ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database); • прикладного ПО; • других компонентов и сервисов, включенных Клиентом в область оценки.
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging). • Based on industry standards and/or best practices. • Incorporate information security throughout the software development life cycle.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS для процессов разработки компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS для процессов разработки своего ПО.
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.		
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines.		

• Appropriate corrections are implemented prior to release. • Code review results are reviewed and approved by management prior to release.		
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	Платформа Yandex.Cloud отвечает за выполнение требований PCI DSS для процедур контроля изменений компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в отношении всех изменений в компонентах, развернутых на платформе Yandex.Cloud.
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.		
6.4.2 Separation of duties between development/test and production environments.		
6.4.3 Production data (live PANs) are not used for testing or development.		
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.		
6.4.5 Change control procedures must include the following:		
6.4.5.1 Documentation of impact.		
6.4.5.2 Documented change approval by authorized parties.		
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.		
6.4.5.4 Back-out procedures.		

6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.		
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS при разработке компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS для процессов разработки своего ПО.
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.		
6.5.2 Buffer overflow.		
6.5.3 Insecure cryptographic storage.		
6.5.4 Insecure communications.		
6.5.5 Improper error handling.		
6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).		
6.5.7 Cross-site scripting (XSS).		
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).		

6.5.9 Cross-site request forgery (CSRF).		
6.5.10 Broken authentication and session management**.**		
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	Платформа Yandex.Cloud отвечает за соблюдение требования PCI DSS в части защиты общедоступных веб-приложений для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за защиту собственных общедоступных веб-приложений, развернутых на платформе Yandex.Cloud.
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение всех необходимых документов и процедур.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Requirements	**Yandex.Cloud**	**Клиент**
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части контроля и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы контроля и управления доступом к компонентам, развернутым на платформе Yandex.Cloud.
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function. • Level of privilege required (for example, user, administrator, etc.) for accessing resources.		
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.		
7.1.3 Assign access based on individual personnel's job classification and function.		
7.1.4 Require documented approval by authorized parties specifying required privileges.		
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:		
7.2.1 Coverage of all system components.		
7.2.2 Assignment of privileges to individuals based on job classification and function.		

7.2.3 Default “deny-all” setting.		
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение всех необходимых документов и процедур.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

Requirement 8:Identify and authenticate access to system components

PCI DSS Requirements	**Yandex.Cloud**	**Клиент**
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части контроля и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы контроля и управления доступом к компонентам, развернутым на платформе Yandex.Cloud.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.		
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.		
8.1.3 Immediately revoke access for any terminated users.		
8.1.4 Remove/disable inactive user accounts within 90 days.		
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.		
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.		
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.		
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.		

8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов аутентификации и управления доступом для компонентов, развернутых на платформе Yandex.Cloud. Для централизованного управления учетными данными рекомендуется использовать SAML-совместимые федерации удостоверений.
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.		
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.		
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.		
8.2.4 Change user passwords/passphrases at least once every 90 days.		
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.		

8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.		
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части многофакторной аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования многофакторной аутентификации для компонентов, развернутых на платформе Yandex.Cloud.
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.		
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.		
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials. • Guidance for how users should protect their authentication credentials. • Instructions not to reuse previously used passwords. • Instructions to change passwords if there is any suspicion the password could be compromised.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов аутентификации и управления доступом для компонентов, развернутых на платформе Yandex.Cloud.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов аутентификации и управления доступом для компонентов, развернутых на платформе Yandex.Cloud.

8.5.1 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	По умолчанию сотрудники Yandex.Cloud не имеют доступа к ресурсам Клиентов, расположенным на платформе Yandex.Cloud.	Требование неприменимо. *требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.) use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов аутентификации и управления доступом для компонентов, развернутых на платформе Yandex.Cloud.
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части аутентификации и управления доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов аутентификации и управления доступом для компонентов, развернутых на платформе Yandex.Cloud.
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение всех	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

	необходимых документов и процедур	

Requirement 9:Restrict physical access to cardholder data

PCI DSS Requirements	**Yandex.Cloud**	**Клиент**
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Платформа Yandex.Cloud обеспечивает физическую безопасность дата-центров, в которых расположены компоненты, обеспечивающие функционирование сервисов в области оценки.	Требование неприменимо, если данные не передаются за пределы платформы Yandex.Cloud. Если данные передаются за пределы платформы, то Клиент отвечает за выполнение требований PCI DSS в части управления физическим доступом для всех мест обработки данных платежных карт.
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.		
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks.		
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.		
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges). • Changes to access requirements. • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).	Платформа Yandex.Cloud обеспечивает физическую безопасность дата-центров, в которых расположены компоненты, обеспечивающие функционирование сервисов в области оценки.	Требование неприменимо, если данные не передаются за пределы платформы Yandex.Cloud. Если данные передаются за пределы платформы, то Клиент отвечает за выполнение требований PCI DSS в части управления физическим доступом для всех мест обработки данных платежных карт.

9.3 Control physical access for onsite personnel to sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	Платформа Yandex.Cloud обеспечивает физическую безопасность дата-центров, в которых расположены компоненты, обеспечивающие функционирование сервисов в области оценки.	Требование неприменимо, если данные не передаются за пределы платформы Yandex.Cloud. Если данные передаются за пределы платформы, то Клиент отвечает за выполнение требований PCI DSS в части управления физическим доступом для всех мест обработки данных платежных карт.
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	Платформа Yandex.Cloud обеспечивает физическую безопасность дата-центров, в которых расположены компоненты, обеспечивающие функционирование сервисов в области оценки.	Требование неприменимо, если данные не передаются за пределы платформы Yandex.Cloud. Если данные передаются за пределы платформы, то Клиент отвечает за выполнение требований PCI DSS в части управления физическим доступом для всех мест обработки данных платежных карт.
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.		
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.		
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.		
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.		
9.5 Physically secure all media.		

9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.	Платформа Yandex.Cloud обеспечивает выполнение требований PCI DSS в части физической безопасности дата-центров и носителей информации, содержащих данные Клиентов, для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за защиту носителей данных (например, автоматизированных рабочих мест (АРМ) пользователей, съемных электронных носителей, бумажных чеков, бумажных отчетов и факсов), если такие применяются в процессах обработки данных платежных карт.
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:		
9.6.1 Classify media so the sensitivity of the data can be determined.		
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.		
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).		
9.7 Maintain strict control over the storage and accessibility of media.	Платформа Yandex.Cloud обеспечивает выполнение требований PCI DSS в части физической безопасности дата-центров и носителей информации, содержащих данные Клиентов, для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за контроль хранения/уничтожения и управление доступом к носителям данных (например, АРМ пользователей, съемным электронным носителям, бумажным чекам, бумажным отчетам и факсам), если такие применяются в процессах обработки данных платежных карт.
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.		
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:		
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.		
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.		

9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	Требование неприменимо.	Клиент отвечает за защиту устройств, считывающих данные с платежных карт путем прямого физического взаимодействия с картой.
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device. • Location of device (for example, the address of the site or facility where the device is located). • Device serial number or other method of unique identification.		
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).		
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).		
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	Платформа Yandex.Cloud обеспечивает выполнение всех необходимых документов и	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

	процедур для сервисов в области оценки.	

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Requirements	**Yandex.Cloud**	**Клиент**
10.1 Implement audit trails to link all access to system components to each individual user.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части регистрации событий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части ведения журналов регистрации событий для компонентов, развернутых на платформе Yandex.Cloud. Клиент может видеть операции над ресурсами в web-консоли Yandex.Cloud. Клиент может обратиться в службу поддержки для получения дополнительной информации из журналов регистрации событий Yandex.Cloud.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части регистрации необходимых типов событий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части регистрации необходимых типов событий для компонентов, развернутых на платформе Yandex.Cloud, а именно: • операционных систем; • баз данных (за исключением PAAS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache
10.2.1 All individual user accesses to cardholder data.		
10.2.2 All actions taken by any individual with root or administrative privileges.		
10.2.3 Access to all audit trails.		
10.2.4 Invalid logical access attempts.		
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and		

elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.		Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database); • прикладного ПО; • других компонентов и сервисов, включенных Клиентом в область оценки.
10.2.6 Initialization, stopping, or pausing of the audit logs.		
10.2.7 Creation and deletion of system-level objects		
10.3 Record at least the following audit trail entries for all system components for each event:	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части регистрации параметров событий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части регистрации параметров событий для компонентов, развернутых на платформе Yandex.Cloud: • операционных систем; • баз данных (за исключением PAAS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database); • прикладного ПО; • других компонентов и сервисов, включенных Клиентом в область оценки.
10.3.1 User identification		
10.3.2 Type of event		
10.3.3 Date and time		
10.3.4 Success or failure indication		
10.3.5 Origination of event		
10.3.6 Identity or name of affected data, system component, or resource		
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части синхронизации времени для компонентов, обеспечивающих	Клиент отвечает за выполнение требований PCI DSS в части синхронизации времени для компонентов, развернутых на платформе Yandex.Cloud. См.
10.4.1 Critical systems have the correct and consistent time.		

10.4.2 Time data is protected. **10.4.3** Time settings are received from industry-accepted time sources.	функционирование сервисов в области оценки.	рекомендации по настройке синхронизации времени с использованием NTP.
10.5 Secure audit trails so they cannot be altered. **10.5.1** Limit viewing of audit trails to those with a job-related need. **10.5.2** Protect audit trail files from unauthorized modifications. **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter. **10.5.4** Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. **10.5.5** Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части защиты журналов регистрации событий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части защиты журналов регистрации событий для компонентов, развернутых на платформе Yandex.Cloud.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. **10.6.1** Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части проверки и анализа зарегистрированных событий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части проверки и анализа зарегистрированных событий для компонентов, развернутых на платформе Yandex.Cloud.

systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).		
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.		
10.6.3 Follow up exceptions and anomalies identified during the review process.		
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части хранения зарегистрированных событий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части хранения зарегистрированных событий для компонентов, развернутых на платформе Yandex.Cloud.
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части фиксации и выявления отказов систем контроля безопасности для компонентов, обеспечивающих функционирование сервисов в области оценки.	Требование неприменимо. *требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов

10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls		
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение всех необходимых документов и процедур.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

Requirement 11: Regularly test security systems and processes

PCI DSS Requirements	Yandex.Cloud	Клиент
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части обнаружения и идентификации авторизованных и неавторизованных беспроводных точек доступа для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части обнаружения и идентификации авторизованных и неавторизованных беспроводных точек доступа для своего периметра безопасности.
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.		
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.		
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части регулярного проведения внешних ASV-сканирований, внутренних сканирований безопасности, а также устранения найденных уязвимостей для компонентов, обеспечивающих функционирование сервисов в области оценки. В область ежеквартальных внешних ASV-сканирований включены, среди прочего, публичные API платформы Yandex.Cloud.	Клиент отвечает за выполнение требований PCI DSS в части регулярного проведения внешних ASV-сканирований, внутренних сканирований безопасности, а также устранения найденных уязвимостей для компонентов, развернутых на платформе Yandex.Cloud. Клиент также отвечает за проведение сканирований внешних IP-адресов. Сканирования должны выполняться согласно опубликованному документу Правила проведения внешних сканирований безопасности
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high-risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.		
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.		

11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.		
11.3 Implement a methodology for penetration testing that includes at least the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115). • Includes coverage for the entire CDE perimeter and critical systems. • Includes testing from both inside and outside of the network. • Includes testing to validate any segmentation and scope reduction controls. • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5. • Defines network-layer penetration tests to include components that support network functions as well as operating systems. • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months. • Specifies retention of penetration testing results and remediation activities results.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части регулярного проведения внешних и внутренних тестирований на проникновение, а также устранения найденных недостатков для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части регулярного проведения внешних и внутренних тестирований на проникновение, а также устранения найденных недостатков для компонентов, развернутых на платформе Yandex.Cloud.
11.3.1 Perform ***external*** penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).		
11.3.2 Perform **internal** penetration testing at least annually and after any significant infrastructure or application upgrade or modification		

(such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).		
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.		
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.		
11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.		
11.4 Use intrusion-detection systems and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части использования методов и систем обнаружения/предотвращения вторжений для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования методов и систем обнаружения/предотвращения вторжений для компонентов, развернутых на платформе Yandex.Cloud.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части использования механизмов контроля целостности файлов для компонентов, обеспечивающих	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов контроля целостности файлов для

11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	функционирование сервисов в области оценки.	компонентов, развернутых на платформе Yandex.Cloud.
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	Платформа Yandex.Cloud обеспечивает для сервисов в области оценки выполнение всех необходимых документов и процедур.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платежных карт.

Requirement 12: Maintain a policy that addresses information security for all personnel

PCI DSS Requirements	**Yandex.Cloud**	**Клиент**
12.1 Establish, publish, maintain, and disseminate a security policy.	Платформа Yandex.Cloud отвечает за выполнение требований PCI DSS в части разработки и соблюдения политики безопасности и других процедур обеспечения ИБ для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части разработки и соблюдения политики безопасности и других процедур обеспечения ИБ для компонентов, развернутых на платформе Yandex.Cloud.
12.1.1 Review the security policy at least annually and update the policy when business objectives or the risk environment change.		
12.2 Implement a risk assessment process, that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части процедур оценки рисков для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части процедур оценки рисков для компонентов, развернутых на платформе Yandex.Cloud.
12.3 Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following:	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части использования критичных технологий для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования критичных технологий для компонентов, развернутых на платформе Yandex.Cloud.
12.3.1 Explicit approval by authorized parties.		
12.3.2 Authentication for use of the technology.		
12.3.3 A list of all such devices and personnel with access.		

12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).		
12.3.5 Acceptable uses of the technology.		
12.3.6 Acceptable network locations for the technologies.		
12.3.7 List of company-approved products.		
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.		
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.		
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.		
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности по обеспечению ИБ для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Yandex.Cloud.

12.4.1 ***Additional requirement for service providers only:*** Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management	Платформа Yandex.Cloud отвечает за выполнение программы соответствия требованиям PCI DSS для компонентов, обеспечивающих функционирование сервисов в области оценки.	Требование неприменимо. *требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов
12.5 Assign to an individual or team the following information security management responsibilities:	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности по обеспечению ИБ для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развернутых на платформе Yandex.Cloud.
12.5.1 Establish, document, and distribute security policies and procedures.		
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.		
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.		
12.5.4 Administer user accounts, including additions, deletions, and modifications.		
12.5.5 Monitor and control all access to data.		
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части обучения сотрудников и повышения их осведомленности о	Клиент отвечает за выполнение требований PCI DSS в части обучения сотрудников и повышения их осведомленности о безопасности
12.6.1 Educate personnel upon hire and at least annually.		

12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	безопасности для компонентов, обеспечивающих функционирование сервисов в области оценки.	для компонентов, развернутых на платформе Yandex.Cloud.
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части проверки потенциальных сотрудников до их приема на работу в сервисы, входящие в область оценки.	Клиент отвечает за выполнение требований PCI DSS в части проверки потенциальных сотрудников до их приема на работу для компонентов, развернутых на платформе Yandex.Cloud.
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	Платформа Yandex.Cloud не передает данные Клиентов сторонним компаниям. Yandex.Cloud отвечает за соблюдение требований PCI DSS в части взаимодействия с сервис-провайдерами, которые могут повлиять на безопасность данных Клиентов.	Клиент отвечает за выполнение требований PCI DSS в части взаимодействия с сервис-провайдерами, которые могут повлиять на безопасность данных платежных карт.
12.8.1 Maintain a list of service providers including a description of the service provided.		
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's CDE.		
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.		
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.		

12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.		
12.9 ***Additional requirement for service providers only*****:** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Платформа Yandex.Cloud заключает с Клиентами договор, в котором явно определена ответственность за безопасность данных.	Требование неприменимо. *требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части реагирования на инциденты и тестирования планов реагирования на инциденты для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части реагирования на инциденты и тестирования планов реагирования на инциденты для компонентов, развернутых на платформе Yandex.Cloud.
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum. • Specific incident response procedures. • Business recovery and continuity procedures. • Data back-up processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. Reference or inclusion of incident response procedures from the payment brands.		
12.10.2 Review and test the plan at least annually, including all elements listed in Requirement 12.10.1.		

12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.		
12.10.4 Provide appropriate training to staff with security breach response responsibilities.		
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.		
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.		

12.11 ***Additional requirement for service providers only:*** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes	Платформа Yandex.Cloud отвечает за проведение периодических проверок выполнения требований PCI DSS для компонентов, обеспечивающих функционирование сервисов в области оценки.	Требование неприменимо. *требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов
12.11.1 ***Additional requirement for service providers only:*** Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program		

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

PCI DSS Requirements	**Yandex.Cloud**	**Клиент**
A1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A1.1 through A1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.	Платформа Yandex.Cloud отвечает за соблюдение требований PCI DSS в части: • предоставления механизмов управления доступом, обеспечивающих изоляцию разных Клиентов; • разграничения сред разных Клиентов; • ведения и хранения журналов регистрации событий в API для каждого Клиента; • информирования Клиентов в случае обнаружения и расследования инцидентов ИБ.	Требование неприменимо. *требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов
A1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.		
A1.2 Restrict each entity's access and privileges to its own cardholder data environment only.		
A1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.		
A1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.		

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

PCI DSS Requirements	**Yandex.Cloud**	**Клиент**
A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either:	Требование неприменимо.	Клиент отвечает за выполнение требований PCI DSS в части

• Confirm the devices are not susceptible to any known exploits for those protocols. ***Or:*** Have a formal Risk Mitigation and Migration Plan in place.	Платформа Yandex.Cloud не использует POS/POI-терминалы.	использования безопасных версий используемых протоколов TLS.
A2.2 Entities with existing implementations (other than as allowed in A.2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.		
A2.3 ***Additional Requirement for Service Providers Only:*** All service providers must provide a secure service offering by June 30, 2016.		