Yandex Cloud

Матрица разделения ответственности PCI DSS v4

Yandex Cloud. Матрица разделения ответственности PCI DSS v4.
Этот документ является составной частью технической документации Yandex Cloud.

Предупреждение об исключительных правах и конфиденциальной информации

Исключительные права на все результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальную собственность), используемые при разработке, поддержке и эксплуатации службы Yandex Cloud, включая, но не ограничиваясь, программы для ЭВМ, базы данных, изображения, тексты, другие произведения, а также изобретения, полезные модели, товарные знаки, знаки обслуживания, коммерческие обозначения и фирменные наименования, принадлежат ООО «Яндекс.Облако» либо его лицензиарам.

Использование результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации в целях, не связанных с разработкой, поддержкой и эксплуатацией службы Yandex Cloud, не допускается без получения предварительного согласия правообладателя. Настоящий документ содержит конфиденциальную информацию ООО «Яндекс.Облако». Использование конфиденциальной информации в целях, не связанных с разработкой, поддержкой и эксплуатацией службы Yandex Cloud, а равно как и разглашение таковой, не допускается. При этом под разглашением понимается любое действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Отношения ООО «Яндекс.Облако» с лицами, привлекаемыми для разработки, поддержки и эксплуатации службы Yandex Cloud, регулируются законодательством Российской Федерации и заключаемыми в соответствии с ним трудовыми и/или гражданско-правовыми договорами (соглашениями). Нарушение требований об охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, а равно как и конфиденциальной информации, влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Контактная информация ООО «Яндекс.Облако» https://cloud.yandex.ru/

Тел.: +7 495 739 7000
Email: cloud_docs@yandex-team.ru
Главный офис: 119021, Россия, г. Москва, ул. Льва Толстого, д. 16

Содержание

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 Network Security Controls	Обоюдная	Обоюдная	Yandex Cloud
2	Apply Secure Configurations to All System Components	Обоюдная	Обоюдная	Yandex Cloud
3	Protect Stored Account Data	Обоюдная	Обоюдная	Yandex Cloud
4	Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	Обоюдная	Обоюдная	Yandex Cloud
5	Protect All Systems and Networks from Malicious Software	Обоюдная	Обоюдная	Yandex Cloud
6	Develop and Maintain Secure Systems and Software	Обоюдная	Обоюдная	Обоюдная
7	Restrict Access to System Components and Cardholder Data by Business Need to Know	Обоюдная	Обоюдная	Обоюдная
8	Identify Users and Authenticate Access to System Components	Обоюдная	Обоюдная	Обоюдная
9	Restrict Physical Access to Cardholder Data	Yandex Cloud	Yandex Cloud	Yandex Cloud
10	Log and Monitor All Access to System Components and Cardholder Data	Обоюдная	Обоюдная	Yandex Cloud
11	Test Security of Systems and Networks Regularly	Обоюдная	Обоюдная	Yandex Cloud
12	Support Information Security with Organizational Policies and Programs	Обоюдная	Обоюдная	Обоюдная
A1	Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers	Yandex Cloud	Yandex Cloud	Yandex Cloud
A2	Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for CardPresent POS POI Terminal Connections	Клиент	Клиент	Клиент
A3	Appendix A3: Designated Entities Supplemental Validation (DESV)	Обоюдная	Обоюдная	Обоюдная

Рекомендуемая последовательность действий Клиента для соответствия требованиям PCI DSS

- Изучить настоящий документ, четко понимать свою зону ответственности
- Построить инфраструктуру, обрабатывающую данные платежных карт (CDE) на платформе Yandex Cloud. Требования и рекомендации по построению такой инфраструктуры приведены в документации по ссылке: https://yandex.cloud/ru/docs/security/standard/all
- 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 Yandex Cloud по требованиям стандарта PCI DSS

Платформа Yandex Cloud соответствует требованиям PCI DSS v4 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. Перечень сервисов определен в Attestation of Compliance (AoC). AoC для платформы Yandex Cloud можно получить на странице https://yandex.cloud/ru/security/standards/pci

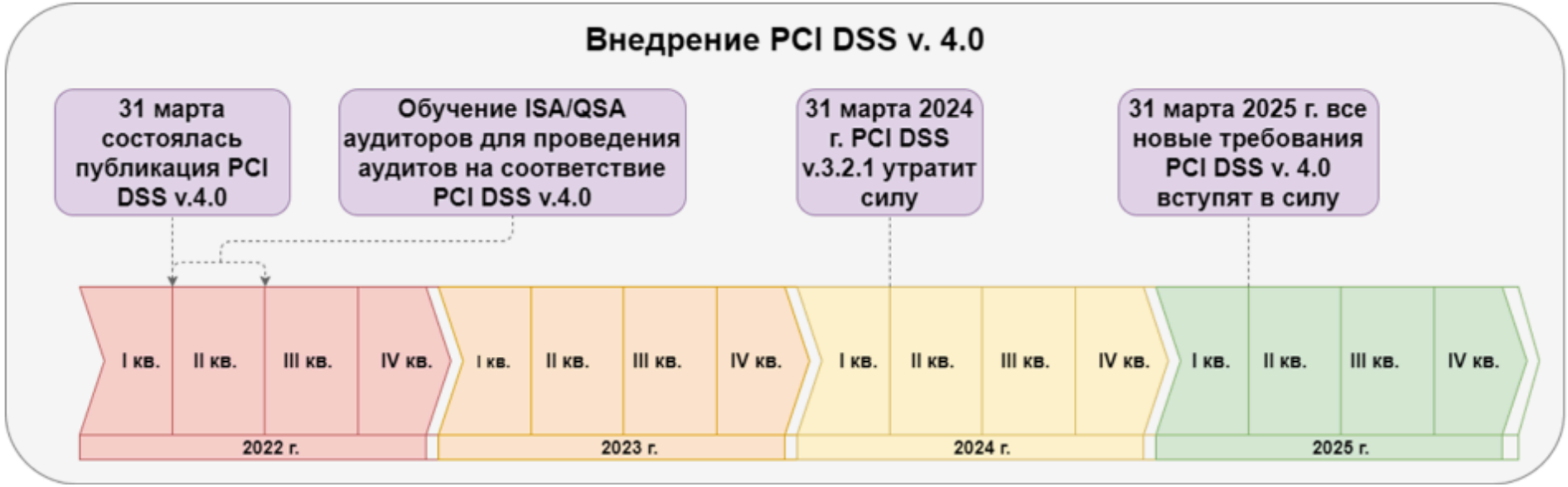
Матрица разделения ответственности PCI DSS v 4.0

Основные изменения PCI DSS v 4.0

- Добавлен новый подход к выполнению требований.
- Добавлены пояснения к критериям области применимости стандарта.
- Добавлены новые требования с отложенным обязательным выполнением.
- Скорректирована терминология и формулировки.
- Перенесена информация из вспомогательных руководств в разделы стандарта.

Полный список изменений версии PCI DSS 4.0 по сравнению с PCI DSS v3.2.1 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf

Согласно плану перехода, пройти QSA-аудит по новой версии PCI DSS 4.0 можно уже сейчас. С третьего квартала 2022 года можно проходить аудит как по версии 3.2.1, так и по версии 4.0. С 31 марта 2024 года PCI DSS 3.2.1 утратит силу.



Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls.

PCI DSS Requirements	Yandex Cloud	Клиент
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.		
Defined Approach Requirements **1.1.1** All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 1 are defined, understood, and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за документирование и выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.
Defined Approach Requirements **1.1.2** Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood. Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 1 are allocated. Personnel are accountable for successful, continuous operation of these requirements	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
1.2 Network security controls (NSCs) are configured and maintained.		
Defined Approach Requirements		

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic. Customized Approach Objective The way that NSCs are configured and operate are defined and consistently applied.	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.	Клиент отвечает за реализацию процессов и процедур в соответствии с требованиями PCI DSS для компонентов, развёрнутых на платформе Yandex Cloud, а именно: • внедрение процедур и 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; • используемый набор сервисов, протоколов и портов; • управление группами безопасности. Для системного управления правилами МЭ рекомендуется использовать группы безопасности.
Defined Approach Requirements **1.2.2** All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1. Customized Approach Objective Changes to network connections and NSCs cannot result in misconfiguration, implementation of insecure services, or unauthorized network connections.		
Defined Approach Requirements **1.2.3** An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks. Customized Approach Objective A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available.		
Defined Approach Requirements **1.2.4** An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment. Customized Approach Objective A representation of all transmissions of account data between system components and across network segments is maintained and available.		
Defined Approach Requirements		

1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need. Customized Approach Objective Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.		
Defined Approach Requirements **1.2.6** Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated. Customized Approach Objective The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.		
Defined Approach Requirements **1.2.7** Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective. Customized Approach Objective NSC configurations that allow or restrict access to trusted networks are verified periodically to ensure that only authorized connections with a current business justification are permitted.		
Defined Approach Requirements **1.2.8** Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations. Customized Approach Objective NSCs cannot be defined or modified using untrusted configuration objects (including files).	Платформа Yandex Cloud отвечает за обеспечение безопасности согласно требованиям PCI DSS для сервисов в области оценки, в том числе безопасное хранение конфигураций сетевых устройств и SDN-сетей.	Клиент отвечает за реализацию процессов и процедур в соответствии с требованиями PCI DSS для компонентов, развёрнутых 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.
1.3 Network access to and from the cardholder data environment is restricted.		
Defined Approach Requirements 1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied. Customized Approach Objective Unauthorized traffic cannot enter the CDE.	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 используется межсетевое экранирование (МЭ) на разных уровнях.	Клиент отвечает за реализацию ограничений сетевого трафика в соответствии с требованиями PCI DSS для компонентов, развёрнутых на платформе Yandex Cloud: • архитектуру проекта и 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.
Defined Approach Requirements 1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied. Customized Approach Objective Unauthorized traffic cannot leave the CDE.		
Defined Approach Requirements 1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE. Customized Approach Objective Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.		

1.4 Network connections between trusted and untrusted networks are controlled.		
Defined Approach Requirements 1.4.1 NSCs are implemented between trusted and untrusted networks. Customized Approach Objective Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.	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 реализован контроль исходящего и входящего трафика средствами МЭ с контролем состояния соединений, а также реализованы меры антиспуфинга.	Клиент отвечает за реализацию ограничений сетевого трафика в соответствии с требованиями PCI DSS для компонентов, развёрнутых на платформе Yandex Cloud: • архитектуру проекта и 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.
Defined Approach Requirements 1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied. Customized Approach Objective Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network.		
Defined Approach Requirements 1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network. Customized Approach Objective Packets with forged IP source addresses cannot enter a trusted network.		
Defined Approach Requirements 1.4.4 System components that store cardholder data are not directly accessible from untrusted networks. Customized Approach Objective Stored cardholder data cannot be accessed from untrusted networks.	Платформа Yandex Cloud обеспечивает для сервисов в области оценки межсетевое экранирование и процессы	Клиент отвечает за конфигурирование клиентских сетей таким образом, чтобы серверы баз данных, в которых могут храниться данные платёжных карт,

	управления им в соответствии с требованиями PCI DSS.	размещались во внутренних сегментах виртуальных сред, недоступных напрямую из недоверенных сетей.
Defined Approach Requirements 1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties. Customized Approach Objective Internal network information is protected from unauthorized disclosure.	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.
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.		
Defined Approach Requirements 1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. Customized Approach Objective Devices that connect to untrusted environments and also connect to the CDE cannot introduce threats to the entity's CDE.	Платформа Yandex Cloud отвечает за безопасность рабочих станций своих пользователей, имеющих доступ к компонентам платформы Yandex Cloud.	Клиент отвечает за установку средств защиты информации и управление ими для всех рабочих мест пользователей, которые имеют доступ к компонентам платформы Yandex Cloud, задействованным в обработке данных платёжных карт.

Requirement 2: Apply Secure Configurations to All System Components

PCI DSS Requirements	Yandex Cloud	Клиент
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood		
Defined Approach Requirements 2.1.1 All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 2 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.
Defined Approach Requirements 2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood. Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 2 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
2.2 System components are configured and managed securely.		
Defined Approach Requirements **2.2.1** Configuration standards are developed, implemented, and maintained to: • Cover all system components.	Платформа Yandex Cloud отвечает за выполнение группы требований 2.2 PCI DSS для компонентов, обеспечивающих	Клиент отвечает за имплементацию настроек безопасности для компонентов, развёрнутых на платформе Yandex Cloud:

• Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment. Customized Approach Objective All system components are configured securely and consistently and in accordance with industry- accepted hardening standards or vendor recommendations.	функционирование сервисов в области оценки.	• операционных систем; • баз данных ((за исключением PAAS-сервисов); • прикладного ПО; • других компонентов и сервисов, включённых Клиентом в область оценки. Клиент отвечает за разделение ресурсов, реализующих функции различных уровней защиты, для компонентов, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements 2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled. Customized Approach Objective System components cannot be accessed using default passwords.		
Defined Approach Requirements 2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR		

• Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need. Customized Approach Objective Primary functions with lower security needs cannot affect the security of primary functions with higher security needs on the same system component.		
Defined Approach Requirements 2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled. Customized Approach Objective System components cannot be compromised by exploiting unnecessary functionality present in the system component.		
Defined Approach Requirements 2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons. Customized Approach Objective System components cannot be compromised by exploiting insecure services, protocols, or daemons.		
Defined Approach Requirements 2.2.6 System security parameters are configured to prevent misuse. Customized Approach Objective System components cannot be compromised because of incorrect security parameter configuration.		
Defined Approach Requirements 2.2.7 All non-console administrative access is encrypted using strong cryptography.	Платформа Yandex Cloud обеспечивает шифрование любого неконсольного административного	Клиент отвечает за имплементацию безопасных протоколов и стойкой криптографии для доступа к

Customized Approach Objective Cleartext administrative authorization factors cannot be read or intercepted from any network transmissions.	доступа для компонентов, обеспечивающих функционирование сервисов в области оценки.	компонентам, развёрнутым на платформе Yandex Cloud.
2.3 Wireless environments are configured and managed securely		
Defined Approach Requirements 2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults. Customized Approach Objective Wireless networks cannot be accessed using vendor default passwords or default configurations.	Требование неприменимо. Платформа Yandex Cloud не использует беспроводные сети для передачи данных пользователей.	Клиент отвечает за настройку параметров безопасности используемых беспроводных сред.
Defined Approach Requirements 2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised. Customized Approach Objective Knowledge of wireless encryption keys cannot allow unauthorized access to wireless networks.		

Protect Account Data

Requirement 3: Protect Stored Account Data.

PCI DSS Requirements	Yandex Cloud	Клиент
3.3 Processes and mechanisms for protecting stored account data are defined and understood.		
Defined Approach Requirements 3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 3 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.
Defined Approach Requirements 3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood. Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 3 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
3.2 Storage of account data is kept to a minimum.		
Defined Approach Requirements		

3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable. Customized Approach Objective Account data is retained only where necessary and for the least amount of time needed and is securely deleted or rendered unrecoverable when no longer needed.	Требование неприменимо. Платформа Yandex Cloud самостоятельно не обрабатывает данные платёжных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе данных платёжных карт.
Defined Approach Requirements 3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. Customized Approach Objective This requirement is not eligible for the customized approach.		
3.3 Sensitive authentication data (SAD) is not stored after authorization.		
Defined Approach Requirements		

3.3.1 SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. Customized Approach Objective This requirement is not eligible for the customized approach.	Требование неприменимо. Платформа Yandex Cloud самостоятельно не обрабатывает данные платёжных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе данных платёжных карт.
Defined Approach Requirements 3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography. Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements 3.3.3 Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. Customized Approach Objective Sensitive authentication data is retained only as required to support issuing functions and is secured from unauthorized access.		
3.4 Access to displays of full PAN and ability to copy PAN is restricted.		
Defined Approach Requirements 3.4.1 PAN is masked when displayed (the BIN 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 the BIN and last four digits of the PAN. Customized Approach Objective	Требование неприменимо. Платформа Yandex Cloud самостоятельно не обрабатывает данные платёжных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе PAN.

PAN displays are restricted to the minimum number of digits necessary to meet a defined business need.		
Defined Approach Requirements 3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. Customized Approach Objective PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.		
3.5 Primary account number (PAN) is secured wherever it is stored.		
Defined Approach Requirements 3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. • Index tokens. • Strong cryptography with associated key- management processes and procedures. Customized Approach Objective Cleartext PAN cannot be read from storage media.	Требование неприменимо. Платформа Yandex Cloud самостоятельно не обрабатывает данные платёжных карт.	Клиент отвечает за процессы обработки, хранения и уничтожения своих данных, в том числе PAN.
3.6 Cryptographic keys used to protect stored account data are secured.		
Defined Approach Requirements	Требование неприменимо. Платформа Yandex Cloud	Клиент отвечает за процессы обработки, хранения и уничтожения

3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms. Customized Approach Objective Processes that protect cryptographic keys used to protect stored account data against disclosure and misuse are defined and implemented.	самостоятельно не обрабатывает данные платёжных карт. Платформа Yandex Cloud предоставляет Клиентам сервис Yandex Key Management Service для шифрования данных. Сервис KMS выполняет требования PCI DSS.	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 платёжных карт при хранении.
Defined Approach Requirements 3.6.1.1 Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4. Customized Approach Objective Accurate details of the cryptographic architecture are maintained and available.	Платформа Yandex Cloud предоставляет Клиентам сервис Yandex Key Management Service для шифрования данных. Сервис KMS выполняет требования PCI DSS.	Требование неприменимо. * Требование может быть применимо для Клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.

3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.		
Defined Approach Requirements 3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data. Customized Approach Objective Strong cryptographic keys are generated.	Требование неприменимо. Платформа Yandex Cloud самостоятельно не обрабатывает данные платёжных 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 платёжных карт при хранении.
Defined Approach Requirements 3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data. Customized Approach Objective Cryptographic keys are secured during distribution.		
Defined Approach Requirements 3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data. Customized Approach Objective Cryptographic keys are secured when stored.		
Defined Approach Requirements 3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod. Customized Approach Objective Cryptographic keys are not used beyond their defined cryptoperiod.		

Defined Approach Requirements 3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations. Customized Approach Objective Keys are removed from active use when it is suspected or known that the integrity of the key is weakened.		
Defined Approach Requirements 3.7.6 Where manual cleartext cryptographic key- management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control. Customized Approach Objective Cleartext secret or private keys cannot be known by anyone. Operations involving cleartext keys cannot be carried out by a single person.		
Defined Approach Requirements 3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys. Customized Approach Objective Cryptographic keys cannot be substituted by unauthorized personnel.		
Defined Approach Requirements 3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in		

writing or electronically) that they understand and accept their key-custodian responsibilities. Customized Approach Objective Key custodians are knowledgeable about their responsibilities in relation to cryptographic operations and can access assistance and guidance when required.		
Defined Approach Requirements 3.7.9 Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers. Customized Approach Objective Customers are provided with appropriate key management guidance whenever they receive shared cryptographic keys.		Требование неприменимо. * Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.

PCI DSS Requirements	Yandex Cloud	Клиент
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.		
Defined Approach Requirements 4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.

Expectations, controls, and oversight for meeting activities within Requirement 4 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.		
Defined Approach Requirements 4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood. Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 4 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
4.2 PAN is protected with strong cryptography during transmission.		
Defined Approach Requirements 4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use. Customized Approach Objective Cleartext PAN cannot be read or intercepted from any transmissions over open, public networks.	Платформа Yandex Cloud использует безопасные криптографические протоколы, обеспечивающие защиту данных при передаче.	Клиент отвечает за процессы безопасной передачи данных платёжных карт, включая использование безопасных протоколов и шифрования. Клиент должен использовать компоненты, поддерживающие протоколы TLS 1.2 и выше. Yandex Cloud рекомендует использовать шифрование данных платёжных карт во всех случаях, включая передачу внутри клиентских сетей и передачу в общедоступных сетях.

Defined Approach Requirements 4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies. Customized Approach Objective Cleartext PAN cannot be read or intercepted from transmissions using end-user messaging technologies.	Требование неприменимо. Платформа Yandex Cloud самостоятельно не обрабатывает данные платёжных карт и не передает данные пользователей в открытом виде.	Клиент отвечает за приведение PAN в нечитаемый вид в случае использования технологий обмена мгновенными сообщениями.

Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks from Malicious Software.

PCI DSS Requirements	Yandex Cloud	Клиент
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.		
Defined Approach Requirements 5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 5 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.
Defined Approach Requirements 5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood. Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 5 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
5.2 Malicious software (malware) is prevented, or detected and addressed.		
Defined Approach Requirements 5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic	Платформа Yandex Cloud отвечает за функционирование антивирусного программного обеспечения для	Клиент отвечает за процессы защиты от вредоносного ПО для компонентов, развёрнутых на

evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware. Customized Approach Objective Automated mechanisms are implemented to prevent systems from becoming an attack vector for malware.	компонентов, обеспечивающих функционирование сервисов в области оценки.	платформе Yandex Cloud и подверженных вирусному заражению.
Defined Approach Requirements 5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware. Customized Approach Objective Malware cannot execute or infect other system components.		
Defined Approach Requirements 5.2.3 Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection. Customized Approach Objective The entity maintains awareness of evolving malware threats to ensure that any systems not protected from malware are not at risk of infection.		
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.		
Defined Approach Requirements 5.3.1 The anti-malware solution(s) is kept current via automatic updates. Customized Approach Objective	Платформа Yandex Cloud отвечает за функционирование антивирусного программного обеспечения для компонентов, обеспечивающих	Клиент отвечает за процессы защиты от вредоносного ПО для компонентов, развёрнутых на платформе Yandex Cloud и

Anti-malware mechanisms can detect and address the latest malware threats.	функционирование сервисов в области оценки.	подверженных вирусному заражению.
Defined Approach Requirements 5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans. OR • Performs continuous behavioral analysis of systems or processes. Customized Approach Objective Malware cannot complete execution.		
Defined Approach Requirements 5.3.3 For removable electronic media, the anti- malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. Customized Approach Objective Malware cannot be introduced to system components via external removable media.	Требование неприменимо. Платформа Yandex Cloud не передаёт данные с использованием съёмных носителей.	Клиент отвечает за выполнение необходимых процедур для защиты компонентов, в том числе съёмных носителей, обрабатывающих данные платёжных карт, от вредоносного ПО.
Defined Approach Requirements 5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1. Customized Approach Objective Historical records of anti-malware actions are immediately available and retained for at least 12 months.	Платформа Yandex Cloud отвечает за функционирование антивирусного программного обеспечения для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы защиты от вредоносного ПО для компонентов, развёрнутых на платформе Yandex Cloud и подверженных вирусному заражению.
Defined Approach Requirements		

5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period. Customized Approach Objective Anti-malware mechanisms cannot be modified by unauthorized personnel.		
5.4 Anti-phishing mechanisms protect users against phishing attacks.		
Defined Approach Requirements 5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. Customized Approach Objective Mechanisms are in place to protect against and mitigate risk posed by phishing attacks.	Платформа Yandex Cloud отвечает за функционирование механизмов защиты от фишинговых атак для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы защиты от фишинговых атак для компонентов, развёрнутых на платформе Yandex Cloud.

Requirement 6: Develop and Maintain Secure Systems and Software.

PCI DSS Requirements	Yandex Cloud	Клиент
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.		
Defined Approach Requirements 6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 6 are defined and adhered to by affected personnel. All	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.

supporting activities are repeatable, consistently applied, and conform to management's intent.		
Defined Approach Requirements 6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood. Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 6 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
6.2 Bespoke and custom software are developed securely.		
Defined Approach Requirements 6.2.1 Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle. Customized Approach Objective Bespoke and custom software is developed in accordance with PCI DSS and secure development processes throughout the software lifecycle.	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.
Defined Approach Requirements 6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. Customized Approach Objective		

Software development personnel remain knowledgeable about secure development practices; software security; and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.		
Defined Approach Requirements 6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release. Customized Approach Objective Bespoke and custom software cannot be exploited via coding vulnerabilities.		
Defined Approach Requirements 6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP , XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.		

• Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client- side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. Customized Approach Objective Bespoke and custom software cannot be exploited via common attacks and related vulnerabilities.		
6.3 Security vulnerabilities are identified and addressed.		
Defined Approach Requirements 6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. Customized Approach Objective New system and software vulnerabilities that may impact the security of account data or the CDE are monitored, cataloged, and risk assessed.	Платформа Yandex Cloud отвечает за процессы управления уязвимостями для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за процессы управления уязвимостями для компонентов, развёрнутых на платформе Yandex Cloud: • операционных систем; • баз данных (за исключением PAAS-сервисов); • прикладного ПО; • других компонентов и сервисов, включённых Клиентом в область оценки.

Defined Approach Requirements 6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management. Customized Approach Objective Known vulnerabilities in third-party software components cannot be exploited in bespoke and custom software.		
Defined Approach Requirements 6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release). Customized Approach Objective System components cannot be compromised via the exploitation of a known vulnerability.		
6.4 Public-facing web applications are protected against attacks.		
Defined Approach Requirements 6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security.	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 конфигурацию и защиту собственных общедоступных веб-приложений, развёрнутых на платформе Yandex Cloud.

– Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web- based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated. Customized Approach Objective Public-facing web applications are protected against malicious attacks.		
Defined Approach Requirements 6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated. Customized Approach Objective Public-facing web applications are protected in real time against malicious attacks.		
Defined Approach Requirements		

6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary. Customized Approach Objective Unauthorized code cannot be present in the payment page as it is rendered in the consumer's browser.		
6.5 Changes to all system components are managed securely.		
Defined Approach Requirements 6.5.1 Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state. Customized Approach Objective All changes are tracked, authorized, and evaluated for impact and security, and changes are managed to avoid unintended effects to the security of system components.	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, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements 6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.		

Customized Approach Objective All system components are verified after a significant change to be compliant with the applicable PCI DSS requirements.		
Defined Approach Requirements 6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls. Customized Approach Objective Pre-production environments cannot introduce risks and vulnerabilities into production environments.		
Defined Approach Requirements 6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed. Customized Approach Objective Job roles and accountability that differentiate between pre-production and production activities are defined and managed to minimize the risk of unauthorized, unintentional, or inappropriate actions.		
Defined Approach Requirements 6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements. Customized Approach Objective Live PANs cannot be present in pre-production environments outside the CDE.		
Defined Approach Requirements 6.5.6 Test data and test accounts are removed from system components before the system goes into production. Customized Approach Objective Test data and test accounts cannot exist in production environments.		

Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know.

PCI DSS Requirements	Yandex Cloud	Клиент
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.		
Defined Approach Requirements 7.1.1 All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 7 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.
Defined Approach Requirements 7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood. Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 7 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
7.2 Access to system components and data is appropriately defined and assigned.		
Defined Approach Requirements 7.2.1 An access control model is defined and includes granting access as follows:	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части контроля и управления	Клиент отвечает за процессы контроля и управления доступом к

• Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function. Customized Approach Objective Access requirements are established according to job functions following least-privilege and need-to- know principles.	доступом для компонентов, обеспечивающих функционирование сервисов в области оценки.	компонентам, развёрнутым на платформе Yandex Cloud.
Defined Approach Requirements 7.2.2 Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities. Customized Approach Objective Access to systems and data is limited to only the access needed to perform job functions, as defined in the related access roles.		
Defined Approach Requirements 7.2.3 Required privileges are approved by authorized personnel. Customized Approach Objective Access privileges cannot be granted to users without appropriate, documented authorization.		
Defined Approach Requirements 7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed.		

• Management acknowledges that access remains appropriate. Customized Approach Objective Account privilege assignments are verified periodically by management as correct, and nonconformities are remediated.		
Defined Approach Requirements 7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use. Customized Approach Objective Access rights granted to application and system accounts are limited to only the access needed for the operability of that application or system.		
Defined Approach Requirements 7.2.6 All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD. Customized Approach Objective Direct unfiltered (ad hoc) query access to cardholder data repositories is prohibited, unless performed by an authorized administrator.	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, развёрнутых на платформе Yandex Cloud.
7.3 Access to system components and data is managed via an access control system(s).		
Defined Approach Requirements 7.3.1 An access control system(s) is in place that restricts access based on a user's need to know and covers all system components. Customized Approach Objective	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части контроля и управления доступом для компонентов,	Клиент отвечает за процессы контроля и управления доступом к компонентам, развёрнутым на платформе Yandex Cloud.

Access rights and privileges are managed via mechanisms intended for that purpose.	обеспечивающих функционирование сервисов в области оценки.	
Defined Approach Requirements 7.3.2 The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function. Customized Approach Objective Individual account access rights and privileges to systems, applications, and data are only inherited from group membership.		
Defined Approach Requirements 7.3.3 The access control system(s) is set to “deny all” by default. Customized Approach Objective Access rights and privileges are prohibited unless expressly permitted.		

Requirement 8: Identify Users and Authenticate Access to System Components.

PCI DSS Requirements	Yandex Cloud	Клиент
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.		
Defined Approach Requirements 8.1.1 All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 8 are defined and adhered to by affected personnel. All	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.

supporting activities are repeatable, consistently applied, and conform to management's intent.		
Defined Approach Requirements 8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood. Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 8 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.		
Defined Approach Requirements 8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed. Customized Approach Objective All actions by all users are attributable to an individual.	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, развёрнутым на платформе Yandex Cloud.
Defined Approach Requirements 8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user. Customized Approach Objective	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, развёрнутых на платформе Yandex Cloud.

All actions performed by users with generic, system, or shared IDs are attributable to an individual person.		
Defined Approach Requirements 8.2.3 Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises. Customized Approach Objective A service provider's credential used for one customer cannot be used for any other 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.
Defined Approach Requirements 8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval. Customized Approach Objective Lifecycle events for user IDs and authentication factors cannot occur without appropriate authorization.	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, развёрнутым на платформе Yandex Cloud.
Defined Approach Requirements 8.2.5 Access for terminated users is immediately revoked. Customized Approach Objective The accounts of terminated users cannot be used.		
Defined Approach Requirements 8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity. Customized Approach Objective Inactive user accounts cannot be used.		
Defined Approach Requirements		

8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity. Customized Approach Objective Third party remote access cannot be used except where specifically authorized and use is overseen by management.		
Defined Approach Requirements 8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session. Customized Approach Objective A user session cannot be used except by the authorized user.		
8.3 Strong authentication for users and administrators is established and managed.		
Defined Approach Requirements 8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • 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 element. Customized Approach Objective An account cannot be accessed except with a combination of user identity and an authentication factor.	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, развёрнутых на платформе Yandex Cloud. Для централизованного управления учётными данными рекомендуется использовать SAML-совместимые федерации удостоверений.
Defined Approach Requirements 8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components. Customized Approach Objective Cleartext authentication factors cannot be obtained, derived, or reused from the interception of communications or from stored data.		

Defined Approach Requirements 8.3.3 User identity is verified before modifying any authentication factor. Customized Approach Objective Unauthorized individuals cannot gain system access by impersonating the identity of an authorized user.		
Defined Approach Requirements 8.3.4 Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed. Customized Approach Objective An authentication factor cannot be guessed in a brute force, online attack.	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 выполнение требований PCI DSS в части использования механизмов аутентификации и управления доступом для компонентов, развёрнутых на платформе Yandex Cloud. Для централизованного управления учётными данными рекомендуется использовать SAML-совместимые федерации удостоверений.
Defined Approach Requirements 8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use. Customized Approach Objective An initial or reset password/passphrase assigned to a user cannot be used by an unauthorized user.		
Defined Approach Requirements 8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.		

Customized Approach Objective A guessed password/passphrase cannot be verified by either an online or offline brute force attack. Defined Approach Requirements 8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used. Customized Approach Objective A previously used password cannot be used to gain access to an account for at least 12 months.		
Defined Approach Requirements 8.3.8 Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords/passphrases. • Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident. Customized Approach Objective Users are knowledgeable about the correct use of authentication factors and can access assistance and guidance when required.	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, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements 8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. Customized Approach Objective	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, развёрнутых на платформе Yandex Cloud.

An undetected compromised password/passphrase cannot be used indefinitely.		Для централизованного управления учётными данными рекомендуется использовать SAML-совместимые федерации удостоверений.
Defined Approach Requirements 8.3.10 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single- factor authentication implementation), then guidance is provided to customer users including: • Guidance for customers to change their user passwords/passphrases periodically. • Guidance as to when, and under what circumstances, passwords/passphrases are to be changed. Customized Approach Objective Passwords/passphrases for service providers' customers cannot be used indefinitely.	По умолчанию сотрудники Yandex Cloud не имеют доступа к ресурсам Клиентов, расположенным на платформе Yandex Cloud. Yandex Cloud предоставляет документацию по использованию сервиса Identity and Access Management — https://yandex.cloud/ru/docs/iam/	Требование неприменимо. * Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.
Defined Approach Requirements 8.3.10.1 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. Customized Approach Objective Passwords/passphrases for service providers' customers cannot be used indefinitely.		Требование неприменимо. * Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.

Defined Approach Requirements 8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access. Customized Approach Objective An authentication factor cannot be used by anyone other than the user to which it is assigned.	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, развёрнутых на платформе Yandex Cloud.
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.		
Defined Approach Requirements 8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access. Customized Approach Objective Administrative access to the CDE cannot be obtained by the use of a single authentication factor.	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, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements 8.4.2 MFA is implemented for all access into the CDE. Customized Approach Objective Access into the CDE cannot be obtained by the use of a single authentication factor.		
Defined Approach Requirements 8.4.3 MFA is implemented for all remote network access originating from outside the entity’s network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity’s network. • All remote access by third parties and vendors. Customized Approach Objective		

Remote access to the entity's network cannot be obtained by using a single authentication factor.		
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.		
Defined Approach Requirements 8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted. Customized Approach Objective MFA systems are resistant to attack and strictly control any administrative overrides.	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, развёрнутых на платформе Yandex Cloud.
8.6 Use of application and system accounts and associated authentication factors is strictly managed.		
Defined Approach Requirements 8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user. Customized Approach Objective	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, развёрнутых на платформе Yandex Cloud.

When used interactively, all actions with accounts designated as system or application accounts are authorized and attributable to an individual person.		
Defined Approach Requirements 8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. Customized Approach Objective Passwords/passphrases used by application and system accounts cannot be used by unauthorized personnel.		
Defined Approach Requirements 8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. Customized Approach Objective Passwords/passphrases used by application and system accounts cannot be used indefinitely and are structured to resist brute-force and guessing attacks.		

Requirement 9: Restrict Physical Access to Cardholder Data.

PCI DSS Requirements	Yandex Cloud	Клиент
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.		

Defined Approach Requirements 9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 9 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.
Defined Approach Requirements 9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood. Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 9 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.		
Defined Approach Requirements 9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE. Customized Approach Objective System components in the CDE cannot be physically accessed by unauthorized personnel.	Платформа Yandex Cloud обеспечивает физическую безопасность дата-центров, в которых расположены компоненты, необходимые для функционирования 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 платёжных карт.
Defined Approach Requirements 9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility. Customized Approach Objective		

Unauthorized devices cannot connect to the entity's network from public areas within the facility.		
Defined Approach Requirements 9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted. Customized Approach Objective Physical networking equipment cannot be accessed by unauthorized personnel.		
Defined Approach Requirements 9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use. Customized Approach Objective Physical consoles within sensitive areas cannot be used by unauthorized personnel.		
9.3 Physical access for personnel and visitors is authorized and managed		
Defined Approach Requirements 9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel. Customized Approach Objective Requirements for access to the physical CDE are defined and enforced to identify and authorize personnel.	Платформа Yandex Cloud обеспечивает физическую безопасность дата-центров, в которых расположены компоненты, необходимые для функционирования 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 платёжных карт.

Defined Approach Requirements 9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel. Customized Approach Objective Requirements for visitor access to the CDE are defined and enforced. Visitors cannot exceed any authorized physical access allowed while in the CDE.		
Defined Approach Requirements 9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration. Customized Approach Objective Visitor identification or badges cannot be reused after expiration.		
Defined Approach Requirements 9.3.4 A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law. Customized Approach Objective Records of visitor access that enable the identification of individuals are maintained.		

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.		
Defined Approach Requirements 9.4.1 All media with cardholder data is physically secured. Customized Approach Objective Media with cardholder data cannot be accessed by unauthorized personnel.	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, съёмных электронных носителей, бумажных чеков, бумажных отчётов и факсов), если такие применяются в процессах обработки данных платёжных карт.
Defined Approach Requirements 9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data. Customized Approach Objective Media are classified and protected appropriately.		
Defined Approach Requirements 9.4.3 Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location. Customized Approach Objective Media is secured and tracked when transported outside the facility.		
Defined Approach Requirements 9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals). Customized Approach Objective Media cannot leave a facility without the approval of accountable personnel.		
Defined Approach Requirements		

9.4.5 Inventory logs of all electronic media with cardholder data are maintained. Customized Approach Objective Accurate inventories of stored electronic media are maintained.	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, съёмным электронным носителям, бумажным чекам, бумажным отчётам и факсам), если такие применяются в процессах обработки данных платёжных карт.
Defined Approach Requirements 9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction. Customized Approach Objective Cardholder data cannot be recovered from media that has been destroyed or which is pending destruction.		
Defined Approach Requirements 9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed. Customized Approach Objective Cardholder data cannot be recovered from media that has been erased or destroyed.		
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.		
Defined Approach Requirements 9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution.	Требование неприменимо.	Клиент отвечает за защиту устройств, считывающих данные с платёжных карт путём прямого физического взаимодействия с картой.

• Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices. Customized Approach Objective The entity has defined procedures to protect and manage point of interaction devices. Expectations, controls, and oversight for the management and protection of POI devices are defined and adhered to by affected personnel.		

Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data.

PCI DSS Requirements	Yandex Cloud	Клиент
Defined Approach Requirements 10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 10 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и процедур согласно требованиям PCI DSS.	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.
Defined Approach Requirements 10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и

Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 10 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.		
Defined Approach Requirements 10.2.1 Audit logs are enabled and active for all system components and cardholder data. Customized Approach Objective Records of all activities affecting system components and cardholder data are captured.	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, развёрнутых на платформе Yandex Cloud, а именно: • операционных систем; • баз данных (за исключением PAAS-сервисов); • прикладного ПО; • других компонентов и сервисов, включённых Клиентом в область оценки.
Defined Approach Requirements 10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol). Customized Approach Objective Sufficient data to be able to identify successful and failed attempts and who, what, when, where, and how for each event listed in requirement 10.2.1 are captured.		
10.3 Audit logs are protected from destruction and unauthorized modifications.		
Defined Approach Requirements 10.3.1 Read access to audit logs files is limited to those with a job-related need. Customized Approach Objective	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части защиты журналов регистрации событий для компонентов,	Клиент отвечает за выполнение требований PCI DSS в части защиты журналов регистрации событий для

Stored activity records cannot be accessed by unauthorized personnel.	обеспечивающих функционирование сервисов в области оценки.	компонентов, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements 10.3.2 Audit log files are protected to prevent modifications by individuals. Customized Approach Objective Stored activity records cannot be modified by personnel.		
Defined Approach Requirements 10.3.3 Audit log files, including those for external- facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify. Customized Approach Objective Stored activity records are secured and preserved in a central location to prevent unauthorized modification.		
Defined Approach Requirements 10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts. Customized Approach Objective Stored activity records cannot be modified without an alert being generated.		
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.		
Defined Approach Requirements 10.4.1 The following audit logs are reviewed at least once 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, network security controls, 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, развёрнутых на платформе Yandex Cloud.

systems/intrusion-prevention systems (IDS/IPS), authentication servers). Customized Approach Objective Potentially suspicious or anomalous activities are quickly identified to minimize impact.		
Defined Approach Requirements 10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically. Customized Approach Objective Potentially suspicious or anomalous activities for other system components (not included in 10.4.1) are reviewed in accordance with the entity's identified risk.		
Defined Approach Requirements 10.4.3 Exceptions and anomalies identified during the review process are addressed. Customized Approach Objective Suspicious or anomalous activities are addressed.		
10.5 Audit log history is retained and available for analysis.		
Defined Approach Requirements 10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis. Customized Approach Objective Historical records of activity are available immediately to support incident response and are retained for at least 12 months.	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, развёрнутых на платформе Yandex Cloud.
10.6 Time-synchronization mechanisms support consistent time settings across all systems.		
Defined Approach Requirements 10.6.1 System clocks and time are synchronized using time-synchronization technology.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части синхронизации времени для	Клиент отвечает за выполнение требований PCI DSS в части синхронизации времени для

Customized Approach Objective Common time is established across all systems.	компонентов, обеспечивающих функционирование сервисов в области оценки.	компонентов, развёрнутых на платформе Yandex Cloud. См. рекомендации по настройке синхронизации времени с использованием NTP.
Defined Approach Requirements 10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s). Customized Approach Objective The time on all systems is accurate and consistent.		
Defined Approach Requirements 10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed. Customized Approach Objective System time settings cannot be modified by unauthorized personnel.		
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.		
Defined Approach Requirements 10.7.1 Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части фиксации и выявления отказов	Требование неприменимо.

promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). Customized Approach Objective Failures in critical security control systems are promptly identified and addressed.	систем контроля безопасности для компонентов, обеспечивающих функционирование сервисов в области оценки.	* Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.
Defined Approach Requirements 10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used). Customized Approach Objective Failures in critical security control systems are promptly identified and addressed.		Клиент отвечает за выполнение требований PCI DSS в части фиксации и выявления отказов систем контроля безопасности для компонентов, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements		

10.7.3 Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls. Customized Approach Objective Failures of critical security control systems are analyzed, contained, and resolved, and security controls restored to minimize impact. Resulting security issues are addressed, and measures taken to prevent reoccurrence.		

Requirement 11: Test Security of Systems and Networks Regularly.

PCI DSS Requirements	Yandex Cloud	Клиент
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.		
Defined Approach Requirements 11.1.1 All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date.	Платформа Yandex Cloud, для сервисов в области оценки, обеспечивает выполнение всех необходимых требований и	Клиент отвечает за выполнение необходимых процедур для компонентов, обрабатывающих данные платёжных карт.

• In use. • Known to all affected parties. Customized Approach Objective Expectations, controls, and oversight for meeting activities within Requirement 11 are defined and adhered to by affected personnel. All supporting activities are repeatable, consistently applied, and conform to management's intent.	процедур согласно требованиям PCI DSS.	
Defined Approach Requirements 11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood. Customized Approach Objective Day-to-day responsibilities for performing all the activities in Requirement 11 are allocated. Personnel are accountable for successful, continuous operation of these requirements.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.		
Defined Approach Requirements 11.2.1 Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts. Customized Approach Objective Unauthorized wireless access points are identified and addressed periodically.	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.
Defined Approach Requirements		

11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification. Customized Approach Objective Unauthorized wireless access points are not mistaken for authorized wireless access points.		
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.		
Defined Approach Requirements 11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high- risk and critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists. Customized Approach Objective The security posture of all system components is verified periodically using automated tools designed to detect vulnerabilities operating inside the network. Detected vulnerabilities are assessed and rectified based on a formal risk assessment framework.	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, развёрнутых на платформе Yandex Cloud. Клиент также отвечает за проведение сканирований внешних IP-адресов. Сканирования должны выполняться согласно опубликованному документу Политика поддержки пользователей при проведении проверки уязвимостей.
Defined Approach Requirements 11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met.		

• Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan. Customized Approach Objective This requirement is not eligible for the customized approach.		
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.		
Defined Approach Requirements 11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope- reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months. Customized Approach Objective A formal methodology is defined for thorough technical testing that attempts to exploit vulnerabilities and security weaknesses via simulated attack methods by a competent manual attacker.	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, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements 11.4.2 Internal penetration testing is performed: • Per the entity's defined methodology,		

• At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV). Customized Approach Objective Internal system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats and ensure that significant changes do not introduce unknown vulnerabilities.		
Defined Approach Requirements 11.4.3 External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV). Customized Approach Objective External system defenses are verified by technical testing according to the entity's defined methodology as frequently as needed to address evolving and new attacks and threats, and to ensure that significant changes do not introduce unknown vulnerabilities.		
Defined Approach Requirements 11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections. Customized Approach Objective		

Vulnerabilities and security weaknesses found while verifying system defenses are mitigated.		
Defined Approach Requirements 11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV). Customized Approach Objective If segmentation is used, it is verified periodically by technical testing to be continually effective, including after any changes, in isolating the CDE from all out- of-scope systems.		
Defined Approach Requirements 11.4.6 Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.		Требование неприменимо. * Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.

• Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV). Customized Approach Objective If segmentation is used, it is verified by technical testing to be continually effective, including after any changes, in isolating the CDE from out-of-scope systems.		
Defined Approach Requirements 11.4.7 Additional requirement for multi-tenant service providers only: Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4. Customized Approach Objective Multi-tenant service providers support their customers' need for technical testing either by providing access or evidence that comparable technical testing has been undertaken.	Платформа Yandex Cloud публикует на своих ресурсах документ Политика поддержки пользователей при проведении проверки уязвимостей.	Клиент должен руководствоваться положениями документа Политика поддержки пользователей при проведении проверки уязвимостей.
11.5 Network intrusions and unexpected file changes are detected and responded to.		
Defined Approach Requirements 11.5.1 Intrusion-detection and/or intrusion- prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date. Customized Approach Objective Mechanisms to detect real-time suspicious or anomalous network traffic that may be indicative of threat actor activity are implemented.	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, развёрнутых на платформе Yandex Cloud.

Alerts generated by these mechanisms are responded to by personnel, or by automated means that ensure that system components cannot be compromised as a result of the detected activity.		
Defined Approach Requirements 11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly. Customized Approach Objective Critical files cannot be modified by unauthorized personnel without an alert being generated.		
11.6 Unauthorized changes on payment pages are detected and responded to.		
Defined Approach Requirements 11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). Customized Approach Objective	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части использования механизмов контроля целостности файлов для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части использования механизмов контроля целостности файлов для компонентов, развёрнутых на платформе Yandex Cloud.

E-commerce skimming code or techniques cannot be added to payment pages as received by the consumer browser without a timely alert being generated. Anti-skimming measures cannot be removed from payment pages without a prompt alert being generated.		

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs.

PCI DSS Requirements	Yandex Cloud	Клиент
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.		
Defined Approach Requirements 12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners. Customized Approach Objective The strategic objectives and principles of information security are defined, adopted, and known to all personnel.	Платформа Yandex Cloud отвечает за выполнение требований PCI DSS в части разработки, соблюдения политики безопасности и других процедур обеспечения ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части разработки, соблюдения политики безопасности и других процедур обеспечения ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements 12.1.2 The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment. Customized Approach Objective		

The information security policy continues to reflect the organization's strategic objectives and principles.		
Defined Approach Requirements 12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities. Customized Approach Objective Personnel understand their role in protecting the entity's cardholder data.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ компонентов, необходимых для функционирования сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части распределения обязанностей и ответственности за обеспечение ИБ для компонентов, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements 12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management. Customized Approach Objective A designated member of executive management is responsible for information security.		
12.2 Acceptable use policies for end-user technologies are defined and implemented.		
Defined Approach Requirements 12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software. Customized Approach Objective The use of end-user technologies is defined and managed to ensure authorized usage.	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, развёрнутых на платформе Yandex Cloud.
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.		

Defined Approach Requirements 12.3.1 Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review. Customized Approach Objective Up to date knowledge and assessment of risks to the CDE are maintained.	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, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements 12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months.		

Customized Approach Objective This requirement is part of the customized approach and must be met for those using the customized approach.		
Defined Approach Requirements 12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities. Customized Approach Objective The entity is able to respond quickly to any vulnerabilities in cryptographic protocols or algorithms, where those vulnerabilities affect protection of cardholder data.		
Defined Approach Requirements 12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans. Customized Approach Objective		

The entity's hardware and software technologies are up to date and supported by the vendor. Plans to remove or replace all unsupported system components are reviewed periodically.		
12.4 PCI DSS compliance is managed.		
Defined Approach Requirements 12.4.1 Additional requirement for service providers only: Responsibility is established by executive management 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. Customized Approach Objective Executives are responsible and accountable for security of cardholder data.	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.
Defined Approach Requirements 12.4.2 Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls. • Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes. Customized Approach Objective The operational effectiveness of critical PCI DSS controls is verified periodically by manual inspection of records.	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.

12.5 PCI DSS scope is documented and validated.		
Defined Approach Requirements 12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current. Customized Approach Objective All system components in scope for PCI DSS are identified and known.	Платформа Yandex Cloud обеспечивает выполнение процедур учёта для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за ведение журнала учёта компонентов, развёрнутых на платформе Yandex Cloud и входящих в область оценки соответствия стандарту PCI DSS.
Defined Approach Requirements 12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. Customized Approach Objective	Платформа Yandex Cloud отвечает за документирование и подтверждение области оценки компонентов, обеспечивающих функционирование сервисов.	Клиент отвечает за документирование и подтверждение области оценки компонентов, развёрнутых на платформе Yandex Cloud и входящих в область оценки соответствия стандарту PCI DSS.

PCI DSS scope is verified periodically, and after significant changes, by comprehensive analysis and appropriate technical measures.		
Defined Approach Requirements 12.5.2.1 Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2. Customized Approach Objective The accuracy of PCI DSS scope is verified to be continuously accurate by comprehensive analysis and appropriate technical measures.	Платформа Yandex Cloud отвечает за документирование и подтверждение области оценки компонентов, обеспечивающих функционирование сервисов.	Требование неприменимо. * Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.
Defined Approach Requirements 12.5.3 Additional requirement for service providers only: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management. Customized Approach Objective PCI DSS scope is confirmed after significant organizational change.	Платформа Yandex Cloud обеспечивает документирование и анализ влияния значительных изменений в организационной структуре 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.
12.6 Security awareness education is an ongoing activity.		
Defined Approach Requirements 12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data. Customized Approach Objective Personnel are knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части обучения сотрудников и повышения их осведомлённости о безопасности для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части обучения сотрудников и повышения их осведомлённости о безопасности для компонентов, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements		

12.6.2 The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data. Customized Approach Objective The content of security awareness material is reviewed and updated periodically.		
Defined Approach Requirements 12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures. Customized Approach Objective Personnel remain knowledgeable about the threat landscape, their responsibility for the operation of relevant security controls, and are able to access assistance and guidance when required.		
12.7 Personnel are screened to reduce risks from insider threats.		
Defined Approach Requirements 12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources. Customized Approach Objective The risk related to allowing new members of staff access to the CDE is understood and managed.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части проверки потенциальных сотрудников до их приёма на работу в сервисы, входящие в область оценки.	Клиент отвечает за выполнение требований PCI DSS в части проверки потенциальных сотрудников до их приёма на работу для компонентов, развёрнутых на платформе Yandex Cloud.
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.		
Defined Approach Requirements		

12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided. Customized Approach Objective Records are maintained of TPSPs and the services provided.	Платформа Yandex Cloud не передаёт 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 платёжных карт.
Defined Approach Requirements 12.8.2 Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE. Customized Approach Objective Records are maintained of each TPSP's acknowledgment of its responsibility to protect account data.		
Defined Approach Requirements 12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement. Customized Approach Objective The capability, intent, and resources of a prospective TPSP to adequately protect account data are assessed before the TPSP is engaged.		
Defined Approach Requirements 12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months. Customized Approach Objective The PCI DSS compliance status of TPSPs is verified periodically.		
Defined Approach Requirements		

12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity. Customized Approach Objective Records detailing the PCI DSS requirements and related system components for which each TPSP is solely or jointly responsible, are maintained and reviewed periodically.		
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.		
Defined Approach Requirements 12.9.1 Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP 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 CDE. Customized Approach Objective TPSPs formally acknowledge their security responsibilities to their customers.	Платформа Yandex Cloud предоставляет всю необходимую информацию по соответствию на портале https://yandex.cloud/ru/security	Требование неприменимо. * Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.
Defined Approach Requirements 12.9.2 Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5). Customized Approach Objective TPSPs provide information as needed to support their customers' PCI DSS compliance efforts.		Требование неприменимо. * Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.		

Defined Approach Requirements 12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup 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. Customized Approach Objective A comprehensive incident response plan that meets card brand expectations is maintained.	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, развёрнутых на платформе Yandex Cloud.
Defined Approach Requirements 12.10.2 At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1. Customized Approach Objective The incident response plan is kept current and tested periodically.		
Defined Approach Requirements 12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents. Customized Approach Objective Incidents are responded to immediately where appropriate.		

Defined Approach Requirements 12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities. Customized Approach Objective Personnel are knowledgeable about their role and responsibilities in incident response and are able to access assistance and guidance when required.		
Defined Approach Requirements 12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Detection of unauthorized wireless access points. Customized Approach Objective Alerts generated by monitoring and detection technologies are responded to in a structured, repeatable manner.	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.
Defined Approach Requirements 12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments. Customized Approach Objective The effectiveness and accuracy of the incident response plan is reviewed and updated after each invocation.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части усовершенствования планов реагирования на инциденты для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части усовершенствования планов реагирования на инциденты для компонентов, развёрнутых на платформе Yandex Cloud.

Defined Approach Requirements 12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected. Customized Approach Objective Processes are in place to quickly respond, analyze, and address situations in the event that cleartext PAN is detected where it is not expected.	Требование неприменимо. Платформа Yandex Cloud самостоятельно не обрабатывает данные платёжных карт.	Клиент отвечает за процедуры реагирования на инциденты, которые должны быть инициированы при обнаружении хранимого PAN в любом месте, где это не ожидается.

Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

PCI DSS Requirements	Yandex Cloud	Клиент
A1.1 Multi-tenant service providers protect and separate all customer environments and data.		
Defined Approach Requirements A1.1.1 Logical separation is implemented as follows: • The provider cannot access its customers' environments without authorization. • Customers cannot access the provider's environment without authorization Customized Approach Objective	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части предоставления механизмов управления доступом, обеспечивающих изоляцию разных Клиентов, и разграничения сред разных Клиентов. Детальная	Требование неприменимо. * Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.

Customers cannot access the provider's environment. The provider cannot access its customers' environments without authorization.	информация представлена в документации: https://yandex.cloud/ru/security/comprehensive-security/isolation-layers	
Defined Approach Requirements A1.1.2 Controls are implemented such that each customer only has permission to access its own cardholder data and CDE. Customized Approach Objective Customers cannot access other customers' environments.		
Defined Approach Requirements A1.1.3 Controls are implemented such that each customer can only access resources allocated to them. Customized Approach Objective Customers cannot impact resources allocated to other customers.		
Defined Approach Requirements A1.1.4 The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing. Customized Approach Objective Segmentation of customer environments from other environments is periodically validated to be effective.	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.	
A1.2 Multi-tenant service providers facilitate logging and incident response for all customers		
Defined Approach Requirements A1.2.1 Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review only by the owning customer. • Log locations are clearly communicated to the owning customer.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части ведения и хранения журналов регистрации событий в API для каждого Клиента.	Требование неприменимо. * Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.

• Log data and availability is consistent with PCI DSS Requirement 10. Customized Approach Objective Log capability is available to all customers without affecting the confidentiality of other customers.		
Defined Approach Requirements A1.2.2 Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer. Customized Approach Objective Forensic investigation is readily available to all customers in the event of a suspected or confirmed security incident.		
Defined Approach Requirements A1.2.3 Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: • Customers can securely report security incidents and vulnerabilities to the provider. • The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1. Customized Approach Objective Suspected or confirmed security incidents or vulnerabilities are discovered and addressed. Customers are informed where appropriate.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части: • ведения и хранения журналов регистрации событий в API для каждого Клиента; • информирования Клиентов в случае обнаружения и расследования инцидентов ИБ. Платформа Yandex Cloud регулярно публикует бюллетени безопасности https://yandex.cloud/ru/docs/security/security-bulletins/	Требование неприменимо. * Требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.

Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for CardPresent POS POI Terminal Connections

PCI DSS Requirements	Yandex Cloud	Клиент
A2.1 POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits.		
Defined Approach Requirements A2.1.1 Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols. Customized Approach Objective This requirement is not eligible for the customized approach.	Требование неприменимо. Платформа Yandex Cloud не использует POS/POI-терминалы.	Клиент отвечает за выполнение требований PCI DSS в части использования безопасных версий используемых протоколов TLS.
Defined Approach Requirements A2.1.2 Additional requirement for service providers only: All service providers with existing connection points to POS POI terminals that use SSL and/or early TLS as defined in A2.1 have a formal Risk Mitigation and Migration Plan in place that includes: • Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, and type of environment. • Risk-assessment results and risk-reduction controls in place. • Description of processes to monitor for new vulnerabilities associated with SSL/early TLS. • Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments. • Overview of migration project plan to replace SSL/early TLS at a future date. Customized Approach Objective This requirement is not eligible for the customized approach.		Требование неприменимо. * требование может быть применимо для клиентов, которые являются поставщиками услуг, в рамках предоставления своих сервисов.

Defined Approach Requirements A2.1.3 Additional requirement for service providers only: All service providers provide a secure service offering. Customized Approach Objective This requirement is not eligible for the customized approach.		

Appendix A3: Designated Entities Supplemental Validation (DESV)

PCI DSS Requirements	Yandex Cloud	Клиент
A3.1 A PCI DSS compliance program is implemented		
Defined Approach Requirements A3.1.1 Responsibility is established by executive management for the protection of account data and a PCI DSS compliance program that includes: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program. • Providing updates to executive management and board of directors on PCI DSS compliance initiatives and issues, including remediation activities, at least once every 12 months. PCI DSS Reference: Requirement 12 Customized Approach Objective This requirement is not eligible for the customized approach.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части определения программы соответствия и распределения обязанностей по обеспечению соответствия.	Клиент отвечает за выполнение требований PCI DSS в части использования определения программы соответствия и распределения обязанностей по обеспечению соответствия.
Defined Approach Requirements A3.1.2 A formal PCI DSS compliance program is in place that includes:		

• Definition of activities for maintaining and monitoring overall PCI DSS compliance, including business-as-usual activities. • Annual PCI DSS assessment processes. • Processes for the continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement). • A process for performing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions. PCI DSS Reference: Requirements 1-12 Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.1.3 PCI DSS compliance roles and responsibilities are specifically defined and formally assigned to one or more personnel, including: • Managing PCI DSS business-as-usual activities. • Managing annual PCI DSS assessments. • Managing continuous validation of PCI DSS requirements (for example, daily, weekly, every three months, as applicable per the requirement). • Managing business-impact analysis to determine potential PCI DSS impacts for strategic business decisions. PCI DSS Reference: Requirement 12 Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.1.4 Up-to-date PCI DSS and/or information security training is provided at least once every 12 months to personnel with PCI DSS compliance responsibilities (as identified in A3.1.3). PCI DSS Reference: Requirement 12 Customized Approach Objective This requirement is not eligible for the customized approach.		

A3.2 PCI DSS scope is documented and validated		
Defined Approach Requirements A3.2.1 PCI DSS scope is documented and confirmed for accuracy at least once every three months and upon significant changes to the inscope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture, settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • For any account data found outside of the currently defined CDE, either 1) securely delete it, 2) migrate it into the currently defined CDE, or 3) expand the currently defined CDE to include it. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections to third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. PCI DSS Reference: Scope of PCI DSS Requirements, Requirement 12. Customized Approach Objective This requirement is not eligible for the customized approach.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части поддержки в актуальном состоянии инфраструктуры для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части поддержки в актуальном состоянии области инфраструктуры, соответствующей требованиям, для компонентов, развёрнутых на платформе Yandex Cloud.

Defined Approach Requirements A3.2.2 PCI DSS scope impact for all changes to systems or networks is determined, including additions of new systems and new network connections. Processes include: • Performing a formal PCI DSS impact assessment. • Identifying applicable PCI DSS requirements to the system or network. • Updating PCI DSS scope as appropriate. • Documented sign-off of the results of the impact assessment by responsible personnel (as defined in A3.1.3). PCI DSS Reference: Scope of PCI DSS Requirements; Requirements 1-12 Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.2.2.1 Upon completion of a change, all relevant PCI DSS requirements are confirmed to be implemented on all new or changed systems and networks, and documentation is updated as applicable. PCI DSS Reference: Scope of PCI DSS Requirements; Requirement 1-12 Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.2.3 Changes to organizational structure result in a formal (internal) review of the impact to PCI DSS scope and applicability of controls. PCI DSS Reference: Requirement 12 Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.2.4 If segmentation is used, PCI DSS scope is confirmed as follows: • Per the entity's methodology defined at Requirement 11.4.1.		

• Penetration testing is performed on segmentation controls at least once every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate the CDE from all outof-scope systems. PCI DSS Reference: Requirement 11 Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.2.5 A data-discovery methodology is implemented that: • Confirms PCI DSS scope. • Locates all sources and locations of cleartext PAN at least once every three months and upon significant changes to the CDE or processes. • Addresses the potential for cleartext PAN to reside on systems and networks outside the currently defined CDE. PCI DSS Reference: Scope of PCI DSS Requirements. Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.2.5.1 Data discovery methods are confirmed as follows: • Effectiveness of methods is tested. • Methods are able to discover cleartext PAN on all types of system components and file formats in use. • The effectiveness of data-discovery methods is confirmed at least once every 12 months. PCI DSS Reference: Scope of PCI DSS Requirements.		

Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.2.5.2 Response procedures are implemented to be initiated upon the detection of cleartext PAN outside the CDE to include: • Determining what to do if cleartext PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Determining how the data ended up outside the CDE. • Remediating data leaks or process gaps that resulted in the data being outside the CDE. • Identifying the source of the data. • Identifying whether any track data is stored with the PANs. Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.2.6 Mechanisms are implemented for detecting and preventing cleartext PAN from leaving the CDE via an unauthorized channel, method, or process, including mechanisms that are: • Actively running. • Configured to detect and prevent cleartext PAN leaving the CDE via an unauthorized channel, method, or process. • Generating audit logs and alerts upon detection of cleartext PAN leaving the CDE via an unauthorized channel, method, or process. PCI DSS Reference: Scope of PCI DSS Requirements, Requirement 12 Customized Approach Objective This requirement is not eligible for the customized approach.		

Defined Approach Requirements A3.2.6.1 Response procedures are implemented to be initiated upon the detection of attempts to remove cleartext PAN from the CDE via an unauthorized channel, method, or process. Response procedures include: • Procedures for the prompt investigation of alerts by responsible personnel. • Procedures for remediating data leaks or process gaps, as necessary, to prevent any data loss. PCI DSS Reference: Requirement 12 Customized Approach Objective This requirement is not eligible for the customized approach.		
A3.3 PCI DSS is incorporated into business-as-usual (BAU) activities.		
Defined Approach Requirements A3.3.1 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of: • Network security controls • IDS/IPS • FIM • Anti-malware solutions • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) • Automated audit log review mechanisms. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Automated code review tools (if used). This bullet is a best practice until its effective date; refer to Applicability Notes below for details. PCI DSS Reference: Requirements 1-12 Customized Approach Objective	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части обработки отказов систем безопасности для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за выполнение требований PCI DSS в части обработки отказов систем безопасности для компонентов, развёрнутых на платформе Yandex Cloud.

This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.3.1.2 Failures of any critical security control systems are responded to promptly. Processes for responding to failures in security control systems include: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure, including root cause, and documenting remediation required to address the root cause. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls. PCI DSS Reference: Requirements 1-12 Customized Approach Objective This requirement is not eligible for the customized approach.		
Defined Approach Requirements A3.3.2 Hardware and software technologies are reviewed at least once every 12 months to confirm whether they continue to meet the organization's PCI DSS requirements. PCI DSS Reference: Requirements 2, 6, 12. Customized Approach Objective This requirement is not eligible for the customized approach.		

Defined Approach Requirements A3.3.3 Reviews are performed at least once every three months to verify BAU activities are being followed. Reviews are performed by personnel assigned to the PCI DSS compliance program (as identified in A3.1.3), and include: • Confirmation that all BAU activities, including A3.2.2, A3.2.6, and A3.3.1, are being performed. • Confirmation that personnel are following security policies and operational procedures (for example, daily log reviews, ruleset reviews for network security controls, configuration standards for new systems). • Documenting how the reviews were completed, including how all BAU activities were verified as being in place. • Collection of documented evidence as required for the annual PCI DSS assessment. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program, as identified in A3.1.3. • Retention of records and documentation for at least 12 months, covering all BAU activities. PCI DSS Reference: Requirements 1-12 Customized Approach Objective This requirement is not eligible for the customized approach.		
A3.4 Logical access to the cardholder data environment is controlled and managed.		
Defined Approach Requirements 3.4.1 User accounts and access privileges to inscope system components are reviewed at least once every six months to ensure user accounts and access privileges remain appropriate based on job function, and that all access is authorized. PCI DSS Reference: Requirement 7 Customized Approach Objective This requirement is not eligible for the customized approach.	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, развёрнутым на платформе Yandex Cloud.

A3.5 Suspicious events are identified and responded to.		
Defined Approach Requirements A3.5.1 A methodology is implemented for the prompt identification of attack patterns and undesirable behavior across systems that includes: • Identification of anomalies or suspicious activity as it occurs. • Issuance of prompt alerts upon detection of suspicious activity or anomaly to responsible personnel. • Response to alerts in accordance with documented response procedures. PCI DSS Reference: Requirements 10, 12 Customized Approach Objective This requirement is not eligible for the customized approach.	Платформа Yandex Cloud отвечает за соблюдение требований PCI DSS в части методологии для оперативного выявления атак и нежелательного поведения для компонентов, обеспечивающих функционирование сервисов в области оценки.	Клиент отвечает за соблюдение требований PCI DSS в части методологии для оперативного выявления атак и нежелательного поведения для компонентов, развёрнутых на платформе Yandex Cloud.

Матрица разделения ответственности подготовлена с учетом следующих документов:

- PCI DSS v4.0 — Mar 2022: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
- Полный список изменений по сравнению с PCI DSS v3.2.1 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf
- Information Supplement: PCI SSC Cloud Computing Guidelines: https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf