

# Yandex.Cloud

**Разделение ответственности при выполнении требований  
ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских)  
операций. Защита информации финансовых организаций. Базовый  
набор организационных и технических мер»**



Yandex.Cloud. Разделение ответственности при выполнении требований ГОСТ Р 57580.1-2017.  
Этот документ является частью технической документации Yandex.Cloud.  
© 2021 ООО «Яндекс.Облако». Все права защищены.

### **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 ими) 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, 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, 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](mailto:cloud_docs@yandex-team.ru)

Главный офис: 119021, Россия, г. Москва, ул. Льва Толстого, д. 16

## Содержание

Введение	5
Область оценки ГОСТ Р 57580 Yandex.Cloud.....	6
Последовательность действий для достижения соответствия требованиям ГОСТ Р 57580.....	8
Разделение ответственности.....	9
Выполнение требований Яндекс.Облаком.....	9
Выполнение требований Клиентом.....	9
Общее разделение ответственности по процессам ГОСТ Р 57580.....	11
Полезные ссылки.....	12
Процесс 1 «Обеспечение защиты информации при управлении доступом».....	13
Подпроцесс «Управление учетными записями и правами субъектов логического доступа».....	13
Подпроцесс «Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа».....	14
Подпроцесс «Защита информации при осуществлении физического доступа».....	15
Подпроцесс «Идентификация и учет ресурсов и объектов доступа».....	17
Процесс 2 «Обеспечение защиты вычислительных сетей».....	18
Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей».....	18
Подпроцесс «Выявление вторжений и сетевых атак».....	19
Подпроцесс «Защита информации, передаваемой по вычислительным сетям».....	20
Подпроцесс «Защита беспроводных сетей».....	21
Процесс 3 «Контроль целостности и защищенности инфраструктуры».....	22
Процесс 4 «Защита от вредоносного кода».....	24
Процесс 5 «Предотвращение утечек информации».....	25
Процесс 6 «Управление инцидентами».....	26
Подпроцесс «Мониторинг и анализ событий защиты информации».....	26
Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них».....	28

Процесс 7 «Защита среды виртуализации» .....	29
Процесс 8 «ЗИ при осуществлении удаленного доступа с использованием мобильных устройств» .....	31
Организация защиты информации и управление защитой информации.....	32
Направление 1 «Планирование процесса системы защиты информации».....	32
Направление 2 «Реализация процесса системы защиты информации».....	32
Направление 3 «Контроль процесса системы защиты информации».....	33
Направление 4 «Совершенствование процесса системы защиты информации» .....	34
Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений .....	35

## **Введение**

Клиенты, реализующие на базе компонентов Yandex.Cloud инфраструктуру, попадающую под действие стандарта ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер» (ГОСТ Р 57580), должны использовать настоящий документ.

Документ описывает разделение ответственности за выполнение требований ГОСТ Р 57580. Часть требований выполняет платформа Yandex.Cloud, часть требований должен выполнить Клиент, часть требований является обоюдной ответственностью сторон.

Разделение ответственности за выполнение большинства требований каждого процесса ГОСТ Р 57580 зависит от используемой модели и типов облачных сервисов.

## Область оценки ГОСТ Р 57580 Yandex.Cloud

Платформа Yandex.Cloud имеет заключение о **четвертом** уровне соответствия в части соблюдения мер защиты информации ГОСТ Р 57580 для уровня защиты информации — **усиленный**.

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

### Infrastructure & Network

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

### Containers

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

### Security

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

### Data Platform

- [Yandex Managed Service for PostgreSQL \(https://cloud.yandex.ru/services/managed-postgresql\)](https://cloud.yandex.ru/services/managed-postgresql)
- [Yandex Managed Service for ClickHouse \(https://cloud.yandex.ru/services/managed-clickhouse\)](https://cloud.yandex.ru/services/managed-clickhouse)
- [Yandex Managed Service for MongoDB \(https://cloud.yandex.ru/services/managed-mongodb\)](https://cloud.yandex.ru/services/managed-mongodb)
- [Yandex Managed Service for MySQL® \(https://cloud.yandex.ru/services/managed-mysql\)](https://cloud.yandex.ru/services/managed-mysql)
- [Yandex Managed Service for Redis™ \(https://cloud.yandex.ru/services/managed-redis\)](https://cloud.yandex.ru/services/managed-redis)
- [Yandex Data Proc \(https://cloud.yandex.ru/services/data-proc\)](https://cloud.yandex.ru/services/data-proc)
- [Yandex Managed Service for Apache Kafka® \(https://cloud.yandex.ru/services/managed-kafka\)](https://cloud.yandex.ru/services/managed-kafka)
- [Yandex Managed Service for Elasticsearch \(https://cloud.yandex.ru/services/managed-elasticsearch\)](https://cloud.yandex.ru/services/managed-elasticsearch)
- [Yandex Database \(https://cloud.yandex.ru/services/ydb\)](https://cloud.yandex.ru/services/ydb)

## Serverless

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

## Operations

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

## **Последовательность действий для достижения соответствия требованиям ГОСТ Р 57580**

Клиенты, которые желают обеспечить соответствие ГОСТ Р 57580 для компонентов, развернутых на платформе Yandex.Cloud, должны соблюдать последовательность действий:

1. Изучить настоящий документ.
2. Построить инфраструктуру на платформе Yandex.Cloud с учетом требований ГОСТ Р 57580 и настоящего документа.
3. Выполнить требования ГОСТ Р 57580 в зоне ответственности Клиента.
4. Выбрать аудитора (с учетом требований соответствующих положений, например п. 9 Положения 683-П или п. 6.1 Положения 684-П) и провести аудит инфраструктуры, развернутой на платформе Yandex.Cloud, на соответствие требованиям ГОСТ Р 57580.

## **Разделение ответственности**

### **Выполнение требований Яндекс.Облаком**

Яндекс.Облако предоставляет Клиентам сервисы Infrastructure & Network, Containers, Serverless, Security, Data Platform, Operations, которые Клиенты могут использовать для обработки и хранения своей информации. Яндекс.Облако обеспечивает выполнение требований ГОСТ 57580.1-2017 в части обслуживаемой инфраструктуры, на базе которой функционируют сервисы IaaS, а также в части сервисов PaaS, размещаемых поверх инфраструктуры IaaS. Для инфраструктурных элементов реализованы технические и организационные меры защиты информации:

- управление учетными записями (сотрудников провайдера и технологическими учетными записями) и правами субъектов логического доступа, включая управление сервисными учетными записями;
- управление процессами идентификации, аутентификации и авторизации при осуществлении логического доступа со стороны сотрудников провайдера;
- физическая защита инфраструктурных элементов, используемых для функционирования сервисов;
- межсетевое экранирование служебных сетей платформы на физическом и виртуальном уровне;
- выявление нетипичной и подозрительной активности на уровне хостов виртуализации;
- управление уязвимостями операционных систем, сетевого оборудования, используемого и разрабатываемого ПО в части служебных сред платформы;
- защита от вредоносного кода на уровнях обслуживающего персонала;
- мониторинг событий информационной безопасности и реагирование на потенциальные нарушения в зоне ответственности провайдера;
- защита сервисных VM для платформенных сервисов;
- защита удаленного доступа обслуживающего персонала.

### **Выполнение требований Клиентом**

В рамках выполнения требований стандарта и процессов безопасности, описанных в ГОСТ 57580.1-2017, для средств, размещаемых Клиентом в виртуальной инфраструктуре, Клиентом должна производиться корректная настройка

параметров функционирования, удовлетворяющая требованиям стандарта ГОСТ 57580.1-2017, а также корректное выполнение процедур и процессов, связанных с обеспечением информационной безопасности. Примерами сущностей, для которых Клиентом самостоятельно должны производиться корректные настройки и на которые должны распространяться процессы безопасности Клиента, могут служить:

- виртуальные серверы, размещаемые в сервисе Compute Cloud или являющиеся частью сервиса Managed Service for Kubernetes;
- базы данных, размещаемые в сервисе Managed Service for PostgreSQL и других сервисах, предоставляющих управляемые базы данных;
- бакеты Object Storage, используемые для хранения данных;
- инстансы других сервисов.

Некоторые защитные меры могут быть реализованы Клиентом с использованием сервисов Яндекс.Облака. Например, могут использоваться такие сервисы, как:

- Virtual Private Cloud с функциональностью Security Groups для разграничения сетевого взаимодействия между инстансами;
- стандартные возможности разделения каталогов ресурсов;
- Key Management Service, предоставляющий возможность использования защищенного хранилища криптографических ключей;
- Yandex Identity and Access Management для управления доступом на уровне пользователей и сервисных учетных записей;
- другие возможности управления доступом, предоставляемые внутри сервисов Managed Service for Kubernetes, управляемых СУБД и др.

Кроме того, для реализации требований Клиентом могут использоваться собственные реализации средств защиты информации, размещаемые в сервисах Яндекс.Облака, либо средства защиты, размещенные в [Yandex Cloud Marketplace](#):

программные и виртуальные межсетевые экраны, программные средства, размещаемые на уровне операционных систем, средства ограничения runtime-среды для Kubernetes и др.

## Общее разделение ответственности по процессам ГОСТ Р 57580

Процесс/подпроцесс ГОСТ Р 57580		Ответственность	
		IaaS	PaaS
Процесс 1 «Обеспечение защиты информации при управлении доступом»	Управление учетными записями и правами субъектов логического доступа	Обоюдная	Обоюдная
	Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа	Обоюдная	Обоюдная
	Защита информации при осуществлении физического доступа	Yandex.Cloud	Yandex.Cloud
	Идентификация и учет ресурсов и объектов доступа	Обоюдная	Обоюдная
Процесс 2 «Обеспечение защиты вычислительных сетей»	Сегментация и межсетевое экранирование вычислительных сетей	Обоюдная	Обоюдная
	Выявление вторжений и сетевых атак	Обоюдная	Yandex.Cloud
	Защита информации, передаваемой по вычислительным сетям	Обоюдная	Обоюдная
	Защита беспроводных сетей	Обоюдная	Yandex.Cloud
Процесс 3 «Контроль целостности и защищенности инфраструктуры»		Обоюдная	Обоюдная
Процесс 4 «Защита от вредоносного кода»		Обоюдная	Yandex.Cloud
Процесс 5 «Предотвращение утечек информации»		Клиент	Клиент
Процесс 6 «Управление инцидентами»	Мониторинг и анализ событий защиты информации	Обоюдная	Обоюдная
	Обнаружение инцидентов защиты информации и реагирование на них	Обоюдная	Обоюдная
Процесс 7 «Защита среды виртуализации»		Обоюдная	Yandex.Cloud
Процесс 8 «ЗИ при осуществлении удаленного доступа с использованием мобильных устройств»		Обоюдная	Обоюдная
Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений		Обоюдная	Обоюдная

## Полезные ссылки

- [Безопасность Yandex.Cloud](#)
- [Матрица разделения ответственности PCI DSS](#)
- [Требования и рекомендации для построения PCI DSS](#)
- [Создание группы безопасности](#)
- [Шифрование секретов в Yandex Managed Service for Kubernetes](#)
- [Шифрование по схеме envelope encryption](#)
- [Рекомендации по управлению доступом к Yandex.Cloud](#)
- [Использование SAML-совместимых федераций удостоверений](#)

Документ подготовлен с учетом следующих источников:

- ФЗ-161 «О национальной платежной системе».
- Положение ЦБ РФ от 9 января 2019 г. № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».
- Положение Банка России от 17 апреля 2019 г. № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».
- ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер».
- ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».

## Разделение ответственности при выполнении требований ГОСТ Р 57580

### Процесс 1 «Обеспечение защиты информации при управлении доступом»

#### Подпроцесс «Управление учетными записями и правами субъектов логического доступа»

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
УЗП.1	Платформа Yandex.Cloud для компонентов, обеспечивающих функционирование сервисов в области оценки, отвечает за:	Клиент для компонентов, развернутых на платформе Yandex.Cloud, отвечает за:
УЗП.2		
УЗП.3		
УЗП.4		
УЗП.5		
УЗП.6		
УЗП.7		
УЗП.8		
УЗП.9		
УЗП.10		
УЗП.11		
УЗП.12		
УЗП.13		
УЗП.14		
УЗП.15		
УЗП.16		
УЗП.17		
УЗП.18		
УЗП.19		
УЗП.20		
УЗП.21		
УЗП.22		
УЗП.23		
УЗП.24		
УЗП.25		
УЗП.26		
УЗП.27		
УЗП.28		
УЗП.29		

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

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
РД.1	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в                      области оценки</b> , отвечает за: — идентификацию и аутентификацию субъектов логического доступа; — организацию управления идентификационными и аутентификационными данными и организацию защиты идентификационных и аутентификационных данных; — авторизацию (разграничение доступа) при осуществлении логического доступа; — регистрацию событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа.	Клиент для компонентов, <b>развернутых на платформе                      Yandex.Cloud</b> , отвечает за: — идентификацию и аутентификацию субъектов логического доступа; — применение многофакторной аутентификации для доступа к ресурсам контура безопасности; — организацию управления идентификационными и аутентификационными данными и организацию защиты идентификационных и аутентификационных данных; — авторизацию (разграничение доступа) при осуществлении логического доступа; — регистрацию событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа.  Для централизованного управления учетными данными рекомендуется использовать <a href="#">SAML-совместимые федерации                      удостоверений</a> .
РД.2		
РД.3		
РД.4		
РД.5		
РД.6		
РД.7		
РД.8		
РД.9		
РД.10		
РД.11		
РД.12		
РД.13		
РД.14		
РД.15		
РД.16		
РД.17		
РД.18		
РД.19		
РД.20		
РД.21		
РД.22		
РД.23		
РД.24		
РД.25		
РД.26		
РД.27		
РД.28		
РД.29		
РД.30		

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
РД.31		
РД.32		
РД.33		
РД.34		
РД.35		
РД.36		
РД.37		
РД.38		
РД.39		
РД.40		
РД.41		
РД.42		
РД.43		
РД.44		

**Подпроцесс «Защита информации при осуществлении физического доступа»**

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ФД.1 — ФД.21	<p>Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области оценки</b>, отвечает за:</p> <ul style="list-style-type: none"> <li>— организацию и контроль физического доступа в помещения, в которых расположены объекты доступа;</li> <li>— регистрацию событий, связанных с физическим доступом.</li> </ul> <p>Платформа Yandex.Cloud обеспечивает физическую безопасность дата-центров, в которых расположены компоненты, обеспечивающие функционирование сервисов в области оценки.</p>	<p>Клиент для компонентов, <b>развернутых на платформе Yandex.Cloud</b>, отвечает за:</p> <ul style="list-style-type: none"> <li>— организацию и контроль физического доступа к объектам доступа, расположенным в публичных (общедоступных) местах (если такие объекты используются).</li> </ul> <p>Требование не применимо, если данные не передаются за пределы платформы Yandex.Cloud. Если данные передаются за пределы платформы, то Клиент отвечает за выполнение</p>
ФД.2		
ФД.3		
ФД.4		
ФД.5		
ФД.6		
ФД.7		
ФД.8		
ФД.9		
ФД.10		
ФД.11		
ФД.12		
ФД.13		
ФД.14		
ФД.15		

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ФД.16		требований ГОСТ Р 58580 в части «Защита информации при осуществлении физического доступа».
ФД.17		
ФД.18		
ФД.19		
ФД.20		
ФД.21		

**Подпроцесс «Идентификация и учет ресурсов и объектов доступа»**

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ИУ.1	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в                      области оценки</b> , отвечает за: — организацию учета и контроль состава ресурсов и объектов доступа; — регистрацию событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа.	Клиент для компонентов, <b>развернутых на платформе                      Yandex.Cloud</b> , отвечает за: — организацию учета и контроль состава ресурсов и объектов доступа; — регистрацию событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа.
ИУ.2		
ИУ.3		
ИУ.4		
ИУ.5		
ИУ.6		
ИУ.7		
ИУ.8		

## Процесс 2 «Обеспечение защиты вычислительных сетей»

### Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей»

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
СМЭ.1	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области                      оценки</b> , отвечает за: — сегментацию и межсетевое экранирование внутренних вычислительных сетей; — защиту внутренних вычислительных сетей при взаимодействии с сетью Интернет; — регистрацию событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей.  Платформа Yandex.Cloud обеспечивает реализацию опорной сети и SDN, а также процедур управления ими в соответствии с требованиями ГОСТ Р 57580.	Клиент для компонентов, <b>развернутых на платформе                      Yandex.Cloud</b> , отвечает за: — сегментацию и межсетевое экранирование внутренних вычислительных сетей; — защиту внутренних вычислительных сетей при взаимодействии интернетом; — регистрацию событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей; — архитектуру проекта и конфигурацию настроек сетевых компонентов Yandex.Cloud; — управление клиентскими виртуальными сетями; — управление группами безопасности, МЭ и маршрутизаторами; — используемый набор сервисов, протоколов и портов.  Для системного управления правилами МЭ рекомендуется использовать <a href="#">группы безопасности</a> .
СМЭ.2		
СМЭ.3		
СМЭ.4		
СМЭ.5		
СМЭ.6		
СМЭ.7		
СМЭ.8		
СМЭ.9		
СМЭ.10		
СМЭ.11		
СМЭ.12		
СМЭ.13		
СМЭ.14		
СМЭ.15		
СМЭ.16		
СМЭ.17		
СМЭ.18		
СМЭ.19		
СМЭ.20		
СМЭ.21		

**Подпроцесс «Выявление вторжений и сетевых атак»**

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
BCA.1	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в                      области оценки</b> , отвечает за: — мониторинг и контроль содержимого сетевого трафика; — регистрацию событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика.	Клиент для компонентов, <b>развернутых на платформе Yandex.Cloud</b> , отвечает за: — мониторинг и контроль содержимого сетевого трафика; — регистрацию событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика; — использование методов и систем обнаружения или предотвращения вторжений.
BCA.2		
BCA.3		
BCA.4		
BCA.5		
BCA.6		
BCA.7		
BCA.8		
BCA.9		
BCA.10		
BCA.11		
BCA.12		
BCA.13		
BCA.14		

**Подпроцесс «Защита информации, передаваемой по вычислительным сетям»**

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ЗВС.1 ЗВС.2	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области оценки</b> , отвечает за выполнение мер по защите информации, передаваемой по недоверенным вычислительным сетям.	Клиент для компонентов, <b>развернутых на платформе Yandex.Cloud</b> , отвечает за выполнение мер по защите информации, передаваемой по недоверенным вычислительным сетям, в том числе за применение протоколов TLS и др. Yandex.Cloud рекомендует использовать шифрование конфиденциальных данных во всех случаях, включая передачу внутри клиентских сетей и передачу в общедоступных сетях.

**Подпроцесс «Защита беспроводных сетей»**

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ЗБС.1 ЗБС.2 ЗБС.3 ЗБС.4 ЗБС.5 ЗБС.6 ЗБС.7 ЗБС.8 ЗБС.9 ЗБС.10	<p>Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области оценки</b>, отвечает за:</p> <ul style="list-style-type: none"> <li>— защиту информации от раскрытия и модификации при использовании беспроводных сетей;</li> <li>— защиту внутренних вычислительных сетей при использовании беспроводных сетей;</li> <li>— регистрацию событий защиты информации, связанных с использованием беспроводных сетей;</li> <li>— мониторинг несанкционированных беспроводных сетей и точек доступа.</li> </ul>	<p>Клиент в случае использования им беспроводных сетей в контуре безопасности отвечает за:</p> <ul style="list-style-type: none"> <li>— защиту информации от раскрытия и модификации при использовании беспроводных сетей;</li> <li>— защиту внутренних вычислительных сетей при использовании беспроводных сетей;</li> <li>— регистрацию событий защиты информации, связанных с использованием беспроводных сетей.</li> </ul>

### Процесс 3 «Контроль целостности и защищенности инфраструктуры»

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ЦЗИ.1	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области                      оценки</b> , отвечает за: — контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации; — организацию и контроль размещения, хранения и обновления ПО информационной инфраструктуры; — контроль состава и целостности ПО информационной инфраструктуры; — регистрацию событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры; — имплементацию и контроль настроек безопасности для PaaS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database.	Клиент для компонентов, <b>развернутых на платформе                      Yandex.Cloud</b> , отвечает за: — контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации; — организацию и контроль размещения, хранения и обновления ПО информационной инфраструктуры; — контроль состава и целостности ПО информационной инфраструктуры; — регистрацию событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры; — имплементацию и контроль настроек безопасности для компонентов, развернутых на платформе Yandex.Cloud: <ul style="list-style-type: none"> <li>• операционных систем;</li> <li>• баз данных (за исключением PaaS-сервисов: Yandex                          Managed Service for Kubernetes®, PostgreSQL, ClickHouse,                          MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch,                          Yandex Data Proc, Yandex Database);</li> <li>• прикладного ПО;</li> <li>• других компонентов и сервисов, включенных                          Клиентом в область оценки.</li> </ul>
ЦЗИ.2		
ЦЗИ.3		
ЦЗИ.4		
ЦЗИ.5		
ЦЗИ.6		
ЦЗИ.7		
ЦЗИ.8		
ЦЗИ.9		
ЦЗИ.10		
ЦЗИ.11		
ЦЗИ.12		
ЦЗИ.13		
ЦЗИ.14		
ЦЗИ.15		
ЦЗИ.16		
ЦЗИ.17		
ЦЗИ.18		
ЦЗИ.19		
ЦЗИ.20		
ЦЗИ.21		
ЦЗИ.22		
ЦЗИ.23		
ЦЗИ.24		
ЦЗИ.25		
ЦЗИ.26		
ЦЗИ.27		
ЦЗИ.28		
ЦЗИ.29		
ЦЗИ.30		
ЦЗИ.31		
ЦЗИ.32		
ЦЗИ.33		

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ЦЗИ.34		
ЦЗИ.35		
ЦЗИ.36		

#### Процесс 4 «Защита от вредоносного кода»

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ЗВК.1	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области                      оценки</b> , отвечает за: — организацию эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры; — организацию и контроль применения средств защиты от вредоносного кода; — регистрацию событий защиты информации, связанных с реализацией защиты от вредоносного кода.	Клиент для компонентов, <b>развернутых на платформе                      Yandex.Cloud</b> , отвечает за: — организацию эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры; — организацию и контроль применения средств защиты от вредоносного кода; — регистрацию событий защиты информации, связанных с реализацией защиты от вредоносного кода.
ЗВК.2		
ЗВК.3		
ЗВК.4		
ЗВК.5		
ЗВК.6		
ЗВК.7		
ЗВК.8		
ЗВК.9		
ЗВК.10		
ЗВК.11		
ЗВК.12		
ЗВК.13		
ЗВК.14		
ЗВК.15		
ЗВК.16		
ЗВК.17		
ЗВК.18		
ЗВК.19		
ЗВК.20		
ЗВК.21		
ЗВК.22		
ЗВК.23		
ЗВК.24		
ЗВК.25		
ЗВК.26		
ЗВК.27		
ЗВК.28		

## Процесс 5 «Предотвращение утечек информации»

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ПУИ.1	<p>Платформа Yandex.Cloud самостоятельно не занимается выполнением бизнес-процессов и (или) технологических процессов, связанных с предоставлением финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств.</p> <p>Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области оценки</b>, обеспечивает выполнение требований ГОСТ Р 57580 в части организации защиты машинных носителей информации (МНИ), содержащих данные Клиентов.</p>	<p>Клиент для компонентов, <b>развернутых на платформе Yandex.Cloud</b>, отвечает за:</p> <ul style="list-style-type: none"> <li>— блокирование не разрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации;</li> <li>— контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации;</li> <li>— организацию защиты машинных носителей информации (МНИ), если такие используются для обработки информации при предоставлении финансовых услуг;</li> <li>— регистрацию событий защиты информации, связанных с реализацией предотвращения утечки информации.</li> </ul> <p>Клиент может использовать сервис <a href="#">Yandex Key Management Service</a> для защиты информации при хранении.</p>
ПУИ.2		
ПУИ.3		
ПУИ.4		
ПУИ.5		
ПУИ.6		
ПУИ.7		
ПУИ.8		
ПУИ.9		
ПУИ.10		
ПУИ.11		
ПУИ.12		
ПУИ.13		
ПУИ.14		
ПУИ.15		
ПУИ.16		
ПУИ.17		
ПУИ.18		
ПУИ.19		
ПУИ.20		
ПУИ.21		
ПУИ.22		
ПУИ.23		
ПУИ.24		
ПУИ.25		
ПУИ.26		
ПУИ.27		
ПУИ.28		
ПУИ.29		
ПУИ.30		
ПУИ.31		
ПУИ.32		
ПУИ.33		

## Процесс 6 «Управление инцидентами»

### Подпроцесс «Мониторинг и анализ событий защиты информации»

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
MAC.1 MAC.2 MAC.3 MAC.4 MAC.5 MAC.6 MAC.7 MAC.8 MAC.9 MAC.10 MAC.11 MAC.12 MAC.13 MAC.14 MAC.15 MAC.16 MAC.17 MAC.18 MAC.19 MAC.20 MAC.21 MAC.22 MAC.23	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области оценки</b> , отвечает за: — организацию мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информатизации, в том числе в соответствии с требованиями к содержанию базового состава мер защиты информации настоящего стандарта; — сбор, защиту и хранение данных регистрации о событиях защиты информации; — анализ данных регистрации о событиях защиты информации; — регистрацию событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации; — регистрацию событий защиты информации для PaaS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database.	Клиент для компонентов, <b>развернутых на платформе Yandex.Cloud</b> , отвечает за: — организацию мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информатизации, в том числе в соответствии с требованиями к содержанию базового состава мер защиты информации настоящего стандарта; — сбор, защиту и хранение данных регистрации о событиях защиты информации; — анализ данных регистрации о событиях защиты информации; — регистрацию событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации; — выполнение требований ГОСТ Р 57580 в части регистрации необходимых типов событий, а именно: <ul style="list-style-type: none"> <li>• операционных систем;</li> <li>• баз данных (за исключением PaaS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database);</li> <li>• прикладного ПО;</li> <li>• других компонентов и сервисов, включенных Клиентом в область оценки.</li> </ul>

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
		Клиент также отвечает за выполнение требований PCI DSS в части синхронизации времени для компонентов, развернутых на платформе Yandex.Cloud. См. <a href="#">рекомендации по настройке синхронизации времени с использованием NTP</a> .

**Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них»**

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
РИ.1	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области                      оценки</b> , отвечает за: — обнаружение и регистрацию инцидентов защиты информации; — организацию реагирования на инциденты защиты информации; — организацию хранения и защиту информации об инцидентах защиты информации; — регистрацию событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них.	Клиент для компонентов, <b>развернутых на платформе                      Yandex.Cloud</b> , отвечает за: — обнаружение и регистрацию инцидентов защиты информации; — организацию реагирования на инциденты защиты информации; — организацию хранения и защиту информации об инцидентах защиты информации; — регистрацию событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них.
РИ.2		
РИ.3		
РИ.4		
РИ.5		
РИ.6		
РИ.7		
РИ.8		
РИ.9		
РИ.10		
РИ.11		
РИ.12		
РИ.13		
РИ.14		
РИ.15		
РИ.16		
РИ.17		
РИ.18		
РИ.19		

**Процесс 7 «Защита среды виртуализации»**

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ЗСВ.1	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области                      оценки</b> , отвечает за: — организацию идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации; — организацию и контроль информационного взаимодействия и изоляции виртуальных машин; — организацию защиты образов виртуальных машин; — регистрацию событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации.	Клиент для компонентов, <b>развернутых на платформе                      Yandex.Cloud</b> , отвечает за: — организацию идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к сервисам и виртуальным машинам; — организацию и контроль информационного взаимодействия и изоляции виртуальных машин; — организацию защиты образов виртуальных машин; — регистрацию событий защиты информации, связанных с доступом к виртуальным машинам.
ЗСВ.2		
ЗСВ.3		
ЗСВ.4		
ЗСВ.5		
ЗСВ.6		
ЗСВ.7		
ЗСВ.8		
ЗСВ.9		
ЗСВ.10		
ЗСВ.11		
ЗСВ.12		
ЗСВ.13		
ЗСВ.14		
ЗСВ.15		
ЗСВ.16		
ЗСВ.17		
ЗСВ.18		
ЗСВ.19		
ЗСВ.20		
ЗСВ.21		
ЗСВ.22		
ЗСВ.23		
ЗСВ.24		
ЗСВ.25		
ЗСВ.26		
ЗСВ.27		
ЗСВ.28		
ЗСВ.29		
ЗСВ.30		
ЗСВ.31		
ЗСВ.32		
ЗСВ.33		

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ЗСВ.34		
ЗСВ.35		
ЗСВ.36		
ЗСВ.37		
ЗСВ.38		
ЗСВ.39		
ЗСВ.40		
ЗСВ.41		
ЗСВ.42		
ЗСВ.43		

**Процесс 8 «ЗИ при осуществлении удаленного доступа с использованием мобильных устройств»**

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ЗУД.1	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области                      оценки</b> , отвечает за: — защиту информации от раскрытия и модификации при осуществлении удаленного доступа; — защиту внутренних вычислительных сетей при осуществлении удаленного доступа; — защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах.	Клиент для компонентов, <b>развернутых на платформе                      Yandex.Cloud</b> , отвечает за: — защиту информации от раскрытия и модификации при осуществлении удаленного доступа; — защиту внутренних вычислительных сетей при осуществлении удаленного доступа; — защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах.
ЗУД.2		
ЗУД.3		
ЗУД.4		
ЗУД.5		
ЗУД.6		
ЗУД.7		
ЗУД.8		
ЗУД.9		
ЗУД.10		
ЗУД.11		
ЗУД.12		

## Организация защиты информации и управление защитой информации

### Направление 1 «Планирование процесса системы защиты информации»

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ПЗИ.1 ПЗИ.2 ПЗИ.3 ПЗИ.4 ПЗИ.5	<p>Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области оценки</b>, отвечает за определение (пересмотр):</p> <ul style="list-style-type: none"> <li>— области применения процесса системы защиты информации;</li> <li>— состава применяемых (а также не применяемых) мер защиты информации из числа мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580;</li> <li>— состава и содержания мер защиты информации, являющихся дополнительными к базовому составу мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580, определяемых на основе актуальных угроз защиты информации, требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации;</li> <li>— порядка применения мер защиты информации в рамках процесса системы защиты информации.</li> </ul>	<p>Клиент для компонентов, <b>развернутых на платформе Yandex.Cloud</b>, отвечает за:</p> <ul style="list-style-type: none"> <li>— области применения процесса системы защиты информации;</li> <li>— состава применяемых (а также не применяемых) мер защиты информации из числа мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580;</li> <li>— состава и содержания мер защиты информации, являющихся дополнительными к базовому составу мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580, определяемых на основе актуальных угроз защиты информации, требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации;</li> <li>— порядка применения мер защиты информации в рамках процесса системы защиты информации.</li> </ul>

### Направление 2 «Реализация процесса системы защиты информации»

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
РЗИ.1 РЗИ.2 РЗИ.3 РЗИ.4	<p>Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области оценки</b>, отвечает за:</p>	<p>Клиент для компонентов, <b>развернутых на платформе Yandex.Cloud</b>, отвечает за:</p>

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
РЗИ.5	<p>— должное применение мер защиты информации;</p> <p>— определение ролей защиты информации, связанных с применением мер защиты информации;</p> <p>— назначение лиц, ответственных за выполнение ролей защиты информации;</p> <p>— доступность реализации технических мер защиты информации;</p> <p>— применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия (в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности), в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации финансовой организации;</p> <p>— обучение, практическую подготовку (переподготовку) работников финансовой организации, ответственных за применение мер защиты информации;</p> <p>— повышение осведомленности (инструктаж) работников финансовой организации в области защиты информации.</p>	<p>— должное применение мер защиты информации;</p> <p>— определение ролей защиты информации, связанных с применением мер защиты информации;</p> <p>— назначение лиц, ответственных за выполнение ролей защиты информации;</p> <p>— доступность реализации технических мер защиты информации;</p> <p>— применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия (в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности), в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации финансовой организации;</p> <p>— обучение, практическую подготовку (переподготовку) работников финансовой организации, ответственных за применение мер защиты информации;</p> <p>— повышение осведомленности (инструктаж) работников финансовой организации в области защиты информации.</p>
РЗИ.6		
РЗИ.7		
РЗИ.8		
РЗИ.9		
РЗИ.10		
РЗИ.11		
РЗИ.12		
РЗИ.13		
РЗИ.14		
РЗИ.15		
РЗИ.16		

### Направление 3 «Контроль процесса системы защиты информации»

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
КЗИ.1	<p>Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области оценки</b>, отвечает за:</p>	<p>Клиент для компонентов, <b>развернутых на платформе Yandex.Cloud</b>, отвечает за:</p>
КЗИ.2		
КЗИ.3		
КЗИ.4		

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
КЗИ.5	<p>— области применения процесса системы защиты информации;</p> <p>— должное применение мер защиты информации в рамках процесса системы защиты информации;</p> <p>— знания работников финансовой организации в части применения мер защиты информации.</p>	<p>— области применения процесса системы защиты информации;</p> <p>— должное применение мер защиты информации в рамках процесса системы защиты информации;</p> <p>— знания работников финансовой организации в части применения мер защиты информации.</p>
КЗИ.6		
КЗИ.7		
КЗИ.8		
КЗИ.9		
КЗИ.10		
КЗИ.11		
КЗИ.12		

#### **Направление 4 «Совершенствование процесса системы защиты информации»**

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
СЗИ.1	<p>Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области оценки</b>, отвечает за деятельность по совершенствованию процессов защиты информации.</p>	<p>Клиент для компонентов, <b>развернутых на платформе Yandex.Cloud</b>, отвечает за деятельность по совершенствованию процессов защиты информации.</p>
СЗИ.2		
СЗИ.3		
СЗИ.4		

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

Меры ГОСТ Р 57580	Ответственность	
	Yandex.Cloud	Клиент
ЖЦ.1	Платформа Yandex.Cloud для компонентов, <b>обеспечивающих функционирование сервисов в области оценки</b> , отвечает за: — защиту информации от раскрытия и модификации при осуществлении удаленного доступа; — защиту внутренних вычислительных сетей при осуществлении удаленного доступа; — защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах.	Клиент для компонентов, <b>развернутых на платформе Yandex.Cloud</b> , отвечает за: — защиту информации от раскрытия и модификации при осуществлении удаленного доступа; — защиту внутренних вычислительных сетей при осуществлении удаленного доступа; — защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах. Клиент также отвечает за проведение контроля защищенности. Анализ уязвимости и тесты на проникновение должны выполняться согласно документу <a href="#">Правила проведения внешних сканирований безопасности</a> .
ЖЦ.2		
ЖЦ.3		
ЖЦ.4		
ЖЦ.5		
ЖЦ.6		
ЖЦ.7		
ЖЦ.8		
ЖЦ.9		
ЖЦ.10		
ЖЦ.11		
ЖЦ.12		
ЖЦ.13		
ЖЦ.14		
ЖЦ.15		
ЖЦ.16		
ЖЦ.17		
ЖЦ.18		
ЖЦ.19		
ЖЦ.20		
ЖЦ.21		
ЖЦ.22		
ЖЦ.23		
ЖЦ.24		
ЖЦ.25		
ЖЦ.26		
ЖЦ.27		
ЖЦ.28		