Разделение ответственности при выполнении требований ГОСТ Р 57580.1-2017

ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер

Yandex Cloud

2023

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, влечт за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Yandex Cloud. Разделение ответственности при выполнении требований ГОСТ Р 57580.1-2017.

Этот документ является составной частью технической документации Yandex Cloud.

Контактная информация ООО «Яндекс.Облако» 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

Оглавление

Введение

Воспользуйтесь этим документом, если инфраструктура, которую вы реализуете на базе компонентов Yandex Cloud, попадает под действие стандарта ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер.

Документ описывает разделение ответственности за выполнение требований ГОСТ Р 57580. Часть требований выполняет платформа Yandex Cloud, часть вы должны выполнять самостоятельно, а часть 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 об оценке соответствии требованиям ГОСТ Р 57580 по усиленному уровню защиты информации. На момент окончания аудита итоговая оценка составила R=0,91 (**пятый уровень соответствия**).

В область оценки входит базовая инфраструктура платформы Yandex Cloud, а также сервисы на её основе:

Infrastructure & Network

- API Gateway (Integration with Yandex Cloud services)
- Application Load Balancer (L7 load balancers)
- Cloud CDN (Content Delivery Network organization)
- Cloud DNS (Domain name management)
- Cloud Interconnect (Dedicated network connections)
- Cloud Logging (Yandex Cloud services logging)
- Compute Cloud (Virtual machines and block storage)
- Network Load Balancer (Network load balancers)
- Object Storage (Scalable data storage)
- Virtual Private Cloud (Cloud network management)
- Monitoring (Collection and visualization of metrics)

Containers

- Container Registry (Managed Docker images)
- Managed Service for Kubernetes (Managed Kubernetes clusters)
- Serverless Containers (Running containers without Kubernetes)

Security

- Identity and Access Management (Identification and access control to cloud resources)
- Certificate Manager (TLS certificate management)
- Key Management Service (Cryptographic keys management)

Lockbox (Create and store secrets)

Audit Trails (Collect and export audit logs)

Data Platform

Data Proc (Managed Apache Hadoop clusters)

Data Streams (Data streams management)

Data Transfer (Data migration and transport tool)

Managed Service for PostgreSQL, ClickHouse, MySQL, Redis, MongoDB, Elasticsearch, Apache Kafka, YDB, Greenplum

Message Queue (Queues for messaging between applications)

Object Storage (Scalable data storage)

Monitoring (Collection and visualization of metrics)

Serverless

API Gateway (Integration with Yandex Cloud services)

Cloud Functions (Running your code as a function)

Data Streams (Data streams management)

Managed Service for YDB (Distributed fault-tolerant SQL DBMS)

Message Queue (Queues for messaging between applications)

Object Storage (Scalable data storage)

Serverless Containers (Running containers without Kubernetes)

Resources & Operations

Identity and Access Management (Identification and access control to cloud resources)

Cloud Logging (Yandex Cloud services logging)

Cloud Organization (Organization service management)

Monitoring (Collection and visualization of metrics);

Resource Manager (Resource management in folders and clouds)

Последовательность действий для достижения соответствия требованиям ГОСТ Р 57580

Если вы хотите, чтобы компоненты, развёрнутые на платформе Yandex Cloud, соответствовали ГОСТ Р 57580, выполните действия:

1. Изучите настоящий документ.
2. Постройте инфраструктуру на платформе Yandex Cloud с учётом требований ГОСТ Р 57580 и настоящего документа.
3. Выполните требования ГОСТ Р 57580 в своей зоне ответственности.
4. Выберите аудитора (с учётом требований соответствующих положений, например п. 9 Положения 683-П или 757-П) и проведите аудит инфраструктуры, развёрнутой на платформе Yandex Cloud, на соответствие требованиям ГОСТ Р 57580.

Разделение ответственности

Выполнение требований Yandex Cloud

Yandex Cloud предоставляет сервисы Infrastructure & Network, Containers, Serverless, Security, Data Platform, Operations, которые вы можете использовать для обработки и хранения своей информации. Yandex Cloud 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 учётными записями сотрудников провайдера и технологическими учётными записями и правами субъектов логического доступа, включая управление сервисными учётными 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 виртуальных машин (ВМ) для платформенных сервисов;
- защита удалённого доступа обслуживающего персонала.

Выполнение требований клиентом

Чтобы соответствовать требованиям стандарта и процессов безопасности, описанных в ГОСТ 57580.1-2017, корректно настройте:

- параметры функционирования средств, которые вы размещаете в виртуальной инфраструктуре, чтобы они удовлетворяли требованиям стандарта ГОСТ 57580.1-2017;
- выполнение процедур и процессов, связанных с обеспечением информационной безопасности.

Примерами сущностей, параметры которых вы должны самостоятельно корректно настроить и на которые должны распространяться ваши процессы безопасности:

- 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 вы можете реализовать с помощью сервисов Yandex Cloud. Вот примеры таких сервисов:

- Virtual Private Cloud с функциональностью Security Groups для разграничения сетевого взаимодействия между инстансами;
- стандартные возможности разделения каталогов ресурсов;
- Key Management Service, который позволяет хранить криптографические ключи в защищённом хранилище;
- Yandex Identity and Access Management для управления доступом на уровне пользователей и сервисных учётных записей;
- другие возможности управления доступом, которые предоставляют Managed Service for Kubernetes®, управляемые СУБД и т. д;
- выбрать меры обеспечения информационной безопасности (ИБ) при развёртывании информационных систем на облачной платформе Yandex Cloud поможет Стандарт по защите облачной инфраструктуры Yandex Cloud.

Кроме того, для реализации требований вы можете использовать собственные средства защиты информации, размещаемые в Yandex Cloud или в Yandex Cloud Marketplace: программные и виртуальные межсетевые экраны, программные средства на уровне операционных систем, средства ограничения runtime-среды для Kubernetes® и др.

Общее разделение ответственности по процессам ГОСТ Р 57580

Процесс	Подпроцесс	Ответственность IaaS/PaaS
Обеспечение защиты информации при управлении доступом	Управление учётными записями и правами субъектов логического доступа	Обоюдная
	Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа	Обоюдная
	Защита информации при осуществлении физического доступа	Yandex Cloud
	Идентификация и учёт ресурсов и объектов доступа	Обоюдная
Обеспечение защиты вычислительных сетей	Сегментация и межсетевое экранирование вычислительных сетей	Обоюдная
	Выявление вторжений и сетевых атак	Обоюдная / Yandex Cloud
	Защита информации, передаваемой по вычислительным сетям	Обоюдная
	Защита беспроводных сетей	Обоюдная / Yandex Cloud
Контроль целостности и защищённости инфраструктуры		Обоюдная
Защита от вредоносного кода		Обоюдная / Yandex Cloud
Предотвращение утечек информации		Клиент

Процесс	Подпроцесс	Ответственность IaaS/PaaS
Управление инцидентами	Мониторинг и анализ событий, связанных с защитой информации (ЗИ)	Обоюдная
	Обнаружение инцидентов защиты информации и реагирование на них	Обоюдная
Защита среды виртуализации		Обоюдная / Yandex Cloud
ЗИ при осуществлении удалённого доступа с использованием мобильных устройств		Обоюдная
Требования к защите информации на этапах жизненного цикла автоматизированных систем и приложений		Обоюдная

Документ подготовлен с учётом следующих источников

Федеральный закон от 27 июня 2011 г. N 161-ФЗ «О национальной платёжной системе».

Положение ЦБ РФ от 9 января 2019 г. N 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 20 апреля 2021 г. N 757-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 учётными записями и правами субъектов логического доступа»

Меры ГОСТ Р 57580: УЗП.1—УЗП.29

Ответственность Yandex Cloud

Организация и контроль использования учётных записей субъектов логического доступа.

Организация и контроль предоставления (отзыва) и блокирования логического доступа.

Регистрация событий защиты информации, связанных с операциями с учётными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа.

Закрепление АРМ пользователей и эксплуатационного персонала за конкретными субъектами логического доступа.

Ответственность клиента

Организация и контроль использования учётных записей субъектов логического доступа.

Организация и контроль предоставления (отзыва) и блокирования логического доступа.

Регистрация событий защиты информации, связанных с операциями с учётными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа.

Закрепление АРМ пользователей и эксплуатационного персонала за конкретными субъектами логического доступа.

Управление учётными записями и правами субъектов логического доступа при использовании SAML-совместимой федерации удостоверений.

Для централизованного управления учётными данными рекомендуется использовать SAML-совместимые федерации удостоверений.

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

Меры ГОСТ Р 57580: РД.1 – РД.44

Ответственность Yandex Cloud

Идентификация и аутентификация субъектов логического доступа.

Организация управления идентификационными и аутентификационными данными.

Организация защиты идентификационных и аутентификационных данных.

Авторизация (разграничение доступа) при осуществлении логического доступа.

Регистрация событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа.

Ответственность клиента

Идентификация и аутентификация субъектов логического доступа.

Применение многофакторной аутентификации для доступа к ресурсам контура безопасности.

Организация управления идентификационными и аутентификационными данными и организация защиты идентификационных и аутентификационных данных.

Авторизация (разграничение доступа) при осуществлении логического доступа.

Регистрация событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа.

Для централизованного управления учётными данными рекомендуется использовать SAML-совместимые федерации удостоверений.

Подпроцесс «Защита информации при осуществлении физического доступа»

Меры ГОСТ Р 57580: ФД.1 – ФД.21

Ответственность Yandex Cloud

Организация и контроль физического доступа в помещения, в которых расположены объекты доступа.

Регистрация событий, связанных с физическим доступом.

Платформа Yandex Cloud обеспечивает физическую безопасность дата-центров, в которых расположены компоненты, обеспечивающие функционирование сервисов в области оценки.

Ответственность клиента

Организация и контроль физического доступа к объектам доступа, расположенным в публичных (общедоступных) местах (если такие объекты используются).

Требование не применимо, если данные не передаются за пределы платформы Yandex Cloud. Если данные передаются за пределы платформы, то вы отвечаете за выполнение требований ГОСТ Р 58580 в части защиты информации при осуществлении физического доступа.

Подпроцесс «Идентификация и учёт ресурсов и объектов доступа»

Меры ГОСТ Р 57580: ИУ.1 – ИУ.8

Ответственность Yandex Cloud

Организация учёта и контроль состава ресурсов и объектов доступа.

Регистрация событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа.

Ответственность клиента

Организация учёта и контроль состава ресурсов и объектов доступа.

Регистрация событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа.

Процесс 2 «Обеспечение защиты вычислительных сетей»

Подпроцесс «Сегментация и межсетевое экранирование вычислительных сетей»

Меры ГОСТ Р 57580: СМЭ.1 – СМЭ.21

Ответственность Yandex Cloud

Сегментация и межсетевое экранирование внутренних вычислительных сетей.

Защита внутренних вычислительных сетей при взаимодействии с сетью Интернет.

Регистрация 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.

Ответственность клиента

Сегментация и межсетевое экранирование внутренних вычислительных сетей.

Защита внутренних вычислительных сетей при взаимодействии интернетом.

Регистрация событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей.

Архитектура проекта и конфигурация 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 группы безопасности.

Подпроцесс «Выявление вторжений и сетевых атак»

Меры ГОСТ Р 57580: ВСА.1 – ВСА.14

Ответственность Yandex Cloud

Мониторинг и контроль содержимого сетевого трафика.

Регистрация событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика

Ответственность клиента

Мониторинг и контроль содержимого сетевого трафика.

Регистрация событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика.

Использование методов и систем обнаружения или предотвращения вторжений

Подпроцесс «Защита информации, передаваемой по вычислительным сетям»

Меры ГОСТ Р 57580: ЗСВ.1 – ЗСВ.2

Ответственность Yandex Cloud

Выполнение мер по защите информации, передаваемой по недоверенным вычислительным сетям.

Ответственность клиента

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: ЗБС.1 – ЗБС.10

Ответственность Yandex Cloud

Защита информации от раскрытия и модификации при использовании беспроводных сетей.

Защита внутренних вычислительных сетей при использовании беспроводных сетей.

Регистрация событий защиты информации, связанных с использованием беспроводных сетей.

Мониторинг несанкционированных беспроводных сетей и точек доступа.

Ответственность клиента

Защита информации от раскрытия и модификации при использовании беспроводных сетей.

Защита внутренних вычислительных сетей при использовании беспроводных сетей.

Регистрация событий защиты информации, связанных с использованием беспроводных сетей.

Процесс 3 «Контроль целостности и защищенности инфраструктуры»

Меры ГОСТ Р 57580: ЦЗИ.1 – ЦЗИ.36

Ответственность Yandex Cloud

Контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации.

Организация и контроль размещения, хранения и обновления ПО информационной инфраструктуры.

Контроль состава и целостности ПО информационной инфраструктуры.

Регистрация событий защиты информации, связанных с результатами контроля целостности и защищённости информационной инфраструктуры.

Имплементация 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.

Ответственность клиента

Контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации.

Организация и контроль размещения, хранения и обновления ПО информационной инфраструктуры.

Контроль состава и целостности ПО информационной инфраструктуры.

Регистрация событий защиты информации, связанных с результатами контроля целостности и защищённости информационной инфраструктуры.

Имплементация и контроль настроек безопасности для компонентов, развёрнутых на платформе Yandex Cloud:

- операционных систем;
- баз данных (за исключением PaaS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database);
- прикладного ПО;
- других компонентов и сервисов, которые вы включили в область оценки.

Процесс 4 «Защита от вредоносного кода»

Меры ГОСТ Р 57580: ЗВК.1 – ЗВК.28

Ответственность Yandex Cloud

Организация эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры.

Организация и контроль применения средств защиты от вредоносного кода.

Регистрация событий защиты информации, связанных с реализацией защиты от вредоносного кода.

Ответственность клиента

Организация эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры.

Организация и контроль применения средств защиты от вредоносного кода.

Регистрация событий защиты информации, связанных с реализацией защиты от вредоносного кода.

Процесс 5 «Предотвращение утечек информации»

Меры ГОСТ Р 57580: ПУИ.1 – ПУИ.33

Ответственность Yandex Cloud

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.

Платформа Yandex Cloud для компонентов, обеспечивающих функционирование сервисов в области оценки, обеспечивает выполнение требований ГОСТ Р 57580 в части организации защиты машинных носителей информации (МНИ), содержащих ваши данные.

Ответственность клиента

Блокирование не разрешенных к использованию и контроль разрешённых к использованию потенциальных каналов утечки информации.

Контроль (анализ) информации, передаваемой по разрешённым к использованию потенциальным каналам утечки информации.

Организация защиты машинных носителей информации (МНИ), если такие используются для обработки информации при предоставлении финансовых услуг.

Регистрация событий защиты информации, связанных с реализацией предотвращения утечки информации.

Клиент может использовать сервис Yandex Key Management Service для защиты информации при хранении.

Процесс 6 «Управление инцидентами»

Подпроцесс «Мониторинг и анализ событий защиты информации»

Меры ГОСТ Р 57580: МАС.1 – МАС.23

Ответственность Yandex Cloud

Организация 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, защита и хранение данных регистрации о событиях защиты информации.

Анализ данных регистрации о событиях защиты информации.

Регистрация событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации.

Регистрация событий защиты информации для PaaS- сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database.

Ответственность клиента

Организация 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, защита и хранение данных регистрации о событиях защиты информации.

Анализ данных регистрации событий защиты информации.

Регистрация 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:

- операционных систем;
- баз данных (за исключением PaaS-сервисов: Yandex Managed Service for Kubernetes®, PostgreSQL, ClickHouse, MongoDB, MySQL®, Redis™, Apache Kafka®, Elasticsearch, Yandex Data Proc, Yandex Database);
- прикладного ПО;
- других компонентов и сервисов, которые вы включили в область оценки.

Вы отвечаете и за выполнение требований PCI DSS в части синхронизации времени для компонентов, развёрнутых на платформе Yandex Cloud (см. рекомендации по настройке синхронизации времени с использованием NTP).

Подпроцесс «Обнаружение инцидентов защиты информации и реагирование на них»

Меры ГОСТ Р 57580: РИ.1 – РИ.19

Ответственность Yandex Cloud

Обнаружение и регистрация инцидентов защиты информации.

Организация реагирования на инциденты защиты информации.

Организация хранения и защита информации об инцидентах защиты информации.

Регистрация событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них.

Ответственность клиента

Обнаружение и регистрация инцидентов защиты информации.

Организация реагирования на инциденты защиты информации.

Организация хранения и защита информации об инцидентах защиты информации.

Регистрация событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них

Процесс 7 «Защита среды виртуализации»

Меры ГОСТ Р 57580: ЗСВ.1 – ЗСВ.43

Ответственность Yandex Cloud

Организация идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации.

Организация и контроль информационного взаимодействия и изоляции виртуальных машин.

Организация защиты образов виртуальных машин.

Регистрация событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации.

Ответственность клиента

Организация идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к сервисам и виртуальным машинам.

Организация и контроль информационного взаимодействия и изоляции виртуальных машин.

Организация защиты образов виртуальных машин.

Регистрация событий защиты информации, связанных с доступом к виртуальным машинам

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

Меры ГОСТ Р 57580: ЗУД.1 – ЗУД.12

Ответственность Yandex Cloud

Защита информации от раскрытия и модификации при осуществлении удалённого доступа.

Защита внутренних вычислительных сетей при осуществлении удалённого доступа.

Защита информации от раскрытия и модификации при её обработке и хранении на мобильных (переносных) устройствах.

Ответственность клиента

Защита информации от раскрытия и модификации при осуществлении удалённого доступа.

Защита внутренних вычислительных сетей при осуществлении удалённого доступа.

Защита информации от раскрытия и модификации при её обработке и хранении на мобильных (переносных) устройствах.

Организация и управление защитой информации

Направление 1 «Планирование процесса системы защиты информации»

Меры ГОСТ Р 57580: ПЗИ.1 – ПЗИ.5

Ответственность Yandex Cloud

Области применения процесса системы защиты информации.

Состав применяемых и не применяемых мер защиты информации из числа мер, определённых в разделах 7, 8 и 9 ГОСТ Р 57580.

Состав и содержание мер защиты информации, являющихся дополнительными к базовому составу мер, определённых 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.

Порядок применения мер защиты информации в рамках процесса системы защиты информации.

Ответственность клиента

Области применения процесса системы защиты информации.

Состав применяемых и не применяемых мер защиты информации из числа мер, определенных в разделах 7, 8 и 9 ГОСТ Р 57580.

Состав и содержание мер защиты информации, являющихся дополнительными к базовому составу мер, определённых 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.

Порядок применения мер защиты информации в рамках процесса системы защиты информации.

Направление 2 «Реализация процесса системы защиты информации»

Меры ГОСТ Р 57580: РЗИ.1 – РЗИ.16

Ответственность Yandex Cloud

Должное применение мер защиты информации.

Определение ролей защиты информации, связанных с применением мер защиты информации.

Назначение лиц, ответственных за выполнение ролей защиты информации.

Доступность реализации технических мер защиты информации.

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, определённых в модели угроз и нарушителей безопасности информации финансовой организации.

Обучение, практическая подготовка (переподготовка) работников финансовой организации, ответственных за применение мер защиты информации.

Повышение осведомленности (инструктаж) работников финансовой организации в области защиты информации.

Ответственность клиента

Должное применение мер защиты информации.

Определение ролей защиты информации, связанных с применением мер защиты информации.

Назначение лиц, ответственных за выполнение ролей защиты информации.

Доступность реализации технических мер защиты информации.

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, определённых в модели угроз и нарушителей безопасности информации финансовой организации.

Обучение, практическая подготовка (переподготовка) работников финансовой организации, ответственных за применение мер защиты информации.

Повышение осведомленности (инструктаж) работников финансовой организации в области защиты информации.

Направление 3 «Контроль процесса системы защиты информации»

Меры ГОСТ Р 57580: КЗИ.1 – КЗИ.12

Ответственность Yandex Cloud

Области применения процесса системы защиты информации.

Должное применение мер защиты информации в рамках процесса системы защиты информации.

Знания работников финансовой организации в части применения мер защиты информации.

Ответственность клиента

Области применения процесса системы защиты информации.

Должное применение мер защиты информации в рамках процесса системы защиты информации.

Знания работников финансовой организации в части применения мер защиты информации.

Направление 4 «Совершенствование процесса системы защиты информации»

Меры ГОСТ Р 57580: СЗИ.1 – СЗИ.4

Ответственность Yandex Cloud

Деятельность по совершенствованию процессов защиты информации.

Ответственность клиента

Деятельность по совершенствованию процессов защиты информации.

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

Меры ГОСТ Р 57580: ЖЦ.1 – ЖЦ.28

Ответственность Yandex Cloud

Защита информации от раскрытия и модификации при осуществлении удалённого доступа.

Защита внутренних вычислительных сетей при осуществлении удалённого доступа.

Защита информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах.

Ответственность клиента

Защита информации от раскрытия и модификации при осуществлении удалённого доступа.

Защита внутренних вычислительных сетей при осуществлении удалённого доступа.

Защита информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах.

Вы отвечаете и за проведение контроля защищенности. Анализ уязвимости и тесты на проникновение должны выполняться согласно документу «Правила проведения внешних сканирований безопасности».

Пояснения по интерпретации требований для различных уровней защиты

В случае необходимости интерпретации применимости требований и проекции усиленного уровня защиты информации на стандартный и минимальный уровни защиты следует руководствоваться информацией из таблицы, представленной по тексту ниже.

Мера: УЗП.14

Содержание мер системы защиты информации

Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 90 дней

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Организационная	Техническая	Неприменимо

Мера: УЗП.15

Содержание мер системы защиты информации

Установление фактов неиспользования субъектами логического доступа предоставленных им прав на осуществление логического доступа на протяжении периода времени, превышающего 45 дней

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Организационная	Техническая	Неприменимо

Пояснение о покрытии мер

Выполнение меры УЗП.14 покрывается выполнением меры УЗП.15, так как УЗП.15 требует установления факта неиспользования субъектами логического доступа предоставленных им прав за меньший период времени (45 дней вместо 90 дней)

Мера: РД.1

Содержание мер системы защиты информации

Идентификация и однофакторная аутентификация пользователей

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Техническая	Техническая	Неприменимо

Мера: РД.2

Содержание мер системы защиты информации

Идентификация и многофакторная аутентификация пользователей

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Пояснение о покрытии мер

Выполнение меры РД.1 покрывается выполнением меры РД.2, так как РД.2 требует использования в качестве метода аутентификации нескольких факторов аутентификации, что включает в себя использование одного фактора

Мера: РД.3

Содержание мер системы защиты информации

Идентификация и однофакторная аутентификация эксплуатационного персонала

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Техническая	Неприменимо	Неприменимо

Мера: РД.4

Содержание мер системы защиты информации

Идентификация и многофакторная аутентификация эксплуатационного персонала

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Техническая

Пояснение о покрытии мер

Выполнение меры РД.3 покрывается выполнением меры РД.4, так как РД.4 требует использования в качестве метода аутентификации нескольких факторов аутентификации, что включает в себя использование одного фактора

Мера: ФД.15

Содержание мер системы защиты информации

Хранение архивов информации средств видеонаблюдения не менее 14 дней

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Неприменимо

Мера: ФД.16

Содержание мер системы защиты информации

Хранение архивов информации средств видеонаблюдения не менее 90 дней

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Пояснение о покрытии мер

Выполнение меры ФД.15 покрывается выполнением меры ФД.16, так как ФД.16 требует хранения информации средств видеонаблюдения более длительный срок (90 дней вместо 14 дней)

Мера: СМЭ.14

Содержание мер системы защиты информации

Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сети Интернет

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Техническая

Мера: СМЭ.15

Содержание мер системы защиты информации

Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сети Интернет

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Техническая	Неприменимо	Неприменимо

Пояснение о покрытии мер

Выполнение меры СМЭ.15 покрывается выполнением меры СМЭ.14, так как СМЭ.15 требует реализации сетевого взаимодействия и сетевой изоляции на более низком уровне (минимум второй уровень вместо третьего)

Мера: ЗБС.4

Содержание мер системы защиты информации

Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше второго (канальный) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с пунктом ЗБС.3 настоящей таблицы

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Мера: ЗБС.5

Содержание мер системы защиты информации

Реализация сетевого взаимодействия и сетевой изоляции на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1, внутренних вычислительных сетей финансовой организации и сегментов вычисленных сетей, выделенных в соответствии с мерой ЗБС.3 настоящей таблицы

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Неприменимо

Пояснение о покрытии мер

Выполнение меры ЗБС.5 покрывается выполнением меры ЗБС.4, так как ЗБС.4 требует реализации сетевого взаимодействия и сетевой изоляции на более низком уровне (минимум второй уровень вместо третьего)

Мера: ЗВК.13

Содержание мер системы защиты информации

Использование средств защиты от вредоносного кода различных производителей, как минимум для уровней:

- физические АРМ пользователей и эксплуатационного персонала;
- серверное оборудование.

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Техническая	Неприменимо	Неприменимо

Мера: ЗВК.13

Содержание мер системы защиты информации

Использование средств защиты от вредоносного кода различных производителей, как минимум для уровней:

- физические АРМ пользователей и эксплуатационного персонала;
- серверное оборудование;
- контроль межсетевого трафика.

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Техническая

Пояснение о покрытии мер

Выполнение меры ЗВК.13 покрывается выполнением меры ЗВК.14, так как ЗВК.14 требует использования различных производителей средств защиты от вредоносного кода на трех уровнях, вместо двух (добавляется уровень контроля межсетевого трафика)

Мера: ПУИ.6

Содержание мер системы защиты информации

Ведение единого архива электронных сообщений с архивным доступом на срок не менее 6 мес. и оперативным доступом на срок не менее 1 мес.

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Неприменимо

Мера: ПУИ.7

Содержание мер системы защиты информации

Ведение единого архива электронных сообщений с архивным доступом на срок не менее 6 мес. и оперативным доступом на срок не менее 3 мес.

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Пояснение о покрытии мер

Выполнение меры ПУИ.6 покрывается выполнением меры ПУИ.7, так как ПУИ.7 требует более длительный минимальный срок оперативного и архивного доступа к электронным сообщениям (архивный доступ – один год вместо 6 месяцев, оперативный доступ – 3 месяца вместо 1 месяца)

Мера: ПУИ.23

Содержание мер системы защиты информации

Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при осуществлении вывода МНИ из эксплуатации или вывода из эксплуатации СВТ, в состав которых входят указанные МНИ, а также при необходимости их передачи в сторонние организации.

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Техническая	Неприменимо	Неприменимо

Мера: ПУИ.24

Содержание мер системы защиты информации

Стирание информации конфиденциального характера с МНИ средствами гарантированного стирания или способом (средством), обеспечивающим невозможность их восстановления, при осуществлении вывода МНИ из эксплуатации или вывода из эксплуатации СВТ, в состав которых входят указанные МНИ, а также при необходимости их передачи в сторонние организации.

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Техническая

Пояснение о покрытии мер

Выполнение меры ПУИ.23 покрывается выполнением меры ПУИ.24, так как ПУИ.24 требует использования средств гарантированного стирания информации, которые обеспечивают невозможность восстановления данных в отличие от перезаписи данных

Мера: ПУИ.25

Содержание мер системы защиты информации

Стирание информации конфиденциального характера с МНИ средствами, обеспечивающими полную перезапись данных, при передаче (перезакреплении) МНИ между работниками и (или) структурными подразделениями финансовой организации

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Техническая	Неприменимо	Неприменимо

Мера: ПУИ.26

Содержание мер системы защиты информации

Стирание информации конфиденциального характера с МНИ средствами гарантированного стирания или способом (средством), обеспечивающим невозможность их восстановления, при передаче (перезакреплении) МНИ между работниками и (или) структурными подразделениями финансовой организации

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Техническая

Пояснение о покрытии мер

Выполнение меры ПУИ.25 покрывается выполнением меры ПУИ.26, так как ПУИ.26 требует использования средств гарантированного стирания информации, которые обеспечивают невозможность восстановления данных в отличие от перезаписи данных

Мера: МАС.15

Содержание мер системы защиты информации

Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение трех лет

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Техническая	Техническая	Неприменимо

Мера: МАС.16

Содержание мер системы защиты информации

Обеспечение возможности доступа к данным регистрации о событиях защиты информации в течение пяти лет

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Пояснение о покрытии мер

Выполнение меры МАС.15 покрывается выполнением меры МАС.16, так как МАС.16 требует хранения данных регистрации о событиях защиты информации более длительный срок (пять лет вместо трех лет)

Мера: РИ.7

Содержание мер системы защиты информации

Определение и назначение ролей, связанных с реагированием на инциденты защиты информации

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Организационная	Неприменимо	Неприменимо

Мера: РИ.8

Содержание мер системы защиты информации

Определение и назначение ролей, связанных с реагированием на инциденты защиты информации - ролей группы реагирования на инциденты защиты информации (ГРИЗИ)

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Организационная	Организационная

Мера: РИ.9

Содержание мер системы защиты информации

Выделение в составе ГРИЗИ следующих основных ролей:

- руководитель ГРИЗИ, в основные функциональные обязанности которого входит обеспечение оперативного руководства реагированием на инциденты защиты информации;
- оператор-диспетчер ГРИЗИ, в основные функциональные обязанности которого входит обеспечение сбора и регистрации информации об инцидентах защиты информации;
- аналитик ГРИЗИ, в основные функциональные обязанности которого входит выполнение непосредственных действий по реагированию на инцидент защиты информации;
- секретарь ГРИЗИ, в основные функциональные обязанности которого входит документирование результатов реагирования на инциденты защиты информации, формирование аналитических отчетов материалов

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Организационная	Организационная

Пояснение о покрытии мер

Выполнение меры РИ.7 покрывается выполнением меры РИ.8 или РИ.9, в свою очередь РИ.8 покрывается выполнением меры РИ.9, так как:

- РИ.7 требует назначить роли, связанные с реагированием на инциденты защиты информации;
- РИ.8 требует создать группу реагирования на инциденты защиты информации (ГРИЗИ), в том числе назначить роли, связанные с реагированием на инциденты защиты информации (РИ.7);
- РИ.9 требует создать группу реагирования на инциденты защиты информации (ГРИЗИ) (что требуется мерой защиты РИ.8), в том числе уточняет роли, связанные с реагированием на инциденты защиты информации (РИ.7)

Мера: РИ.17

Содержание мер системы защиты информации

Обеспечение возможности доступа к информации об инцидентах защиты информации в течение трех лет

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Техническая	Техническая	Неприменимо

Мера: РИ.18

Содержание мер системы защиты информации

Обеспечение возможности доступа к информации об инцидентах защиты информации в течение пяти лет

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Пояснение о покрытии мер

Выполнение меры РИ.17 покрывается выполнением меры РИ.18, так как РИ.18 требует хранения информации об инцидентах защиты информации более длительный срок (пять лет вместо трех лет)

Мера: ЗСВ.1

Содержание мер системы защиты информации

Разграничение и контроль осуществления одновременного доступа к виртуальным машинам с АРМ пользователей и эксплуатационного персонала только в пределах одного контура безопасности

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Неприменимо

Мера: ЗСВ.2

Содержание мер системы защиты информации

Разграничение и контроль осуществления одновременного доступа к виртуальным машинам с АРМ пользователей и эксплуатационного персонала только в пределах одного контура безопасности на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Пояснение о покрытии мер

Выполнение меры ЗСВ.1 покрывается выполнением меры ЗСВ.2, так как ЗСВ.2 добавляет к уже описанной в мере защиты ЗСВ.1 реализации уточнение в виде контроля осуществления одновременного доступа к виртуальным машинам с АРМ пользователей и эксплуатационного персонала на третьем или ниже уровнях семиуровневой стандартной модели взаимодействия открытых систем

Мера: ЗСВ.3

Содержание мер системы защиты информации

Разграничение и контроль осуществления одновременного доступа виртуальных машин к системе хранения данных в пределах контура безопасности

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Неприменимо

Мера: ЗСВ.4

Содержание мер системы защиты информации

Разграничение и контроль осуществления одновременного доступа виртуальных машин к системе хранения данных в пределах контура безопасности на уровне не выше третьего (сетевой) по семиуровневой стандартной модели взаимодействия открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Пояснение о покрытии мер

Выполнение меры ЗСВ.3 покрывается выполнением меры ЗСВ.4, так как ЗСВ.4 добавляет к уже описанной в мере защиты ЗСВ.3 реализации уточнение в виде контроля осуществления одновременного доступа виртуальных машин к системе хранения данных на третьем или ниже уровнях семиуровневой стандартной модели взаимодействия открытых систем

Мера: ЗСВ.6

Содержание мер системы защиты информации

Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Неприменимо

Мера: ЗСВ.7

Содержание мер системы защиты информации

Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине с одного АРМ пользователя или эксплуатационного персонала

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Пояснение о покрытии мер

Выполнение меры ЗСВ.6 покрывается выполнением меры ЗСВ.7, так как ЗСВ.7 добавляет к уже описанной в мере защиты ЗСВ.6 реализации уточнение в виде ограничения подключения лишь с одного АРМ пользователя или эксплуатационного персонала

Мера: ЗСВ.30

Содержание мер системы защиты информации

Контроль завершения сеанса работы пользователей с виртуальными машинами

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Неприменимо

Мера: ЗСВ.31

Содержание мер системы защиты информации

Контроль завершения сеанса работы пользователей с виртуальными машинами и обеспечение последующей работы виртуальной машины с использованием базового образа

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Пояснение о покрытии мер

Выполнение меры ЗСВ.30 покрывается выполнением меры ЗСВ.31, так как ЗСВ.31 добавляет к уже описанной в мере защиты ЗСВ.30 реализации уточнение в виде последующей после завершения сеанса работы виртуальной машины с использованием базового образа

Мера: РЗИ.11

Содержание мер системы защиты информации

Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 4 класса

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Неприменимо	Техническая

Мера: РЗИ.12

Содержание мер системы защиты информации

Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 5 класса

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Неприменимо	Техническая	Неприменимо

Мера: ЗРИ.13

Содержание мер системы защиты информации

Применение сертифицированных по требованиям безопасности информации средств защиты информации не ниже 6 класса

Уровень защиты информации

Минимальный (3)	Стандартный (2)	Усиленный (1)
Техническая	Неприменимо	Неприменимо

Пояснение о покрытии мер

Выполнение меры РЗИ.13 покрывается выполнением меры РЗИ.11 или РЗИ.12, в свою очередь РЗИ.12 покрывается выполнением меры РЗИ.11, так как:

- требования к средствам защиты информации 4 класса выше, чем требования к средствам защиты информации 5 или 6 класса;
- требования к средствам защиты информации 5 класса выше, чем требования к средствам защиты информации 6 класса