Приказ Минцифры России от 04.06.2026 N 508 "Об утверждении Методических рекомендаций по обеспечению соблюдения требований к информационно-телекоммуникационной инфраструктуре, в том числе облачной, для размещения информационных систем органов исполнительной власти и органов местного самоуправления"

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 4 июня 2026 г. N 508

ОБ УТВЕРЖДЕНИИ МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ПО ОБЕСПЕЧЕНИЮ СОБЛЮДЕНИЯ ТРЕБОВАНИЙ К ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЕ, В ТОМ ЧИСЛЕ ОБЛАЧНОЙ, ДЛЯ РАЗМЕЩЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ И ОРГАНОВ МЕСТНОГО САМОУПРАВЛЕНИЯ

В целях определения единого подхода органов исполнительной власти Российской Федерации и органов местного самоуправления к созданию и управлению защищенной информационно-телекоммуникационной инфраструктурой для размещения информационных систем органов исполнительной власти и органов местного самоуправления для обеспечения достижения национальной цели "Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы", установленной Указом Президента Российской Федерации от 7 мая 2024 г. N 309, приказываю:

1. Утвердить прилагаемые Методические рекомендации по обеспечению соблюдения требований к информационно-телекоммуникационной инфраструктуре, в том числе облачной, для размещения информационных систем органов исполнительной власти и органов местного самоуправления (далее - Методические рекомендации).

2. Департаменту развития облачных сервисов (Бурлаков П.И.) обеспечить направление Методических рекомендаций в высшие исполнительные органы субъектов Российской Федерации.

Министр
М.И.ШАДАЕВ

Утверждены
приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 04.06.2026 N 508

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ СОБЛЮДЕНИЯ ТРЕБОВАНИЙ К ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЕ В ТОМ ЧИСЛЕ ОБЛАЧНОЙ, ДЛЯ РАЗМЕЩЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНОВ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ И ОРГАНОВ МЕСТНОГО САМОУПРАВЛЕНИЯ

I. Общие положения

1. Настоящие Методические рекомендации разработаны с целью обеспечения потребности органов исполнительной власти и органов местного самоуправления (далее - потребители) в защищенной инфраструктуре с учетом требований по использованию импортозамещенного аппаратного и программного обеспечения в целях унификации подхода к ее созданию и управлению.

2. Для целей настоящих Методических рекомендаций применяются следующие понятия:

инфраструктура - информационно-телекоммуникационная инфраструктура, представляющая собой совокупность вычислительных, телекоммуникационных, программных и иных средств, предназначенных для обеспечения размещения и функционирования информационных систем и ресурсов;

аппаратные ресурсы - составная часть информационно-телекоммуникационной инфраструктуры, представляющая собой физическое оборудование и устройства;

контур - логически и/или физически изолированная (выделенная) часть инфраструктуры, предназначенная для размещения и эксплуатации целевых информационных систем и ресурсов и/или служебных ресурсов (систем, данных, сервисов), обеспечивающих работу целевых информационных систем (например, средства управления, мониторинга, безопасности, резервного копирования), с заданными границами доступа, сетевой связностью и правилами администрирования;

кластер - группа узлов, совместно выполняющих единую функцию, в которой каждый узел является аппаратным и/или программным модулем, входящим в общую группу устройств с единым управлением и участвующим в хранении/обработке информации;

синтетическая полная копия - полная резервная копия, формируемая на стороне системы резервного копирования из уже имеющихся копий: последней полной и последующих инкрементальных (дифференциальных), без повторного считывания всех данных с исходной системы;

утилизация - фактически используемая информационной системой (информационным ресурсом) доля доступной производительности (реальной или виртуальной емкости оборудования) инфраструктуры в общем объеме предоставляемых (приобретенных) ресурсов инфраструктуры.

II. Общие рекомендации к инфраструктуре

3. Потребитель обеспечивает функционирование инфраструктуры в непрерывном круглосуточном режиме для надежного функционирования размещенных на ней информационных систем. Все виды сервисного, технического и иных видов обслуживания потребитель производит без остановки систем и снижения основных технологических параметров.

4. Потребитель обеспечивает наличие необходимых телекоммуникационных ресурсов в инфраструктуре для организации каналов связи с публичными и закрытыми сетями, которые могут быть использованы для соединения размещаемых информационных систем с внешними системами по отношению к инфраструктуре. Также для размещения критичных информационных систем следует предусмотреть возможность подключения каналов связи минимум от двух различных операторов связи.

5. Инфраструктура для размещения информационных систем и ресурсов создается на выделенных ресурсах, используемых только для обеспечения деятельности органов исполнительной власти и органов местного самоуправления. В целях исключения рисков по возможному получению несанкционированного доступа, вмешательства или влияния не допускается использование общих ресурсов с иными заказчиками инфраструктуры, не являющимися органами исполнительной власти Российской Федерации или органами местного самоуправления.

6. Потребитель реализует инфраструктуру в соответствующих объеме и структуре, определяемых с учетом требований планируемых к размещению на ней информационных систем. Для минимизации рисков недостаточного использования выделенных ресурсов и недопущения перегрузки и деградации функционирования размещенных на инфраструктуре информационных систем рекомендуется организовать мониторинг утилизации инфраструктуры.

III. Рекомендации к составу и организации инфраструктуры

7. Инфраструктура может быть реализована в виде:

а) набора аппаратных ресурсов, предусматривающего развертывание информационных систем на

физической аппаратной базе (серверы, системы хранения, сетевое оборудование) без виртуализации;

б) виртуализированного представления аппаратных ресурсов с использованием платформы виртуализации путем создания и управления виртуальными машинами (комплекс виртуальных вычислительных ресурсов, ресурсов хранения данных и прочих сопутствующих ресурсов);

в) гибридной инфраструктуры, сочетающей набор физических и виртуализированных сервисов с распределением нагрузок между ними в зависимости от требований по безопасности, доступности и производительности.

8. Для создания инфраструктуры используется оборудование, включенное в единый реестр российской радиоэлектронной продукции, созданный в соответствии с постановлением Правительства Российской Федерации от 10 июля 2019 г. N 878.

9. Для аппаратных ресурсов рекомендовано обеспечить:

а) соответствие требуемой производительности, определяемой технической архитектурой и нагрузочными характеристиками размещаемых информационных систем;

б) соответствие принципам необходимой избыточности, отказоустойчивости и отсутствия одиночных точек отказа по критичным компонентам (контроллеры, блоки питания, сетевые интерфейсы, дисковые группы/носители, управляющие и коммутирующие компоненты);

в) необходимую степень резервирования и отказоустойчивости, для достижения требуемого уровня доступности;

г) горизонтальное масштабирование (наращивание вычислительных ресурсов и емкости без переработки архитектуры инфраструктуры);

д) поддержку развертывания и эксплуатации платформ виртуализации;

е) совместимость с архитектурой x86, а при необходимости - с E2K (Эльбрус), включая поддержку требуемых отечественных операционных систем и драйверов.

10. Архитектурными решениями при создании инфраструктуры не рекомендуется ограничивать выбор и использование:

а) платформ виртуализации;

б) операционных систем;

в) систем резервного копирования и восстановления;

г) средств мониторинга и сбора метрик утилизации ресурсов;

д) средств защиты информации (при условии, что соответствующие продукты разрешены/допущены к применению регуляторами и соответствуют установленным требованиям).

11. Телекоммуникационная инфраструктура сети передачи данных обеспечивает внутреннюю связность всех инженерных и ИТ-контуров (включая контуры управления/мониторинга), а также внешнюю связность с публичными и/или закрытыми сетями/узлами, доступ к которым необходим для функционирования размещаемых информационных систем.

12. Потребитель обеспечивает отказоустойчивость телекоммуникационной инфраструктуры за счет проектирования и реализации:

а) линейно-кабельных сооружений и кабельных трасс, обеспечивающих размещение коммутационного и каналообразующего оборудования в резервированной конфигурации;

б) прокладки линий связи в объеме, достаточном для расчетной нагрузки, с технологическим запасом и резервированием;

в) подключения оборудования к коммутационной инфраструктуре в отказоустойчивой конфигурации (исключение одиночных точек отказа на уровне подключения).

13. При размещении телекоммуникационного оборудования в помещениях, не предназначенных для основного ИТ-оборудования, такие помещения оборудуются в соответствии с требованиями, установленными для серверных помещений (по инженерным системам, доступу, безопасности и эксплуатации) в части, относящейся к размещаемому оборудованию.

14. Проектные параметры сети, в том числе ее характеристики, топология, емкость коммутационного и каналообразующего оборудования, а также пропускная способность линий/каналов связи определяются на основании:

а) расчетного профиля трафика между узлами размещаемых систем и их внутренними/внешними пользователями;

б) требований к задержкам/потерям/доступности (при наличии);

в) технологического запаса, достаточного для планируемого роста и пиковых нагрузок.

15. Рекомендуется обеспечить физическую независимость кабельных трасс для достижения целевого уровня отказоустойчивости. Все критичные линии/каналы связи (магистральные и/или обеспечивающие подключение к внешним сетям, а также внутренние магистрали между ключевыми узлами) следует организовать по двум независимым кабельным трассам, проходящим по непересекающимся маршрутам и исключающим общие точки отказа (в том числе общие кабельные сооружения/шахты/короба/вводы в здании - по возможности).

16. Инфраструктура хранения данных может быть реализована в виде:

а) аппаратной системы хранения данных, предусматривающей выполнение развертывания и эксплуатации на физической базе (контроллеры/полки дисков, SAN/NAS-оборудование), в которой функции хранения реализованы преимущественно на уровне специализированных аппаратных ресурсов и встроенного программного обеспечения;

б) программно-определяемой системы хранения, предусматривающей предоставление ресурсов хранения в виде виртуализированного/абстрагированного представления, формируемого программной платформой (кластер на стандартных x86-серверах с дисками), которая объединяет дисковые ресурсы в единый пул и обеспечивает создание/управление томами, политиками отказоустойчивости, производительности и распределения данных на уровне программно-определяемого слоя, как основного способа управления;

в) гибридной инфраструктуры хранения, предусматривающей сочетание аппаратных ресурсов и программно-определяемого хранения с распределением данных и нагрузок между ними в зависимости от требований к безопасности, доступности, производительности, стоимости и особенностей приложений (критичные (низколатентные) нагрузки могут располагаться на аппаратной системе хранения данных, масштабируемые/универсальные/системные - в программно-определяемой системе хранения данных).

17. Сеть хранения/передачи данных рекомендуется изолировать, логически и/или физически отделить от иных сетей передачи данных (пользовательских, серверных, управления, мониторинга), с контролируемыми точками межсетевого взаимодействия.

18. Потребитель обеспечивает двукратный запас пропускной способности сети хранения/передачи данных: суммарная пропускная способность обеспечивает работу при отказе одного из элементов/путей (режимы 1+1 и N+1), сохраняя требуемую производительность при потере одного коммутатора, линка, контроллера, пути доступа (эквивалент "удвоенного" ресурса относительно расчетной нагрузки).

19. Потребитель обеспечивает резервирование связности в кластере хранения данных сети хранения/передачи данных:

а) для каждого узла распределенного кластера хранения данных рекомендуется обеспечить наличие не менее двух независимых путей подключения;

б) горизонтальные связи (межузловой обмен/репликация) выполняются с резервированием и исключением общих точек отказа по маршруту.

20. Сеть хранения/передачи данных обеспечивает масштабирование и аварийное включение резерва:

а) наличие технологического запаса по портам (пропускной способности, адресному пространству, ресурсам, узлам);

б) возможность подключения и ввода в работу резервного оборудования без остановки сервисов (при целевом круглосуточном режиме).

21. В составе инфраструктуры рекомендуется предусмотреть и ввести в эксплуатацию систему резервного копирования, обеспечивающую отказоустойчивое, защищенное создание, хранение и восстановление резервных копий данных и конфигураций.

22. Система резервного копирования включает в себя:

а) хранилище резервных копий с отказоустойчивой конфигурацией и мерами защиты информации;

б) сервер(а) управления и выполнения задач резервного копирования (восстановления);

в) программное обеспечение системы резервного копирования для централизованного управления, разграничения доступа и учета операций.

23. Серверы управления системой резервного копирования допускается реализовывать как виртуальные, так и физические при соблюдении требований по доступности и производительности.

24. Для каждого потребителя данных и информационных систем выделяется отдельное оборудование (логически или физически) и обеспечиваются:

а) выделенные серверы управления системой резервного копирования (отдельная установка в контуре управления);

б) выделенные дисковые группы (репозитории) для хранения резервных копий, исключающие смешивание данных и несанкционированный доступ между различными владельцами данных и информационных систем.

25. В рамках создаваемой системой резервного копирования рекомендуется создавать резервные копии в объеме, достаточном для восстановления значимых функций и данных размещаемых информационных систем, включая, но не ограничиваясь:

а) полным и/или инкрементным образом виртуальных машин;

б) конфигурацией систем, инфраструктурных сервисов и средств защиты информации;

в) данными приложений и баз данных.

26. Система резервного копирования обеспечивает восстановление в сроки, установленные во внутренних стандартах и регламентах владельцев данных и информационных систем (по защите информации и/или обеспечению непрерывности).

27. Система резервного копирования обеспечивает передачу данных для резервного копирования со

скоростью не ниже доступной суммарной пропускной способности используемой сети резервного копирования (с учетом выделенных лимитов/политик), без создания неприемлемой деградации сервисов.

28. Система резервного копирования обеспечивает выполнение обязательных функций:

а) агентский и/или безагентский режимы резервного копирования (в том числе полное сохранение вычислительных машин и/или произвольных данных);

б) резервное копирование баз данных приложений с обеспечением целостной копии данных, пригодной для надежного восстановления, используя функционал сервера базы данных с фиксацией консистентности состояния данных;

в) автоматическое/автоматизированное создание резервных копий всех предусмотренных типов (полные/инкрементальные/дифференциальные);

г) поддержка синтетических полных резервных копий;

д) возобновление передачи при обрыве связи с продолжением с точки прерывания и оптимизацию сетевого взаимодействия;

е) ведение каталога резервных копий (инвентаризация, поиск, сопоставление с объектами, версионность);

ж) управление жизненным циклом резервных копий (политики хранения (удаления), дедупликация (сжатие) - при наличии, контроль заполнения, защита от удаления).

29. Инфраструктуру рекомендуется оснастить централизованной системой мониторинга, обеспечивающей непрерывный сбор, хранение, отображение, передачу и анализ показателей состояния и загрузки компонентов инфраструктуры.

30. Система мониторинга обеспечивает настраиваемый сбор и обработку метрик, включая:

а) состояние сервисов и узлов, входящих в состав системы (доступность, ошибки, деградации);

б) аварийные события и предупреждения (фиксация, классификация, уведомления);

в) пороговые значения (настройка порогов, предиктивные/ранние предупреждения, эскалации);

г) передачу требуемых типов метрик в регламентированной форме во внешнюю (пользовательскую) систему(ы) мониторинга;

д) утилизацию вычислительных ресурсов;

е) утилизацию систем хранения (занятое/свободное дисковое пространство, IOPS/задержки, состояние устройств/пулов/томов).

31. Система мониторинга обеспечивает просмотр графиков/панелей по выбранным метрикам и периодам, формирование сводных отчетов по настроенным метрикам (по объектам, группам объектов, потребителям/контурам), выгрузку данных для отчетности и аналитики (в форматах, поддерживаемых системой).

32. Система мониторинга обеспечивает хранение всех типов собираемых метрик и связанных событий (в необходимом для их использования объеме) не менее установленного срока, иметь возможность поиска, агрегирования и анализа метрик за весь срок хранения для целей расследования инцидентов, планирования емкости и подготовки отчетности.

33. Потребитель обеспечивает целостность и сохранность данных мониторинга, предусматривая:

а) синхронизацию времени источников метрик (корректная временная шкала);

б) контролируемый доступ к настройкам и данным мониторинга (разграничение прав);

в) сохранность данных мониторинга при отказах (резервирование/резервное копирование по принятой архитектуре).

34. При создании инфраструктуры из общего пула ресурсов, предназначенных для размещения информационных систем, рекомендуется выделять и изолировать друг от друга:

а) контуры размещения информационных систем потребителей;

б) контуры управления инфраструктурой (управление вычислением/хранением/сетью/виртуализацией/оркестрацией);

в) контуры средств защиты информации (журналирование, мониторинг ИБ, управление доступом, реагирование и т.п.).

35. Контуры обработки и хранения пользовательских данных (в том числе персональных данных) следует изолировать от остальных контуров инфраструктуры. Вместе с тем допускается совмещение контуров управления инфраструктурой и средств защиты информации для целей оптимизации ресурсов при создании малых объемов инфраструктуры.

36. Сегментирование исключает несанкционированные взаимодействия между контурами и обеспечивает контролируемые точки доступа между ними (по утвержденным правилам).

37. Для каждого контура инфраструктуры потребитель реализует выделенную подсистему мониторинга, обеспечивающую независимый контроль функционирования аппаратных средств инфраструктуры, ключевых систем и программного обеспечения, обеспечивающих функционирование инфраструктуры и размещение информационных систем, каналов связи и сетевых сервисов, в том числе обеспечивающих информационную безопасность, участвующих в предоставлении инфраструктурных услуг размещения информационных систем.

38. Инфраструктура обеспечивает достаточный объем аппаратных и программных ресурсов для размещения целевых информационных систем и работы служебных контуров без деградации установленных показателей доступности и производительности, с учетом технологического запаса.

IV. Рекомендации к условиям и параметрам функционирования инфраструктуры

39. Варианты размещения инфраструктуры определяются с учетом требований по обеспечению информационной безопасности, надежности и производительности информационных систем, для размещения которых создается инфраструктура.

40. Машинные залы центра обработки данных являются наиболее универсальным вариантом размещения государственных информационных систем и иных информационных систем государственных органов, позволяющим учесть наиболее высокие требования по обеспечению информационной безопасности, надежности и производительности инфраструктуры.

41. Помещения центра обработки данных для размещения инфраструктуры организуются в соответствии с требованиями свода правил СП 541.1325800.2024, которые распространяются на проектирование зданий и сооружений центров обработки данных, а также помещений центров обработки данных в составе зданий.

42. Размещение инфраструктуры в машинных залах центра обработки данных рекомендуется использовать для любых и в том числе значимых и критичных для ведомств информационных систем.

43. Для размещения информационных систем, которые не являются значимыми и/или критичными для функционирования ведомств и для которых не установлены требования по обеспечению доступности на уровне отношения суммарного времени простоя за год к длительности года не ниже 99,5%, допустимо

использовать серверные помещения в зданиях размещения потребителя или оператора инфраструктуры. В этом случае потребитель инфраструктуры самостоятельно определяет требуемые условия, достаточные для обеспечения требуемого режима и надежности функционирования размещаемых информационных систем. Вместе с тем для серверных помещений рекомендуется учитывать требования свода правил СП 541.1325800.2024 в части разделов 6.2 "Требования к информационной зоне", 6.3 "Требования к телекоммуникационной зоне" для размещения оборудования с общей мощностью менее 250 кВт.

44. Потребитель создает инфраструктуру с учетом:

Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. N 117;

требований, установленных Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденными приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. N 378;

Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств, утвержденных приказом Федеральной службы безопасности Российской Федерации от 18 марта 2025 г. N 117.

45. Класс защищенности и уровень защищенности информации инфраструктуры не может быть ниже класса защищенности и уровня защищенности информации размещаемых информационных систем потребителей.

46. Потребитель обеспечивает аттестацию планируемой к использованию для размещения государственных информационных систем инфраструктуры по форме согласно приложению N 4 к Порядку организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденному приказом Федеральной службы по техническому и экспортному контролю от 29 апреля 2021 г. N 77.

47. Целевая надежность инфраструктуры определяется требованиями к надежности размещаемых на ней информационных систем с учетом их архитектуры. Критерием надежности является время доступности инфраструктуры для функционирования размещенных на ней информационных систем. Инфраструктура гарантирует доступность информационных систем на уровне отношения суммарного времени простоя за год к длительности года не ниже 99,5%, за исключением, когда для информационных систем допустима и определена более низкая доступность.

48. Для обеспечения высокой надежности функционирования программные, программно-аппаратные средства, позволяющие обеспечить выполнение значимых функций информационных систем, размещенных на инфраструктуре, следует развернуть в отказоустойчивой конфигурации, обеспечивающей восстановление выполнения значимых функций в установленный оператором (обладателем информации) во внутренних стандартах и регламентах по защите информации интервал времени восстановления.

49. Потребитель обеспечивает отказоустойчивость функционирования размещенных на инфраструктуре информационных систем. Отказоустойчивость инфраструктуры может обеспечиваться за счет дублирующих компонентов в составе самого оборудования либо путем создания кластера оборудования.

50. Для обеспечения отказоустойчивости в условиях глобальных аварий и отказов оборудования потребитель реализует специальные меры по обеспечению катастрофоустойчивости, гарантирующие возобновление работы критических информационных систем после серьезной аварии, последствия которой

невозможно устранить локально в требуемый регламентами функционирования размещенных информационных систем срок.

51. Для обеспечения катастрофоустойчивости потребитель создает дублирующий контур инфраструктуры и обеспечивает репликацию между основным и дублирующим контурами. Дублирующая инфраструктура обеспечивает 100% объема хранения данных, при этом в части вычислительных мощностей может быть менее производительной основной.

52. Для размещения на инфраструктуре информационных систем, категорированных как значимые объекты критической информационной инфраструктуры, потребитель обеспечивает меры по организации надлежащего использования программных и аппаратных компонентов инфраструктуры субъектами критической информационной инфраструктуры на принадлежащих им значимых объектах критической информационной инфраструктуры в соответствии со следующими актами:

Указом Президента Российской Федерации от 1 мая 2022 г. N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации";

Указом Президента Российской Федерации от 30 марта 2022 г. N 166 "О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации";

постановлением Правительства Российской Федерации от 14 ноября 2023 г. N 1912 "О порядке перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации".

53. Для инфраструктуры, на которой размещаются информационные системы, являющиеся значимыми объектами критической информационной инфраструктуры, Потребитель: реализует соответствующие меры по обеспечению безопасности объекта согласно требованиям приказа Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. N 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации", в том числе обеспечивает использование отказоустойчивых технических средств, резервирование средств и систем, контроль безотказного функционирования средств и систем, резервное копирование информации, возможность восстановления информации, возможность восстановления программного обеспечения при нештатных ситуациях, контроль предоставляемых вычислительных ресурсов и каналов связи.

V. Рекомендации по оптимизации создания и использования инфраструктуры

54. Развертывание инфраструктуры рекомендуется спланировать поэтапно в соответствии со сроками действительной готовности к эффективному использованию инфраструктуры с обеспечением целевого уровня показателей утилизации ресурсов.

55. Объем, состав и архитектура инфраструктуры определяются требованиями по производительности и архитектуре размещаемых на ней информационных систем. При этом рекомендуется сформировать план по созданию и расширению инфраструктуры (далее - План) в соответствии с этапами жизненного цикла размещаемых на данной инфраструктуре информационных систем.

56. При создании инфраструктуры под размещение впервые разрабатываемой информационной системы в Плане рекомендуется зафиксировать постепенное развертывание ресурсов инфраструктуры под контур разработки, контур тестирования, при необходимости под предпродуктивный контур, под продуктивный контур.

57. При потребностях в расширении инфраструктуры под растущую нагрузку информационных систем потребитель проводит умощнение ресурсов руководствуясь как прогнозом роста нагрузки, который должен отражаться и поддерживаться в актуальном состоянии в Плане, так и фактическими показателями утилизации компонентов инфраструктуры. Не допускается увеличение ресурсов без достижения

достаточного уровня утилизации соответствующих компонентов инфраструктуры.

58. Одним из действенных методов оптимизации расходов на инфраструктуру является процесс контроля утилизации и соответствующего частичного сокращения низко утилизированного ресурса и/или запрета на доумощнение инфраструктуры при наличии недостаточно утилизированных ресурсов того же типа, на которые поступает запрос по умощнению на в этом же контуре инфраструктуры.

59. Для контроля утилизации компонентов инфраструктуры потребитель реализует систему сбора метрик для постоянного мониторинга утилизации ресурсов/оборудования, а также устанавливает диапазоны для показателей утилизации для каждого типа ресурсов, в том числе для процессоров, оперативной памяти, ssd памяти, дисковой памяти.

60. В случае приобретения инфраструктуры в качестве услуги, при недостижении целевого диапазона утилизации, потребитель принимает меры по технической переконфигурации (сокращению) недостаточно утилизируемого компонента инфраструктуры и выполнению сокращения заказа соответствующего ресурса для недопущения неэффективного расходования средств.

61. В случае наличия собственной инфраструктуры или приобретения инфраструктуры без возможности уменьшения заказа, потребитель формирует резерв из свободных ресурсов и использует его для целей умощнения высоконагруженных элементов инфраструктуры, например, для высоконагруженных виртуальных машин, требующих умощнения или для других информационных систем или информационных ресурсов, размещенных на этой же инфраструктуре.

62. Отдельные ресурсы инфраструктуры могут быть использованы по модели совместного использования разными информационными системами и потребителями, размещающими свои информационные системы в рамках одного контура инфраструктуры. Такой подход допустим в случае использования модели "общественного облака" в соответствии с требованиями постановления Правительства Российской Федерации от 10 июля 2024 г. N 929 "Об утверждении Положения о государственной единой облачной платформе" (далее - постановление N 929).

63. Совместное использование ресурсов может осуществляться посредством совместного использования объектного хранилища разными информационными системами, кластеров размещения баз данных, каналов связи, систем хранения данных, переподписок на процессорные ядра и др.

64. При размещении нескольких информационных систем в контурах потребителей с использованием облачного подхода по созданию и управлению инфраструктурой, контуры управления и контуры обеспечения информационной безопасности могут быть едиными для многих размещаемых систем, что существенно оптимизирует расходы на управление и обеспечение информационной безопасности инфраструктуры.

65. Для органов исполнительной власти и органов местного самоуправления целесообразно использовать подтвержденные подходы и конкретные меры по минимизации затрат на эксплуатацию инфраструктуры. Рекомендуется использовать накопленный опыт по созданию государственной единой облачной платформы (в настоящее время платформа функционирует в рамках постановления N 929, ранее в формате эксперимента в соответствии с постановлением Правительства Российской Федерации от 28 августа 2019 г. N 1114).

Облачный подход позволяет размещать информационные системы различных ведомств на общих контурах виртуальных ресурсов, применять единые контуры управления и обеспечения информационной безопасности, обеспечивать совместное использование систем хранения данных, обеспечивать независимый мониторинг утилизации ресурсов и оперативно перераспределять их в зависимости от фактической утилизации. Кроме того, применение единого пула облачной инфраструктуры позволит использовать требуемые ресурсы в момент их востребованности и исключить существенные затраты на невостребованный объем оборудования.