Проект

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

(МИНЦИФРЫ РОССИИ)

ПРИКАЗ

_____ № _____

Москва

Об утверждении Требований к обеспечению информационной безопасности в рамках предоставления облачных услуг посредством государственной единой облачной платформы

В соответствии с абзацем вторым подпункта «в» пункта 2 постановления Правительства Российской Федерации от 10 июля 2024 г. № 929 «Об утверждении Положения о государственной единой облачной платформе», п р и к а з ы в а ю:

Утвердить прилагаемые Требования к обеспечению информационной безопасности в рамках предоставления облачных услуг посредством государственной единой облачной платформы.

Министр М.И. Шадаев

УТВЕРЖДЕНЫ
приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от _____ № _____

ТРЕБОВАНИЯ
к обеспечению информационной безопасности в рамках предоставления облачных услуг посредством государственной единой облачной платформы

1. Настоящие Требования разработаны с целью обеспечения устойчивого функционирования государственной единой облачной платформы с надлежащим уровнем информационной безопасности в соответствии с законодательством Российской Федерации, а также предотвращения (минимизации) ущерба и отказа функционирования информационно-телекоммуникационной инфраструктуры, в рамках которой поставщиками предоставляются облачные услуги (далее – информационно-телекоммуникационная инфраструктура).

2. Информационно-телекоммуникационная инфраструктура не должна быть ниже класса защищенности и уровня защищенности информации информационных систем потребителей, а также должна соответствовать Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом Федеральной службой по техническому и экспортному контролю от 11 февраля 2013 г. № 17[1] (далее – Требования о защите информации), и Требованиям о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств, утвержденным приказом Федеральной службы безопасности Российской Федерации от 18 марта 2025 г. № 117[2].

3. Определение актуальных угроз безопасности информации, обрабатываемой в государственной единой облачной платформе, осуществляется в соответствии с пунктом 14.3 Требований о защите информации.

4. В рамках организации процесса мониторинга инцидентов информационной безопасности должны реализовываться меры, направленные на защиту государственной единой облачной платформы от атак, направленных на отказ в обслуживании, предусмотренные подпунктом «б» пункта 25(1) Требований о защите информации, и выполняться требования к средствам государственной

---

1 Зарегистрирован Министерством юстиции Российской Федерации 31 мая 2013 г., регистрационный № 28608, с изменениями, внесенными приказами Федеральной службы по техническому и экспортному контролю от 15 февраля 2017 г. № 27 (Зарегистрирован Министерством юстиции Российской Федерации 14 марта 2017 г., регистрационный № 45933), от 28 мая 2019 г. № 106 (Зарегистрирован Министерством юстиции Российской Федерации 13 сентября 2019 г., регистрационный № 55924), от 28 августа 2024 г. № 159 (Зарегистрирован Министерством юстиции Российской Федерации 24 октября 2024 г., регистрационный № 79900).

2 Зарегистрирован Министерством юстиции Российской Федерации 26 марта 2025 г., регистрационный № 81647.

системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[3].

5. Поставщиками должна создаваться и поддерживаться в актуальном состоянии комплексная система обеспечения информационной безопасности информационно-телекоммуникационной инфраструктуры, которая служит для обеспечения информационной безопасности информационно-телекоммуникационной инфраструктуры от несанкционированного воздействия третьих лиц в соответствии с моделью угроз и нарушителей безопасности информации государственной единой облачной платформы.

6. Оценка соответствия систем защиты информации объектов информатизации, входящих в государственную единую облачную платформу, должна подтверждаться за счет действующих аттестатов или выполнения процедуры аттестации информационных систем, в том числе государственных информационных систем, потребителя, действующих аттестатов соответствия или выполнения процедуры аттестации для информационно-телекоммуникационной инфраструктуры поставщиков.

7. Программные и аппаратные компоненты информационно-телекоммуникационной инфраструктуры должны быть реализованы на отечественных продуктах, включенных в соответствующие реестры Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации и Министерства промышленности и торговли Российской Федерации, а средства защиты информации должны иметь соответствующий сертификат Федеральной службы безопасности Российской Федерации или Федеральной службы по техническому и экспортному контролю.

8. Технические средства, которые обрабатывают информацию, средства защиты информации, а также средства, которые обеспечивают функционирование центров обработки данных, должны размещаться на территории Российской Федерации.

9. Комплексная система обеспечения информационной безопасности информационно-телекоммуникационной инфраструктуры должна включать следующие подсистемы:

а) подсистема физической защиты должна обеспечивать контроль и управление доступом, исключающие несанкционированный физический доступ к техническим средствам, средствам обработки информации, средствам защиты информации, машинным носителям информации, средствам обеспечения функционирования информационных систем;

б) подсистема анализа защищенности должна обеспечивать выявление уязвимостей системного и прикладного программного обеспечения, размещаемого в кластере систем управления информационно-телекоммуникационной инфраструктурой путем автоматизированного (инструментального) анализа защищенности информационных систем посредством сетевого поиска уязвимостей («сетевого сканирования»);

---

[3] Приказ Федеральной службы безопасности Российской Федерации от 6 мая 2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» (Зарегистрирован Министерством юстиции Российской Федерации 31 мая 2019 г., регистрационный № 54801).

в) подсистема межсетевого экранирования и предотвращения вторжений должна осуществлять сетевое сегментирование, контроль трафика и защиты от атак уровня сети информационного обмена различных информационных систем и сервисов информационно-телекоммуникационной инфраструктуры, а также информационных систем потребителей между собой и внешними сетями общего доступа;

г) подсистема криптографической защиты информации должна обеспечивать защиту сетевого информационного обмена между информационными системами кластера систем управления информационно-телекоммуникационной инфраструктурой и внешними подключениями для уполномоченных лиц службы технической поддержки поставщиков, информационными системами потребителей, размещенных в информационно-телекоммуникационной инфраструктуре, и внешними подключениями для уполномоченных лиц службы технической поддержки потребителей. Средства подсистемы криптографической защиты информации должны обеспечивать криптографическую защиту на основе российских криптографических алгоритмов;

д) подсистема антивирусной защиты должна обеспечивать защиту информационно-телекоммуникационной инфраструктуры от вредоносного программного обеспечения. Подсистема антивирусной защиты информационно-телекоммуникационной инфраструктуры не предназначена для защиты вычислительных машин информационных систем потребителей;

е) подсистема выявления и управления инцидентами информационной безопасности должна осуществлять сбор и анализ событий безопасности, регистрируемых на компонентах информационно-телекоммуникационной инфраструктуры, а также оперативное выявление инцидентов информационной безопасности и оповещение уполномоченных лиц, ответственных за защиту информации;

ж) подсистема защиты среды виртуализации должна идентифицировать и аутентифицировать субъекты доступа и объекты доступа в виртуальной инфраструктуре, управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, регистрацию событий безопасности в виртуальной инфраструктуре, доверенную загрузку серверов виртуализации, контроль управления перемещением вычислительных машин, контроль целостности виртуальной инфраструктуры и ее конфигураций;

з) подсистема контроля привилегированных пользователей должна обеспечивать контроль, мониторинг и запись сессий доступа привилегированных пользователей к целевым информационным системам в режиме реального времени с возможностью принудительного прерывания сессии, контроль буфера обмена при установленных подключениях к целевым информационным системам, возможность автоматического блокирования привилегированным пользователям доступа к предоставляемым облачным услугам при выполнении ими запрещенных действий, просмотр сохраненных видеозаписей сессий с возможностью быстрого поиска фрагмента видеозаписи по заданным параметрам, возможность создания ролей пользователей подсистемы с различным набором прав доступа, возможность

сортировки, поиска и фильтрации событий по различным критериям и построения отчетов;

и) подсистема защиты от несанкционированного доступа должна обеспечивать защиту от несанкционированного доступа и управление доступом персонала службы технической поддержки поставщиков к информационно-телекоммуникационной инфраструктуре.

10. До начала использования облачных услуг, предоставляемых посредством государственной единой облачной платформы, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации проверяет соответствие информационно-телекоммуникационной инфраструктуры поставщика требованиям по информационной безопасности, что должно подтверждаться наличием у поставщика действующего аттестата соответствия требованиям по защите информации, оформляемого органом по аттестации[4].

11. Информационно-телекоммуникационная инфраструктура не предназначена для обработки сведений, составляющих государственную тайну.

---

[4] Приложение № 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. № 77 (Зарегистрирован Министерством юстиции Российской Федерации 10 августа 2021 г., регистрационный № 64589).