МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

(МИНЦИФРЫ РОССИИ)

ПРИКАЗ

02.12.2025 № 1106

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 02.12.2025 № 1106

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[1] 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[2] предоставляются облачные услуги[3] (далее – информационно-телекоммуникационная инфраструктура).

2. Информационно-телекоммуникационная инфраструктура должна соответствовать:

а) требованиям о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117[4] (далее – Требования о защите информации);

б) требованиям, установленным 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, утвержденным приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. № 378[5] (далее – Состав и содержание организационных и технических мер с использованием средств криптографической защиты информации);

в) требованиям о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений,

---

[1] Абзац второй пункта 2 Положения о государственной единой облачной платформе, утвержденного постановлением Правительства Российской Федерации от 10 июля 2024 г. № 929 (далее – Положение о государственной единой облачной платформе).

[2] Абзац третий пункта 2 Положения о государственной единой облачной платформе.

[3] Абзац пятый пункта 2 Положения о государственной единой облачной платформе.

[4] Зарегистрирован Министерством юстиции Российской Федерации 16 июня 2025 г., регистрационный № 82619.

[5] Зарегистрирован Министерством юстиции Российской Федерации 18 августа 2014 г., регистрационный № 33620.

с использованием шифровальных (криптографических) средств, утвержденным приказом Федеральной службы безопасности Российской Федерации от 18 марта 2025 г. № 117[6] (далее – Требования о защите информации с использованием шифровальных (криптографических) средств).

3. 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 абзацем вторым пункта 59 Требований о защите информации.

Мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации должны выполняться только аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[7], а в период действия переходного периода – организациями, имеющими действующее соглашение о сотрудничестве (взаимодействии) с Федеральной службой безопасности Российской Федерации (Национальным координационным центром по компьютерным инцидентам) в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты[8].

4. Программные и аппаратные компоненты информационно-телекоммуникационной инфраструктуры должны быть реализованы на решениях, включенных в единый реестр российских программ для электронных вычислительных машин и баз данных в соответствии с Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 16 ноября 2015 г. № 1236, и (или) реестр российской промышленной продукции в соответствии с Правилами формирования и ведения реестра российской промышленной продукции, состав сведений, включаемых в реестр, порядок включения таких сведений в реестр и исключения их из реестра, в том числе размещения таких сведений в государственной информационной системе промышленности, и порядок предоставления сведений, включенных в реестр, утвержденными постановлением Правительства Российской Федерации от 17 июля 2015 г. № 719.

Использование программных и аппаратных компонентов информационно-телекоммуникационной инфраструктуры субъектами критической информационной инфраструктуры Российской Федерации на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации

---

[6] Зарегистрирован Министерством юстиции Российской Федерации 26 марта 2025 г., регистрационный № 81647.

[7] Подпункт «г» пункта 1 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» (далее – Указ № 250).

[8] Подпункт «б» пункта 5 Указа № 250, приказ Федеральной службы безопасности Российской Федерации от 1 ноября 2022 г. № 543 «Об определении переходного периода, предусмотренного подпунктом «б» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250» (зарегистрирован Министерством юстиции Российской Федерации 1 декабря 2022 г., регистрационный № 71291); с изменением, внесенным приказом Федеральной службы безопасности Российской Федерации от 21 июля 2025 г. № 282 (зарегистрирован Министерством юстиции Российской Федерации 19 августа 2025 г., регистрационный № 83223).

должно быть реализовано в соответствии с Правилами перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 14 ноября 2023 г. № 1912[9].

5. Средства защиты информации, используемые в информационно-телекоммуникационной инфраструктуре, должны:

а) иметь действующие сертификаты в соответствии с пунктом 3 Положения о системе сертификации средств защиты информации, утвержденного приказом Федеральной службы по техническому и экспортному контролю от 3 апреля 2018 г. № 55[10] и (или) в соответствии с пунктом 3 Требований о защите информации с использованием шифровальных (криптографических) средств;

б) соответствовать пункту 11 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21[11], в том числе в части контроля отсутствия недекларированных возможностей программного обеспечения данных[12];

в) соответствовать требованиям к защите персональных данных при их обработке в информационных системах персональных данных потребителей[13] в соответствии с пунктом 9 Состава и содержания организационных и технических мер с использованием средств криптографической защиты информации.

6. Технические средства, обрабатывающие информацию, средства защиты информации, а также средства, обеспечивающие функционирование центров обработки данных, должны размещаться на территории Российской Федерации.

7. Для обеспечения защиты информации, содержащейся в информационно-телекоммуникационной инфраструктуре, каждый поставщик должен определить структурное подразделение, ответственное за защиту информации, а также за обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

8. В ходе функционирования информационно-телекоммуникационной инфраструктуры структурным подразделением, указанным в пункте 7 настоящих Требований, должны проводиться следующие мероприятия:

---

[9] В соответствии с пунктом 5 постановления Правительства Российской Федерации от 14 ноября 2023 г. № 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» пункты 1 и 2 данного акта действуют до 1 сентября 2030 г.

[10] Зарегистрирован Министерством юстиции Российской Федерации 11 мая 2018 г., регистрационный № 51063; с изменениями, внесенными приказами Федеральной службы по техническому и экспортному контролю от 5 августа 2021 г. № 121 (зарегистрирован Министерством юстиции Российской Федерации 27 октября 2021 г., регистрационный № 65594) и от 19 сентября 2022 г. № 172 (зарегистрирован Министерством юстиции Российской Федерации 19 октября 2022 г., регистрационный № 70614).

[11] Зарегистрирован Министерством юстиции Российской Федерации 14 мая 2013 г., регистрационный № 28375; с изменениями, внесенными приказами Федеральной службы по техническому и экспортному контролю от 23 марта 2017 г. № 49 (зарегистрирован Министерством юстиции Российской Федерации 25 апреля 2017 г., регистрационный № 46487) и от 14 мая 2020 г. № 68 (зарегистрирован Министерством юстиции Российской Федерации 8 июля 2020 г., регистрационный № 58877).

[12] Пункт 6 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

[13] Абзац четвертый пункта 2 Положения о государственной единой облачной платформе.

а) выявление и оценка угроз безопасности информации;

б) контроль конфигурации информационно-телекоммуникационной инфраструктуры;

в) управление уязвимостями;

г) мониторинг информационной безопасности;

д) контроль уровня защищенности информации, содержащейся в информационно-телекоммуникационной инфраструктуре;

е) обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты.

9. Информационно-телекоммуникационная инфраструктура поставщика должна соответствовать требованиям безопасности информации, что должно подтверждаться наличием у поставщиков аттестата соответствия требованиям по защите информации по форме согласно приложению № 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[14].

[14] Зарегистрирован Министерством юстиции Российской Федерации 10 августа 2021 г., регистрационный № 64589.