МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

(МИНЦИФРЫ РОССИИ)

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 76222
от "01" декабря 2023 г.

ПРИКАЗ

01.11.2023 936

Москва

Об утверждении требований о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети «Интернет»

В соответствии с частью 2 статьи 10^{2-1} Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», пунктом 1 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418,

ПРИКАЗЫВАЮ:

Утвердить прилагаемые требования о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети «Интернет».

Министр М.И. Шадаев

УТВЕРЖДЕНЫ
приказом Министерства
цифрового развития, связи
и массовых коммуникаций
Российской Федерации
от 04.12.2023 № 936

ТРЕБОВАНИЯ
о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети «Интернет»

1. Настоящие требования являются обязательными для провайдеров хостинга при осуществлении ими деятельности по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»).

2. Для обеспечения защиты информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет», провайдером хостинга назначается структурное подразделение или должностное лицо (работник), ответственное (ответственный) за защиту информации.

3. Провайдер хостинга осуществляет непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее – ГосСОПКА)[1], в том числе информирует Федеральную службу безопасности Российской Федерации о компьютерных инцидентах на информационных ресурсах путем направления сведений в Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ) в течение 24 часов с момента их обнаружения в соответствии с определенными НКЦКИ форматами[2], а также осуществляет прием и обработку уведомлений и запросов НКЦКИ по вопросам, связанным с обнаружением, предупреждением и ликвидацией последствий компьютерных атак и реагированием на компьютерные инциденты[3]. Взаимодействие провайдера хостинга с ГосСОПКА может осуществляться через НКЦКИ, а также через отраслевой или корпоративный центр ГосСОПКА.

4. В рамках реализации мер по выявлению и устранению причин и последствий компьютерных атак провайдер хостинга обязан:

---

[1] Пункты 2, 3 статьи 4 и части 1, 5 статьи 5 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[2] Подпункт 4.9 пункта 4 Положения о Национальном координационном центре по компьютерным инцидентам, утвержденного приказом ФСБ России от 24 июля 2018 г. № 366 (зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный № 52109) (далее – Положение о НКЦКИ).

[3] Подпункт 5.1 пункта 5 Положения о НКЦКИ.

а) в случае получения информации от НКЦКИ об информационных ресурсах, которые функционируют на вычислительных мощностях провайдера хостинга и участвуют в компьютерных атаках на информационные ресурсы Российской Федерации, принять меры по устранению причин возникновения компьютерных атак в течение 12 часов с момента поступления соответствующей информации, в том числе отключать подобные информационные ресурсы;

б) в случае поступления от Федеральной службы безопасности Российской Федерации, Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Центра мониторинга и управления сетью связи общего пользования (далее – ЦМУ ССОП)[4], информации о выявленных уязвимостях принять необходимые меры в целях оперативного устранения выявленных уязвимостей и минимизации возможных последствий;

в) при поступлении информации от НКЦКИ об индикаторах компьютерных атак осуществлять поиск индикаторов и предоставление информации в НКЦКИ в течение 4 часов с момента поступления указанной информации от НКЦКИ. Поиск индикаторов осуществляется по хранимой информации со следующими атрибутами:

исходный и целевой сетевые адреса;

исходный и целевой порты;

протокол транспортного уровня (TCP, UDP);

время начала сессии;

запросы на преобразование доменных имен, включая запрашиваемое доменное имя, тип записи, ответное значение, используемый сервер имен и временной штамп запроса и ответа (полученного с DNS-серверов провайдера хостинга, обслуживающего вычислительные мощности, предоставляемые для размещения информации в информационной системе, постоянно подключенной к сети «Интернет»).

5. В целях обеспечения выполнения обязанностей, предусмотренных подпунктом «в» пункта 4 настоящих требований, провайдер хостинга обязан осуществлять сбор и хранение данных о взаимодействии лиц, которым провайдер хостинга предоставляет вычислительные мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет», с пользователями сети «Интернет» (далее – внешние сетевые ресурсы) в течение одного года со дня окончания осуществления указанного взаимодействия.

6. С целью обеспечения контроля и фильтрации входящего и исходящего сетевого трафика провайдер хостинга при наличии технических средств должен принимать меры по обнаружению и предотвращению вторжений в случае их обнаружения.

7. Провайдер хостинга на узлах сети, обеспечивающих соединение с внешними сетевыми ресурсами, должен принимать необходимые меры по выявлению и последующему предотвращению распределенных атак, направленных на отказ в обслуживании (DDoS-атак), с вычислительных ресурсов своих

---

[4] Постановление Правительства Российской Федерации от 13 февраля 2019 г. № 136 «О Центре мониторинга и управления сетью связи общего пользования».

пользователей, а также обеспечивает взаимодействие с ЦМУ ССОП в рамках противодействия DDoS-атакам.

8. Провайдер хостинга при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет», обязан использовать информацию о местоположении использования сетевых адресов, предоставляемую ЦМУ ССОП, информацию, предоставляемую национальной системой доменных имен[5], а также серверы точного времени (NTP серверы), расположенные на территории Российской Федерации.

9. Провайдер хостинга обеспечивает настройку фильтрации сетевого трафика (взаимодействия) с внешними сетевыми ресурсами сетевым адресам информационных ресурсов пользователей в зависимости от способа идентификации и (или) аутентификации лиц, обратившихся к провайдеру хостинга, определенных в порядке, установленном Правительством Российской Федерации в соответствии с частью 5 статьи 10^{2-1} Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

10. В целях обеспечения защиты информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет», а также для противодействия компьютерным атакам провайдер хостинга осуществляет взаимодействие с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в порядке, установленном Правительством Российской Федерации в соответствии с частью 3 статьи 10^{2-1} Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

---

[5] Статья 14.2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».