Федеральная служба по надзору в сфере образования и науки (Рособрнадзор)

ЗАМЕСТИТЕЛЬ РУКОВОДИТЕЛЯ

ул. Садовая-Сухаревская, д. 16,
Москва, К-51, ГСП-4, 127994
телефон/факс: (495) 608-61-58
ИНН 7701537808

04.03.2022 № 04-45

На № _____

Руководителям органов исполнительной власти субъектов Российской Федерации, осуществляющих государственное управление в сфере образования

В рамках подготовки к государственной итоговой аттестации в 2022 году (далее – ГИА) и в соответствии с информацией, поступившей из Федеральной службы по техническому и экспортному контролю, Федеральная служба по надзору в сфере образования и науки сообщает.

При наличии возможности приостановить работу по обновлению применяемого в информационных системах, задействованных при организации и проведении ГИА, иностранного программного обеспечения и программно-аппаратных средств, страной происхождения которых является США и страны Европейского союза, а также исключить их автоматическое централизованное обновление посредством сети «Интернет».

В целях повышения защищенности сайтов, задействованных в ходе процедур, связанных с подготовкой и проведением ГИА, рекомендуется:

провести инвентаризацию служб и веб-сервисов, используемых для функционирования официальных сайтов и размещенных на периметре информационной инфраструктуры (далее – службы и веб-сервисы);

отключить неиспользуемые службы и веб-сервисы;

усилить требования к парольной политике администраторов и пользователей сайтов, исключив при этом использование паролей, заданных по умолчанию, отключить сервисные и неиспользуемые учетные записи;

обеспечить сетевое взаимодействие с применением защищенных актуальных версий протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов);

исключить применение на сайтах сервисов подсчета и сбора данных о посетителях, сервисов предоставления информации о местоположении и иных сервисов, разработанных иностранными организациями (например, сервисов onthe.io, ReCAPTCHA, YouTube, Google Analytics, Google Maps, Google Translate);

исключить возможность использования встроенных видео- и аудио-файлов, интерфейсов взаимодействия API, «виджетов» и других ресурсов, загружаемых со сторонних сайтов, заменив их при необходимости гиперссылкой на такие ресурсы.

В целях повышения устойчивости сайтов к распределенным атакам, направленным на отказ в обслуживании (DdoS-атакам), необходимо принять следующие первоочередные меры защиты информации:

обеспечить настройку правил средств межсетевого экранирования, направленных на блокировку неразрешенного входящего трафика;

обеспечить фильтрацию трафика прикладного уровня с применением средств межсетевого экранирования уровня приложений (web application firewall (WAF)), установленных в режим противодействия атакам;

активировать функции защиты от атак отказа в обслуживании (DDoS- атак) на средствах межсетевого экранирования и других средствах защиты информации;

ограничить количество подключений с каждого IP-адреса (например, установить на веб-сервере параметр rate-limit);

блокировать входящий трафик, поступающий с IP-адресов, страной происхождения которых являются США, страны Европейского союза или иной страной, являющейся источником компьютерных атак;

блокировать трафик, поступающий из «теневого Интернета» через Tor-браузер (список узлов, которые необходимо заблокировать содержится по адресу https://www.dan.me.uk/tornodes).

Просим довести указанную информацию до образовательных организаций, а также провести необходимые мероприятия по повышению защищенности информационной инфраструктуры, задействованной в организации и проведении ГИА, с учетом изложенных рекомендаций.

И.К. Круглинский

Прокофьева Елена Борисовна
(495) 608-73-76, prokofieva@obrnadzor.gov.ru