



МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНПРОСВЕЩЕНИЯ РОССИИ)

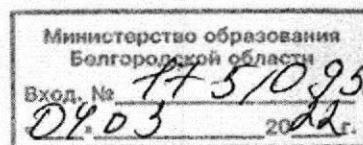
Департамент цифровой
трансформации и больших данных

Каретный Ряд, д. 2, Москва, 127006
Тел. (495) 587-01-10, доб. 3300
E-mail: d04@edu.gov.ru

03.03.2022 № 04-147

О мерах по повышению защищенности
информационной инфраструктуры
системы образования

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



Уважаемые коллеги!

Согласно письмам ФСТЭК России от 28 февраля 2022 г. № 240/22/952, № 240/22/953 и № 240/22/960 (В. Лютиков) о подготовке к проведению компьютерных атак на информационную инфраструктуру Российской Федерации, направленных на получение конфиденциальной информации, а также на нарушение функционирования и вывод из строя информационной инфраструктуры органов государственной власти, в том числе через компрометацию и нарушения функционирования зарубежными хакерскими группировками официальных сайтов органов государственной власти и организаций Российской Федерации Департамент цифровой трансформации и больших данных (далее – Департамент) сообщает следующее.

Предполагается, что проведение компьютерных атак планируется осуществлять через внедрение в обновления иностранного программного обеспечения вредоносного программного обеспечения. При этом распространение обновлений с вредоносными вложениями может осуществляться через центры обновлений (официальные сайты) разработчиков иностранного программного

обеспечения, размещаемые в сети «Интернет».

Учитывая изложенное, Департамент обращает внимание на необходимость (при наличии возможности) приостановить работы по обновлению применяемого в информационных системах 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».

Также в целях повышения защищенности информационных систем и ресурсов (особенно региональных информационных систем доступности дошкольного образования), включая официальные сайты региональных органов власти и органов местного самоуправления, а также образовательных организаций (далее – ИСР), Департамент рекомендует:

провести инвентаризацию служб и веб-сервисов, используемых для функционирования ИСР 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 ИСР, 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 в ИСР 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, Google Analytics);

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.

Таким образом, в целях повышения устойчивости ИСР к распределенным атакам, направленным на отказ в обслуживании (DdoS-атакам), Департамент просит:

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 Тог-браузер (список узлов, которые необходимо заблокировать содержится по адресу <https://www.dan.me.uk/tornodes>).

Вместе с тем, Департамент сообщает, что анализ угроз безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся политической обстановки, показывает, что зарубежными хакерскими группировками, в частности хакерской группировкой ANONYMOUS, в социальных сетях и мессенджерах размещается информация о призывах к администраторам информационных систем раскрыть сведения об особенностях функционирования информационных систем, предоставлении аутентификационной информации и наличии уязвимостей с целью проникновения в информационные системы и размещения противоправной информации.

С целью предотвращения получения зарубежными хакерскими группировками информации об особенностях функционирования информационных систем Министерства просвещения Российской Федерации просим принять

дополнительные меры по следующим направлениям работ:

проинформировать администраторов и пользователей информационных систем о недопущении распространения информации о функционировании информационной системы, передаче сторонним лицам своей аутентификационной информации;

проинформировать администраторов и пользователей информационных систем об ответственности за нарушение требований в области информационной безопасности;

усилить контроль над действиями в информационной системе администраторов и пользователей;

провести внеплановую смену паролей администраторов и пользователей, используемых для доступа в информационные системы;

исключить (при возможности) удаленный доступ посредством сети «Интернет» к информационным системам для администраторов и пользователей;

обеспечить (при возможности) двухфакторную аутентификацию администраторов информационных систем.

Вышеизложенные рекомендации просим довести до сотрудников и работников региональных органов власти, местного самоуправления и образовательных организаций.

О выполнении указанных мер и рекомендаций просим проинформировать Департамент в установленном порядке, а также по адресам электронной почты: kolesova-av@edu.gov.ru, bezlyudskiy-ap@edu.gov.ru в срок до 10 марта 2022 года.

Директор Департамента

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 0B4AD6A6F47CC63C5316D56418FB4B2C40F28227
Владелец Горобец Андрей Валерьевич
Действителен с 15.07.2021 по 15.10.2022

А.В. Горобец

Кудрявцев Д.В.
(495) 587-01-10, доб. 3323
(495) 587-01-10, доб. 3263