МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ АЛТАЙСКОГО КРАЯ
(МИНОБРНАУКИ АЛТАЙСКОГО КРАЯ)

ул. Ползунова, 36, г. Барнаул, 656043
телефон: 29-86-00, факс: 29-86-59
E-mail: info@22edu.ru

10.03.2022 № 23-05/17/472

На № _____

О мерах по повышению защищенности информационной инфраструктуры системы образования

Муниципальные органы управления образованием

Краевые государственные организации, подведомственные Министерству образования и науки Алтайского края

На основании информации ФСТЭК России 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 Министерство образования и науки Алтайского края сообщает следующее (далее – «Министерство»).

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, Министерство 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.

В целях повышения защищенности информационных систем и ресурсов (далее – ИСР) (особенно региональных информационных систем доступности дошкольного образования), включая официальные сайты образовательных организаций рекомендовано:

провести инвентаризацию служб и веб-сервисов, используемых для функционирования ИСР и размещенных на периметре информационной ин-

фраструктуры (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 аудиофайлов, 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) необходимо:

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).

Вместе с тем 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 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.

Вышеуказанные рекомендации просим довести до подведомственных муниципальных учреждений.

Заместитель министра Л.С. Терновая

Семикин С.А.,
(3852) 29-86-96