**Письмо №1373 от 23 декабря 2022 года**

**О мерах по повышению защищенности информационной инфраструктуры системы образования**

**Руководителям ОО**

В соответствии с письмом Министерства просвещения Российской Федерации от 19.12.2022 № 04-961 «О мерах по повышению защищенности информационной инфраструктуры системы образования», письмом Министерства образования и науки Республики Дагестан №06-18059/10-18/22 от 23.12.2022г. МКУ «Управления образования» информирует о необходимости выполнения мер и рекомендаций Минпросвещения России по обеспечению кибербезопасности.

Согласно инструктивным письмам 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, сайтов образовательных организаций сообщаем 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, обращаем внимание на необходимость (при наличии возможности) приостановить работы по обновлению применяемого 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, включая официальные сайты региональных органов власти и органов местного самоуправления, а также образовательных организаций (далее — ИСР), рекомендуем:

* 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, кеСАРТСНА, УоиТиЬе, Google Analytics, Google Maps, Cioogle Translate, Google Analytics);
* исключить возможность использования встроенных видео- и аудио-файлов, интерфейсов взаимодействия АРТ, «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 (То№атакам), просим:

* 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 f1rewall (WAF)), установленных в режим противодействия атакам;
* активировать функции защиты от атак отказа в обслуживании на средствах межсетевого экранирования и других средствах защиты информации; ограничить количество подключений с каждого ТР-адреса (например, установить на веб-сервере параметр rate-limit);
* блокировать входящий трафик, поступающий с 1Р-адресов, страной происхождения которых являются США, страны Европейского союза или иной страной, являющейся источником компьютерных атак;
* блокировать трафик, поступающий из «теневого Интернета» через Тот--браузер (список узлов, которые необходимо заблокировать содержится по адресу https://www.dan.me.uk/tornodes).

Вместе с тем, сообщаем, 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, руководителей образовательных организаций просим принять дополнительные меры по следующим направлениям работ:

1. проинформировать администраторов и пользователей информационных систем о недопущении распространения информации о функционировании информационной системы, передаче сторонним лицам своей аутентификационной информации;
2. проинформировать администраторов и пользователей информационных систем об ответственности за нарушение требований в области информационной безопасности;
3. усилить контроль над действиями в информационной системе администраторов и пользователей;
4. провести внеплановую смену паролей администраторов и пользователей, используемых для доступа в информационные системы;
5. исключить (при возможности) удаленный доступ посредством сети
6. «Интернет» к информационным системам для администраторов и пользователей;
7. обеспечить (при возможности) двухфакторную аутентификацию администраторов информационных систем.

Вышеизложенные рекомендации просим довести до работников образовательных организаций.

Начальник МКУ «УО»: Х.Исаева

*Исп.Магомедова У.К.*

*Тел: 8 903 482 57 46*