Муниципальное казенное
учреждение
«Управление образования»
муниципального района
«Кобяйский улус (район)»
Республики Саха (Якутия)
ПРИКАЗ

Саха Өрөспүүбүлүкэтин
«Кэбээйи улууһа (оройуона)»
муниципальнай оройуонун
уорэ5ин салалтатын
муниципальнай казеннай тэрилтэтэ
БИРИКЭЭС

678300 РС (Я) Кобяйский улус п. Сангар , ул. Ленина, 107а, fax. (41163) 2-14-08, tel (41163) 2-14-08 kobuuo1@mailru

Регистрационный № 130 «10» марта 2022 г

О мерах по повышению защищенности
информационной инфраструктуры в образовательных учреждениях

Согласно письму министерства образования и науки РС(Я) от 05.03.2022 г. № 07/01-19/1877, с целью предотвращения получения зарубежными хакерскими группировками информации об особенностях функционирования информационных систем образовательных учреждений и для принятия дополнительных мер, приказываю:

1. Руководителям образовательных учреждений рекомендовать:

1.1. отключить неиспользуемые службы и веб-сервисы;
1.2. усилить требования к парольной политике администраторов и пользователей ИСР, исключив при этом использование паролей, заданных по умолчанию, отключить сервисные и неиспользуемые учетные записи;
1.3. обеспечить сетевое взаимодействие с применением защищенных актуальных версий протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов);
1.4. 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);
1.5. 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.
1.6. обеспечить настройку правил средств межсетевого экранирования, направленных на блокировку неразрешенного входящего трафика;
1.7. обеспечить фильтрацию трафика прикладного уровня с применением средств межсетевого экранирования уровня приложений (web application firewall (WAF)), установленных в режим противодействия атакам;
1.8. активировать функции защиты от атак отказа в обслуживании (DDoS-атак) на средствах межсетевого экранирования и других средствах защиты информации;
1.9. ограничить количество подключений с каждого IP-адреса (например, установить на веб-сервере параметр rate-limit);
1.10. блокировать входящий трафик, поступающий с IP-адресов, страной происхождения которых являются США, страны Европейского союза или иной страной, являющейся источником компьютерных атак;
1.11. блокировать трафик, поступающий из «теневого Интернета» через Tor-браузер (список узлов, которые необходимо заблокировать содержится по адресу https://www.dan.me.uk/tornodes).

1.12. проинформировать администраторов и пользователей информационных систем о недопущении распространения информации о функционировании информационной системы, передаче сторонним лицам своей аутентификационной информации;
1.13. 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;
1.14. провести внеплановую смену паролей администраторов и пользователей, используемых для доступа в информационные системы;
1.15. исключить (при возможности) удаленный доступ посредством сети «Интернет» к информационным системам для администраторов и пользователей;
1.16. обеспечить (при возможности) двухфакторную аутентификацию администраторов информационных систем.

2. Контроль исполнения настоящего приказа возложить на руководителей образовательных учреждений.

Начальник **И.М.Неустроева**

С приказом (распоряжением) работник ознакомлен « » 2 г.

Личная подпись