УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ НГО

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
Г И М Н А З И Я № 41
(МАОУ «Гимназия № 41»)

П Р И К А З

«15» апреля 2022 г. № 28

г. Новоуральск

О принятии дополнительных мер
по информационной безопасности

В соответствии с письмами Министерства образования и молодежной политики Свердловской области от 05.03.2022 № 02-01-81/2566 «О мерах по повышению защищенности информационной инфраструктуры», от 04.04.2022 № 02-01-82/3893, от 06.04.2022 № 02-01-82/4065, от 12.04.2022 № 02-01-82/4273, письмом Министерства цифрового развития и связи Свердловской области от 14.04.2022 № 41-01-81/1478, в целях реализации дополнительных мер по повышению защищенности объектов информационной инфраструктуры, информационной системы и информационно-телекоммуникационных сетей МАОУ «Гимназия № 41» от угроз безопасности, связанных с противоправными и преднамеренными действиями зарубежных хакерских группировок,

ПРИКАЗЫВАЮ:

1. Принять к исполнению Перечень рекомендованных мер защиты информации информационной инфраструктуры МАОУ «Гимназия № 41», указанный в письмах Министерства образования и молодежной политики Свердловской области от 05.03.2022 № 02-01-81/2566 «О мерах по повышению защищенности информационной инфраструктуры», от 04.04.2022 № 02-01-82/3893, от 06.04.2022 № 02-01-82/4065, от 12.04.2022 № 02-01-82/4273, письме Министерства цифрового развития и связи Свердловской области от 14.04.2022 № 41-01-81/1478 (Приложение).
2. Черкуновой Аоле Юрьевне, заместителю директора, обеспечить взаимодействие с обслуживающей организацией АО «Гринатом» по выполнению Перечня рекомендованных мер защиты информации информационной инфраструктуры МАОУ «Гимназия № 41».
3. Заместителям директора Черкуновой Аоле Юрьевне, Хомей Ольге Михайловне до 30 апреля 2022 года провести инвентаризацию общедоступных информационных ресурсов (веб-сайтов, порталов) путем внешнего сканирования блока публичных IP- адресов, принадлежащих МАОУ «Гимназия № 41».
4. Заместителям директора Черкуновой Аоле Юрьевне, Хомей Ольге Михайловне до 30 апреля 2022 года провести анализ компьютерного программного обеспечения, используемого в образовательном процессе.
5. Хомей Ольге Михайловне, заместителю директора, информировать сотрудников о:

1) недопустимости использования иностранных цифровых решений и программ для организации видеоконференций, в том числе Zoom, Zello, Webex, Discord, Skype;

2) перечне наиболее популярных и общественных сервисов и цифровых решений иностранных компаний, деятельность которых полностью или частично ограничена на территории Российской Федерации, а также перечне рекомендованных аналогов.

6. Ограничить использование обезличенных учетных записей на сетевом оборудовании.

7. Отключить удаленный доступ к системам и сетям, предоставляя его только на согласованной заявке и на короткий промежуток времени для выполнения работ.

8. Всем сотрудникам проводить проверку электронных носителей на предмет наличия вредоносного программного обеспечения.

9. Контроль исполнения приказа оставляю за собой.

Директор А.В. Великов

Приложение к приказу
от 15.04. 2022 № 28

Перечень дополнительных мер по повышению защищенности объектов информационной инфраструктуры, информационной системы и информационно-телекоммуникационных сетей МАОУ «Гимназия № 41» от угроз безопасности, связанных с противоправными и преднамеренными действиями зарубежных хакерских группировок

1) Проводить проверку наличия вредоносного программного обеспечения в поступающих неизвестных (незапрашиваемых) электронных сообщениях (письмах, документах), а открытие писем с адреса: noreply@mvd.msk.ru – запретить;

2) Заблокировать получение пользователями систем и сетей электронных писем, имеющих вложения с расширениями ADE, ADP, .APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH;

3) Ограничить применение и осуществлять контроль невозможности подключения неучтенных съемных машинных носителей информации и мобильных устройств;

4) Обеспечить создание резервных копий защищаемой информации, обрабатываемой пользователями, исключив при этом хранение в облачных сервисах;

5) Проводить проверку актуальности версий программного обеспечения средств защиты информации, применяемых для обеспечения безопасности объектов информационной инфраструктуры (далее ИИ), а также их баз данных, осуществляемая не реже чем раз в 3 дня, при наличии их обновлений – незамедлительное применение этих обновлений;

6) Минимизировать использование неподдерживаемых версий операционных систем (далее — ОС) Microsoft Windows (включая устаревшие версии Windows 10). Убедиться, что на всех автоматизированных рабочих местах под управлением Windows 7/Windows 8/Windows Server 2008 R2/ Windows Server 2012, где по каким-либо причинам невозможен переход на более новые версии ОС, установлено обновление KB2871997 (https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/the-importance-of-kb2871997-and-kb2928120-for-credential/ba-p/2 58478); Отключить автоматическое обновление программного обеспечения компании Microsoft;

7) Провести проверку на объектах ИИ соблюдения ограничений на использование программного обеспечения, не относящегося к производственной и образовательной деятельности и не требуемого для выполнения должностных обязанностей работников объектов ИИ;

8) Провести проверку на объектах ИИ соблюдения ограничений на использование программного обеспечения, сервисов и цифровых решений иностранных компаний, деятельность которых полностью или частично ограничена на территории Российской Федерации (*в соответствии с перечнем, направленным МОиМП СО от 12.04.2022 № 02-01-82/4273*), при установке программного обеспечения отдавать приоритет рекомендованным аналогам (https://catalog.arppsoft.ru/replacement, https://reestr.digital.gov.ru/);

9) Запретить отправку событий безопасности во внешние иностранные сервисы (Cloud SIEM, Cloud EDR, SOC и MDR);

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

11) 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;

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

13) Исключить применение иностранных систем видеоконференции, в том числе Zoom, Skype, а также систем удаленного доступа (RAdmin, TeamViewer, AnyDesk);

14) В целях предотвращения возможности использования систем удаленного доступа для реализации угроз безопасности информации ограничить (по возможности исключить) доступ к системам удаленного доступа из сети «Интернет» к информационным системам для администраторов и пользователей. Осуществлять доступ к системам удаленного доступа из сети «Интернет» рекомендуется с использованием VPN-сетей и только с IP-адресов, закрепленных за автономными системами Российской Федерации;

15) Запретить установку стороннего программного обеспечения пользователям самостоятельно, без разрешения администратора. Перед установкой программного обеспечения и обновлений на объект инфраструктуры обеспечить его проверку на предмет наличия вредоносного программного обеспечения;

16) В случае выявления признаков компьютерных инцидентов в системах и сетях необходимо незамедлительно проинформировать о них Национальный координационный центр по компьютерным инцидентам (тел.: +7 (916) 901-07-42; эл. почта: info@cert.gov.ru)