Перечень организационно-технических мер по повышению защищенности объекта информационной инфраструктуры.

Организационно-технические меры:

1) исключить, на рабочих местах Школы, применение сервисов предоставления информации о местоположении и иных сервисов, разработанных иностранными организациями (например, сервисов onthe.io, ReCAPTCHA, YouTube, Google Analytics, Google Maps, Google Translate), отклонять запросы геолокации;

2) исключить, на рабочих местах Школы, возможность использования модификаций интернет-браузеров посредствам установки дополнительных расширений(плагинов), имеющих различную функциональность (блокирование рекламы, обеспечение хранения паролей и т.д.);

3) исключить осуществление входов в любые социальные сети по средствам использования оборудования школы, имеющее доступ в сеть Интернет;

4) исключить, на рабочих местах Школы, применение иностранных систем видеоконференции, в том числе Zoom, Skype, Meet, а также систем удаленного доступа (RAdmin, TeamViewer, AnyDesk);

5) исключить подключение и использование в сети Школы личных средств вычислительной техники (ноутбуков, планшетов, смартфонов), модемов;

6) исключить использование съемных машинных носителей информации без сканирования антивирусной системой;

7) исключить подключение к оборудованию Школы личных средств вычислительной техники (ноутбуков, планшетов, смартфонов, модемов) в качестве коммутационного средства для выхода в сеть Интернет;

8) исключить установки программного обеспечения на оборудование Школы без согласования;

9) исключить установки обновлений установленного программного обеспечения без согласования, отклонять все запросы обновления;

10) недопущении распространения информации о функционировании информационной системы Школы. Передаче сторонним лицам своей аутентификационной информации (логины, пароли, информацию об установленном оборудовании);

11) не пересылать информацию на личную электронную почту (по не защищенному каналу) данные, содержащие конфиденциальную информацию;

12) не открывать любые сомнительные ссылки из почтовых сообщений, скачивать сомнительные файлы из сети «Интернет»;

13) создан отдельный электронный почтовый адрес **prv-antivir@yandex.ru**, на который пользователи информационной системы должны присылать письма, которые могут содержать вредоносное содержание (ссылку или вложение);

14) соблюдения ограничений на использование программного обеспечения, не относящегося к производственной деятельности и не требуемого для выполнения должностных обязанностей работников Школы;

15) Информируем пользователей информационной системы о необходимости безопасной работы с электронной почтой, а именно:

- внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;
- не открывать письма от неизвестных адресатов;
- проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
- не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com, и т.д.);
- не нажимать на ссылки из письма, если они заменены на слова, не наводить на них мышкой и просматривать полный адрес сайтов;
- проверять ссылки, даже если письмо получено от другого пользователя информационной системы;
- не открывать вложения, особенно если в них содержаться документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;
- внимательно относится к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;
- в случае появления сомнений — направлять полученное письмо как вложение администратору информационной системы по адресу **prv-antivir@yandex.ru**.

16) проинформировать пользователей информационных систем об ответственности за нарушение требований в области информационной безопасности;