Письмо №183 от 01 марта 2022 года

**О безопасности информационных ресурсов**

**Руководителям ОО**

В соответствии с письмом Министерства цифрового развития Республики Дагестан №09-09-482/22 от 26.02.2022г. МКУ «Управление образования» сообщает, что в настоящее время все чаще поступают данные о формировании угроз безопасности, обусловленные хакерскими атаками на информационные ресурсы органов государственной власти Российской Федерации.

Так, с января 2022 года на официальные электронные адреса федеральных и региональных органов государственной власти Российской Федерации под видом официальных запросов из различных госорганов злоумышленники направляют электронные письма, содержащие запросы о предоставлении сведений, содержащих вредоносное программное обеспечение (далее – ВПО), предназначенное для получения скрытого удаленного доступа к системе. В целях затруднения обнаружения антивирусными средствами ВПО упаковывается в архив, разбитый на две части, которые впоследствии также архивируются.

В целях нейтрализации выявленных угрозообразующих факторов необходимо:

1. Использовать на всех объектах информационно-телекоммуникационной сети сертифицированные ФСБ России антивирусные средства с актуальными антивирусными базами.
2. Настроить на всех автоматизированных рабочих местах (далее – АРМ) периодическую (не реже 1 раза в месяц) полную антивирусную проверку системных и пользовательских каталогов операционной системы, а также полную (не реже 1 раза в месяц) антивирусную проверку всех несъемных носителей информации.
3. Настроить на всех АРМ процедуру принудительной антивирусной проверки подключаемых внешних носителей информации.
4. Организовать на сервере электронной почты антивирусную проверку всех входящих писем и периодическую проверку накопленной электронной корреспонденции, фильтрацию входящей электронной корреспонденции на предмет наличия спам сообщений, а также электронных писем, содержащих во вложении исполняемые файлы (.exe, .bat, .cpl, .dll, .jar, .msi, .scr и т.д.).
5. Проводить осмотр вложений электронных писем, поступающих на публичный (опубликованный в сети «Интернет») почтовый адрес организации, на выделенном АРМ с установленной на нем операционной системы семейства Linux и свободно распространяемым пакетом офисных программ. Целью указанных мероприятий является проверка вложенных электронных документов на предмет наличия ВПО, признаком которых может являться появление сообщений об ошибках в работе офисных программ при открытии вложенных электронных документов. В случае появления указанных сообщений об ошибках, необходимо удалять электронные письма, содержащие вложения, предположительно зараженные ВПО, и не открывать указанные вложения на других АРМ.
6. Осуществлять антивирусную проверку входящего веб-трафика, а также его фильтрацию с использованием контент-фильтров (сайтов развлекательного характера и сайтов социальных сетей, запрет посещения потенциально опасных сайтов, запрет загрузки исполняемых файлов).
7. Своевременно устанавливать критические обновления безопасности для прикладного программного обеспечения, в том числе офисных пакетов, средств просмотра PDF документов, интернет-браузеров, средств работы с Flash и Java приложениями.
8. Отключить в настройках офисных программ возможность работы со встроенными в документы макросами.
9. Осуществить настройку системы разграничения прав доступа в операционной системе с целью предоставления пользователям минимально необходимого перечня прав доступа (ограничить возможность установки программного обеспечения, создания файлов в системных директориях, запуска исполняемых файлов из пользовательских каталогов).

Учитывая возросшее количество хакерских атак в последнее время, данную работу необходимо провести в максимально кратчайшие сроки. В связи с изложенным, просим в срок до 20 апреля 2022 года в установленном порядке направить на почту uma196565@mail.ru информацию о проведенной работе.

Начальник МКУ «УО»: Х.Исаева

*Исп.Магомедова У.К.*

*Тел.: 8 903 482 57 46*