РОССИЙСКАЯФЕДЕРАЦИЯ
РОСТОВСКАЯ ОБЛАСТЬ
муниципальное бюджетное дошкольное образовательное учреждение
г.Шахты Ростовской области «Детский сад №36»
346530, г.Шахты Ростовской области, ул. Парижская Коммуна,8-а
тел. 8(8636)22-10-51; E-mail: mdoy_36@mail.ru

ПРИКАЗ

«27» октября 2022г. № 140
О мерах по повышению уровня
информационной безопасности

В рамках исполнения Указа Президента Российской Федерации от 19 октября 2022 г. № 757 «О мерах, осуществляемых в субъектах Российской Федерации в связи с Указом Президента Российской Федерации от 19 октября 2022 г. № 756» на основании приказа министерства общего и профессионального образования Ростовской области от 20.10.2022 № 1041 «О мерах по повышению уровня информационной безопасности» с целью повышения уровня информационной безопасности, во исполнение приказа Департамента образования г. Шахты от 26.10.2022 № 410 «О мерах по повышению уровня информационной безопасности»

ПРИКАЗЫВАЮ:

1. И.о. главного бухгалтера Толмачевой Наталье Александровне, заместителю заведующего по ВМР Троневой Марии Ивановне:
   1.1. Обеспечить выполнение в Организации следующих мероприятий:
   1.1.1. Исключение использования средств антивирусной защиты иностранного производства, иностранных облачных систем и почтовых серверов; регулярное обновление баз средств антивирусной защиты до актуальных версий.
   1.1.2. Исключение использования для организации видеоконференций иностранных цифровых решений и программ, в том числе Zoom, Zello, Webex, Discord, Microsoft Teams, Skype, Googgle Meet.
   1.1.3. Исключение приобретения иностранного программного обеспечения при наличии отечественных аналогов.
   1.1.4. Максимальное ограничение использования иностранных сетевых сервисов API, загружаемых виджетов и т.д.
   1.1.5. Регулярную смену паролей (с обязательным использованием исключительно сложных паролей длительностью не менее 12 знаков, включая цифры, буквы, верхний и нижний регистр).
   1.1.6. В случае наличия удаленного доступа пользователей, особенно администраторов, к информационной инфраструктуре Организации – усиление контроля, в том числе с использованием двухфакторной аутентификации, и защиты всех протоколов удаленного доступа, включая RDP, VNC, TELNET, SSH.
   1.1.7. Контроль за своевременным удалением аккаунтов уволенных сотрудников и исключением их доступа к информационной

инфраструктуре Организации.

1.1.8. Регулярный аудит информации в социальных сетях и на сайтах, как личной, так и информации Организации, на предмет наличия недостоверных сведений компрометирующего характера.

1.1.9. Регулярное резервное копирование данных и конфигураций для обеспечения возможности оперативного восстановления; хранение резервных копий исключительно в изолированной, включая съемные носители, среде, в том числе недоступной из сети «Интернет».

1.1.10. Сохранение используемых программных модулей, библиотек и иных ресурсов, расположенных в иностранных репозиториях, на локальных ресурсах.

1.1.11. Исключение возможности доступа третьих лиц к конфиденциальной информации и передачи им таковой по открытым каналам связи, включая электронную почту.

1.1.12. Проведение аудита правил информационной безопасности.

1.1.13. Максимально возможное ограничение доступа к сети «Интернет» и из нее.

1.1.14. Дополнительная установка (по возможности) отечественных межсетевых экранов для повышения степени эшелонированности защиты информационной инфраструктуры Организации.

1.1.15. Для используемого в Организации программного обеспечения иностранного производства – исключение доступа из сети Организации к серверам его обновлений и лицензирования.

1.1.16. Внедрение сегментации и микросегментации для гранулярного контроля трафика, прежде всего ограничение доступа, в том числе для внутренних пользователей, к инфраструктурным сервисам: AD, SCCM, DNS и т.д.

1.1.17. Проведение сканирования инфраструктуры на наличие открытых нелигитимных и уязвимых сервисов; защита ключевых сервисов соответствующими решениями, в том числе в части защиты веб-приложений и серверов – фильтрацией трафика с помощью Web Application.

1.2. Регламентировать меры по повышению уровня информационной безопасности соответствующими нормативными актами Организации.

2. Ответственность за выполнение мероприятий, указанных в подпункте 1.1 пункта 1 настоящего приказа, возложить на:
- и.о. главного бухгалтера Толмачевой Наталье Александровне,
- заместителя заведующего по ВМР Троневу Марию Ивановну.

3. Контроль исполнения приказа оставляю за собой.

Заведующий Н.Ю. Астахова

С приказом ознакомлены:

И.о. главного бухгалтера / Толмачева Н.А. «27» 10 2022г.

Заместитель заведующего по ВМР / Тронева М.И. «27» 10 2022г.