РОССИЙСКАЯ ФЕДЕРАЦИЯ

РОСТОВСКАЯ ОБЛАСТЬ

МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ «ТАЦИНСКИЙ РАЙОН»

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ЖИРНОВСКАЯ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА

ПРИКАЗ

24 октября 2022 г. № 307 п. Жирнов

О мерах по повышению информационной безопасности в МБОУ Жирновской СОШ

Во исполнение Указа Президента Российской Федерации № 757 от 19 октября 2022 года «О мерах, осуществляемых в субъектах Российской Федерации в связи с Указом Президента Российской Федерации от 19 октября 2022 г. № 756», а также в целях повышения уровня информационной безопасности и недопущения нарушения функционирования информационной инфраструктуры Ростовской области, Приказ Министерства общего и профессионального образования Ростовской области № 1041 от 20.10.2022 г., на основании приказа Отдела образования Администрации Тацинского района № 287 / 2 от 24.10.2022 г.

ПРИКАЗЫВАЮ:

Лебедевой Е.Н., зам. директора по УВР, ответственной за информационную безопасность в МБОУ Жирновской СОШ, Скрынниковой О.П., учителю информатики, ответственной за организацию доступа к сети Интернет и работу системы контентной фильтрации:

1. Исключить использование иностранных цифровых решений и программ для организации видеоконференций, в том числе Zoom, Zello, Webex, Discord, Microsoft Teams, Skype, Google Meet.
2. Исключить приобретение иностранного программного обеспечения при наличии отечественных аналогов.
3. Максимально ограничить использование иностранных сетевых сервисов API, загружаемых виджетов и других.
4. Исключить использование иностранных облачных систем и почтовых серверов.
5. Обеспечить регулярную смену паролей; использование исключительно сложных паролей, не менее 12 знаков (с цифрами, буквами, верхним и нижним регистром).
6. Проводить регулярный аудит информации, размещаемой в социальных сетях и на сайтах, как личной, так и информации организации на предмет наличия недостоверных данных компрометирующего характера.
7. Проводить регулярное резервирование данных и конфигураций для обеспечения возможности оперативного восстановления.
8. Обеспечить хранение резервных копий исключительно в изолированной, недоступной из сети Интернет, среде, в том числе на съемных носителях.

9. Исключить возможности доступа или передачи конфиденциальной информации третьим лицам, в том числе передачу конфиденциальной информации по открытым каналам связи, включая электронную почту.
10. Обеспечить проведение аудита правил безопасности; максимальное ограничение доступа в сеть Интернет.
11. Закрыть доступ для программного обеспечения иностранного производства из сети к серверам обновлений и лицензирования.
12. Внедрить 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.
13. Провести сканирования инфраструктуры на наличие открытых нелегитимных и уязвимых сервисов; защиту ключевых сервисов соответствующими решениями, например, в части защиты веб-приложений и серверов можно обеспечить фильтрацию трафика с помощью Web Application.
14. Контроль за исполнением настоящего приказа оставляю за собой.

Директор С.Я. Шкодин

С приказом ознакомлены: Е.Н. Лебедева

О.П. Скрынникова