ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
РОСТОВСКОЙ ОБЛАСТИ

«ДОНСКОЙ ТЕХНИКУМ КУЛИНАРНОГО ИСКУССТВА И БИЗНЕСА»

ПРИКАЗ

«24» октября 2022 года № 57/1

г. Ростов-на-Дону

О мерах по повышению уровня
информационной безопасности
в ГБПОУ РО «ДонТКИиБ»

Во исполнение Указа Президента Российской Федерации № 250 от 1 мая 2022 года «О дополнительных мерах по обеспечению информационной безопасности», 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», приказа Министерства общего и профессионального образования Ростовской области № 1041 от 20.10.2022 года «О мерах по повышению уровня информационной безопасности», а также в целях повышения уровня информационной безопасности и недопущения нарушения функционирования информационной инфраструктуры ГБПОУ РО «ДонТКИиБ»

ПРИКАЗЫВАЮ:

1. Системному администратору, Авилову И.А., обеспечить выполнение следующих мер по повышению уровня информационной безопасности:

1.1. Регулярное обновление баз антивирусных средств защиты до актуальных версий; исключение использования средств антивирусной защиты иностранного производства.

1.2. Исключение использования иностранных цифровых решений и программ для организации видеоконференций, в том числе Zoom, Zello, Webex, Discord, Microsoft Teams, Skype, Google Meet.

1.3. Исключение приобретения иностранного программного обеспечения при наличии отечественных аналогов.

1.4. Максимальное ограничение использования иностранных сетевых; сервисов API, загружаемых виджетов и других.

1.5. Исключение использования иностранных облачных систем и почтовых серверов.

1.6. Регулярную смену паролей; использование исключительно сложных паролей, не менее 12 знаков (с цифрами, буквами, верхним и нижним регистром).

1.7. Особый контроль защиты удаленных пользователей, особенно администраторов: использование двухфакторной аутентификации, усиление защиты всех используемых протоколов удаленного доступа, включая RDP, VNC, TELNET, SSH.

1.8. Контроль за своевременным удалением аккаунтов уволенных сотрудников.

1.9. Регулярный аудит информации, размещенной в социальных сетях и на сайтах, как личной, так и информации организации на предмет наличия недостоверных данных компрометирующего характера.

1.10. Регулярное резервирование данных и конфигураций для обеспечения возможности оперативного восстановления.

1.11. Хранение резервных копий исключительно в изолированной, недоступной из сети «Интернет», среде, в том числе на съемных носителях.

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

1.13. Исключение возможности доступа или передачи конфиденциальной информации третьим лицам, в том числе передачу конфиденциальной информации по открытым каналам связи, включая электронную почту.

1.14. Проведение аудита правил безопасности; максимальное ограничение доступа в сеть «Интернет» и из нее; рассмотрение вариантов дополнительной установки отечественных межсетевых экранов для повышения; эшелонированности защиты.

1.15. Закрытие доступа для программного обеспечения иностранного производства из вашей сети к серверам обновлений и лицензирования.

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.

1.17. Проведение 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.

2. Персональную ответственность за выполнение мер по повышению уровня информационной безопасности, указанных в пункте 1 настоящего приказа, возложить на заместителя директора по безопасности, Санжарова А.А.

Директор ГБПОУ РО «ДонТКИиБ» И.В. Данилова