Приложение 12
к приказу МАУДО «ДПШ»
от 31.08.2020 № 276/1-од

Инструкция
по использованию корпоративной сети передачи данных

I. Общие правила работы

1. Работа в локальной вычислительной сети (далее – ЛВС) производится работниками МАУДО «ДПШ» с целью получения необходимой информации для выполнения возложенных на них должностных обязанностей в рамках работы в информационных системах персональных данных (далее – ИСПДн).
2. Работа в ЛВС производится с помощью базового компьютера и иных дополнительных устройств.
3. Запрос на установку базового компьютера, его настройку и установку сетевого программного обеспечения осуществляется руководителем подразделения по предварительной письменной заявке, написанной на имя директора МАУДО «ДПШ» в виде служебной записки.
4. Для идентификации пользователя ЛВС работнику выдается имя (учетная запись) и пароль. Имя и пароль необходимы для идентификации в ЛВС и получении доступа к ресурсам сети (сетевым дискам, принтерам и программам). Имя и пароль работника должны быть уникальны в сети. За уникальность и сохранность пароля отвечает пользователь. Пароль – информация конфиденциальная, конфиденциальность обеспечивается самим пользователем и средствами операционных систем.
5. Запрещается сообщать пароль другим пользователям ЛВС и работать под чужим паролем.
6. Пользователи ЛВС обязаны ознакомиться с данными правилами.

II. Технические нормы и правила

7. При нарушении нормальной работы сети и в случае обнаружения неисправности любого компьютерного и сетевого оборудования, а также при сбое или неправильной работе программного обеспечения пользователь обязан немедленно сообщить ответственному за обеспечение безопасности ИСПДн.
8. Поддержка и сопровождение установленного системного и сетевого программного обеспечения осуществляется ответственным за обеспечение безопасности ИСПДн.
9. При необходимости использования нового программного обеспечения, пользователь обязан согласовать его использование с ответственным за обеспечение безопасности ИСПДн.
10. По первому требованию технического специалиста пользователь обязан освободить компьютер для контроля или выполнения регламентных работ.
11. Все действия, связанные с установкой программного обеспечения, а также предоставлением доступа к конкретным ресурсам сети, осуществляются по предварительной письменной заявке, написанной на имя ответственного за обеспечение безопасности ИСПДн, в виде служебной записки.

12. Ответственность за работоспособность клиентского программного обеспечения рабочих станций сети подразделения несет отдел информационно-технического обеспечения.

13. Ответственный за обеспечение безопасности персональных данных в ИСПДН ведёт перечень базовых компьютеров сети организации. Каждая запись содержит следующую информацию:

- имя компьютера;
- используемая операционная система;
- модель монитора;
- ресурсы, предоставляемые другим компьютерам;
- список установленного программного обеспечения;
- должность допущенного сотрудника.

14. В ЛВС осуществляется мониторинг сетевых событий. Полученные при этом электронные журналы событий используются ответственным за обеспечение безопасности персональных данных в ИСПДн для анализа работы сети, а также могут служить доказательством неправомерных действий пользователей.

III. Права и обязанности пользователей сети

15. Пользователь, использующий носители информации, несет ответственность за антивирусную чистоту содержащихся на них данных.

16. В случае получения носителя информации из сомнительного источника пользователь обязан проверить его на «вирусы». Если у него возникли сомнения, то он вправе пригласить ответственного за обеспечение безопасности ИСПДН для повторной проверки.

17. Пользователю категорически запрещается открывать подозрительные почтовые сообщения и вложенные в них файлы.

18. Пользователь обязан немедленно прекратить работу за компьютером, и обратится к ответственному за обеспечение безопасности ИСПДн для выяснения причин и выработки мер восстановления нормального функционирования корпоративной сети в случаях:

- подозрения на заражение вирусами;
- обнаружения заражения вирусами;
- нарушением безопасности работы сети.

19. Каждый пользователь в индивидуальном порядке отвечает за понимание и правильное отношение к правилам безопасности систем, которые они используют.

20. В программах, использующие парольную защиту, пользователи обязаны выбирать качественные пароли и периодически самостоятельно менять их.

IV. Ответственность пользователей сети

21. Пользователи, нарушившие нормальное (безопасное) функционирование сети, повлекшее за собой материальный и моральный ущерб организации, должностным лицам и пользователям сети несут ответственность.

22. Ответственность пользователей сети должна определяться действующим законодательством и административными мерами.

23. Административные меры должны быть соизмеримы с объектом ответственности.

V. Пользователям запрещается

24. Самостоятельно переставлять и передвигать, а также подключать компьютерную технику в помещении (в том числе при проведении генеральных уборок, перестановке мебели и пр.).

25. Самостоятельно производить установку, настройку, модификацию и тестирование сетевого аппаратного или программного обеспечения.

26. Передавать по сети информацию, оскорбляющую честь и достоинство других абонентов сети, содержащую призывы к насилию, разжиганию межнациональной розни, информацию в зашифрованном виде, а также передавать информацию за пределы организации, если это не входит в должностные обязанности пользователей.

27. Использовать ресурсы корпоративной сети для осуществления любого рода личной или посторонней коммерческой деятельности.

28. Предпринимать какие-либо действия прямо или косвенно направленные на нарушение нормальной работы сетевого оборудования и разрушение общих информационных ресурсов.

29. Передавать кому-либо свой пароль, работать под чужим регистрационным именем, а также осуществлять любые действия, связанные с получением паролей и регистрационных записей.

VI. Безопасность и устойчивость сети

30. Составляющие безопасности сети:

- конфиденциальность - защита от несанкционированного получения информации;
- целостность - защита от несанкционированного изменения информации;
- доступность - защита от несанкционированного удержания информации и ресурсов.

Прямое или косвенное нарушение одной из данных составляющих является нарушением безопасности сети.

31. Ответственный за обеспечение безопасности ИСПДн обязан обеспечивать и поддерживать безопасность всех компонентов ЛВС.

32. Ответственный за обеспечение безопасности ИСПДн должен обеспечивать антивирусную защиту программного обеспечения.

33. Для обеспечения устойчивости и безопасности сети ответственный за обеспечение безопасности персональных данных в ИСПДн обязан проводить регулярные регламентные работы.