Правила работы в локальной вычислительной сети

1. Общие правила работы

1.1 Работа в локальной вычислительной сети (ЛВС) производится сотрудниками предприятия с целью получения необходимой информации для выполнения возложенных на них должностных обязанностей.

1.2 Работа в ЛВС предприятия производится с помощью базового компьютера и иных дополнительных устройств.

1.3 Запрос на установку базового компьютера, его настройку и установку сетевого программного обеспечения осуществляется руководителем подразделения по предварительной письменной заявке, написанной на имя Генерального директора предприятия в виде служебной записки.

1.4 Для идентификации пользователя ЛВС сотруднику выдается имя (учетная запись) и пароль. Имя и пароль необходимы для идентификации в ЛВС предприятия и получении доступа к ресурсам сети (сетевым дискам, принтерам и программам). Имя и пароль сотрудника должны быть уникальны в сети. За уникальность и сохранность пароля отвечает пользователь. Пароль – информация конфиденциальная, конфиденциальность обеспечивается самим пользователем и средствами операционных систем.

1.5 Запрещается сообщать пароль другим пользователям ЛВС и работать под чужим паролем.

1.6 Пользователи ЛВС обязаны ознакомиться с данными правилами.

2. Технические нормы и правила

2.1. Для каждого управления (отдела) выделено дисковое пространство на сервере в соответствии с текущими квотами, для хранения документов, связанных с выполнением должностных обязанностей.

2.2. При входе в ЛВС под своим именем и паролем происходит автоматическое подключение сетевого диска. В зависимости от того в каком отделе зарегистрирован пользователь будет доступен тот или иной сетевой диск. Никто, кроме сотрудников своего отдела и администраторов сети, не имеет доступ к информации, хранящиеся на сетевом диске.

2.3. Для обмена информацией между отделами доступен общий ресурс – автоматически подключаемый сетевой диск. Доступ к этому сетевому диску имеют абсолютно все зарегистрированные пользователи сети. Хранить документы на общем ресурсе не рекомендуется, т.к. он автоматически очищается в ночь на первое число каждого месяца. За удаление информации на нем администраторы сети ответственности не несут.

2.4. Категорически запрещается выкладывать важную информацию на общих ресурсах ЛВС. За размещение на общем ресурсе сети важной информации персональную ответственность несет пользователь, выложивший ее.

2.5. По умолчанию, в соответствии с корпоративной политикой любому вновь зарегистрировавшемуся пользователю доступ к локальным и сетевым дисководам, CD-ROM, портам USB запрещен.

2.6. 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 в отдел технического (программного) обеспечения.

2.7. Поддержка и сопровождение установленного системного и сетевого программного обеспечения осуществляется отделом технического обеспечения.

2.8. При необходимости использования нового программного обеспечения, пользователь обязан согласовать его использование с начальником отдела технического обеспечения.

2.9. По первому требованию технического специалиста пользователь обязан освободить компьютер для контроля или выполнения регламентных работ.

2.10. Все действия, связанные с установкой программного обеспечения, а также предоставлением доступа к конкретным ресурсам сети, осуществляются по предварительной письменной заявке, написанной на имя генерального директора, в виде служебной записки.

2.11. Ответственность за работоспособность клиентского программного обеспечения рабочих станций сети подразделения несут отделы технического и программного обеспечения.

2.12. В ЛВС предприятия установлено ограничение на объем отправляемой и принимаемой корреспонденции.

2.13. Системный администратор предприятия ведет перечень базовых компьютеров сети организации. Каждая запись содержит следующую информацию:

тип компьютера;

используемая операционная система;

составляющие системного блока (дополнительные устройства);

модель монитора;

IP-адрес компьютера;

ресурсы, предоставляемые другим компьютерам;

список установленного программного обеспечения;

ФИО ответственного пользователя;

дата заполнения.

2.14. В ЛВС осуществляется мониторинг сетевых событий. Перечень событий, подлежащих протоколированию, определяется отделом технического обеспечения. Полученные при этом электронные журналы событий используются системным администратором для анализа работы сети, а также могут служить доказательством неправомерных действий пользователей.

3. Права и обязанности пользователей сети

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

3.2. В случае получения носителя информации из сомнительного источника пользователь обязан проверить его на «вирусы». Если у него возникли сомнения, то он вправе пригласить специалиста из технического отдела для повторной проверки.

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

3.4. Пользователь обязан немедленно прекратить работу за компьютером, и обратится к специалистам технического отдела для выяснения причин и выработки мер восстановления нормального функционирования корпоративной сети в случаях:

подозрения на заражение вирусами;

обнаружения заражения вирусами;

нарушением безопасности работы сети.

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

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

3.7. В целях защиты от подбора системного пароля пользователя наложено ограничение: при неправильном вводе пароля более 5 раз, учетная запись пользователя блокируется. Блокировку может снять только системный администратор (специалист технического отдела).

3.8. Для надежной и безопасной работы основных сервисов функционирующих в сети, а также информации пользователей, отдел технического обеспечения обязан проводить полное или частичное резервное копирование баз данных по плану проведения резервного копирования.

4. Ответственность пользователей сети

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

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

4.3. Административные меры должны быть соизмеримы с объектом ответственности.

5. Пользователям запрещается

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

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

5.3. 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.

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

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

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

6. Безопасность и устойчивость сети

6.1. 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 компонент является нарушением безопасности сети.

6.2. Отдел технического обеспечения обязан обеспечивать и поддерживать безопасность всех компонентов ЛВС.

6.3. Отдел технического обеспечения должен обеспечивать антивирусную защиту программного обеспечения.

6.4. Для обеспечения устойчивости и безопасности сети отдел технического обеспечения обязан проводить регулярные регламентные работы.