	Код
Форма по ОКУД	
по ОКПО	60886984

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ
«ЦЕНТР КУЛЬТУРЫ И СПОРТА «ГЕОЛОГ» ГОРОДА САЛЕХАРДА
(наименование организации)

Номер документа	Дата составления
66/од	01.10.2021

ПРИКАЗ

**Об утверждении инструкции
по работе в сети Интернет в муниципальном автономном учреждении культуры
«Центр культуры и спорта «Геолог» города Салехарда**

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 03.04.2020),

п р и к а з ы в а ю:

1. Утвердить инструкцию по работе в сети Интернет в муниципальном автономном учреждении культуры «Центр культуры и спорта «Геолог» города Салехарда, согласно приложению к настоящему приказу (далее – инструкция).
2. Отделу кадровой работы и делопроизводства ознакомить с настоящим приказом работников учреждения.
3. Системному администратору отдела обеспечения безопасности и жизнедеятельности, осуществлять контроль за соблюдением работниками учреждения инструкции по работе в сети Интернет.
4. Признать утратившим силу приказ от 16.10.2020 № 82/од «Об утверждении инструкция по работе в сети Интернет в муниципальном бюджетном учреждении культуры «Центр культуры и спорта «Геолог» города Салехарда».
5. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. директора Е.В. Макарова

Ознакомление на обороте:

Утверждена
приказом МАУК ЦКиС «Геолог»
от 01.10.2021 № 66/од

Инструкция
по работе в сети Интернет в муниципальном автономном учреждении культуры «Центр культуры и спорта «Геолог» города Салехарда

1. Общие положения

1.1. Настоящая инструкция разработана с целью регламентации использования сетевых сервисов и работы в сети Интернет в муниципальном автономном учреждении культуры «Центр культуры и спорта «Геолог» города Салехарда (далее – Учреждение).

2. Работа в сети Интернет

2.1. Пользователи используют программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей.

2.2. Все программы, используемые для доступа к сети Интернет, должны быть утверждены системным администратором и на них должны быть настроены необходимые уровни безопасности.

2.3. Использование сети Интернет разрешается только в рабочее время.

2.4. Все файлы, загружаемые с помощью сети Интернет, должны проверяться на вирусы с помощью утвержденных в Учреждении антивирусных программ.

2.5. Во время работы в сети Интернет запрещается:

2.5.1. использование сети Интернет в коммерческих целях;

2.5.2. преднамеренная рассылка вирусов через сеть Интернет;

2.5.3. предоставление служебной информации для общего доступа, а также информации, касающейся устройства и архитектуры локальной вычислительной сети (ЛВС), в т.ч. схемы ЛВС и ее сегментов, точек подключения, информацию о назначенных рабочим станциям IP адресах и именах, используемых на серверах, средствах удаленного доступа и т.п.;

2.5.4. предоставление любой информации в общий доступ на рабочей станции;

2.5.5. распространение через сеть Интернет информации, запрещенной действующим законодательством или не соответствующей морально-этическим нормам ее получателей, а также рассылка обманных, беспокоящих или угрожающих сообщений и рассылка незапрашиваемых сообщений (спама);

2.5.6. размещение в гостевых книгах, форумах, конференциях сообщения, содержащие грубые и оскорбительные выражения.

2.5.7. скачивание и запуск исполняемых файлов без согласования с системным администратором;

2.5.8. использование анонимных прокси-серверов.

3. Работа с электронной почтой:

3.1. Электронная почта предоставляется сотрудникам Учреждения только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.

3.2. Все электронные письма, создаваемые и хранимые на компьютерах Управления, являются собственностью Учреждения и не считаются персональными.

3.3. Учреждение оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины. Содержимое электронного письма не может

быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.

3.4. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы. Использование внешних почтовых сервисов запрещено.

3.5. Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.

3.6. Нельзя открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.

3.7. Справочники электронных адресов сотрудников Учреждения не могут быть доступны всем и являются конфиденциальной информацией.

3.8. Никто из посетителей или временных служащих не имеет права использовать электронную почту Учреждения.

3.9. Пользователи не должны позволять кому-либо посылать письма от чужого имени.

3.10. Нельзя осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

3.11. Почтовые сервера должны быть сконфигурированы так, чтобы отвергать письма, адресованные не на компьютеры Учреждения.

3.12. Журналы почтовых серверов должны проверяться на предмет выявления использования неутвержденных почтовых клиентов сотрудниками Учреждения, и о таких случаях должно докладываться ответственному за защиту информации.

4. Ответственность

4.1. Вся информация о ресурсах, посещаемых сотрудниками Учреждения, протоколируется и, при необходимости, может быть предоставлена руководителям подразделений, а так же руководству Учреждения для детального изучения.

4.2. Контроль за соблюдением настоящих правил возлагается на лицо исполняющего функции системного администратора Учреждения. В случае выявления нарушений и злоупотреблений могут быть применены нижеуказанные меры на установленный период или до устранения причин, повлекших за собой принятие настоящих мер:

4.2.1. Персонально к нарушителю:

- отключение доступа в сеть Интернет;
- лишение возможности работы за компьютером;
- уменьшение ежемесячной нормы потребления трафика;
- ограничение доступа к информационным ресурсам сети Интернет;
- ограничение на использование электронной почты;
- принятие административных мер воздействия.

4.2.2. К рабочей станции или серверу:

- отключение доступа в сеть Интернет;
- отключение возможности работы в локальной сети;
- физическое отключение от ЛВС;
- удаление информации из общего доступа.