

УТВЕРЖДАЮ

И.о. директора ИЛФ СО РАН

Шайхисламов И.Ф.

«03» мая 2023 г.

Инструкция

по регламентации работы пользователей локальной вычислительной сети ИЛФ СО РАН

1. Общие положения.
2. Порядок предоставления доступа к работе в локальной вычислительной сети (ЛВС).
3. Требования по информационной безопасности к пользователю ЛВС.

1. Общие положения.

1.1. Инструкция по регламентации работы пользователей в локальной вычислительной сети (далее - ЛВС) в процессе ее промышленной эксплуатации (далее - Инструкция) предназначена для руководителей и сотрудников ИЛФ СО РАН (далее - Институт) и регулирует порядок допуска пользователей к работе в ЛВС.

1.2. Положения Инструкции обязательны для исполнения всеми пользователями ЛВС.

1.3. Все пользователи ЛВС должны быть ознакомлены с Инструкцией и предупреждены о возможной ответственности за ее нарушение.

2. Порядок предоставления доступа к работе в ЛВС.

2.1. Для работы в ЛВС каждый пользователь должен получить соответствующий доступ. Под доступом понимается получение каждым пользователем ЛВС разрешения начальника структурного подразделения (или ответственного должностного лица) на право работы с информацией в ЛВС с учетом его служебных обязанностей и необходимости наличия доступа в сеть Интернет.

2.2. Руководитель структурного подразделения (или ответственное должностное лицо) передает информацию о сотрудниках, которым по служебным обязанностям необходим доступ к информации, находящейся в ЛВС, и (или) доступ в сеть Интернет, в отдел по информационным технологиям и безопасности (далее - ОИТиБ). При этом руководителем структурного подразделения определяются права доступа пользователей и разделы информации, на которые распространяется доступ.

2.3. Доступ пользователей к работе в локальной вычислительной сети организует администратор ЛВС при получении разрешения от начальника структурного подразделения (или ответственного должностного лица).

3. Требования по информационной безопасности к пользователю ЛВС.

3.1. В соответствии с требованиями нормативных документов и положениями эксплуатационной документации на ЛВС к пользователям предъявляются требования по информационной безопасности, знание и выполнение которых каждым пользователем строго обязательно.

3.2. Пользователь ЛВС обязан:

- знать правила информационной безопасности и принятые меры по защите ресурсов ЛВС (в части его касающейся);
- рассматривать выполнение обязанностей по информационной безопасности как обязательное условие при работе в ЛВС;
- при работе на своём автоматизированном рабочем месте (далее - АРМ), а также работе в ЛВС, выполнять только служебные задания;
- при необходимости установки на рабочей станции дополнительного программного обеспечения (далее - ПО) обращаться с соответствующей служебной запиской к руководителю структурного подразделения;
- не отключать установленные администратором ЛВС антивирусные средства;
- при появлении оповещений от антивирусных средств об обнаружении вредоносных программ немедленно сообщить об этом администратору ЛВС;
- в случае необходимости использования переносных носителей информации, поступивших из других подразделений, учреждений, предприятий и организаций, прежде всего провести проверку этих носителей на отсутствие вредоносных программ штатными средствами антивирусного ПО, установленного на АРМ;

- при решении задач с защищаемой информацией использовать только учтенные носители информации, которые прошли проверку в отделе ИТиБ;
- немедленно выполнять предписания администратора ЛВС, относящиеся к работе в локальной вычислительной сети;
- предоставлять свою рабочую станцию администратору ЛВС для контроля.

3.3. Требования к пользователю по сохранности пароля:

3.3.1. Все пользователи ЛВС обязаны:

- выполнять требования парольной политики при работе на АРМ (см. Приложение 1);
- сохранять пароль в тайне;
- не сообщать свой пароль другому лицу, даже если это должностное лицо;
- вводить личный пароль и другие учетные данные только убедившись, что клавиатура находится вне поля зрения других лиц.

3.3.2. Пользователю запрещается фиксировать свои учетные данные (пароли, идентификаторы) на твердых носителях.

3.4. Пользователю ЛВС запрещается:

- самовольно вносить изменения в конструкцию, конфигурацию, подключение АРМ к сети и другие элементы ЛВС;
- самостоятельно производить установку любого ПО;
- оставлять свою рабочую станцию, авторизованную в сети, без контроля;
- допускать к подключенной в сеть АРМ посторонних лиц;
- запускать на своей рабочей станции или другой рабочей станции сети любые системные или прикладные программы, не входящие в состав программного обеспечения АРМ (см. Приложение 2);
- иметь игровые программы на АРМ;
- работать с защищаемой информацией с использованием неучтенных носителей информации;
- производить копирование защищаемой информации на неучтенные носители информации (в том числе и для временного хранения информации);
- работать на АРМ с защищаемой информацией при обнаружении любых нарушений в работе АРМ или появлении сообщений о наличии вредоносных программ.

3.5. Ответственность пользователя при работе в сети:

3.5.1. Пользователь несет персональную ответственность за соблюдение установленных требований во время работы в ЛВС.

3.5.2. Ответственность за допуск пользователя к ЛВС и установленные ему полномочия несет руководитель структурного подразделения, подтвердивший полномочия данного пользователя.

3.5.3. Пользователи ЛВС, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по Закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством России.

Приложения:

1. Парольная политика, используемая на АРМ пользователей в ЛВС ИЛФ СО РАН.
2. Перечень программного обеспечения, устанавливаемого при первичной настройке АРМ пользователя ЛВС ИЛФ СО РАН.

Начальник отдела ИТиБ



В.Н. Басов

Парольная политика, используемая на АРМ пользователей в ЛВС ИЛФ СО РАН

1. Настройку парольной политики рабочих станций домена осуществляет администратор ЛВС.
2. Парольная политика включает в себя следующие положения:
 - наличие пароля обязательно;
 - наименьшая длина пароля составляет 8 символов;
 - пароль отвечает требованиям к сложным паролям (используются символы не менее трех из четырех категорий – заглавные буквы латинского алфавита, строчные буквы латинского алфавита, цифры, символы, отличающиеся от букв и цифр);
 - минимальный срок действия пароля составляет 1 день;
 - максимальный срок действия пароля составляет 90 дней;
 - количество неудачных попыток входа блокировки учетной записи пользователя составляет 3 раза;
 - время блокировки учетной записи пользователя после исчерпания разрешенного количества неудачных попыток входа составляет 3 минуты;
 - текущий пароль не может повторять ни одного из 3-х предыдущих паролей.

**Перечень программного обеспечения,
устанавливаемого при первичной настройке АРМ пользователя ЛВС ИЛФ СО РАН**

1. Первичная настройка АРМ выполняется сотрудником ОИТиБ.
2. В процессе первичной настройки АРМ может быть установлено следующее системное ПО:
 - операционная система семейства «Microsoft Windows»;
 - операционная система семейства «Linux»;
 - драйверы для системной платы и установленных на неё внутренних устройств;
 - драйверы подключаемого к станции периферийного оборудования.
3. В процессе первичной настройки АРМ может быть установлено следующее прикладное ПО:
 - пакет программ офисного назначения «Microsoft Office»;
 - пакет программ офисного назначения «Libre Office» / «Open Office»;
 - пакет антивирусных программ «Kaspersky Endpoint Security»;
 - веб-обозреватель (один или несколько) «Mozilla Firefox», «Google Chrome», «Яндекс-браузер», «Спутник»;
 - программа для работы с архивированными файлами в формате ZIP «7-Zip»;
 - программа для просмотра и преобразования электронных документов в формате PDF «PDF24»;
 - программа для просмотра и преобразования матричных графических файлов различных форматов «XnView»;
 - программа для просмотра электронных документов в формате DJVU «STDU Viewer»;
 - программа включения классического интерфейса операционных систем семейства «Microsoft Windows» «Classic Shell».