МФТИ it
УПРАВЛЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ИНСТРУКЦИЯ

пользователя персонального компьютера МФТИ

1. Общие положения

1.1. Инструкция определяет права и обязанности пользователей персональных компьютеров (далее - ПК) МФТИ и обязательна для выполнения всеми сотрудниками МФТИ, работающими на постоянной или временной основе.

1.2. Данная инструкция разработана на основе:

- Положения об информационно-технологическом пространстве МФТИ;
- Положения о корпоративной сети передачи данных (далее - КСПД) МФТИ;
- Положения об антивирусной защите МФТИ.

1.3. Целью настоящей инструкции является:

- регулирование работы пользователей с компьютерным оборудованием, КСПД и программным обеспечением (далее - ПО);
- распределение сетевых ресурсов коллективного пользования;
- определение мер по поддержанию необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к ней, обеспечение отсутствия контрафактного ПО;
- уменьшение рисков умышленного или неумышленного неправильного использования сетевых ресурсов, ПО;
- предотвращение ненадлежащего использования компьютерного оборудования, КСПД и ПО.

1.4. Действие настоящих правил распространяется на пользователей любого компьютерного оборудования (компьютеры, компьютерная периферия, коммуникационное оборудование), подключенного к КСПД предприятия, а также на пользователей, осуществляющих удаленный доступ к оборудованию из КСПД и удаленный доступ к КСПД.

1.5. Управление информационных технологий (далее - УИТ) в лице отдела эксплуатации аппаратных систем и программных средств (далее - ОЭАСПС) имеет право проверять исполнение положений данной инструкции без предварительного уведомления пользователей.

2. Порядок работы

2.1. К работе на ПК допускаются сотрудники МФТИ, работающие на постоянной и временной основе, прошедшие инструктаж и получившие средство аутентификации пользователя в КСПД МФТИ – корпоративный аккаунт (логин пользователя и пароль), в соответствии с «Положением об информационно-технологическом пространстве МФТИ»

2.2. Доступ к информационным системам (далее - ИС) МФТИ, доступ к которым не осуществляется с помощью корпоративного аккаунта, предоставляется в соответствии с «Регламентом

управления правами и предоставления доступа пользователям в информационные системы МФТИ»

2.3. Работа в КСПД каждому работнику разрешена только на определённых компьютерах, только в определённое время, с использованием только своего корпоративного аккаунта, только с разрешенными программами и сетевыми ресурсами.

2.4. Пользователь, подключенного к КСПД компьютера — лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

2.5. Все пользователи ПК МФТИ, получают ограниченный уровень доступа к ресурсам своих компьютеров (уровень пользователя) и обязаны работать только с разрешенным уровнем доступа. Административный доступ к своему ПК может быть предоставлен пользователю в обоснованных исключительных случаях на основании служебной записки на имя начальника ОЭАСПС установленного образца и подписания соглашения локального администратора.

2.6. Сотрудники ОЭАСПС, с целью повышения уровня безопасности работы КСПД и проведения плановых работ по техническому обслуживанию ПК, могут без уведомления пользователей проводить соответствующие работы (инсталляция нового ПО по сети на компьютеры пользователей, установка обновлений операционных систем и ПО, сканирование на вирусы и др.)

2.7. Установку, удаление, модернизацию, настройку операционной системы, ПО и иные подобные действия на компьютерах пользователей, обслуживаемых УИТ, могут выполнять только сотрудники ОЭАСПС.

3. Обязанности

Пользователь ПК обязан:

3.1. Ознакомиться с настоящей инструкцией и правилами работы в КСПД до начала работы на компьютерном оборудовании.

3.2. Пользоваться только разрешенным типовым ПО и не допускать использования ПО с нарушением лицензионных соглашений.

3.3. Пройти инструктаж в службе технической поддержки ОЭАСПС и лично получить корпоративный аккаунт для работы в КСПД.

3.4. Самостоятельно создать пароль для входа на ПК. Пароль должен содержать не менее 8 символов и состоять из букв и цифр. Пароль не должен совпадать с днем рождения пользователя или его номером телефона и прочей информацией, которую можно легко подобрать путем сопоставления с данными пользователя.

3.5. В случае, если пользователь забыл свой пароль, он должен обратится в техническую поддержку ОЭАСПС и попросить изменить пароль. В этом случае оператор технической поддержки имеет право потребовать, чтобы пользователь лично явился к нему и предъявил паспорт. Если пользователь забыл свой пароль от используемых ИТ сервисов, но помнит пароль от личного

кабинета на сайте mipt.ru, то он может самостоятельно восстановить (сменить) пароль через личный кабинет.

3.6. Пользоваться только своим корпоративным аккаунтом для входа на ПК и доступа к сетевым сервисам. Передача данных корпоративного аккаунт кому-либо запрещена.

3.7. Использовать компьютерное оборудование исключительно для деятельности, предусмотренной служебной необходимостью и должностными инструкциями. Использование их в других целях (для компьютерных игр, просмотра фильмов развлекательного характера, посещения социальных сетей, неслужебной переписки по электронной почте) запрещено.

3.8. Бережно относиться к оборудованию, соблюдать правила его эксплуатации. В конце рабочего дня выключать компьютер.

3.9. Пользователю КСПД рекомендуется хранить файлы и данные, с которыми он работает, только в сетевых папках (сетевых дисках). Эта мера гарантирует сохранность данных.

3.10. Рационально пользоваться ограниченными разделяемыми ресурсами (дисковой памятью компьютеров и сетевых папок, в том числе общего пользования, пропускной способностью локальной сети) и расходными материалами.

3.11. Обработка электронных документов и баз данных должна производиться только теми программами, которые для этого предназначены.

3.12. Выполнять требования сотрудников ОЭАСПС, а также лиц, назначенных ответственными за эксплуатацию конкретного оборудования.

3.13. Выполнять обязательные рекомендации и предписания сотрудников ОЭАСПС, направленные на обеспечение безопасности КСПД.

3.14. Предоставлять доступ к сетевому оборудованию, ПК, печатающим устройствам сотрудникам ОЭАСПС для проверки исправности и соответствия установленным правилам работы.

3.15. Немедленно сообщать в техническую поддержку ОЭАСПС об обнаруженных проблемах в использовании предоставленных ресурсов (несанкционированный доступ к оборудованию, информации, ее искажение или уничтожение), а также о фактах нарушения настоящей инструкции кем-либо. ОЭАСПС, при необходимости, с привлечением других специалистов и службы безопасности МФТИ, должны провести расследование указанных фактов и принять соответствующие меры.

3.16. Сообщать в ОЭАСПС об известных каналах утечки информации, способах и средствах обхода или разрушения механизмов защиты информации.

3.17. При появлении сообщений антивирусного ПО о потенциальной опасности или факте заражения, немедленно сообщить об этом в ОЭАСПС и далее действовать по его указаниям.

3.18. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь обязан сообщить об этом в техническую поддержку ОЭАСПС.

3.19. Работники МФТИ, допущенные к обработке на ПК персональных данных, обязаны соблюдать «Положение о защите персональных данных МФТИ»; допущенные к обработке на ПК

конфиденциальной информации, охраняемой в режиме коммерческой тайны, обязаны выполнять положение «О режиме коммерческой тайны в МФТИ».

3.20. Работники МФТИ, использующие при работе на ПК электронно-цифровые подписи (далее ЭЦП), обязаны соблюдать правила использования ЭЦП, изложенные в «Инструкции по делопроизводству МФТИ». Использовать только свою ЭЦП, на передавать кому-бы то ни было электронный носитель ЭЦП, не копировать ЭЦП, не сообщать пин-код от носителя ЭЦП. Не использовать ЭЦП при наличии оснований полагать, что конфиденциальность данной ЭЦП нарушена.

4. Права

Пользователь ПК имеет право:

4.1. Подать заявку в техническую поддержку ОЭАСПС на получение прав доступа к сетевым ресурсам группового использования.

4.2. Подать заявку в техническую поддержку ОЭАСПС на устранение неисправности аппаратной и программной части ПК.

4.3. Подавать заявки на закупку нового и модернизацию компьютерного оборудования персонального пользования.

4.4. Получать консультацию у сотрудников ОЭАСПС по работе с компьютерным оборудованием и программным обеспечением общего пользования, по вопросам компьютерной безопасности.

5. Ограничения

Пользователям ПК запрещается:

5.1. Допускать посторонних лиц к работе на закрепленном компьютере (кроме случаев, связанных с выполнением работ специалистами ОЭАСПС в рамках своих служебных и должностных обязанностей, или по указанию руководителя подразделения).

5.2. Использовать ПК, печатающие устройства, сетевые ресурсы для деятельности не обусловленной служебной необходимостью и должностной инструкцией.

5.3. Создавать помехи работе других пользователей, работе компьютеров и сети.

5.4. Самостоятельно устанавливать или удалять любое ПО на компьютерах, изменять настройки операционной системы и приложений.

5.5. Повреждать, уничтожать или фальсифицировать информацию, размещенную на ПК, серверах и сетевых папках.

5.6. Вскрывать компьютеры, сетевое и периферийное оборудование, разбирать, изменять настройку оборудования общего пользования, подключать к компьютеру дополнительное оборудование без ведома сотрудников ОЭАСПС, изменять настройки BIOS, а также производить загрузку ПК с дискет, дисков, FLASH-накопителей и др.

5.7. Самовольно подключать компьютер к КСПД, а также изменять IP и MAC-адрес компьютера, выданный ОЭАСПС, устанавливать дополнительные сетевые протоколы, изменять конфигурацию настроек сетевых протоколов. Передача данных в сеть с использованием других IP и MAC адресов в качестве адреса отправителя, является распространением ложной информации и создает угрозу безопасности информации на других компьютерах.

5.8. Пользователю ПК запрещается оставлять без присмотра компьютер, на котором выполнен вход в операционную систему (например, на обеденный перерыв). Обязательно использование экранных заставок с паролем, которые не позволяют нелегальному пользователю получить доступ к компьютеру в отсутствие владельца (активируется нажатием клавиш Windows+L). Расположение рабочего места пользователей, работающих с информацией конфиденциального характера, должно исключать просмотр со стороны посторонних лиц документов на столе и информации на мониторах компьютерной техники.

5.9. Получать и передавать в сеть информацию, противоречащую законодательству и нормам морали общества, конфиденциальную информацию, распространять через сеть информацию, которая охраняется законодательством об интеллектуальной собственности, либо задевающую честь и достоинство граждан, а также рассылать обманные, угрожающие и др. сообщения.

5.10. Предпринимать попытки обхода систем безопасности КСПД.

5.11. Использовать иные формы доступа к сети, за исключением разрешенных ОЭАСПС, пытаться обходить установленный межсетевой экран.

5.12. Осуществлять попытки несанкционированного доступа к ресурсам КСПД, проводить или участвовать в сетевых атаках и сетевом взломе. Производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) ПК и серверов КСПД и передаваемой по сети информации, равно как и любых других компьютеров в глобальной сети Интернет.

5.13. Использовать КСПД для распространения рекламы, коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

5.14. Передавать другим лицам данные своего корпоративного аккаунта и параметры доступа к информационным системам МФТИ (логин и пароль) к компьютеру, а также предоставлять доступ к своему ПК пользователям других сетей (например, посредством proxy-server, socks-proxy, open relay и т.п.).

5.15. Использовать, распространять и хранить программы, предназначенные для осуществления несанкционированного доступа, взлома паролей, для нарушения функционирования компьютерного оборудования и компьютерных сетей, а также компьютерные вирусы и любые программы ими инфицированные, использовать, распространять и хранить программы сетевого управления и мониторинга, осуществляющих сканирование сети (различные «трассеры», «сниферы», сканеры портов и т.п.), без письменного разрешения начальника ОЭАСПС, с объяснением служебной необходимости подобных действий.

5.16. Использовать в работе съемные носители информации без разрешения начальника ОЭАСПС, а также неучтенные съёмные носители информации (в том числе для временного хранения или переноса информации). Съемные носители информации, перед началом работы с ними, обязательно должны пройти проверку антивирусной программой.

5.17. В целях обеспечения антивирусной защиты КСПД пользователям запрещается приостанавливать или прекращать работу штатного антивирусного средства.

5.18. Хранить информацию, связанную с деятельностью МФТИ, в сетевых папках с неавторизованным (анонимным) общим доступом.

5.19. Хранить на ПК и в сетевых папках файлы, не относящихся к выполнению служебных обязанностей сотрудника (музыка, фотографии, игры, видео, виртуальные CD и т.п.).

6. Правила работы с электронной почтой

6.1. Электронная почта предоставляется сотрудникам МФТИ только для выполнения ими своих служебных обязанностей. Использование ее в личных целях запрещено.

6.2. Для исполнения своих служебных обязанностей сотрудники МФТИ должны использовать только корпоративную почту.

6.3. Все электронные письма, создаваемые и хранимые на компьютерах и почтовых серверах МФТИ, являются собственностью МФТИ и не считаются персональными.

6.4. МФТИ оставляет за собой право получить доступ к персональной электронной почте работников, если на это будут веские причины. Содержимое электронного письма не может быть раскрыто третьим лицам, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.

6.5. В случае если с помощью электронного письма должна быть послана конфиденциальная информация, она должна быть зашифрована так, чтобы ее мог прочитать только тот, кому она предназначена, с использованием утвержденных на предприятии программ и алгоритмов.

6.6. Вся информация, классифицированная как конфиденциальная, при передаче ее через открытые сети, такие как Интернет, обязательно должна быть предварительно зашифрована.

6.7. Пользователи не должны позволять кому-либо посылать письма от своего имени.

6.8. Пользователям запрещается использовать чужой или несуществующий адрес электронной почты в качестве адреса отправителя.

6.9. В качестве клиентов электронной почты могут использоваться только утверждённые и установленные ОЭАСПС почтовые программы.

6.10. Категорически запрещено открывать или запускать приложения, полученные по электронной почте из неизвестного источника, с подозрительным названием и (или) не затребованные пользователем.

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

6.12. Отправлять по электронной почте, большие файлы (особенно музыку, видео и фото личного характера), за исключением случаев, связанных со служебной необходимостью.

7. Работа с веб-ресурсами

7.1. Пользователям ПК предоставляется право использовать только разрешенные программы для доступа к веб-ресурсам сети Интернет (Интернет браузеры), которые должны быть настроены на необходимые уровни безопасности, и только для выполнения своих должностных обязанностей.

7.2. Использование ресурсов сети Интернет не должно создавать потенциальную угрозу МФТИ.

7.3. Вся информация о сеансах доступа пользователей к ресурсам Интернет (дата, время, длительность, локальный адрес) могут протоколироваться.

7.4. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему соответствующих санкций.

7.5. Сотрудникам МФТИ, пользующимся Интернетом, запрещено передавать (сохранять) материал, который является непристойным, содержит порнографическую информацию, нарушает законодательство РФ в части использования объектов интеллектуальной собственности, а также не относящимся к деятельности МФТИ.

7.6. Все файлы, загружаемые с помощью сети Интернет, должны проверяться на вирусы/шпионское ПО с помощью утвержденных антивирусных программ.

7.7. При работе в Интернет, в случае появления самопроизвольных предложений (требований) установить ПО, расширения, оптимизировать работу Интернет браузеров, подписаться на рассылку и совершить другие, явно незапрашиваемые пользователем действия, всегда отвечать - нет.

7.8. При работе с веб-ресурсами запрещено:

- использование ресурсов Интернета (облачных файловых хранилищ, ftp серверов и др., не принадлежащих МФТИ) для хранения служебной информации;
- устанавливать какие-либо программы или расширения Интернет браузеров, скачанные из Интернет;
- запрещается подписываться на листы рассылок с использованием адресов корпоративной почты, если это не связано с исполнением служебных обязанностей;
- получать и передавать через КСПД информацию, противоречащую законодательству и нормам морали общества, конфиденциальную информацию, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения;
- получать доступ к информационным ресурсам КСПД или сети Интернет, не являющихся публичными, без разрешения их собственника;
- играть в различные online-игры;

- использовать различные сайты и программы для анонимного доступа в сеть Интернет;
- использовать программы для зарабатывания денег в сети Интернет, таких как Spedia, Web Money и им подобных;
- скачивание музыкальных и видео файлов, а также файлов, не имеющих отношения к текущим служебным обязанностям работника.
- посещать социальные сети Интернет, если это не связано с выполнением служебных обязанностей.

8. Ответственность

8.1. Пользователь несёт ответственность за всю информацию, хранящуюся на ПК, а также за его техническое состояние.

8.2. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в КСПД и за ее пределами.

8.3. В зависимости от последствий невыполнения требований настоящей Инструкции, а также других обязательных руководящих документов МФТИ, к пользователю могут быть применены соответствующие меры дисциплинарной ответственности.