Приложение № 5
к приказу Комитета по внешним
связям Санкт-Петербурга
от 27.01.2015 № 1-17

ИНСТРУКЦИЯ
пользователя персонального компьютера при работе в локальной вычислительной сети Смольного в Комитете по внешним связям Санкт-Петербурга

1. Общие положения

Целью настоящей Инструкции является регулирование работы пользователей персональных компьютеров при работе в локальной вычислительной сети Смольного (далее – сеть), а также распределении сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа. Инструкция содержит необходимые требования по обеспечению совместной работы, более эффективному использованию сетевых ресурсов и уменьшению риска неправомерного их использования.

1.1. Государственному гражданскому служащему и работнику, замещающему должность, не являющуюся должностью государственной гражданской службы в Комитете по внешним связям Санкт-Петербурга (далее – Комитет) (далее – пользователь) разрешена работа только на определенных компьютерах, в определенное регламентом время и только с разрешенными программами и сетевыми ресурсами.

1.2. Пользователь подключенного к сети компьютера – лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю прав доступа к компьютеру.

1.3. Каждый пользователь использует индивидуальное «имя пользователя» для своей идентификации в сети, выдаваемое службой технической поддержки в соответствии с заявкой.

1.4. Каждый пользователь самостоятельно задает пароль для входа в компьютерную сеть. При этом пароль должен содержать не менее 6 символов и состоять из букв и цифр. Рекомендации по использованию пароля приведены в Приложении к настоящей Инструкции. Консультацию по использованию пароля можно получить в Управлении информационной безопасности и технической защиты информации Комитета по информатизации и связи (далее – Управление).

1.5. Каждый пользователь должен использовать только свое имя пользователя и пароль для входа в компьютер, локальную сеть и сеть Интернет (если данный ресурс подключен). Передача имени пользователя и пароля третьим лицам, за исключением специалистов Управления для решения служебных задач, категорически запрещена.

1.6. В случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах

несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере, или на каком-либо другом, пользователь должен немедленно сообщить об этом в Управление, сотруднику (работнику) Комитета, назначенному ответственным за защиту информации (далее – специалист, ответственный за защиту информации).

1.7. Специалист, ответственный за защиту информации, – лицо, следящее за правильным функционированием сети и комплексной защитой обрабатываемой информации. Специалист, ответственный за защиту информации, вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на обеспечение безопасности информации и повышение эффективности использования сетевых ресурсов.

1.8. Специалист, ответственный за защиту информации, имеет право отключить компьютер пользователя от сети в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции.

1.9. Управление информирует пользователей, посредством уведомления через электронную почту, обо всех плановых профилактических работах, которые могут привести к частичной или полной неработоспособности сети на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам сети;

1.10. Пользователь должен ознакомиться с настоящей Инструкцией. Обязанность ознакомления пользователя с Инструкцией лежит на специалисте, ответственном за защиту информации, и на руководителе структурного подразделения.

2. Работа за компьютером

2.1. Запрещено самостоятельно вскрывать компьютер и вынимать его комплектующие. При возникновении неисправностей необходимо обратиться в службу технической поддержки Смольного.

2.2. Все кабели, соединяющие системный блок с другими устройствами, следует вставлять (вынимать) только при выключенном компьютере. Исключение составляют USB-устройства, они могут быть подключены к включенному компьютеру.

2.3. Запрещено самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение на компьютере.

2.4. Запрещено аварийно завершать работу компьютера кнопкой «Reset» или отключением от электросети. Необходимо корректно завершать работу компьютера, через кнопку «Пуск» в панели задач. В случае невозможности корректного завершения работы компьютера обращаться в службу технической поддержки Смольного.

2.5. Запрещено подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям.

2.6. Перед началом работы пользователь должен:

включить выключатель сетевого фильтра. При включении кнопка должна начать светиться;

включить источник бесперебойного питания (ИБП) и выждать 5 секунд

(если установлен ИБП);

включить монитор (если выключен);

включить компьютер кнопкой «Power». Дождаться загрузки операционной системы (ОС);

войти в систему, используя свои личные имя пользователя и пароль.

2.7. По завершении рабочего дня компьютер необходимо выключить и обесточить, для этого пользователь должен:

закрыть все открытые программы и документы, сохранив нужные изменения;

с помощью меню «Пуск – Завершение работы» выключить компьютер и дождаться завершения работы;

выключить монитор;

выключить ИБП, нажав кнопку на передней панели (если установлен ИБП);

выключить сетевой фильтр.

2.8. При отключении электроэнергии ИБП позволяет компьютеру оставаться в рабочем состоянии до 5-10 минут. При отключении электроэнергии в помещении пользователь должен в немедленном порядке провести выключение компьютера в соответствии с пунктом 2.7. Инструкции.

3. Общие правила работы в локальной вычислительной сети Смольного

3.1. Пользователи сети обязаны:

3.1.1. Соблюдать правила работы в сети, оговоренные настоящей Инструкцией.

3.1.2. При доступе к внешним ресурсам сети, соблюдать правила, установленные Управлением, для используемых ресурсов.

3.1.3. При уходе с рабочего места, необходимо активизировать средства защиты от несанкционированного доступа к информации при помощи сочетания клавиш «Ctrl+Alt+Del» и выбрав пункт «Блокировка».

3.1.3. Немедленно сообщать в Управление об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции. Управлением проводится расследование указанных фактов и принимаются соответствующие меры.

3.1.4. Не разглашать известную конфиденциальную информацию (имя пользователя и пароль), необходимую для безопасной работы в сети.

3.1.5. Выполнять предписания специалиста, ответственного за защиту информации, направленные на обеспечение безопасности сети.

3.1.6. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в службу технической поддержки.

3.2. Пользователи сети имеют право:

3.2.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках, если иное не предусмотрено по согласованию с Управлением.

3.2.2. Обращаться за помощью в Управление при решении задач с использованием ресурсов сети.

3.2.3. Вносить предложения по улучшению работы с тем или иным ресурсом.

3.3. Пользователям сети запрещено:

3.3.1. Использовать любые программы, не предназначенные для выполнения прямых служебных обязанностей.

3.3.2. Разрешать посторонним лицам пользоваться вверенным пользователю компьютером (кроме случаев подключения/отключения ресурсов, выполняемого специалистами службы технической поддержки по заявке, согласованной с Управлением).

3.3.3. Самостоятельно устанавливать или удалять установленные программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.

3.3.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

3.3.5. Вскрывать сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет и других носителей.

3.3.6. Самовольно подключать компьютер к сети, а также изменять настройки сети компьютера. Подключение к сети оборудования, не принадлежащего Комитету, категорически запрещено, так как создает угрозу безопасности информации.

3.3.7. Получать и передавать в сеть информацию, противоречащую действующему законодательству Российской Федерации, представляющую служебную или государственную тайну, а также конфиденциальную информацию, в том числе персональные данные.

3.3.8. Использовать иные формы доступа к информационно-телекоммуникационной сети «Интернет», за исключением способов, разрешенных Управлением.

3.3.9. Осуществлять попытки несанкционированного доступа к ресурсам сети, проводить или участвовать в сетевых атаках и сетевом взломе.

4. Работа с электронной почтой

4.1. Электронная почта предоставляется пользователю только для выполнения своих прямых служебных обязанностей по служебной записке руководителя соответствующего структурного подразделения Комитета. Использование ее в личных целях запрещено. Создание почтового ящика проводится службой технической поддержки по заявке, согласованной с Управлением.

4.2. Комитет оставляет за собой право получить доступ к электронной почте пользователей. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.

4.3. Исходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности.

4.4. Использование электронной почты третьими лицами запрещено.

4.5. В качестве клиентов электронной почты могут использоваться только согласованные Управлением почтовые программы.

5. Работа в информационно-телекоммуникационной сети «Интернет»

5.1. Доступ к информационно-телекоммуникационной сети «Интернет» для пользователей предоставляется по служебной записке руководителя соответствующего структурного подразделения Комитета и только на выделенных для работы с Интернет ресурсом персональных компьютерах.

5.2. Пользователи используют поиск информации в информационно-телекоммуникационной сети «Интернет» только в случае, если это необходимо для выполнения своих должностных обязанностей.

5.3. По использованию Интернет ведется статистика, которая хранится на электронных носителях на Узле телематических служб Смольного.

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

5.5. Пользователям, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство Российской Федерации.

5.6. Программное обеспечение, используемые для работы в информационно-телекоммуникационной сети «Интернет», должно быть согласовано с Управлением.

5.7. При необходимости переноса рабочих материалов, полученных из информационно-телекоммуникационной сети «Интернет», на персональный компьютер пользователя, требуется их проверка при помощи антивирусных программ, согласно Инструкции по организации антивирусной защиты в Комитете по внешним связям Санкт-Петербурга.

5.8. Пользователи, должны соблюдать эту политику после предоставления им доступа к информационно-телекоммуникационной сети «Интернет».

6. Ответственность

6.1. Пользователь отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.

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

6.3. Узел телематических служб Смольного отвечает за бесперебойное функционирование вверенной ему сети, качество предоставляемых пользователям сервисов.

6.4. За нарушение настоящей инструкции пользователь может быть отстранен от работы в сети.

Приложение
к Инструкции пользователя
персонального компьютера при работе
в локальной вычислительной сети
Смольного в Комитете по внешним
связям Санкт-Петербурга

РЕКОМЕНДАЦИИ
по использованию пароля

1. Пароль должен включать в себя алфавитно-цифровые символы. Рекомендуется использовать буквы латинского алфавита. Кроме алфавитно-цифровых символов разрешается использовать, например, символы знаков препинания.
2. Минимальная длина пароля не должна быть менее 6 (шести) символов.
3. Пароль меняется не реже 1 раза в 30 дней.
4. Разрешается не более 6 попыток неверного ввода пароля.
5. Последние 6 паролей не должны повторяться.
6. Пароль для подключения к локальной сети должен регулярно обновляться самим пользователем.
7. Смена пароля пользователя осуществляется после входа в систему под своей учетной записью при помощи комбинации клавиш - Ctrl+Alt+Delete, а затем нажатием кнопки «Смена пароля» и действий в соответствии с предлагаемым алгоритмом (Ввод старого пароля, ввод нового пароля и его подтверждение).