КОПИЯ

Согласовано
Совет КГБПОУ СИЭК
Протокол № 14
«09» декабря 2020 г.

Утверждаю
Директор КГБПОУ СИЭК
Л.М. Шевандронова
«09» декабря 2020 г.

РАБОЧАЯ ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПК ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ (ФАЙЛАМИ) В КГБПОУ СИЭК

г. Спасск-Дальний

2020

1. Общие положения инструкции

1.1. Целью настоящей инструкции является регулирование работы инженера-программиста и пользователей, для эффективного использования и распределения сетевых ресурсов коллективного пользования, поддержания необходимого уровня защиты информации, ее сохранности, соблюдения прав доступа к информации, уменьшение риска умышленного или неумышленного неправильного использования сетевых ресурсов.

1.2. Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью КГБ ПОУ СИЭК и предоставляются работникам для осуществления ими их должностных обязанностей.

1.3. По уровню ответственности и правам доступа к сети пользователи сети разделяются на следующие категории: инженер-программист и пользователи;

1.4. 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 ней;

1.5. Каждый сотрудник может создать и изменять свой пароль для входа в персональный компьютер. Пароль изменяется из пункта меню «Панель управления – Учетные записи пользователей – Изменение своего пароля». Регистр и язык имеют значение. Пользователи должны помнить свои пароли.

1.6. В случае нарушения правил пользования сетью, связанных с используемым им компьютером, пользователь сообщает инженеру-программисту, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений;

1.7. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере ли каком-либо другом, пользователь должен немедленно сообщить об этом инженеру-программисту;

1.8. Пользователи обязаны выполнять предписания инженера-программиста по работе с компьютером и сетью.

1.9. Инженер-программист - лицо, обслуживающее персональные компьютеры КГБ ПОУ СИЭК и следящее за правильным функционированием сети. Инженер-программист дает разрешение на подключение компьютера к сети, выдает IP-адрес

компьютеру, создает учетную запись электронной почты для пользователя. Самовольное подключение является нарушением правил пользования сетью;

1.10. Инженер-программист информирует пользователей 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;

2. Инструкция по работе в локальной сети

2.1. Пользователи сети обязаны:

2.1.1. Соблюдать правила работы в сети, оговоренные настоящей инструкцией;

2.1.2. При доступе к внешним ресурсам сети, соблюдать правила, установленные системными администраторами для используемых ресурсов;

2.1.3. Немедленно сообщать инженеру-программисту об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо. Инженер-программист, при необходимости, с помощью других специалистов, должен провести расследование указанных фактов и принять соответствующие меры;

2.1.4. Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы в сети;

2.1.5. Обеспечивать беспрепятственный доступ инженеру-программисту к сетевому оборудованию и компьютерам пользователей, для организации профилактических и ремонтных работ;

2.1.6. Выполнять предписания инженера-программиста, направленные на обеспечение безопасности сети;

2.1.7. В случае обнаружения неисправности (например, сильный посторонний шум или запах, необычное поведение затрудняющее работу) компьютерного оборудования или программного обеспечения, пользователь должен обратиться к инженеру-программисту.

2.1.8. Удалять с сетевых ресурсов устаревшие или не используемые файлы.

2.2. Пользователи сети имеют право:

2.2.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках. Инженер-программист вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов;

2.2.2. Обращаться к инженеру-программисту по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка на компьютере коллективного доступа), должны санкционироваться инженером-программистом;

2.2.3. Обращаться за помощью к инженеру-программисту при решении задач использования ресурсов сети;

2.2.4. Вносить предложения по улучшению работы с ресурсом.

2.3. Пользователям сети запрещено:

2.3.1. Разрешать посторонним лицам пользоваться вверенным им компьютером (кроме случаев подключения/отключения ресурсов);

2.3.2. Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования с администрацией и инженером-програмистом;

2.3.3. Самостоятельно устанавливать или удалять установленные инженером-программистом сетевые программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;

2.3.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;

2.3.5. Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с инженером-программистом, изменять настройки BIOS, а также производить загрузку рабочих станций с дискет;

2.3.6. Самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданный инженером-программистом. Передача данных в сеть с использованием других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах;

2.3.7. Работать с каналоемкими ресурсами (видео, аудио, радио, чаты, файлообменные сети, torrent и др.) без согласования с системным администратором сети. При сильной перегрузке канала вследствие использования каналоемких ресурсов доступ пользователя вызвавшего перегрузку, может быть прекращен;

2.3.8. Получать и передавать в сеть информацию, противоречащую действующему законодательству РФ и нормам морали общества, представляющую коммерческую или

государственную тайну;

2.3.9. Обхождение учетной системы безопасности, системы статистики, ее повреждение или дезинформация;

2.3.10. Использовать иные формы доступа к сети Интернет, за исключением разрешенных инженером-программистом.

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

2.3.12. Использовать сеть для массового распространения рекламы (спам), коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.

4. Инструкция по работе с электронной почтой

4.1. Электронная почта предоставляется сотрудникам организации только для выполнения своих служебных обязанностей. Использование ее для пересылки файлов в личных целях запрещено. Создание или имение параметров почтового ящика проводится инженером-программистом по просьбе администрации;

4.2. На рабочем месте допускается использовать только ящики электронной почты, предоставленные или одобренные администрацией. Прямой доступ к другим почтовым системам может быть блокирован.

4.3. Все электронные письма, создаваемые и хранимые на компьютерах организации, являются собственностью организации и не считаются персональными;

4.4. Организация оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины.

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

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

5. Инструкция по работе в сети Интернет

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

5.2. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, протоколируются и могут использоваться для принятия решения о применении к нему санкций;

5.3. Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство РФ;

5.4. Все программы, используемые для доступа к сети Интернет, должны быть утверждены инженером-программистом и на них должны быть настроены необходимые уровни безопасности;

5.5. Запрещено получать и передавать через сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения;

5.6. Запрещено обращаться к ресурсам сети Интернет несвязанных непосредственно с выполнением своих должностных обязанностей в рабочее время, а также к ресурсам с сомнительным содержанием.

5.7. Запрещается скачивать и запускать с любых ресурсов любые исполняемые файлы без согласования с инженером-программистом.

6. Работа со съемными носителями информации (Флешки, переносные жесткие диски, цифровые фотоаппараты, телефоны и т.д)

6.1. Подключение съемных носителей следует производить при включенном компьютере и загруженной операционной системой.

6.2. Существует большое количество вирусов предназначенных для повреждения информации на флэшках (эти вирусы на зараженном ПК постоянно загружены в оперативную память и отслеживают порты на предмет подключения съемных устройств), если Вам нужно скопировать информацию с Вашей флэшки на посторонний ПК, перед подключением включайте блокировку записи (если она предусмотрена конструкцией Вашей флэшки).

6.3. Не извлекайте флэшку из ПК в момент обращения к ней, это может привести к потере данных и повреждению устройства. Если же в момент отключения флэшки от ПК выполнялась операция записи, в файловой системе флэшки неизбежно появятся ошибки. Если при попытке извлечь флэшку через значок "Безопасное извлечение устройства" появляется диалоговое окно "Проблема при извлечении "Запоминающее устройство для USB": Устройство Универсальный том не может быть остановлено прямо

сейчас. Попробуйте остановить его позже", значит, открыты какие-то файлы с флэшки. Закройте их и повторите попытку. Для сохранности данных не рекомендуется открывать файлы данных со сменных носителей.

6.4. Рекомендуется совершать обмен файлами данных через электронную почту. Перед копированием файлов данных с внешних носителей настоятельно рекомендуется проверить носитель с помощью антивируса. Запрещается запускать или переписывать с любых внешних носителей любые исполняемые файлы (приложения или командные файлы с расширениями exe, bat, com, cmd, inf, dll, scr) без согласования с системным администратором.

Подписан: Шевандронова Людмила Марсовна
DN: ИНН=251002051306, СНИЛС=04295010330, E=siek25@yandex.ru, C=RU, S=Приморский край, L=Спасск-Дальний, O="КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ "" СПАССКИЙ ИНДУСТРИАЛЬНО-ЭКОНОМИЧЕСКИЙ КОЛЛЕДЖ""", G=Людмила Марсовна, SN=Шевандронова, CN=Шевандронова Людмила Марсовна
Дата: 2021.02.17 08:47:50+10'00'