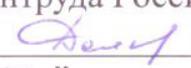


Утверждаю

Руководитель – главный эксперт
по медико-социальной экспертизе
ФКУ «ГБ МСЭ по Ульяновской области»
Минтруда России


“ 01 ” 06 2014 г.

Политика информационной безопасности в ФКУ «ГБ МСЭ по Ульяновской области» Минтруда России

1. Общие сведения

IP-адрес- это сокращение от английского Internet Protocol Address, то есть уникальный идентификатор компьютера, подключенного к сети.

LPT - международный стандарт параллельного интерфейса для подключения периферийных устройств персонального компьютера.

USB-устройство- последовательный интерфейс передачи данных для среднескоростных и низкоскоростных периферийных устройств в вычислительной технике.

АРМ- Автоматизированное рабочее место.

ИБП- Источник бесперебойного питания.

Операционная система (ОС)- программа которая осуществляет диалог с пользователем, управляет компьютером, его ресурсами, запускает другие программы. ОС загружается при включении компьютера.

Периферийные устройства — внешние устройства подключенные к компьютеру (Принтер, сканер, колонки и т.д.)

Пользователь- сотрудник организации, использующий для выполнения служебных обязанностей персональный компьютер, подключенный к ЛВС и информацию, хранящуюся и обрабатываемую в электронном виде.

Программное обеспечение- совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ

ПЭВМ- компьютер, предназначенный для личного использования, цена, размеры и возможности которого удовлетворяют запросам большого количества людей.

Сеть интернет- всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных.

Сервер- компьютер, подключенный к сети, на котором установлена и функционирует административная программа, управляющая доступом ко всей сети или к ее части и ее ресурсам (например, дисками или принтерами), а также предназначенный для хранения файлов базы данных коллективного пользования и для обработки запросов к ним, поступающих от пользователей рабочих станций.

Системный администратор- сотрудник, должностные обязанности

которого подразумевают обеспечение штатной работы парка компьютерной техники, сети и программного обеспечения, а также обеспечение информационной безопасности в организации.

СКЗИ- средства криптографической защиты информации

Спам- массовая рассылка коммерческой, политической и иной рекламы (информации) или иного вида сообщений лицам, не выразившим желания их получать.

Учетная запись- запись, содержащая сведения, которые пользователь сообщает о себе некоторой компьютерной системе.

Файл- законченная именованная совокупность информации, хранящаяся в памяти компьютера.

Электронный ключ- это устройство, предназначенное для защиты программ и данных от несанкционированного использования и тиражирования;

ЭЦП- электронно цифровая подпись.

1. Политика информационной безопасности

1.1. По уровню ответственности и правами доступа к сети пользователи сети разделяются на следующие категории: программист-системные администраторы и пользователи;

1.2. Каждый сотрудник пользуется индивидуальным именем пользователя, выдаваемым отделом информационно-статистического обеспечения, для своей идентификации в сети и в системе ЕАВИИАС МСЭ;

1.3. Каждый сотрудник должен пользоваться только своим именем пользователя и паролем для входа в компьютер, локальную сеть, сеть интернет и в систему ЕАВИИАС МСЭ Передача их кому-либо запрещена;

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

1.5. 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 или каком-либо другом, пользователь должен немедленно сообщить об этом в отдел информационно-статистического обеспечения;

1.6. Отдел информационно-статистического обеспечения - отдел, обслуживающий сервер и следящий за правильным функционированием сети. Отдел информационно - статистического обеспечения дает разрешение на подключение компьютера к сети, выдает IP-адрес компьютеру, создает учетную запись электронной почты и системы ЕАВИИАС МСЭ для пользователя. Самовольное подключение является серьезнейшим нарушением правил пользования сетью;

1.7. Отдел информационно - статистического обеспечения заранее 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;

1.8. Отдел информационно - статистического обеспечения 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.

2. Работа за компьютером

2.1. Запрещено самостоятельно разбирать компьютер и все его комплектующие. При возникновении неисправностей необходимо обратиться в отдел информационно - статистического обеспечения;

2.2. Все кабели, соединяющие системный блок с другим устройствами, следует вставлять и вынимать только при выключенном компьютере. Исключением составляют USB-устройства: они могут быть подключены к включенному компьютеру;

2.3. Запрещено аварийно завершать работу компьютера или отключать от электросети. Завершайте работу компьютера правильно, через кнопку (Пуск);

2.4. Запрещено подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям. (Нельзя ставить у батареи и других нагревательных приборов);

2.5. По завершению рабочего дня компьютер необходимо выключить и обесточить;

2.6. Перед началом работы пользователь должен:

- Включить сетевой фильтр;
- При наличии - включить источник бесперебойного питания (ИБП) и выждать 5 секунд;
- Включить монитор;
- Включить компьютер. Дождаться загрузки операционной системы (ОС);
- Войти в систему, используя свои личные имя пользователя и пароль.

2.7. По завершению работы пользователь должен:

- Закрыть все открытые программы и документы, сохранив нужные изменения;
- С помощью меню «Пуск->Завершение работы» выключить компьютер и дождаться завершения работы. (Системный блок перестанет «мигать» и «шуметь»);
- Выключить монитор;
- При наличии - выключить источник бесперебойного питания (ИБП), нажав кнопку на передней панели;
- Выключить сетевой фильтр.

2.8. При отключении электроэнергии источник бесперебойного питания (ИБП) позволяет компьютеру оставаться в рабочем состоянии от 5 до 10 минут.

При отключении электроэнергии в помещении пользователь должен в немедленном порядке провести правильное выключение компьютера.

2.9 Поддерживать на автоматизированном рабочем месте (АРМ) чистоту и порядок;

2.10 Ежедневно протирать поверхность системного блока слегка влажной (не мокрой) тряпкой при выключенном компьютере.

3. Работа в сети

3.1. Пользователи сети обязаны:

– Немедленно сообщать начальнику отдела информационно - статистического обеспечения об обнаруженных проблемах в использовании предоставляемых ресурсов, а также о фактах нарушения настоящей инструкции кем-либо;

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

– Обеспечивать беспрепятственный доступ специалистам отдела информационно - статистического обеспечения к сетевому оборудованию и компьютерам пользователей для организации профилактических и ремонтных работ;

– В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в отдел информационно- статистического обеспечения;

– При доступе к внешним ресурсам сети Internet, соблюдать правила, установленные отделом информационно - статистического обеспечения для используемых ресурсов;

3.2. Пользователи сети имеют право:

– Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции рамках, если иное не предусмотрено по согласованию с отделом информационно-статистического обеспечения. Специалисты отдела информационно-статистического обеспечения 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;

– Обращаться к программисту-системному администратору 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 отделом информационно-статистического обеспечения;

– Обращаться за помощью в отдел информационно-статистического обеспечения при решении задач использования ресурсов сети;

– Вносить предложения по улучшению работы с ресурсом.

3.3. Пользователям сети запрещено:

– Разрешать посторонним лицам пользоваться вверенным им

компьютером (кроме случаев подключения/отключения ресурсов, выполняемого специалистами отдела информационно-статистического обеспечения);

- Использовать программы, не предназначенные для выполнения прямых служебных обязанностей без согласования со специалистами отдела информационно-статистического обеспечения;

- Самостоятельно устанавливать или удалять установленные отделом информационно-статистического обеспечения программы на компьютерах, подключенных к сети, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов;

- Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю;

- Вскрывать компьютеры, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование без согласования с отделом информационно-статистического обеспечения, а также производить загрузку рабочих станций с дискет, дисков, флешек;

- Самовольно подключать компьютер к сети, а также изменять IP-адрес компьютера, выданным отделом информационно-статистического обеспечения. 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;

- Работать с каналоемкими ресурсами (video, audio, chat и др.) без согласования с начальником отдела информационно-статистического обеспечения. При сильной перегрузке канала вследствие использования каналоемких ресурсов текущий сеанс пользователя, вызвавшего перегрузку, будет прекращен;

- Получать и передавать в сеть информацию, противоречащую действующему законодательству РФ и нормам морали общества, представляющую государственную тайну;

- Обходить учетную систему безопасности, систему статистики, вносить дезинформацию;

- Использовать иные формы доступа к сети Интернет, за исключением разрешенных отделом информационно-статистического обеспечения;

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

- 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. Работа с электронной почтой

4.1. Электронная почта предоставляется сотрудникам организации только для выполнения своих прямых служебных обязанностей. Использование ее в личных целях запрещено. Создание почтового ящика проводится отделом

информационно-статистического обеспечения по служебной записке;

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

4.3. Конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы наиболее безопасными;

5. Эксплуатация электронных ключей и электронных цифровых подписей (ЭЦП)

5.1. Электронный ключ - это устройство, предназначенное для защиты программ и данных от несанкционированного использования и тиражирования;

5.2. Электронный ключ подключается к параллельному (LPT) или USB порту компьютера;

5.3. Электронный ключ для LPT порта при нормальном функционировании не вносит помех в работу принтера и других периферийных устройств, подключенных через него.

5.4. Правила эксплуатации и хранения электронного ключа:

- Оберегайте электронный ключ от механических воздействий (падения, сотрясения, вибрации и т.п.), от воздействия высоких и низких температур, агрессивных сред, высокого напряжения; все это может привести к его поломке;

- Не прилагайте излишних усилий при подсоединении электронного ключа к компьютеру и периферийного устройства к электронному ключу;

- Не допускайте попадания на электронный ключ (особенно на его разъемы) пыли, грязи, влаги и т.п. При засорении разъемов электронного ключа примите меры для их очистки. Для очистки корпуса и разъемов используйте сухую ткань. Использование органических растворителей недопустимо;

- Не разбирайте электронный ключ. Это может привести к поломке его корпуса, а также к порче или поломке элементов печатного монтажа и, как следствие - к ненадежной работе или выходу из строя самого электронного ключа;

В случае неисправности или неправильного функционирования электронного ключа обращайтесь к фирме-разработчику прикладного ПО;

5.5. Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Значение реквизита получается в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП;

5.6. Операторы по использованию ЭЦП обязаны обеспечивать ее сохранность, неразглашение и нераспространение;

5.7. За две недели до окончания срока действия ключей ЭЦП, оператор обязан уведомить об этом уполномоченное лицо;

5.8. В организации должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации с закрытыми

ключами ЭЦП и шифрования, который должен полностью исключать возможность несанкционированного доступа к ним;

5.9. Должен быть утвержден список лиц, имеющих доступ к ключевой информации.

5.10. Для хранения носителей закрытых ключей ЭЦП и шифрования в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами с двумя экземплярами ключей;

5.11. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства АРМ со встроенными СКЗИ;

5.12. Должны быть предусмотрены меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленными СКЗИ;

5.13. Установленное на АРМ программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам;

5.14. Администрирование должно осуществляться доверенными лицами;

5.15. В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям (ЭЦП и шифрования), должна быть проведена смена ключей, к которым он имел доступ;

Не допускается:

- Снимать несанкционированные копии с ключевых носителей;
- Знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным;
- Выводить секретные ключи на дисплей (монитор) ПЭВМ или принтер;
- Устанавливать ключевой носитель в считывающее устройство (дисковод) ПЭВМ АРМ, не предусмотренных функционированием системы, а также в другие ПЭВМ;
- Записывать на ключевой носитель постороннюю информацию.

6. Проведение резервного копирования информационных ресурсов

6.1 Ответственными за резервное копирование информации и базы данных учреждения являются сотрудники отдела информационно-статистического обеспечения.

6.2 Резервное копирование подлежит не реже одного раза в квартал в систему хранения данных (СХД) и содержит копии служебной информации с жестких дисков ПК сотрудников ФКУ «ГБ МСЭ по Ульяновской области» Минтруда России.

6.3 Ежедневному резервному копированию подлежит база данных ЕАВИИАС МСЭ (FMBA_MSE_1361)

6.4 Хранению подлежат текущая копия, и не менее двух предыдущих копий.