

УТВЕРЖДАЮ

Руководитель Государственного бюджетного учреждения «Многофункциональный центр по предоставлению государственных и муниципальных услуг Кабардино-Балкарской Республики»



А.А. Афаунов

2015 г.

ПОЛОЖЕНИЕ
О порядке использования работниками компьютерных и
информационных ресурсов
в Государственном бюджетном учреждении «Многофункциональный
центр
по предоставлению государственных и муниципальных
услуг Кабардино-Балкарской Республики»

Нальчик
2015

I. ОБЩИЕ ПОЛОЖЕНИЯ.

1. Настоящее Положение устанавливает единый порядок использования компьютерных и информационных ресурсов в составе информационной системы ГБУ МФЦ, в отношении всех пользователей компьютерных и информационных ресурсов МФЦ.

2. В настоящем Положении указанные ниже понятия означают следующее:

Информационная система – комплекс компьютерных и информационных ресурсов МФЦ, включая данные, информацию, программное обеспечение, аппаратные средства, средства обслуживания и телекоммуникации, а также средства взаимодействия с другими сетями.

Компьютерные ресурсы – хост-компьютеры, серверы файлов, рабочие станции, автономные компьютеры, мобильные компьютеры, являющиеся как собственностью МФЦ, так и арендуемые у сторонних организаций, и функционирующие, как в локальной сети МФЦ, так и вне ее.

Информационные ресурсы – системы управления базами данных, внутренние и внешние сети связи (интернет, коммерческие интерактивные службы и системы электронной почты), системы общего и внутреннего документооборота, системы юридических баз данных, подсистема формирования отчетности, а также другое программное обеспечение и базы данных, являющиеся как собственностью МФЦ, так и арендуемые у сторонних организаций и функционирующие как в локальной сети МФЦ, так и вне ее.

Пользователи – сотрудники МФЦ, а также независимые подрядчики и другие лица, использующие компьютерные или информационные ресурсы МФЦ.

Сетевое имя – буквенно-цифровой код со специальными символами, служащий для авторизации пользователя в информационной системе МФЦ.

Пароль – секретное слово, которое должен знать пользователь для работы в информационной системе МФЦ. Пароль является составной частью системы авторизации и предоставления прав доступа пользователя к компьютерным и информационным ресурсам МФЦ, а также обеспечивает защищенность информационной системы МФЦ от несанкционированного доступа.

3. Устанавливаемый настоящим Положением порядок призван обеспечить надлежащее использование компьютерных и информационных ресурсов МФЦ их пользователями, и имеет целью предотвращение несанкционированного доступа в информационную систему МФЦ, обеспечение информационной безопасности при эксплуатации компьютерных и информационных ресурсов МФЦ, являющихся как собственностью МФЦ, так и арендуемых у сторонних организаций.

4. Порядок эксплуатации компьютерных и информационных ресурсов МФЦ предполагает следующее:

- к использованию компьютерных ресурсов МФЦ допускаются лица, обладающие навыками работы с компьютерной техникой, необходимыми для квалифицированного выполнения служебных обязанностей;
- пользователи **обязаны** использовать компьютерные ресурсы эффективно, придерживаясь правил этики, соблюдая требования настоящего Положения;

- каждый пользователь лично отвечает за свои действия при работе в информационной системе МФЦ;
- пользователи должны выполнять требования нормативных документов по обеспечению информационной безопасности и **самостоятельно** заботиться о защите и обеспечении конфиденциальности информации, которую они создают, отправляют или получают в электронном виде, вне зависимости от мер безопасности, предпринимаемых в этом направлении отделом автоматизации МФЦ;
- в целях обеспечения информационной безопасности сотрудники МФЦ, наделенные соответствующими полномочиями, вправе проверять любой или все элементы информационной системы, включая электронную почту;
- компьютерные и информационные ресурсы, являющиеся как собственностью МФЦ, так и арендуемые у сторонних организаций, должны использоваться сотрудниками МФЦ исключительно в служебных целях.

5. Ненадлежащее исполнение пользователем правил работы с компьютерными и информационными ресурсами МФЦ, установленных настоящим Положением, влечет применение к такому лицу мер дисциплинарного воздействия на усмотрение руководства МФЦ вплоть до увольнения.

II. ОПРЕДЕЛЕНИЕ ПОРЯДКА ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

1. Доступ к информационным ресурсам МФЦ предоставляется ответственными администраторами Отдела Автоматизации (ОА) каждому пользователю индивидуально, в соответствии с должностными обязанностями и исходя из специфики решаемых им задач, на основании заявки установленной формы, подписанной руководителем соответствующего структурного подразделения, в котором работает пользователь.

2. Доступ пользователей к информационным ресурсам МФЦ, содержащим конфиденциальную информацию, предоставляется только с разрешения руководства МФЦ. К данным информационным ресурсам относятся:

Системы и базы данных, содержащие информацию, отнесенную в установленном порядке к служебной или коммерческой тайне.

3. Регистрация лиц, не являющихся сотрудниками МФЦ, производится на основании служебной записки на имя начальника отдела автоматизации, с резолюцией управляющего МФЦ или его заместителей.

4. В случае если обязанности временно отсутствующего сотрудника исполняет другое лицо, не имеющее права доступа к соответствующим компьютерным или информационным ресурсам МФЦ, замещающему сотруднику, по согласованию с руководством данного подразделения, на основании письменной заявки в ОА, с указанием **необходимых сроков**, временно предоставляется доступ к таким ресурсам.

5. Любые изменения прав доступа сотруднику производятся на основании служебной записки начальника соответствующего подразделения с обоснованием.

6. При длительном отсутствии сотрудника на рабочем месте (командировка, отпуск, болезнь и т.п.) доступ к сети данного пользователя может быть заблокирован на время его отсутствия по распоряжению начальника соответствующего подразделения.

7. При увольнении сотрудника МФЦ он лишается права доступа к соответствующим компьютерным и информационным ресурсам со дня, указанного в обходном листе, и через месяц такой пользователь удаляется из сети. Начальник подразделения, в котором

работает увольняемый, должен своевременно подать заявку на предоставление другому сотруднику, замещающему уволенного, необходимого уровня доступа для выполнения работы.

8. При переводе сотрудника в другое подразделение МФЦ, начальник подразделения, в которое сотрудник переведен, должен составить заявку установленной формы на предоставление новых прав доступа переводимому сотруднику.

III. ПОРЯДОК ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНЫХ РЕСУРСОВ

1. Каждый сотрудник несет ответственность за соблюдение правил настоящего Положения.

2. На каждом пользовательском компьютере МФЦ штатным образом должен быть задействован персональный пароль на включение. Пароль на включение определяется пользователями самостоятельно и устанавливается специалистом ОА. Этот пароль должны знать только пользователи, имеющие право работать на данном компьютере, и, в обязательном порядке, сотрудник ОА. Категорически запрещается хранение паролей на включение компьютера в открытом виде на бумажном или электронном носителе.

3. Всякий раз, покидая рабочее место, пользователь обязан выключить компьютер или заблокировать его клавиатурой способом, делающим невозможным доступ к данным, расположенным на компьютере и в локальной сети МФЦ. К средствам блокировки доступа к компьютеру относятся, в частности, программы-заставки типа «screen saver», установленные на обязательное использование пароля. Запустить подобную программу можно при помощи так называемых «горячих» клавиш или специально созданной для этого кнопки или иконки. Детальную консультацию по этим вопросам, а также соответствующую настройку производят сотрудники ОА, ответственные за сопровождение компьютерных ресурсов подразделения.

4. Во избежание заражения компьютерными вирусами файлов локальной сети МФЦ пользователи обязаны периодически проверять информацию на локальном диске, а также всю приходящую извне (получаемую по электронным видам связи, на магнитных носителях и пр.)

5. В случае аппаратных или программных сбоев пользователь обязан зафиксировать выдаваемое сообщение об ошибках и обратиться в ОА.

6. Просмотр и тестирование демонстрационных версий программных продуктов, предлагаемых сторонними разработчиками, должны быть организованы на основании служебной записки на имя начальника ОА, и проводиться с санкции руководства ОА.

7. Для предотвращения несанкционированного доступа к данным и для исключения возможности создания помех при проведении в ночное время процедур резервного копирования данных, сотрудники обязаны выключать компьютеры по окончании рабочего дня, если технологией работы не предполагается иного. Работа вычислительной техники в ночное время в отсутствие сотрудника на рабочем месте должна быть письменно согласована с ОА.

8. Пользователи должны соблюдать условия всех программных лицензий, авторские права, нормативные акты, касающиеся интеллектуальной собственности.

9. Сотрудники, выполнение должностных обязанностей которых вступает в противоречие с требованиями настоящего Положения, обязаны довести данную информацию до сведения ОА.

10. Запрещается:

- Использовать вычислительную технику не по назначению, в т.ч. для хранения неслужебной информации, компьютерных игр и т.п.

- Самостоятельно вносить изменения в конфигурацию программного обеспечения, устанавливать системные и прикладные, включая почтовые, программы, в том числе купленные МФЦ.
- Проносить и использовать на территории МФЦ какое-либо программное обеспечение, вычислительную технику и комплектующие к ней без согласования с ОА.
- Категорически запрещается самостоятельная установка и несанкционированное использование модемов.
- Допуск к работе с вычислительной техникой посторонних лиц.
- Использовать в подразделениях вычислительную технику, не состоящую на учете в МФЦ.

IV. ПОРЯДОК РАБОТЫ В ЛОКАЛЬНОЙ СЕТИ МФЦ И ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ

1. В целях обеспечения безопасности и надежности хранения данных в информационной системе МФЦ за каждым пользователем закрепляется сетевое имя. При первом входе в информационную систему МФЦ пользователь должен определить известный только ему секретный сетевой пароль. Пользователь несет ответственность за сохранность своих паролей для входа в систему. Индивидуальные пароли запрещено распечатывать, хранить в сети или передавать другим лицам. Пользователи несут полную ответственность за все действия, которые кто-либо совершит с компьютерными и информационными ресурсами МФЦ с помощью их пароля. Порядок назначения и смены сетевых паролей описан в **Приложении № 1 к настоящему Положению**. Этот порядок может меняться с изменением состава программных средств, используемых в МФЦ.
2. Вход в информационную систему Филиала должен осуществляться только под своим сетевым именем **и только на своем рабочем месте**. При необходимости организации группового или технологического (не персонифицированного) рабочего места в информационной системе МФЦ, по согласованию с ОА, создается возможность входа под именем специального пользователя системы с установленным правом доступа, пароль которого должен быть известен только перечисленным в служебной записке сотрудникам.
3. Разглашение кому-либо как личного, так и не персонифицированного сетевого **пароля и работа не на своем рабочем месте** признаются дисциплинарными проступками, подрывающими информационную безопасность МФЦ.
4. Категорически запрещается пересылать по электронной почте или с помощью других средств электронной связи МФЦ, а также отображать и хранить на компьютерах МФЦ материалы, содержащие непристойные изображения, слова или выражения, клеветнические или оскорбительные высказывания, угрозы, противозаконные материалы, а также информацию, не связанную с исполнением служебных обязанностей. Пользователь, получивший подобные материалы, должен незамедлительно сообщить о случившемся своему руководителю.
5. Пользователи при работе с электронной почтой не должны использовать чужое имя отправителя. Пользователям настоятельно рекомендуется указывать в отправляемых по электронной почте письмах тему ("Subject") в логической связи с содержанием сообщения.
6. Пользователям запрещается изменять или копировать расположенный в общих папках Почтовой системы или в сети файл, принадлежащий другому пользователю, не получив предварительно разрешения владельца файла. Возможность читать, изменять или копировать общедоступный файл, принадлежащий другому пользователю, сама по себе не свидетельствует о наличии права читать, изменять или копировать этот файл.

7. Для предотвращения блокировки сетевых программ и разрушения общих (хранящихся в сети) данных запрещается аварийно завершать процесс работы с сетевыми программами какими-либо способами, отличными от штатных (например, выключением или перезагрузкой компьютера).

8. Категорически запрещается хранить информацию, не предназначенную для общего использования всеми сотрудниками МФЦ, и размещать программное обеспечение в каталогах и папках общего доступа информационной системы МФЦ. Данные каталоги предназначены для хранения общедоступных данных и обмена не конфиденциальными данными между пользователями, и поэтому находящаяся в них информация не может быть защищена соответствующим образом.

9. Обеспечение работы с общими данными сотрудников одного или разных подразделений возможно либо через создание рабочих групп пользователей с уникальным уровнем доступа к этим данным, либо через использование средств электронной почты.

10. Запрещается самостоятельно производить подключение компьютеров, сетевых принтеров и других устройств к розеткам локальной и телефонной сети МФЦ без согласования с сотрудниками ОА, ответственными за их эксплуатацию.

V. ПОРЯДОК РАБОТЫ С РЕСУРСАМИ ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

1. Доступ к глобальной сети Интернет рассматривается как доступ к внешним информационным ресурсам, необходимым сотрудникам МФЦ исключительно для решения служебных задач. Регламентирование этого типа доступа преследует две основных цели:

- Снижение рисков, связанных с работой в глобальной сети как неконтролируемой среде, содержащей потенциальные угрозы информационной целостности и работоспособности внутренней информационной системы.
- Оптимизация информационного трафика и контроль за ним с целью повышения эффективности доступа сотрудников к глобальной сети и недопущения утечки служебной информации из информационной сети МФЦ во внешнюю среду и иных несанкционированных действий.

2. В целях оптимизации информационного трафика при работе пользователей в сети Интернет и контроль за ним вводится система полного протоколирования работы в ней. Это означает ограничение использования наборов сетевых протоколов, а также постоянную фиксацию информации о посещениях Интернет-сайтов сотрудниками в журналах на серверах доступа.

3. Статистика посещений сотрудниками Интернет-сайтов (с указанием фамилий, дат, времени и наименований сайтов) периодически докладывается руководству МФЦ, а также в отдел по работе с персоналом. В случаях злоупотреблений и использования доступа в Интернет в неслужебных целях в отношении нарушителей применяются меры административного воздействия, регламентируемые соответствующими внутренними нормативными документами.

4. В необходимых случаях для определенных пользователей возможны персональные настройки доступа к строго определенным сайтам Интернет.

VI. ОБЩИЙ ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ЛОКАЛЬНОЙ СЕТИ МФЦ ИЗВНЕ

1. Предоставление доступа к информационной сети МФЦ из внешнего мира (из глобальных сетей или с удаленных рабочих мест) рассматривается как источник повышенных рисков вследствие невозможности осуществления эффективного контроля за точкой удаленного доступа.
2. При необходимости организации такого доступа, в каждом конкретном случае, на основании письменной заявки от руководителя подразделения ОА принимает решение о возможности и способах реализации удаленного доступа к информационным ресурсам.
3. Меры по предоставлению удаленного доступа к конкретным информационным ресурсам, определенные ОА, дополняют требования данного Положения и являются обязательным при осуществлении удаленного доступа. Категорически запрещается самостоятельная установка средств и программного обеспечения удаленного доступа.

Приложения:

1. Инструкция о назначении пароля пользователями информационной системы МФЦ.
2. Извлечения из Уголовного Кодекса Российской Федерации.

К «Положению о порядке использования сотрудниками МФЦ компьютерных и информационных ресурсов»

**Инструкция
о назначении пароля пользователями
вычислительной сети МФЦ**

1. Пароль - это секретное слово (сочетание заглавных и прописных букв, цифр и символов), которое должен знать пользователь для регистрации в вычислительной сети МФЦ. Пароль является составной частью системы авторизации и предоставления прав доступа пользователя к компьютерным и информационным ресурсам МФЦ. Для обеспечения защищенности информационной системы МФЦ от несанкционированного доступа минимальная длина пароля устанавливается равной **семи (7)** символам.

2. В качестве пароля пользователя для доступа в локальную вычислительную сеть МФЦ не разрешается использовать дату или год рождения, имя или фамилию пользователя, а также простые комбинации клавиш наподобие "1111111", "1234567", "qwerty12".

3. Пароль должен отвечать требованиям сложности.

Пароль не должен содержать имя учетной записи пользователя или фрагмента имени пользователя длиной более двух символов. Пароль должен содержать символы, относящиеся к трем из следующих четырех категорий:

- латинские заглавные буквы (A – Z);
- латинские строчные буквы (a – z);
- цифры (0 – 9);
- отличные от букв и цифр символы (например , !,\$,#,%).

Проверка соблюдения этих требований выполняется при изменении или создании паролей.

4. Для предотвращения компрометации паролей осуществляется их периодическая смена не реже чем один раз в два месяца. Вновь устанавливаемый пароль не должен совпадать с использовавшимся ранее: система исключает установку использовавшегося ранее пароля.

5. В локальной сети МФЦ функционируют сервера с операционной системой **Windows 2008 R2** и рабочие станции с операционной системой **Windows 7**. Смена паролей производится при получении сообщения о том, что срок действия пароля истекает в какой-либо одной из систем.

6. Пользователю отводится некоторое время (несколько "горячих" регистраций), в которое можно отказаться от немедленной смены пароля. Рекомендуется проводить смену пароля, если у ответственного за сопровождение компьютерной техники имеется возможность оказать помощь пользователю в случае ошибочных действий при смене пароля. Запрещается расходовать все отведенные "горячие" регистрации, т.к. после использования последней вход в локальную сеть будет заблокирован.

Приложение № 2

К «Положению о порядке использования сотрудниками МФЦ компьютерных и информационных ресурсов»

Извлечения из Уголовного Кодекса Российской Федерации

Ст. 272 Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо **исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.**

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо **исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.**

Ст. 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются **лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.**

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок **от трех до семи лет.**

Ст. 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо **обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.**

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок **до четырех лет.**