КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ И АРХИВ КЪУЛЫКЪУ
КЪАБАРТЫ-МАЛКЪАР РЕСПУБЛИКАНЫ АРХИВ СЛУЖБАСЫ
АРХИВНАЯ СЛУЖБА КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ

УНАФЭ БУЙРУКЪ ПРИКАЗ

13 декабря 2017 г. № 65

Налшык къ Нальчик ш г. Нальчик

Об утверждении Инструкции по работе с компьютерной информационной сетью и сетевыми ресурсами сети Интернет в Архивной службе Кабардино-Балкарской Республики

В целях определения прав и обязанностей сотрудников Архивной службы КБР при работе с компьютерной сетью, сообщениями электронной почты, сетевыми ресурсами сети общего доступа Интернет,

п р и к а з ы в а ю:

1. Утвердить прилагаемую Инструкцию по работе с компьютерной информационной сетью и сетевыми ресурсами сети Интернет в Архивной службе Кабардино-Балкарской Республики.

2. Ознакомить под роспись всех сотрудников с настоящей Инструкцией.

3. Контроль за исполнением настоящего приказа возложить на заместителя руководителя А.О. Гуртуева.

Руководитель **Ш.Х.Шогенов**

УТВЕРЖДЕНА
приказом Архивной службы КБР
от 13 декабря 2017 года № 65

ИНСТРУКЦИЯ
по работе с компьютерной информационной сетью и сетевыми ресурсами сети Интернет в Архивной службе Кабардино-Балкарской Республики

Настоящая Инструкция определяет права и обязанности сотрудников Архивной службы КБР при работе с компьютерной сетью Архивной службы КБР, сообщениями электронной почты и сетевыми ресурсами сети общего доступа Интернет.

1. Введение

Компьютерной локальной вычислительной сетью Архивной службы КБР (ЛВС) называется совокупность компьютеров, кабелей, сетевых адаптеров, работающих под управлением сетевой операционной системы и разрешенного прикладного программного обеспечения (ПО) и оборудования, позволяющего использовать ресурсы локальной вычислительной сети.

Файл-сервер - компьютер, выделенный из группы персональных компьютеров для хранения информации, баз данных или выполнения какой-либо сервисной задачи без непосредственного участия человека.

Веб-сервер – компьютер в ЛВС на котором установлено программное обеспечение, выполняющее функции веб-сервера, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы.

Веб-ресурс – любой информационный ресурс в сети Интернет.

E-mail или электронная почта - технология и служба по пересылке и получению электронных сообщений (называемых «письма», «электронные письма» или «сообщения») между пользователями компьютерной сети (в том числе - Интернета).

Действие настоящих правил распространяется на пользователей любого компьютерного оборудования (компьютеры, компьютерная периферия, коммуникационное оборудование), подключенного к ЛВС и сети Интернет.

1.1. Целью настоящей Инструкции является:

- регулирование работы пользователей с компьютерным оборудованием, ЛВС и ПО;
- распределение сетевых ресурсов коллективного пользования;
- определение мер по поддержанию необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к ней, обеспечение использования только лицензионного ПО;
- уменьшение рисков умышленного или неумышленного искажения информации, сетевых ресурсов и ПО;

- упорядочивание использования компьютерного оборудования ЛВС с целью повышения эффективности выполнения поставленных задач и планов, а также осуществления другой деятельности, предусмотренной служебной необходимостью;

- предотвращение ненадлежащего использования компьютерного оборудования, ЛВС и ПО;

- регламентирование использования подразделениями почтового ящика для получения и обработки электронной информации и почтовых сообщений;

- упорядочивания работы пользователей с веб-ресурсами.

1.2. Персональные компьютеры (ПК), серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование ЛВС, коммуникационные средства являются собственностью Архивной службы КБР и предоставляются сотрудникам для осуществления ими их должностных обязанностей.

1.3. Локальная вычислительная сеть Архивной службы КБР (ЛВС) предназначена для:

- доступа к файлам и базам на сервере. ЛВС позволяет одновременно нескольким пользователям работать с одним и тем же файлом, хранящемся на центральном файл-сервере и производить с ним различные действия;

- передачи файлов. ЛВС позволяет быстро копировать файлы любого размера с сервера на другой компьютер без использования переносных носителей информации;

- доступа к информации и файлам. ЛВС позволяет запускать прикладные программы на сервере с любой из рабочих станций, работать с базами данных и файлами, расположенными на сервере;

- предоставления разделенного доступа к принтерам. ЛВС позволяет нескольким пользователям на различных рабочих станциях использовать совместно один или несколько принтеров;

- доступа пользователей к сети Интернет.

2. Общие положения

2.1. К работе с ЛВС допускаются сотрудники, прошедшие обучение навыкам работы с компьютерной техникой, инструктаж по технике безопасности и получившие соответствующие уникальные средства аутентификации в ЛВС организации - это учётная запись (логин) пользователя и пароль в отделе правового и информационного обеспечения, контроля за исполнением архивного законодательства (далее - ПИОКИАЗ) Архивной службы КБР и закрепленные за определенным компьютером.

2.2. Работа с ЛВС каждому работнику разрешена только на определенных компьютерах, в определенное время (в пределах установленного рабочего графика), только со своей учетной записью пользователя и паролем и только с разрешенными программами и сетевыми ресурсами. В случае необходимости выполнения работ вне указанного времени, на других компьютерах и с другими программами, необходимо согласовать данный вопрос с руководителями соответствующих подразделений и отделом ПИОКИАЗ.

2.3. Пользователь, подключенный к ЛВС 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.

2.4. Категорически запрещается доступ к компьютерам и работе в ЛВС Архивной службы КБР посторонним лицам. В случае выявления нарушений сотрудники отдела ПИОКИАЗ имеют право отстранить виновного от пользования компьютером или принять иные меры, необходимые для предотвращения выявленного нарушения, и сообщить о данном факте руководителю Архивной службы КБР и начальнику соответствующего подразделения.

2.5. Сотрудник отдела ПИОКИАЗ имеет право отключить компьютер пользователя от ЛВС в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, а также при выявлении распространения компьютерных вирусов. О данном факте сотрудник отдела ПИОКИАЗ обязан незамедлительно сообщить руководителю соответствующего подразделения.

2.6. Все пользователи ЛВС при подключении получают ограниченный уровень доступа к ресурсам своих компьютеров (уровень пользователя) и обязаны работать только с разрешенным уровнем доступа. Для получения административного уровня доступа к ЛВС и ресурсам компьютера, необходимо письменно указать необходимость работы на компьютере и ЛВС организации с повышенным уровнем доступа и получить письменное разрешение у руководителя Архивной службы КБР.

2.7. Доступ к ресурсам файл-сервера для каждого пользователя ЛВС разграничивается в зависимости от возложенных на исполнителя задач. Беспрепятственные создание, копирование, удаление и другие операции с электронными документами возможны для каждого пользователя только в назначенных для него папках на файл-сервере.

2.8. Сотрудники отдела ПИОКИАЗ, с целью повышения уровня безопасности работы ЛВС, могут без уведомления пользователей проводить соответствующие работы (инсталляция нового программного обеспечения на компьютеры пользователей, сканирование на вирусы и др.)

3. Пользователь ЛВС обязан:

3.1. Ознакомиться с настоящей Инструкцией и правилами по технике безопасности до начала работы на компьютерном оборудовании.

3.2. Соблюдать правила работы в корпоративной ЛВС, оговоренные настоящей Инструкцией.

3.3. Пользоваться только разрешенным ПО и не допускать использования ПО с нарушением лицензионных условий.

3.4. Пройти инструктаж и получить личные уникальные средства аутентификации в ЛВС (имя пользователя, пароль) для работы с оборудованием с ограниченным доступом.

3.5. Использовать индивидуальное имя пользователя для своей идентификации в сети. Индивидуальное имя пользователя назначается в отделе ПИОКИАЗ.

3.6. Не создавать самостоятельно пароль для входа в ЛВС. Пользоваться только своим именем пользователя и паролем для входа в локальную сеть. Передача таких данных кому-либо запрещена.

3.7. При доступе к внешним ресурсам ЛВС, соблюдать правила, установленные настоящей Инструкцией, для используемых и разрешенных ресурсов.

3.8. Использовать компьютерное оборудование исключительно для деятельности, предусмотренной служебной необходимостью и должностными регламентами (инструкциями).

3.9. Бережно относиться к оборудованию, соблюдать правила его эксплуатации.

3.10. Рационально пользоваться ограниченными разделяемыми ресурсами (дисковой памятью файл-сервера общего пользования, пропускной способностью локальной сети) и расходными материалами.

3.11. Выполнять обязательные рекомендации и предписания специалистов отдела ПИОКИАЗ и ответственных лиц по компьютерной безопасности, направленные на обеспечение безопасности ЛВС.

3.12. Предоставлять доступ к сетевому оборудованию и компьютеру сотрудникам отдела ПИОКИАЗ для проверки исправности и соответствия ПО установленным правилам работы.

3.13. Немедленно сообщать в отдел ПИОКИАЗ 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. Сотрудники отдела ПИОКИАЗ должны провести расследование указанных фактов, принять соответствующие меры и сообщить о них начальнику соответствующего подразделения и руководителю Архивной службы КБР.

3.14. Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли), необходимую для безопасной работы ЛВС.

3.15. Немедленно отключить от ЛВС компьютер, при появлении сообщений антивирусного ПО о потенциальной опасности заражения, сообщить об этом в отдел ПИОКИАЗ и далее действовать по его указаниям.

3.16. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь обязан выключить компьютер от сети и сообщить об этом в отдел ПИОКИАЗ.

4. Пользователи ЛВС имеют право:

4.1. Подать заявку в отдел ПИОКИАЗ на получение прав доступа к оборудованию общего пользования.

4.2. Подавать заявки руководителю своего подразделения на закупку нового и модернизацию компьютерного оборудования персонального пользования.

4.3. Получать консультацию у сотрудников отдела ПИОКИАЗ по работе с компьютерным оборудованием и программным обеспечением общего пользования, по вопросам компьютерной безопасности.

4.4. В случае несогласия, обжаловать руководителю соответствующего подразделения действия сотрудников отдела ПИОКИАЗ.

4.5. Использовать в работе предоставленные им и разрешенные сетевые ресурсы.

4.6. Обращаться в отдел ПИОКИАЗ 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 общего доступа к папкам компьютера), должны санкционироваться отделом ПИОКИАЗ.

4.7. Для повышение эффективности использования сетевых ресурсов, сотрудники отдела ПИОКИАЗ вправе ограничивать доступ к некоторым сетевым ресурсам пользователей вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры.

5. Пользователям ЛВС запрещается:

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

5.2. Использовать оборудование, сетевые программы для деятельности, не обусловленной служебной необходимостью и должностной инструкцией.

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

5.4. Самостоятельно устанавливать или удалять любое ПО на компьютерах, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.

Установку, удаление, модернизацию, настройку операционной системы, ПО и иные подобные действия на компьютере пользователя выполняют только специалисты отдела ПИОКИАЗ.

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

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

Перемещение компьютерного оборудования допускается в исключительных случаях, а именно: пожарной опасности, других угроз жизни и здоровью людей или угроз повреждения имущества.

5.7. Самовольно подключать компьютер к ЛВС организации, а также изменять IP и MAC-адрес компьютера, выданный отделом ПИОКИАЗ, устанавливать дополнительные сетевые протоколы, изменять конфигурацию настроек сетевых протоколов без предварительного уведомления сотрудников отдела ПИОКИАЗ.

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. Работать с каналоемкими ресурсами (real video, real audio, chat и др.) без согласования с руководством подразделения и отдела ПИОКИАЗ.

5.9. Получать и передавать в сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую или государственную тайну, 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 учетной системы безопасности, системы статистики, ее повреждения или дезинформации.

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

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

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

5.14. Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь не имеет права пользоваться чужими именами и паролями (случайно ставшими ему известными) для входа в сеть, читать чужую электронную почту, причинять вред данным, принадлежащих другим пользователям.

5.15. Закрывать доступ к информации паролями без согласования с руководителями подразделений и сотрудниками отдела правового и информационного обеспечения, контроля за исполнением архивного законодательства.

5.16. Передавать другим лицам свои личные атрибуты доступа (регистрационное имя и пароль) к компьютеру, а также предоставлять доступ к каналам сети пользователям других сетей (например, посредством proxy-server, socks-proxy, open relay и т.п.).

5.17. 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 предупреждения и разрешения отдела ПИОКИАЗ, а также разрешения руководителей соответствующих подразделений, с объяснением служебной необходимости подобных действий.

5.18. Предоставлять доступ к компьютерному оборудованию незарегистрированным пользователям.

5.19. Использовать в работе съемные носители информации без обязательной проверки антивирусной программой.

5.20. Переносить без особой необходимости информацию, связанную с деятельностью подразделения, с компьютера на компьютер.

5.21. Хранить на сетевых дисках и серверах файлы, не относящихся к выполнению служебных обязанностей сотрудника (музыка, фотографии, игры, видео, виртуальные CD и т.п.).

6. Работа с электронной почтой.

6.1. Каждое подразделение Архивной службы КБР имеет свой адрес электронной почты. Логин и пароль от почтового ящика предоставляются отделом ПИОКИАЗ и не подлежат передаче посторонним лицам. Самостоятельно изменять пароль к почтовому ящику запрещается.

6.2. Электронная почта предоставляется сотрудникам только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено. Все электронные письма, создаваемые и хранимые на компьютерах Архивной службы КБР, являются собственностью Архивной службы КБР и не считаются персональными.

6.3. Архивная служба КБР оставляет за собой право получить доступ к личной электронной почте работников, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто третьим лицам, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов.

6.4. В случае использования цифровых подписей почтовые клиенты должны быть сконфигурированы так, чтобы каждое сообщение подписывалось цифровой подписью отправителя.

6.5. В случае если с помощью электронного письма должна быть послана конфиденциальная информация или информация, являющаяся собственностью Архивной службы КБР, или другая важная информация, она должна быть зашифрована так, чтобы ее мог прочитать только тот, кому она предназначена, с использованием утвержденных для этих целей программ и алгоритмов.

6.6. Вся информация, классифицированная как критическая, конфиденциальная или относится к коммерческой тайне, при передаче ее через открытые сети, такие как Интернет, обязательно должна быть предварительно зашифрована.

6.7. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности организации.

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

6.9. В качестве клиентов электронной почты могут использоваться только лицензионные программные продукты или почтовые программы.

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

6.11. Запрещено осуществлять переход по ссылкам, содержащимся в текстах электронных сообщений. Перед открытием файл вложения электронного письма необходимо скопировать на жесткий диск ПЭВМ и проверить антивирусной программой.

6.12. В случае, если открытие почтового вложения сопровождается запросом о внесении изменений в ПО операционной системы, ошибкой прикладного ПО или вложение содержит набор символов, необходимо немедленно прекратить его обработку.

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

6.14. Запрещено использовать несуществующие обратные адреса при отправке электронных писем.

6.15. Запрещено 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 ЛВС предоставлено право использовать только разрешенные программы для поиска информации в сети Интернет и только для выполнения своих должностных обязанностей.

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

7.3. Вся информация о сеансах доступа пользователей к ресурсам Интернет (дата, время, длительность, название ресурса, локальный адрес) протоколируется и накапливается в архиве.

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, пользующимся Интернетом, запрещено передавать (сохранять) материал, который является непристойным, содержит порнографическую информацию, нарушает законодательство России в части использования объектов интеллектуальной собственности, а также не относящимся к деятельности Архивной службы КБР.

7.6. Все программы, используемые для доступа к сети Интернет, не должны нарушать лицензионные условия их использования и в них должны быть настроены необходимые уровни безопасности.

7.7. При работе с веб-ресурсами запрещено:

- получать и передавать через ЛВС 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;
- получать доступ к информационным ресурсам ЛВС или сети Интернет, не являющихся публичными, без разрешения их собственника;
- играть в различные Онлайн игры (онлайн казино и тому подобные);
- 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 сотрудника, без согласования с руководством и отделом ПИОКИАЗ.

8. Ответственность.

8.1. Пользователь компьютера отвечает за всю информацию, хранящуюся на нем, технически исправное состояние вверенной ему техники.

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

8.3. В зависимости от последствий невыполнения предписаний, предусмотренных в настоящей Инструкции, а также других обязательных условий работы с компьютерным оборудованием и ЛВС, к пользователю могут быть применены соответствующие санкции в виде предупреждения, выговора, лишения премии, временного отстранения от работы в сети ЛВС, удержания заработной платы, увольнения и т.д., определяемых по представлению руководителя подразделения, в котором работает пользователь и руководителя отдела ПИОКИАЗ.

8.4. Нарушение данной Инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей, системы или ЛВС компьютеров, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации и Кабардино-Балкарской Республики, а также возмещение пользователем действительного ущерба, причиненного такими действиями.

8.5. Вся полнота ответственности за установку, использование и хранение на вверенном компьютерном оборудовании, ПК не утвержденного или не лицензионного ПО, несанкционированное распространение информации, являющейся интеллектуальной собственностью, возлагается на пользователя.