Приложение №1
к приказу директора
от 29.06.2012 г. № 134

МИНОБРНАУКИ РОССИИ

**Кумертауский филиал
федерального государственного
бюджетного образовательного учреждения
высшего профессионального образования
«Оренбургский государственный
университет»
(Кумертауский филиал ОГУ)**

УТВЕРЖДАЮ
Директор_____В.А.Анищенко
«28» июня 20 12 г.

ИНСТРУКЦИЯ

_____№_____
г. Кумертау

«Пользователя компьютерным оборудованием»

1. Основные понятия

1.1. Компьютерной локальной вычислительной сетью (далее – ЛВС) Кумертауского филиала ОГУ (далее – Филиала) называется совокупность компьютеров, кабелей, сетевых адаптеров, работающих под управлением сетевой операционной системы и разрешенного прикладного программного обеспечения (далее – ПО) и оборудования, явно не указанного в данной инструкции, но позволяющего использовать ресурсы ЛВС Филиала.

ЛВС предназначена для:

- **предоставления разделенного доступа к файлам.** ЛВС позволяет одновременно нескольким пользователям работать с одним и тем же файлом, хранящимся на центральном файл-сервере и производить с ним различные действия.
- **передачи файлов.** ЛВС позволяет быстро копировать файлы любого размера с одной рабочей станции на другую 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.
- **удаленного доступа к оборудованию.**

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

1.3. ПК, серверы, ПО, оборудование корпоративной ЛВС Филиала, коммуникационное оборудование и пользователи, образуют систему корпоративной локальной сети Филиала.

1.4. 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 неправильного использования сетевых ресурсов, ПО;
- упорядочивание использования компьютерного оборудования корпоративной ЛВС Филиала с целью повышения эффективности выполнения производственных планов и осуществления другой деятельности предусмотренной производственной необходимостью;
- предотвращение ненадлежащего использования компьютерного оборудования, ЛВС и ПО.

1.5. Действие настоящей инструкции распространяется на пользователей любого компьютерного оборудования (компьютеры, компьютерная периферия, коммуникационное оборудование), подключенного к ЛВС Филиала, а также на пользователей, осуществляющих удаленный доступ к оборудованию из ЛВС Филиала и удаленный доступ к ЛВС Филиала.

2. Общие положения

2.1. Настоящая Инструкция определяет права и обязанности пользователей компьютерным оборудованием

2.2. К работе за компьютерным оборудованием Филиала допускаются лица, работающие в Филиале на основе трудового или гражданско-правового договора, прошедшие инструктаж, получившие соответствующие учётные записи (логин) пользователя и пароль в отделе информационных технологий (далее ОИТ) и закрепленные за определенным компьютером.

2.3. Работа с ЛВС Филиала каждому работнику разрешена только на определенных компьютерах, в определенное время (в пределах установленного графика рабочего времени), только со своей, полученной в ОИТ 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 получить согласованное с заведующим ОИТ разрешение директора Филиала.

2.4. Пользователь — 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.

2.5. Для работы на компьютере других лиц, кроме закрепленного за ним пользователя и его руководителя структурного подразделения, необходимо получить разрешение директора Филиала с согласованием заведующего ОИТ. После получения соответствующего разрешения, пользователь обязан зарегистрироваться на компьютере, под своей, полученной в отделе информационных технологий, учетной записью (логином).

2.6. В случае выявления нарушений настоящей инструкции пользования, сотрудники ОИТ имеют право отстранить виновного от пользования компьютером или принять иные меры, необходимые для предотвращения выявленного нарушения, и сообщить о таком факте директору Филиала и его заместителю по безопасности и организационно-правовым вопросам.

2.7. Сотрудник ОИТ имеет право отключить компьютер пользователя от ЛВС в случае, если с данного компьютера производились попытки несанкционированного доступа к информации других компьютеров, и при других серьезных нарушений настоящей инструкции. О данном факте сотрудник ОИТ обязан незамедлительно сообщить директору Филиала и его заместителю по безопасности и организационно-правовым вопросам.

2.8. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящей инструкции, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им или каком-либо другом компьютере, о фактах использования неразрешенного или не лицензионного ПО, пользователь должен немедленно сообщить об этом своему непосредственному руководителю и в ОИТ. При этом ОИТ обязан проанализировать поступившую информацию и безотлагательно уведомить директора и зам. директора по БиОПВ Филиала об указанных фактах.

2.9. Все пользователи Филиала 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 ресурсам компьютера, необходимо письменно указать необходимость работы на компьютере и ЛВС Филиала с повышенным уровнем доступа и получить письменное разрешение у директора Филиала (административный доступ к ресурсам необходим для корректной работы некоторого программного обеспечения — для этого специалисты ОИТ могут произвести дополнительные настройки данного ПО, позволяющие работать с административным уровнем, при этом не предоставляя повышенных привилегий пользователю).

2.10. Сотрудники ОИТ, с целью повышения уровня безопасности работы ЛВС Филиала, могут без уведомления пользователей проводить соответствующие работы (инсталляция нового программного обеспечения по сети на компьютеры пользователей, сканирование на вирусы и др.)

3. Обязанности пользователей

Пользователь обязан:

3.1. Ознакомиться с настоящей Инструкцией и правилами работы в ЛВС перед началом работы на компьютерном оборудовании.

3.2. Строго соблюдать правила работы в корпоративной ЛВС, оговоренные настоящей Инструкцией.

3.3. Пользоваться только разрешенным ПО (перечень которого устанавливается «Паспортом программного обеспечения подразделения», утверждаемым директором Филиала) и не допускать использования ПО с нарушением лицензионных условий.

3.4. Пройти инструктаж и получить личные уникальные средства аутентификации в ЛВС Филиала (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 ОИТ.

3.6. Пользоваться только своим именем пользователя и паролем для регистрации на компьютере. Передача таких данных кому-либо запрещена.

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

3.8. Использовать компьютерное оборудование исключительно для деятельности, предусмотренной производственной необходимостью и должностными инструкциями.

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

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

3.11. Выполнять требования сотрудников ОИТ, а также лиц, назначенных ответственными за эксплуатацию конкретного оборудования.

3.12. Выполнять обязательные рекомендации и предписания специалистов ОИТ направленные на обеспечение безопасности ЛВС.

3.13. Предоставлять доступ к сетевому оборудованию и компьютеру сотрудникам ОИТ для проверки исправности и соответствия установленным правилам работы.

3.14. Немедленно сообщать в ОИТ 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. ОИТ, при необходимости, с привлечением других специалистов и заместителя директора Филиала по безопасности и организационно-правовым вопросам, должны провести расследование указанных фактов и принять соответствующие меры.

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

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

3.17. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь обязан сообщить об этом в ОИТ.

3.18. Запись информации на (или с) сменный носитель производиться только в отделе информационных технологий или специально закрепленными работникам в определенном корпусе и только на специальные носители, принадлежащие Филиалу. Использование сменных носителей информации на рабочих компьютерах строго запрещено (доступ открывается только по письменному разрешению директора Филиала и в этом случае пользователь сам отвечает за безопасность и сохранность используемых данных), исключение составляют пользователи копицентров.

3.19. Сохранять рабочие документы только в папке «Мои документы». Хранить документы на «Рабочем столе» или в другой области диска строго запрещено.

3.20. Раз в месяц производить резервное копирование с перемещением архивного файла на сетевое хранилище (Параметры доступа к сетевому хранилищу определяют сотрудники ОИТ).

3.21. Для обмена информацией между компьютерами других структурных подразделений необходимо использовать сетевые общедоступные ресурсы (Параметры доступа к сетевым общедоступным ресурсам определяют сотрудники ОИТ).

3.22. Для передачи информации подразделениям, находящихся в других корпусах, необходимо использовать средства электронной почты или специальные сменные носители информации.

4. Права пользователя

Пользователи имеют право:

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

4.2. Подавать заявки своему непосредственному руководителю на закупку нового и модернизацию компьютерного оборудования персонального пользования.

4.3. Подавать заявки своему непосредственному руководителю на закупку нового программного обеспечения.

4.4. Получать консультацию у сотрудников ОИТ по работе с компьютерным оборудованием и программным обеспечением общего пользования, по вопросам компьютерной безопасности.

4.5. В случае несогласия, обжаловать руководителю подразделения действия ОИТ.

4.6. Использовать в работе предоставленные им и разрешенные сетевые ресурсы, в оговоренных в настоящей инструкции рамках, если иное не предусмотрено по согласованию с ОИТ. Сотрудники ОИТ 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.

4.7. Обращаться в ОИТ 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, должны санкционироваться ОИТ.

4.8. Вносить предложения по внедрению новых современных технологий, по улучшению производительности труда и организации рабочего места (согласованием ОИТ).

5. Пользователям запрещается

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

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

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

5.4. Самостоятельно устанавливать или удалять любое ПО на компьютерах, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов. Данный вид работ выполняют только сотрудники ОИТ.

5.5. Удалять, модернизировать и перемещать служебную информацию, используемую в работе. Данные действия производятся только с разрешения непосредственного руководителя структурного подразделения и с согласованием сотрудников ОИТ.

5.6. Повреждать, уничтожать или фальсифицировать информацию.

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

5.8. Перемещать компьютерное оборудование (допускается в исключительных случаях, а именно: пожарной опасности, других угроз жизни и здоровью людей или угроз повреждения имущества).

5.9. Самовольно подключать компьютер к ЛВС Филиала, а также изменять IP и MAC-адрес компьютера, выданный ОИТ, устанавливать дополнительные сетевые протоколы, изменять конфигурацию настроек сетевых протоколов без предварительного уведомления отдела системного администрирования. 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.

5.10. Работать с каналоемкими ресурсами (real video, real audio, chat и др.) без согласования с руководством Филиала и ОИТ.

5.11. 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.

5.12. Предпринимать попытки обхода учетной системы безопасности, системы статистики, ее повреждения или дезинформации.

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

5.14. 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.

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

5.16. 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.

5.17. Закрывать доступ к информации паролями без согласования с руководителем подразделения и ОИТ.

5.18. 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.).

5.19. 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 информационных технологий, а также разрешения службы безопасности Филиала, с объяснением служебной необходимости подобных действий.

5.20. Предоставлять доступ к компьютерному оборудованию незарегистрированным пользователям без согласования с ОИТ.

5.21. Использовать в работе съемные носители информации без разрешения сотрудников ОИТ. Съемные носители информации, перед началом работы с ними, обязательно должны пройти проверку антивирусной программой.

5.22. Переносить информацию, связанную с деятельностью Филиала, с компьютера на компьютер (не распространяется, если перенос осуществляется внутри отдела).

5.23. Хранить информацию, связанную с деятельностью Филиала, в папках с общим доступом

5.24. Хранить файлы, не относящихся к выполнению служебных обязанностей сотрудника (музыка, фотографии, игры, видео, виртуальные CD и т.п.)

6. Работа с электронной почтой

6.1. Электронная почта предоставляется работникам Филиала для выполнения своих служебных обязанностей. Использование электронной почты в личных целях запрещено.

6.2. Электронная почта предоставляется на основании служебной записки директору Филиала.

6.3. Перед использованием электронной почты пользователь должен ознакомиться с настоящей инструкцией и регламентом использования корпоративной электронной почтовой системы работниками Филиала.

6.4. Все электронные письма, создаваемые и хранимые на компьютерах Филиала, являются собственностью Филиала, и не считаются персональными. Удаление и перемещение писем строго запрещается и производиться только с разрешения непосредственного руководителя и с согласованием ОИТ.

6.5. Филиал оставляет за собой право получить доступ к 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.

6.6. Категорически запрещается передавать параметры доступа к почтовому ящику третьим лицам.

6.7. При использования цифровых подписей почтовые клиенты должны быть сконфигурированы так, чтобы каждое сообщение подписывалось цифровой подписью отправителя.

6.8. В случае если с помощью электронного письма должна быть послана конфиденциальная информация или информация, являющаяся собственностью Филиала, или другая важная информация, она должна быть зашифрована так, чтобы ее мог прочитать только тот, кому она предназначена, с использованием утвержденных в Филиале программ и алгоритмов.

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

6.10. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности Филиала.

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

6.12. В качестве клиентов электронной почты могут использоваться только лицензионные программные продукты и утвержденные ОИТ почтовые программы.

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

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

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

6.16. Отправлять по электронной почте, большие файлы (особенно музыку, видео и фото), за исключением случаев, связанных со служебной необходимостью.

7. Работа с веб-ресурсами

7.1. Доступ к веб-ресурсам Интернет имеют только пользователи, назначенные распоряжением директора Филиала с установленными лимитами по приему и передачи интернет трафика.

7.2. Доступ к веб-ресурсам Интернет ограничен. Категорически запрещается посещать следующие категории сайтов: о наркотиках; о насилии; о терроризме; сайты содержащие нецензурную лексику; сайты связанные с азартными и прочими играми; об оружии; порносайты; чаты; социальные сети; сайты электронных почтовых серверов, не являющихся почтовыми системами Филиала.

7.3. Пользователями должны использоваться только разрешенные программы для поиска информации в сети Интернет и только для выполнения своих должностных обязанностей.

7.4. Перед использованием веб-ресурсов Интернет пользователь обязан: ознакомиться с настоящей инструкцией и инструкцией по организации антивирусной защиты; убедиться, что антивирусная программа имеет последние обновления и обеспечивает заданный уровень защиты.

7.5. Пользователи, не имеющие доступ к веб-ресурсам Интернет, могут посещать официальные сайты Филиала и Оренбургского государственного университета для получения служебной информации и чтения новостей.

7.6. Доступ к информационным системам через Интернет имеют только руководители структурных подразделений Филиала, назначенные приказом ректора ОГУ. Доступ осуществляется с помощью логина и пароля. Действия пользователей в данном случае регламентируется нормативными документами и инструкциями ОГУ.

7.7. Использование ресурсов сети Интернет не должно создавать потенциальную угрозу Филиалу.

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

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

7.10. Сотрудникам Филиала, пользующимся Интернетом, запрещено передавать (сохранять) материал, который является непристойным, содержит порнографическую информацию, нарушает законодательство РФ в части использования объектов интеллектуальной собственности, а также не относящимся к деятельности Филиала.

7.11. Все программы, используемые для доступа к сети Интернет, не должны нарушать лицензионные условия их использования.

7.12. Все файлы, загружаемые с помощью сети Интернет, должны проверяться на вирусы/шпионское ПО с помощью утвержденных антивирусных программ.

7.13. При работе с веб-ресурсами запрещено:

7.14. 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;

7.15. получать доступ к информационным ресурсам ЛВС или сети Интернет, не являющихся публичными, без разрешения их собственника;

7.16. играть в различные игры;

7.17. использовать различные сайты и программы для анонимного доступа в сеть Интернет;

7.18. использовать программы для зарабатывания денег в сети интернет, таких как Spedia, Web Money и им подобных;

7.19. скачивание музыкальных и видео файлов, а также файлов, не имеющих отношения к текущим служебным обязанностям работника, без согласования с руководством и ОИТ.

8. Ответственность

8.1. Пользователь компьютера отвечает за всю информацию, которую использует в своей служебной деятельности и за 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. За невыполнение предписаний, предусмотренных настоящей Инструкцией, а также других обязательных условий работы с компьютерным оборудованием и ЛВС к пользователю могут быть в установленном порядке применены дисциплинарные взыскания.

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 РФ, а также возмещение пользователем действительного ущерба, причиненного такими действиями.

8.5. Вся полнота ответственности за установку, использование и хранение на вверенном компьютерном оборудовании, не утвержденного ПО, несанкционированное распространение информации, относящейся к конфиденциальной информации и коммерческой тайне Филиала, возлагается на пользователя.

Приложение № 1

№ *п/п*	***Сотрудник***	***Подпись***	***Дата***
1	*2*	*3*	*4*

Руководитель
структурного подразделения подпись И.О. Фамилия

Согласовано:
Должность подпись И.О. Фамилия
Должность подпись И.О. Фамилия
Должность подпись И.О. Фамилия