Утверждено
распоряжением администрации
города Кировска от _____ № _____

ПОЛОЖЕНИЕ
об общих правилах использования информационных ресурсов администрации города Кировска и муниципальных учреждений города Кировска

1. Общие положения

1.1. Настоящее положение об общих правилах использования информационных ресурсов администрации города Кировска и муниципальных учреждений города Кировска (далее - Положение) разработано в целях упорядочения отношений, связанных с безопасным режимом поиска, обработки, хранения и передачи информации в электронном виде, для обеспечения условий эффективной информационной поддержки функционирования локально вычислительной сети администрации города Кировска и информационной безопасности.

1.2. Настоящее Положение обязательно к применению всеми пользователями, находящимися в локально вычислительной сети администрации города Кировска.

1.3. В настоящем Положении использованы следующие термины:

администратор – сотрудник службы информационных технологий МКУ «Центр учета и отчетности муниципальных учреждений города Кировска», ответственный за работоспособность прикладных автоматизированных систем, операционных систем, сетевого и телекоммуникационного оборудования;

информационная безопасность - состояние защищенности информационных ресурсов учреждения, находящегося в локально вычислительной сети (далее – Учреждение), выраженное в способности противостоять или противодействовать случайным или преднамеренным деструктивным воздействиям естественного или искусственного характера на нормальный процесс функционирования автоматизированных технологий, способным нанести ущерб владельцам и пользователям информации и поддерживающей инфраструктуре;

информационные ресурсы - информация (отдельные документы и отдельные массивы документов, документы и массивы документов), создаваемая, обрабатываемая и хранящаяся в информационных системах Учреждения;

информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

пользователь - сотрудник, обращающийся к информационной системе за получением необходимой ему информации и пользующийся ею**.**

1.4. В настоящем Положении используются следующие сокращения:

СИТ – служба информационных технологий;

АИБ - администратор информационной безопасности;

ЛВС – локально-вычислительная сеть администрации города Кировска;

БНИ – бумажный носитель информации;

ИТ - информационные технологии;

ИР - информационные ресурсы;

ПК - персональный компьютер;

СП - структурное подразделение администрации города Кировска, муниципальных учреждений;

СЭД – система электронного документооборота «DocsVision»;

ПО – программное обеспечение.

1.5. Положение определяет права и обязанности пользователей и регулирует отношения в организации работы с ИР, осуществляемые с помощью ИТ.

1.6. ИР должны использоваться работниками только для выполнения ими своих служебных обязанностей.

1.7. Администрирование информационных систем осуществляется сотрудниками СИТ.

1.8. Контроль соблюдения положения осуществляет АИБ в пределах своих полномочий.

1.9. Регламент технической и информационной поддержки пользователей объектов информатизации (далее – Регламент) утверждается отдельным распоряжением администрации города Кировска.

1.10. Пользователю предоставляется право использования информационных ресурсов на основании заявок, шаблоны которых предоставляются СИТ. Заявки, с подписью руководителя СП, в отсканированном виде пересылаются в СЭД, либо передаются на БНИ в СИТ.

2. Правила пользования информационными ресурсами

2.1. Пользователю предоставляется право доступа к ИР в информационных системах только по его персональной учетной записи и личному паролю, также к ИР в соответствии с его служебными обязанностями и порядком предоставления прав доступа к информационным ресурсам в соответствии с разделом 3 настоящего Положения.

С персональной учетной записью пользователь получает доступ:

- к общей папке СП на файловом сервере для совместного использования работниками СП;
- к другим общим папкам Учреждения, доступ к которым необходим для исполнения служебных обязанностей (по заявке руководителя СП или руководителя Учреждения);
- к персональному почтовому ящику электронной почты;
- к сетевым периферийным устройствам СП (принтеры, сканеры и т.п. в соответствии с заявкой).

2.2. Все документы для совместного использования пользователями СП Учреждения должны размещаться в общей папке СП.

2.3. Пользователи обязаны ежемесячно проводить проверку документов, хранимых на сетевых ресурсах, удалять устаревшие, дублирующиеся и ненужные файлы. Файлы, предназначенные для длительного хранения, необходимо хранить в архивном виде.

2.4. Основным средством доступа к ИР является ПК. За каждым ПК закрепляется ответственный пользователь, определяемый руководителем СП при установке ПК.

2.5. Установка и настройка ПК производится СИТ по Заявке на установку компьютерного оборудования, согласованной с АИБ. СИТ присваивает ПК имя в сети Microsoft согласно правилам использования единого каталога Active Directory.

2.6. СИТ оснащает ПК пользователей программным обеспечением в стандартной конфигурации.

2.7. Установка дополнительного программного обеспечения выполняется по Заявке в СИТ, в соответствии с Регламентом.

2.8. Пользователю **ЗАПРЕЩАЕТСЯ:**

2.8.1. Хранить файлы, не связанные с исполнением должностных обязанностей, в том числе развлекательного характера (фильмы, игры, музыку), на жестком диске ПК и своих сетевых ресурсах. Такие файлы могут быть удалены сотрудниками СИТ без предварительного уведомления пользователя и без возможности их восстановления.

2.8.2. Самостоятельно устанавливать, модифицировать или копировать программное обеспечение на ПК.

2.8.3. Оставлять компьютерную технику включенной в нерабочее время (на ночь, на выходные и нерабочие праздничные дни).

2.8.4. Использовать компьютерную технику в целях, не связанных с должностными обязанностями.

2.8.5. Использовать ИР, к которым у пользователя нет прав доступа. Возможность доступа пользователя к ресурсам, не предусмотренным его служебными обязанностями, не означает права на их использование.

2.8.6. Передавать право доступа к ИР и пароли доступа другим пользователям.

2.8.7. Осуществлять доступ к ИР с использованием учетных данных (имени и пароля) других пользователей.

2.8.8. Менять настройки BIOS (CMOS) своего ПК.

2.8.9. Изменять сетевые настройки своего ПК (IP-адрес, MAC-адрес, сетевое имя ПК, добавлять/убирать протоколы и службы и т.п.).

2.8.10. Активизировать на своих ПК средства беспроводного доступа (WiFi, Bluetooth и т.п.).

2.8.11. Вскрывать процессорный блок ПК, самостоятельно добавлять дополнительные устройства, менять конфигурацию ПК.

2.8.12. Подключать к ПК модемы, сотовые телефоны, фотоаппараты, USB-драйвы и другие устройства, устанавливать на ПК устройства записи на внешние носители (CD/DVD-RW, дисководы, стримеры и т.п.). Указанные подключения производятся СИТ по Заявке на установку компьютерного оборудования.

2.8.13. Открывать общий доступ к локальным дискам и папкам своего ПК.

2.8.14. Подключать к ЛВС личные ПК или ПК, принадлежащие работникам сторонних организаций.

2.8.15. Заниматься любым исследованием вычислительной сети при помощи специальных программ (сканеров, сниферов и пр. программ сканирования сети).

2.9. Пользователь не должен допускать работы других пользователей на своем ПК.

2.10. Пользователь отвечает за сохранение конфиденциальности информации на экране своего монитора. При временном отсутствии на рабочем месте или присутствии посторонних, имеющих возможность видеть конфиденциальную информацию на экране монитора, пользователь должен принудительно заблокировать компьютер (нажать WIN-L или Ctrl-Alt-Delete, а затем Enter).

2.11. При работе с электронными документами (добавлении в них новых данных, внесении изменений и исправлений) пользователь ПК самостоятельно несет ответственность за ту часть работы, которая не была им сохранена. Пользователь обязан производить периодическое сохранение открытых документов, в которые он внес изменения. За потерю несохраненной информации СИТ ответственности не несет.

2.12. О любых отклонениях от штатного режима работы программных или аппаратных средств пользователь должен обращаться в СИТ.

2.13. При передаче ПК другому пользователю СИТ производит полное переформатирование жесткого диска ПК.

2.14. При использовании паролей доступа к ИР пользователь руководствуется правилами парольной защиты в компьютерных системах в соответствии с разделом 4 настоящего Положения.

2.15. Пользователь обязан выполнять требования правил антивирусной защиты в соответствии с разделом 5 настоящего Положения.

2.16. При работе с электронной почтой пользователь должен выполнять правила использования электронной почты в соответствии с разделом 6 настоящего Положения.

2.17. Работа пользователей с ресурсами сети Интернет регулируется правилами использования ресурсов сети Интернет, утвержденными в разделе 7 настоящего Положения.

2.18. На ПК пользователя активирована система блокировки с паролем и временем срабатывания - не более 15 мин.

2.19. СИТ не несет ответственности за сохранность файлов, расположенных на ПК пользователя. Все важные документы пользователи обязаны хранить на сетевых ресурсах Учреждения.

3. Порядок предоставления прав доступа к информационным ресурсам

3.1. Предоставление прав доступа сотрудникам Учреждения к ИР осуществляется СИТ на основании заявки, подписанной сотрудником, руководителем СП, согласованной с АИБ.

3.2. Предоставление прав доступа работникам сторонних организаций к ИР Учреждения осуществляется по решению главы администрации города Кировска с предварительным обязательным согласованием с АИБ и подготовкой технического описания подключения.

3.3. За каждым ИР СИТ закрепляет ответственного администратора. Обязанности администратора включают техническую работу по настройке ИР в части предоставления прав доступа к нему.

3.4. При увольнении работника его права доступа ко всем ИР аннулируются, а учетная запись блокируется.

3.5. В случае длительного (свыше двух месяцев) отсутствия сотрудника (отпуск по уходу за ребенком, болезнь, отпуск без сохранения заработной платы итд.) его права доступа ко всем информационным ресурсам блокируются. Специалисты, ответственные за кадровый учет, должны информировать СИТ о кадровых перемещениях, длительных отсутствиях и увольнении пользователей.

3.6. Предоставление удаленного доступа (через сеть Интернет или модемные пулы) сотрудникам Учреждения к внутренним ИР производится только в исключительных случаях по решению главы администрации города Кировска, предварительно согласованного с АИБ.

4. Правила парольной защиты

4.1. Учетная запись (идентификатор) и пароль пользователя в компьютерной системе являются идентификационными данными, на основании которых сотруднику Учреждения предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности обрабатываемой (создаваемой, передаваемой и хранимой) пользователем информации.

4.2. Настоящее положение определяет правила выбора, смены и хранения для следующих видов паролей:

- пароль для входа в ЛВС;
- пароль для входа в прикладные автоматизированные системы;
- пароли администраторов операционных и автоматизированных систем, сетевого и телекоммуникационного оборудования.

4.3. Настоящие правила обязательны для выполнения всеми пользователями. С Пользователь несет ответственность за правильность выбора, конфиденциальность и регулярную смену своих индивидуальных паролей, а также за все действия в автоматизированной системе, произведенные с использованием его идентификатора и пароля.

4.4. **Использование личных паролей**:

При выборе, смене и хранении паролей компьютерных систем пользователь должен руководствоваться следующими правилами:

4.4.1. Сменить временный пароль

При предоставлении пользователю прав в автоматизированной системе администраторы СИТ сообщают ему временный пароль, который пользователь обязан сменить при первом входе в систему.

4.4.2. Хранить свои пароли в тайне

Пользователь обязан обеспечить конфиденциальность своих личных паролей. Запрещается передавать свои пароли другим работникам. Допускается хранение пароля, записанного на бумажном носителе, в недоступном для других пользователей месте (например, в личном сейфе работника).

4.4.3. Не использовать чужие идентификационные данные

Запрещается пользоваться чужими идентификационными данными и паролями для работы в компьютерных системах.

4.4.4. Регулярно производить смену паролей

Пользователь обязан регулярно (не реже 1 раза в 90 дней) менять свои пароли. Смена пароля в обязательном порядке производится также при нарушении его конфиденциальности, в том числе при возникновении подозрения о том, что пароль стал известен другому лицу. Смену пароля следует производить в рабочие дни (с понедельника по пятницу) с 9 ч до 16 ч. В случае непредвиденных обстоятельств или вопросов по смене пароля обратиться за помощью в СИТ.

4.4.5. Правильно выбирать пароли

В качестве личного пароля пользователь должен самостоятельно выбрать последовательность длиной не менее 6 символов, включающую в себя буквы, цифры. При выборе нового пароля запрещается повторное или «циклическое» использование старых паролей. Новый пароль должен отличаться от предыдущего не менее чем в 4 символах.

4.4.6. В качестве пароля запрещается использовать:

- последовательность символов, состоящую только из цифр (в том числе даты, номера телефонов и т.д.);
- последовательность повторяющихся символов;
- подряд идущие в раскладке клавиатуры или в алфавите символы (например, qwerty, wsxedc, фывапр, abcdef, абвгде и т.п.);
- осмысленные русские (английские) слова, набранные на латинском (русском) регистре;
- имена собственные (например, Наташа, Москва, Compaq, Coca Cola и т.п.);
- ассоциированную с работником информацию, которую легко узнать (например, фамилия, адрес, идентификатор пользователя в системе, марка автомобиля и т.д.);
- ассоциированное с данной компьютерной системой сочетание символов (например, outlook, windows XP и т.п.).

*Пример получения «правильного» пароля: second + 7 = **se7Cond** (пароль).*

4.4.7. Использовать разные пароли для критичных систем.

Пользователи должны выбирать разные пароли на доступ в автоматизированные системы, связанные с учетом и движением денежных средств, материальных и иных ценностей. Для других автоматизированных систем допускается использование одинакового пароля.

4.5. **Использование паролей администраторами СИТ**:

4.5.1. Пароли администраторов должны удовлетворять требованиям, изложенным в п.4.4.6, а также соответствовать следующим критериям:

- длина пароля должна быть не менее 15 символов;
- пароль должен содержать не менее одного спецсимвола;
- пароль должен содержать не менее одной цифры;
- должны быть изменены пароли, установленные в системе по умолчанию.

4.5.2. Не допускается использование одинаковых паролей администраторов для различных систем.

4.5.3. Администратор должен подключаться к оборудованию (операционной системе) с правами администратора только для исполнения административных функций. Недопустимо использование идентификатора администратора для решения прикладных задач.

4.5.4 Если в системе несколько администраторов, то каждый из них должен работать под своим уникальным именем пользователя. Использование разделяемых (общих) административных учетных записей допускается только по согласованию с АИБ.

4.5.5. В случае изменения функциональных обязанностей или увольнения администратора все известные ему пароли должны быть незамедлительно изменены новым администратором системы.

4.6 При наличии соответствующих возможностей в операционных и автоматизированных системах должны быть установлены следующие **параметры управления парольной защитой**:

4.6.1 Минимальная длина паролей - не менее 6 символов.

4.6.2 Период смены пароля - не более 90 дней.

4.6.3 Время задержки между попытками ввода пароля - не менее 5 сек.

4.6.4 Максимальное количество попыток неверного ввода пароля до временного блокирования идентификатора пользователя - не более 5 попыток.

4.6.5 Время сброса накопленных ошибок при вводе паролей - не менее 10 мин.

4.6.6 Количество предыдущих паролей, которые не должен повторять новый пароль - не менее 5.

4.6.7 Должна быть включена обязательная смена пароля при первом входе пользователя в систему (при назначении временного пароля администратором системы).

4.6.8 На ПК должна быть активирована система автоматического гашения экрана (экранная заставка) с паролем и временем срабатывания - не более 15 мин.

5. Правила использования антивирусной защиты

5.1. Средства антивирусной защиты обязательны к применению и должны быть установлены и активизированы:

- на межсетевых экранах на выходе в Интернет;
- на почтовых серверах;
- на файловых серверах;
- на персональных компьютерах.

5.2. Запрещается подключение к ЛВС компьютерного оборудования без штатно функционирующих средств антивирусной защиты (должно быть установлено лицензионно чистое антивирусное ПО, корректно настроенное, активизированное, использующее актуальные базы вирусных сигнатур).

5.3. Средствами антивирусной защиты должна контролироваться:

- информация, входящая из глобальных сетей во внутреннюю сеть;
- информация, передаваемая по электронной почте, системе электронного документооборота;
- информация, хранящаяся на файловых и почтовых серверах, на официальном сайте;
- информация, хранящаяся на ПК;
- информация, поступающая на ПК или в корпоративную сеть с внешних носителей информации (CD/DVD, flash-накопители и т.п.).

5.4. Состав используемых антивирусных средств устанавливается СИТ и должен соответствовать операционным системам, применяемым на ПК и серверах Учреждения.

5.5. Сотрудники СИТ должны обеспечить установку и настройку антивирусных средств.

5.6. В целях соблюдения антивирусной безопасности пользователи обязаны:

5.6.1. Предпринимать обязательные меры для предотвращения возможности заражения ПК вирусами:

- не производить считывание информации с мобильных носителей (дискеты, CD/DVD-диски, USB-драйвы и т.п.) без их предварительной проверки на отсутствие вирусов;

- не использовать и не передавать другим пользователям файлы, полученные из ЛВС или сети Интернет, а также по внутренней электронной почте (MS Outlook), без их предварительной проверки на наличие вируса;

- не открывать файлы, прикрепленные к электронному письму, полученному от неизвестного абонента, с сомнительной темой, подозрительного содержания;

- не запускать и не устанавливать никакого программного обеспечения, скачанного из сети Интернет.

5.6.2. При обнаружении на ПК вируса:

- остановить работу с информационными системами (в том числе электронной почтой MS Outlook);

- немедленно поставить в известность о вирусном заражении сотрудников СИТ;

- начать работу с ПК только после получения разрешения от системных администраторов СИТ.

5.7. Обязанности по сопровождению средств антивирусной защиты возлагаются на СИТ.

5.8. В рамках сопровождения средств антивирусной защиты СИТ проводит следующие работы:

- выбор, приобретение и использование средств антивирусной защиты;

- тестирование средств антивирусной защиты и их подготовка к применению пользователями;

- получение и установка обновлений средств антивирусной защиты баз вирусных сигнатур (в соответствии с рекомендациями производителей);

- обеспечение антивирусной защиты серверов Учреждения;

- обеспечение автоматического обновления средств антивирусной защиты и баз вирусных сигнатур, установленных на ПК;

- контроль работы средств антивирусной защиты;

- проведения лечения ПК и серверов в случае их вирусного заражения;

- устранение последствий вирусного заражения;

- участие в расследованиях причин вирусного заражения;

- выявление и ограничение путей распространения вирусов.

6. Правила использования электронной почты

6.1. Размер почтового ящика пользователя ограничен 2 Гб. В случае превышения указанного лимита прием корреспонденции для пользователя прекращается до момента появления свободного места в почтовом ящике.

6.2. Электронная почта используется для обмена служебной информацией в виде текстовых сообщений или документов в электронном виде.

6.3. Блокируются исходящие и входящие электронные сообщения следующего вида:

- сообщения без темы;

- сообщения, одновременно адресованные более 20 корреспондентам;

- сообщения, содержащие вложенные файлы (расширения - .exe, .dll, .pif и т.п.);

- сообщения, содержащие более 10 вложенных файлов;

- сообщения размером свыше 10 Мб.

6.4. Для уменьшения размера электронных сообщений и объединения нескольких вложенных файлов в один рекомендуется использовать программы для сжатия (компрессии) вложенных документов (например, WinRar).

6.5. Пользователям **ЗАПРЕЩАЕТСЯ:**

- производить рассылку материалов рекламного (непрофильного) и развлекательного характера;

- производить массовую рассылку писем неслужебного характера;

- пересылать исполняемые файлы (с расширениями - .exe, .dll, .pif и т.п.);

- пересылать мультимедийные файлы (аудио и видео), не относящиеся к служебной деятельности;

- производить рассылку вредоносных программ или файлов, зараженных вирусами;

- использовать личную почту для пересылки служебной информации в сети Интернет.

6.6. Пользователям запрещается отправка в незащищенном виде электронных сообщений, содержащих персональные данные. Информацию о способах защиты сообщений можно получить у АИБ.

7. Правила использования ресурсов сети Интернет

7.1. Сотруднику Учреждения предоставляется право доступа к ресурсам сети Интернет для выполнения им своих должностных обязанностей.

7.2. Сотруднику Учреждения предоставляется доступ к ресурсам сети Интернет (достаточный для выполнения большинства служебных заданий) или доступ к специализированным сервисам сети Интернет.

7.3. Используемые в Учреждении системы доступа в Интернет могут ограничивать доступ пользователя к отдельным ресурсам Интернет, а также загрузку отдельных типов файлов.

7.4. Технические средства доступа в сети Интернет ведут статистику работы пользователей (посещаемые сайты, объем передаваемого трафика, время работы и т.д.).

7.5. Право доступа к специализированным ресурсам сети Интернет предоставляется на основании заявки, подписанной руководителем СП и согласованной с АИБ.

7.6. Для доступа к ресурсам сети Интернет используются только разрешенные АИБ программные средства, установка и настройка которых осуществляются специалистами СИТ.

7.7. Пользователям **ЗАПРЕЩАЕТСЯ:**

- самостоятельно устанавливать программные средства для доступа и работы с ресурсами сети Интернет;

- самостоятельно подключать к ПК и использовать такие средства доступа к сети Интернет, как модем, мобильный телефон и т.п.;

- посещать ресурсы сети Интернет, информационное содержание которых не связано с выполнением должностных обязанностей;

- загружать музыкальные, видео файлы, подключаться к потоковым аудио, видео каналам;

- копировать (скачивать) и устанавливать любое программное обеспечение из сети Интернет;

- использовать почтовые серверы сети Интернет для отправки по электронной почте информации, связанной с исполнением служебных обязанностей;

- использовать Интернет-службы обмена сообщениями (Skype, Viber и т.п.);

- передавать и размещать в сети Интернет информацию, содержащую персональные данные.

8. Порядок использования дисководов и портов ввода/вывода на персональных компьютерах

8.1. В целях предотвращения несанкционированного копирования с ПК конфиденциальной информации, а также информации, содержащей персональные данные, ограничения возможности пользователя установить вредоносное или нелицензионное программное обеспечение **запрещается** использование накопителей и внешних интерфейсов на съемные носители.

8.2. На всех вновь закупаемых и переустанавливаемых ПК блокируются дисководы (FDD, устройств CD/DVD-RW и др.), а также порты ввода/вывода (USB, LPT, COM и др.).

8.3. Конфигурация ПК централизованно контролируется АИБ.

8.4. Дисководы и порты ввода/вывода ПК для конкретного пользователя могут быть активизированы в случае служебной необходимости на основании заявки на открытие доступа к штатным дисководам и портам ввода/вывода ПК;

8.5. Если служебная необходимость использования дисководов и портов ввода/вывода на ПК отпала, руководитель СП должен сообщить АИБ о необходимости восстановления стандартной конфигурации компьютера (блокировании дисководов, устройств записи CD-ROM, портов ввода-вывода).

8.6. Контроль за соблюдением порядка использования дисководов и портов ввода/вывода на ПК осуществляет АИБ.

9. Ответственность

9.1. Пользователь несет ответственность:

- за все действия в автоматизированной системе, произведенные с использованием своего идентификатора и пароля;
- за сохранность вверенного ему движимого имущества (компьютерной и оргтехники).

9.2. Ответственность за системную поддержку, организационное и методическое сопровождение пользователей в части антивирусной защиты ПК и обеспечение антивирусной защиты серверов, электронной почты и Интернет-трафика Учреждения несет АИБ.
