ИНСТРУКЦИЯ

о порядке пользования вычислительной техникой и программным обеспечением в муниципальном бюджетном общеобразовательном учреждении «Средняя общеобразовательная школа №39» г. Белгорода

1. Общие положения

1.1. Настоящая Инструкция определяет порядок пользования вычислительной техникой, программным обеспечением и работы в информационной вычислительной сети муниципальному бюджетному общеобразовательному учреждению «Средняя общеобразовательная школа №39» г. Белгорода (далее - Школа) и международной информационной сети Интернет.

1.2. Компьютерные и телекоммуникационные ресурсы и службы включают в себя следующее: многофункциональные серверы, рабочие станции, автономные компьютеры, мобильные компьютеры и другое оборудование, программное обеспечение, а также внутренние и внешние сети святи (сеть Интернет, системы электронной почты и т.д.). к которым прямо или косвенно обращаются вычислительные устройства Школы.

2. Порядок пользования вычислительной и оргтехникой и программным обеспечением

2.1. Пользователи должны соблюдать правила техники безопасности, пожарной безопасности и инструкции о правилах работы с вычислительной и оргтехникой.

2.2. Каждый пользователь должен пройти инструктаж по безопасности труда на конкретном рабочем месте. Ответственность за соблюдение техники безопасности несет непосредственный руководитель пользователя.

2.3. Цель, методы и содержание работ с вычислительной и оргтехникой должны соответствовать должностным обязанностям пользователя.

2.4. Пользователям запрещается самостоятельно:

2.4.1 Отключать сетевое оборудование общего пользования.

2.4.2. Изменять конфигурацию, производить ремонт вычислительной и оргтехники.

2.4.3. Подключать периферийные устройства, не предусмотренные для конкретного рабочего места.

2.4.4. Устанавливать новое или модифицировать имеющееся системное, офисное, прикладное, сетевое и другие виды программного обеспечения. Необходимость замены (модификации, новой установки и т.п.) программного обеспечения определяется руководителем пользователя в соответствии с выполняемыми обязанностями и проводится только техническими специалистами.

2.5. Пользователь должен знать и уметь пользоваться тем антивирусным программным обеспечением, которое находится на его компьютере. Перед проведением любых операций с внешним носителем информаций пользователь обязан произвести антивирусную проверку внешнего носителя информации. При отсутствии антивирусного программного обеспечения или его неработоспособности пользоваться компьютером запрещается. В случае невозможности излечения внешнего носителя информации от вируса пользователь ставит об этом в известность ответственного за обеспечение информационной безопасности, который производит соответствующие данной ситуации действия. Пользователю категорически запрещается производить какие-либо действия с информацией зараженного вирусом внешнего носителя.

3. Основы зашиты информации

3.1. Пользователь должен знать и уметь сохранять необходимую информацию либо на сменных носителях, либо в сетевом хранилище. Чаще всею информацию защищают от:
- физической утраты:
- удаления, изменения, порчи в результате использования нелицензионного программного обеспечения.
- порчи, изменения, удаления компьютерными вирусами и подобными им программами;
- несанкционированного изменения, просмотра, удаления посторонними лицами.

Физическая утрата информации может произойти из-за:
- выхода из строя носителя информации;
- кражи компьютера или носителя информации:
- стихийного бедствия;
- нарушения правил эксплуатации вычисли тельной техники и носителей информации.

Меры по предотвращению физической утраты информации:
- резервное копирование ценной информации:
- хранение и установка вычислительной техники и носителей информации в охраняемых и защищенных от внешних воздействий помещениях.

Меры но предотвращению воздействия на информацию со стороны компьютерных вирусов и подобных программ приведены в инструкции по организации антивирусной защиты компьютеров.

4. Порядок доступа, работы и хранения информации в сети

4.1. Доступ в сеть:

4.1.1. Доступ (прекращение или изменение вида доступа) к ресурсам сети работников Школы осуществляется системным администратором на основании представления руководителя и обоснования необходимости доступа к ресурсам сети.

4.1.2. Пользователям не разрешается самостоятельно устанавливать либо изменять настройки программного обеспечения для работы в сети.

4.1.3. Для каждого пользователя создается учетная запись (присваивается уникальный идентификатор (имя пользователя) и назначается пароль) для работы в сети и с электронной почтой. Пользователь несет ответственность за сохранность своих паролей для входа в сеть и работы с электронной почтой. Индивидуальные пароли запрещено распечатывать, хранить в сети или передавать другим лицам. В случае утери пароля пользователь обязан немедленно обратиться к системному администратору, администратору безопасности сети для смены пароля.

4.2. Работа в сети:

4.2.1. Компьютерные и телекоммуникационные службы и ресурсы сети не могут быть использованы для передачи или хранения коммерческих либо личных объявлений, рекламных материалов, разрушительных программ (вирусов и/или самовоспроизводимого кода), политических материалов или любой другой информации, на работу с которой у пользователя нет

полномочий либо предназначенной для личного пользования.

4.2.2. Ложные, навязчивые, непристойные, клеветнические, оскорбительные, угрожающие или противозаконные материалы запрещается пересылать по электронной почте или с помощью других средств электронной связи, а также отображать и хранить на компьютерах сети. Пользователи, заметившие или получившие подобные материалы, должны немедленно сообщить об этом своему непосредственному руководителю и администратору безопасности.

4.2.3. Пользователи должны тщательно продумывать содержание сообщений электронной почты и других электронных документов, как если бы это было письменное послание. Рекомендуется согласовывать с получателем форматы отправляемых файлов.

4.2.4. Пользователям запрещается изменять или копировать файл, принадлежащий другому пользователю, не получив предварительно разрешения владельца файла.

4.2.5. Пользователи должны соблюдать условия всех программных лицензий, авторское право и иные федеральные нормативные правовые акты, касающиеся интеллектуальной собственности.

4.2.6. Пользователь не имеет право: работать от имени другого пользователя, осуществлять несанкционированный доступ к информационным ресурсам, ему не предназначенным, предпринимать другие действия, приводящие к незаконному просмотру, копированию, модификации или удалению информационных ресурсов.

4.2.7. Пользователи обязаны осуществлять обмен данными, расположенными па персональных компьютерах (подключенных к сети) или на сервере сети, используя сетевые программные средства обмена информацией. Запрещается использование внешних носителей информации для обмена данными между пользователями сети.

4.2.8. Пользователь обязан информировать системного администратора, администратора безопасности и своего непосредственного руководителя о любых нарушениях сохранности информационных ресурсов и (или) о возможности появления таких нарушений, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе компьютера и (или) сети в целом.

4.3. Хранение информации в сети:

4.3.1. Все информационные материалы, связанные с обеспечением работы Департамента, необходимо хранить на серверах сети, кроме отдельных случаев, согласованных с вышестоящим руководителем. Администратор сети осуществляет копирование всех данных на архивный носитель в установленные сроки.

4.3.2. Пользователям запрещается хранить на серверах информационные материалы, несвязанные с функциональными обязанностями, материалы развлекательного характера, игры.

4.3.3. Запрещено создание и хранение документированной информации, отнесенной к государственной тайне, на компьютерах, подключенных к общей сети. Использование, обработка и хранение конфиденциальной информации в том числе информации с пометкой «Для служебного пользования») осуществляется в соответствии с нормативными актами,

регламентирующими порядок работы с такой информацией и только после проведения соответствующих мероприятий по защите информации от несанкционированного доступа и от утечки по техническим канатам.

5. Порядок осуществления доступа и обмена информационными ресурсами в международной информационной сети Интернет

5.1. Подключение пользователей к международной информационной сети Интернет и или электронной почте производится системным, администратором в соответствии с заявкой руководителя.

5.2. После установки (настройки) программного обеспечений для работы с сетью Интернет и или электронной почтой системным администратором запрещается изменение любых параметров, касающихся подключения к серверам сети и используемых протоколов.

5.3. При работе в сети Интернет пользователям запрещается:

5.3.1. Пересылка документов для служебного пользования, а также содержащих конфиденциальную информацию, по сети Интернет или электронной почте.

5.3.2. Использование сети Интернет для развлечения и получения информации, не относящейся к функциональным обязанностям пользователя.

5.3.3. Доступ к сети Интернет и электронной почте не со своего рабочего места с использованием данных свои учетной записи.

5.3.4. Предоставление доступа к сети Интернет с использованием данных своей учетной записи другим лицам.

5.3.5. Публикация своего адреса электронной почты в электронных каталогах и на поисковых машинах сети Интернет.

5.3.6. Подписка по электронной почте на различные рекламные материалы, диеты рассылки электронные журналы и т.п. не связанные с выполнением пользователем функциональных обязанностей.

5.3.7. Открытие (запуск на выполнение) файла, полученного из сети Интернет или по электронной почте, без предварительной проверки его антивирусным программным обеспечением. При нарушении пункта 5.3. пользователь без предупреждения отключается от работы в сети Интернет, при этом в известность ставится его непосредственный руководитель и администратор информационной безопасности.

6. Ответственность за нарушение требований Инструкции

Данная инструкция обязательна для выполнения всеми пользователями сети. Руководитель обязан ознакомить каждого работника с настоящей инструкцией под роспись. За неисполнение или ненадлежащее исполнение настоящей Инструкции работники Школы несут ответственность в соответствии с действующим законодательством.

7. Контроль за исполнением Инструкции

Контроль за исполнением настоящей Инструкции возлагается на администратора информационной безопасности, системного администратора, а также на руководителя Школы.