Муниципальное автономное общеобразовательное учреждение
«Средняя общеобразовательная школа № 133»
г. Пермь

ПРИНЯТО
Педагогическим советом школы
«31» августа 2015 г.
Протокол № 1

УТВЕРЖДАЮ:
Директор школы

_____
/Адамова Э.В.
«31» августа 2015 г.

ПОЛОЖЕНИЕ № 33
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ НА ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРАХ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ШКОЛЫ

1. Общие положения.

1.1. Целью настоящего Положения является определение основных требований, обязательных для исполнения при работе на персональных компьютерах (ПК) в локальной вычислительной сети школы.

1.2. Положение распространяется на выполнение любых работ посредством ПК.

1.3. Сотрудники школы, не работающие в кабинете информатики (в дальнейшем - пользователи) допускаются к работе на ПК только после ознакомления с настоящим Положением и Инструкцией по предоставлению доступа к сети и работе с антивирусными программами под роспись. Ответственность за ознакомление с Положением несет руководитель медиацентра, в котором осуществляется работа на ПК.

1.4. Контроль за исполнением требований настоящего Положения возлагается на руководителя медиацентра.

2. Требования к ПК в Школе.

2.1. ПК в школе должны удовлетворять следующим требованиям:

2.1.1. Все ПК должны быть подключены к ЛВС школы;

2.1.2. Отсутствуют или отключено аппаратное и программное обеспечение для передачи данных, минуя ЛВС;

2.1.3. Отсутствуют или отключены устройства для работы со сменными носителями информации (дисководы гибких дисков, CD ROM, Flash - носители) за исключением ПК руководителя медиацентра;

2.1.4. Опечатан системный блок;

2.1.5. Имеется паспорт компьютера, подписанные сотрудниками медиацентра, с перечисленными в нем техническими характеристиками, установленным системным программным обеспечением;

2.1.6. Имеется список пользователей ПК, допущенных к работе с указанием ответственного за эксплуатацию данного ПК;

2.1.7. Установлено антивирусное программное обеспечение. Обновление **антивирусных баз не реже "5" раз в неделю;**

2.1.8. Вход в BIOS закрыт паролем. Отключена загрузка ПК с внешних носителей (FDD, CD, LAN,...);

2.1.9. Смена пароля пользователя на доступ к ПК должна производится не реже 1 раза в 3 месяца, для администраторов не реже 1 раза в месяц;

2.1.10. Для ПК с операционной системой Win 2000, XP, 2003 правами "администратора" обладают только сотрудники медиацентра;

2.1.11. Для ПК с процессором 3-го поколения и выше файловая система основного раздела должна быть NTFS;

2.1.12. Папка для обмена информацией по ЛВС должна быть доступна на запись для файловых систем FAT, для систем NTFS - только на "Запись" и "Чтение содержимого папки".

При наличие на ПК диска с файловой системой NTFS папка для обмена должна располагаться только на этом диске.

2.2. Решение об изменении предъявляемых требований к отдельным ПК принимается руководитель медиацентра.

2.3. Копирование информации на компьютерах с отключенными устройствами для работы со сменными носителями информации осуществляет через руководителя медиацентра. Информацию для передачи по электронной почте при отсутствии возможности передает сотрудник медиацентра.

3. Порядок предоставления прав доступа к ПК, ресурсам и программам ЛВС Школы.

3.1. Предоставление сотрудникам школы прав доступа к необходимым для работы программам ЛВС выполняется по заявке сотрудников школы. При изменении должностных обязанностей сотрудника директор и/или заместитель директора по УВР направляет в медиацентр служебную записку на аннулирование прав доступа.

3.2. Предоставление лицам, не работающим в школе, но находящимся на территории МАОУ «СОШ №133», прав доступа к необходимым для работы программам ЛВС выполняется по служебной записке в медиацентр, согласованной с директором Школы. В служебной записке отражается наименование программы, причина предоставления доступа, период, на который необходимо предоставить доступ, фамилия, имя, отчество и паспортные данные лица, которому предоставляется доступ, имя компьютера и MAC- адрес, с которого необходим доступ.

3.3. Директор школы своим распоряжением определяет перечень сотрудников школы, имеющих доступ к каждому конкретному ПК.

3.4. Постоянный доступ к сети Интернет и личным почтовым ящикам предоставляется по письменному разрешению директора школы.

4. Пользователям запрещается:

4.1. использовать компоненты программного и аппаратного обеспечения в неслужебных целях;

4.2. посещать в Интернет сайты, содержащие информацию, не входящую в круг служебных обязанностей работника;

4.3. получать и отправлять по электронной почте программное обеспечение без согласования с руководителем медиацентра;

4.4. изменять параметры сетевой идентификации компьютера (имя, IP адрес);

4.5. предоставлять права удаленного доступа к системным ресурсам своего ПК (корневой раздел жесткого диска, на котором установлена операционная система, каталоги, в которых установлена операционная система);

4.6. самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые системные программные и аппаратные средства, не предусмотренные паспортом ПК;

4.7. отключать свой ПК от ЛВС;

4.8. снимать пломбу с компьютера;

4.9. предоставлять закреплённый за ними ПК в пользование другим лицам или сотрудникам, не имеющим права доступа согласно настоящего положение за исключением технического обслуживающего персонала;

4.10. записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации (гибких магнитных дисках и т.п.);

4.11. оставлять включенный без присмотра свой ПК, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

4.12. оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

4.13. использовать и хранить на рабочих местах съемные носители информации (Flash- карты, ZIP-приводы и т.п., в том числе цифровые фотокамеры) без специального разрешения;

4.14. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению конфликтной ситуации. Об обнаружении такого рода ошибок ставить в известность сотрудников медиацентра.

4.15. предпринимать попытки взлома компьютерной защиты ПК других пользователей, ЛВС Школы, ресурсов сторонних организаций;

4.16. предпринимать действия, направленные на несанкционированное получение прав доступа к программам, базам данных и иной информации, хранящейся в ЛВС, на ПК других пользователей;

4.17. сообщать кому бы то ни было, кроме непосредственного руководителя (записывать в доступном месте), свой пароль (пароли);

4.18. посылать в электронном виде информацию, содержащую сведения ограниченного распространения без применения программного обеспечения для ее защиты;

4.19. использовать файлы, полученные по почте, через Интернет или со сменных носителей без предварительной проверки на наличие вирусов;

4.20. получать и использовать удалённый доступ на управление ПК других пользователей и серверов.

5. Действия при возникновении неисправностей.

5.1. В случае неправильной работы программного обеспечения, обнаружении вирусов, технической неисправности ПК ставить в известность сотрудников медиацентра.

5.2. В случае проблем при работе с Интернет, электронной почтой обращаться в медиацентр.

6. Разграничение ответственности по информационной безопасности.

6.1. Ответственность за безопасность загруженной информации через Интернет и электронную почту, возлагается на пользователя осуществившего приём этой информации. Если пользователь не выявлен, то ответственность несёт лицо, закрёплённое за ПК;

6.2. Ответственность за информационную безопасность при работе в ЛВС Школы установку и обновление сетевого антивирусного программного обеспечения, своевременную установку заплат программных систем возлагается на сотрудников медиацентра.

7. Контроль за соблюдением требований по обеспечению информационной безопасности.

7.1. Контроль за соблюдением требований по обеспечению информационной безопасности осуществляют сотрудники медиацентра.

7.2. Использование Пользователями ПК, доступа в Интернет и электронной почты может наблюдаться, протоколироваться и периодически проверяться.

7.3. В целях проведения проверок устойчивости компьютерной защиты, соблюдения Пользователями требований настоящего Положения ответственными сотрудниками медиацентра могут проводиться проверочные мероприятия, не нарушающие целостность и работоспособность аппаратно-программных средств.

8. Ответственность.

8.1. За неисполнение требований по информационной безопасности сотрудники школы несут административную и дисциплинарную ответственность.

8.2. Ответственность за сохранность пломб, установленных на ПК, несет пользователь ПК. В случае нарушения целостности пломб, руководителем медиацентра совместно с директором Школы, проводится служебное расследование, с целью выявления нарушения и составления акта.