

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 № 34
РЕГЛАМЕНТ ПО РАБОТЕ УЧИТЕЛЕЙ И УЧАЩИХСЯ МАОУ «СОШ № 133» В
СЕТИ ИНТЕРНЕТ

I. Общие положения

"Точка доступа" к сети Интернет предназначена для обслуживания учителей и учеников школы. Сотрудники и учащиеся школы допускаются к работе на бесплатной основе.

К работе в Интернете допускаются пользователи, прошедшие предварительную регистрацию у администраторов соответствующих локальных сетей.

Выход в Интернет осуществляется с 8.00 до 19.00 (кроме воскресенья). Последняя пятница месяца - день профилактики.

Предоставление сеанса работы в Интернете осуществляется, как правило, через прокси- сервер на основании предварительной записи в журнале администратора соответствующей локальной сети или при наличии свободных мест в зависимости от категории пользователя:

- учащимся предоставляется доступ в компьютерных классах согласно расписанию занятий (график работы компьютерных классов составляется на основании ежемесячно подаваемых служебных записок на имя заместителя директора по ИКТ с приложением расписания занятий и учебных планов);
- учителям предоставляется доступ согласно ежемесячно подаваемым служебным запискам на имя заместителя директора (выдается регистрационное имя, пароль и график работы), но не менее 2 часов в неделю (ресурс может делиться на кванты времени, равные не менее 30 минутам);
- остальным пользователям предоставляется доступ при наличии резерва пропускной способности канала передачи.

Для работы в Интернете необходимо иметь при себе документ, удостоверяющий личность пользователя (пропуск учащегося, пропуск учителя или регистрационные карточки с логином и паролем).

По всем вопросам, связанным с доступом в Интернет, следует обращаться к администраторам соответствующих локальных сетей.

II. Правила работы

При входе в кабинет необходимо обратиться к администратору за разрешением для работы. При наличии свободных мест после регистрации в журнале учета посетителю

предоставляется в зале рабочая станция. Для доступа в Интернет и использования электронной почты установлены программные продукты, т.н. браузер "Internet Explorer" либо "Mozilla Firefox" (рекомендован по соображениям информационной безопасности), и клиент электронной почты "Mozilla Thunderbird", "Evolution". Отправка электронной почты с присоединенной к письму информацией, запись информации на дискеты и CD-диски осуществляются у администратора. Дополнительно установлено программное обеспечение: офисный пакет (OpenOffice или аналог), графический редактор растровой графики (GIMP или аналог).

1. Пользователь обязан выполнять все требования администратора.
2. В начале работы пользователь обязан зарегистрироваться в системе, т.е. ввести свое регистрационное имя (логин) и пароль.
3. За одним рабочим местом должно находиться не более одного пользователя.
4. Запрещается работать под чужим регистрационным именем, сообщать кому-либо свои регистрационные данные, одновременно входить в систему более чем с одной рабочей станции.
5. Каждому пользователю при наличии технической возможности предоставляется персональный каталог, предназначенный для хранения личных файлов общим объемом не более 5 Мб, а также возможность работы с почтовым ящиком для отправки и получения электронной почты.
6. Пользователю разрешается записывать полученную информацию на сменные носители (дискеты, usb-накопители и т.п.) только через рабочую станцию администратора. Все сменные носители должны предварительно проверяться на наличие вредоносного ПО.
7. Разрешается использовать оборудование только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения гуманитарных и культурных проектов. Любое использование оборудования в коммерческих целях запрещено.
8. Запрещена передача информации, представляющей коммерческую или государственную тайну, распространение информации, порочащей честь и достоинство граждан.
9. Запрещается работать с трафикоемкими ресурсами (видео, аудио, веб-чат, сетевые игры и др.) без согласования с администратором.
10. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.
11. Администратор сети обязан вести регулярный мониторинг трафика локальной сети при помощи соответствующих средств мониторинга. При выявлении признаков подозрительного трафика или появлении открытых портов на рабочих станциях и/или сервере совместного доступа он должен:
 - Прервать сеанс связи рабочей станции, генерирующей данные, вызвавшие подозрение.
 - Поставить в известность пользователя этой рабочей станции.
 - После окончания работы пользователя выполнить внеочередную проверку жесткого диска рабочей станции на наличие вредоносного ПО, при необходимости восстановить данные на жестком диске с резервной копии.
 - При обнаружении дополнительного открытого tcp-порта на рабочей станции администратора или на сервере совместного доступа к сети Интернет обратиться в

компанию, осуществляющую техническую поддержку, либо устранить проблему самостоятельно (при наличии необходимой квалификации).

- Пользователь обязан сохранять оборудование в целостности и сохранности.
- Пользователь обязан помнить свой пароль. В случае утраты пароля пользователь обязан сообщить об этом системному администратору.

При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность. За административное нарушение, не влекущее за собой порчу имущества и вывод оборудования из рабочего состояния, пользователь получает первое предупреждение и лишается права выхода в Интернет сроком на 1 месяц. При повторном административном нарушении пользователь лишается доступа в Интернет.

При возникновении технических проблем пользователь обязан поставить в известность администратора локальной сети.

III. Правила регистрации

Для доступа в Интернет пользователям необходимо пройти процесс регистрации.

1. Регистрационные логин и пароль учащиеся получают у заместителя директора через своего классного руководителя или учителя информатики.
2. Регистрационные логин и пароль учителя получают у заместителя директора при предъявлении удостоверения личности и письменного заявления.
3. После ввода сетевого имени и пароля пользователь получает сообщение об ошибке (тогда ее необходимо исправить) либо доступ.
4. Перед работой необходимо ознакомиться с памяткой и расписаться в журнале учета работы в Интернете, который хранится у администратора.

IV. Памятка по использованию ресурсов сети Интернет

1. В начале работы пользователь обязан зарегистрироваться в системе, т.е. ввести свое имя регистрации и пароль. После окончания работы необходимо завершить свой сеанс работы с операционной системой стандартным способом.
2. За одним рабочим местом должно находиться не более одного пользователя.
3. Запрещается работать под чужим регистрационным именем, сообщать кому-либо свой пароль, одновременно входить в систему более чем с одной рабочей станции.
4. Каждый пользователь при наличии технической возможности может иметь персональный каталог, предназначенный для хранения личных файлов общим объемом не более 5 Мб. Аналогично может быть предоставлена возможность работы с почтовым ящиком. При возникновении проблем необходимо обратиться к дежурному администратору.
5. Пользователю разрешается переписывать полученную информацию на сменные носители, которые предварительно проверяются на наличие вирусов на рабочей станции администратора.
6. Разрешается использовать оборудование классов для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения проектов. Любое использование оборудования в коммерческих целях запрещено.

7. Правовые отношения регулируются Законом "Об информации, информатизации и защите информации", Законом "О государственной тайне", Законом "Об авторском праве и смежных правах", статьями Конституции об охране личной тайны, статьями Гражданского кодекса и статьями Уголовного кодекса о преступлениях в сфере компьютерной информации.

8. Запрещается работать с трафикоемкими ресурсами (видео, аудио, веб-чат, сетевые игры и др.) без согласования с администратором.

9. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.

10. Пользователю запрещается перезагружать компьютер без согласования с администратором локальной сети.

При возникновении технических проблем пользователь обязан поставить в известность администратора локальной сети.

V. Программное обеспечение, рекомендованное к использованию для получения доступа к сети Интернет

Для работы с интернет-ресурсами и технического обеспечения доступа к сети Интернет Министерство образования Пермского края рекомендует использовать следующее программное обеспечение, распространяющееся на бесплатной основе либо включенное в состав операционной системы.

1. Рабочее место администратора:

1. Операционная система: Microsoft Windows XP Pro либо ASP Linux <1> 11.

2. Программа просмотра веб-страниц (браузер): Mozilla Firefox.

3. Программа работы с электронной почтой: Mozilla Thunderbird или Evolution.

4. Антивирусная программа: ClamAV с базами, актуализируемыми не реже чем раз в неделю. Допускается использование коммерческих антивирусных программ при условии соблюдения Лицензионных соглашений.

5. Офисный пакет: OpenOffice 2.x. Допускается использование коммерческих офисных пакетов при условии соблюдения Лицензионных соглашений.

6. Графический редактор для обработки растровых изображений: GIMP 2.x.

7. Средства авторизованного удаленного доступа к сменным носителям: SMB-сеть (стандартные средства операционных систем семейства Windows) либо NFS.

8. Средства мониторинга сетевого трафика: Ethereal.

9. Средства удаленного управления рабочими станциями пользователей: VNC.

2. Рабочее место пользователя:

1. Операционная система: Microsoft Windows XP Pro либо ASP Linux <1> 11.

2. Программа просмотра веб-страниц (браузер): Mozilla Firefox.

3. Программа работы с электронной почтой: Mozilla Thunderbird или Evolution.

4. Офисный пакет: OpenOffice 2.x. Допускается использование коммерческих офисных пакетов при условии соблюдения Лицензионных соглашений.

5. Графический редактор для обработки растровых изображений: GIMP 2.x.

6. Средства авторизованного удаленного доступа к жестким дискам: SMB-сеть (стандартные средства операционных систем семейства Windows) либо NFS.

3. Сервер совместного доступа к сети Интернет.

1. Операционная система: ASP Linux <1> 11.

<1> Рекомендуется использовать наиболее новый дистрибутив Linux семейств ASP, SuSE, Mandriva или аналогичный, поставщик которого предлагает не менее чем 30-дневную поддержку и выпускает обновления не реже чем 2 раза в год.

2. Прокси-сервер: Squid 2.x.
3. Средства IP-маршрутизации: IP-tables.
4. Антивирусная программа: ClamAV с базами, актуализируемыми не реже чем раз в неделю. Допускается использование коммерческих антивирусных программ при условии соблюдения Лицензионных соглашений.
5. Средства мониторинга сетевой активности: tcpdump, Ethereal.
6. Средства анализа локальной сети: nmap.
7. Средства удаленного управления сервером: OpenSSH.

VI. Рекомендации по настройке программного обеспечения

Для обеспечения бесперебойной и безопасной работы программно-аппаратных средств обеспечения доступа к сети Интернет рекомендуется выполнение следующих рекомендаций по настройке программного и аппаратного обеспечения:

1. Рабочее место администратора.

Настройки операционной системы должны исключать длительную работу оператора ПЭВМ с правами суперпользователя (администратора).

Должен быть обеспечен удобный (не более чем в 1 действие) способ проверки сменных носителей на наличие вредоносных программ.

Должна быть обеспечена возможность одновременного подключения от 5 до 10 сменных носителей с обеспечением к ним авторизованного сетевого доступа.

Доступ к сменным носителям, подключенным к рабочей станции администратора, должен быть обеспечен средствами локальной вычислительной сети.

2. Рабочее место пользователя.

Настройки операционной системы должны исключать длительную работу оператора ПЭВМ с правами суперпользователя (администратора).

Должен быть обеспечен удобный (не более чем в 1 действие) способ сетевого доступа к сменным носителям, подключенным к ПЭВМ администратора.

Должна быть обеспечена возможность автоматической удаленной проверки жестких дисков рабочей станции на наличие вредоносного ПО.

Подключение сменных носителей к другим рабочим станциям должно быть исключено (дисководы демонтированы, отключены программными средствами операционной системы либо заблокированы аппаратными заглушками; usb-порты, за исключением используемых для обеспечения функционирования рабочих станций, отключены программными средствами операционной системы либо заблокированы аппаратными заглушками).

3. Сервер совместного доступа к сети Интернет.

Настройки операционной системы должны исключать длительную работу оператора ПЭВМ с правами суперпользователя (администратора).

Программно-аппаратный комплекс не должен включать средства локального управления ЭВМ <2> (клавиатуру, мышь, монитор).

<2> В крайнем случае допускается отъединение сервера совместного доступа с рабочим местом администратора, в таком случае это требование не выполняется.

Программное обеспечение должно включать сервер периодического запуска служб, настроенный на автоматический запуск службы удаленной проверки жестких дисков рабочих станций на наличие вредоносного ПО.

Настройки средств IP-маршрутизации или межсетевого экрана должны исключать возможность удаленного доступа к внутренним ресурсам сети.

4. Архивирование.

Рабочее место администратора должно включать в себя привод DVD-RW (или аналог), предназначенный для еженедельного архивирования создаваемой информации. Архив должен включать не менее 3 копий (принцип "отец - дед - сын").

Должен быть создан архивный образ жесткого диска рабочей станции пользователя для аварийного восстановления системы.