Министерство образования Республики Карелия
государственное бюджетное общеобразовательное учреждение Республики Карелия
«Специальная (коррекционная) общеобразовательная школа – интернат № 21»
(ГБОУ РК «Школа-интернат № 21»)

УТВЕРЖДАЮ
Директор ГБОУ РК «Школа-интернат № 21»
_____И.А.Неровня
01.12.2014 г.

ПОЛОЖЕНИЕ О ПОЛИТИКЕ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ И ДОСТУПЕ В ИНТЕРНЕТ

государственного бюджетного общеобразовательного учреждения Республики Карелия «Специальная (коррекционная) общеобразовательная школа-интернат № 21»

1. Общие положения

1.1. Настоящее Положение регламентирует использование в ГБОУ РК «Школа-интернат №21» (далее – «школа») политику безопасности локальной вычислительной сети (далее - ЛВС) и является обязательным для исполнения всеми участниками образовательного процесса.

1.2. Настоящее положение составлено в соответствии со следующими Федеральными законами (далее – ФЗ) и документами:

- ФЗ «О безопасности» №2446-1;
- ФЗ «О правовой охране программ для электронных и вычислительных машин и баз данных» №3523-1;
- ФЗ «О государственной тайне» №5485-1;
- ФЗ «О связи» №15-ФЗ;
- ФЗ «Об информации, информатизации и защите информации» №24-ФЗ;
- ФЗ «Об участии в международном информационном обмене» №85-ФЗ;
- ФЗ «Об оперативно-розыскной деятельности» №144-ФЗ;
- «Гражданским кодексом РФ».
- Уставом школы.

1.3. Обеспечение безопасности ЛВС осуществляется комплексно с помощью технических средств и организационных мероприятий.

2. Оценка угроз безопасности.

Угроза	Источник	Степень опасности	Способы предотвращения
Выход из строя устройств	Естественный износ	Низкая	Резервное копирование информации и дублирование устройств, своевременная замена устройств
	Неполадки в линии электроснабжения	Средняя	Технические средства защиты
	Умышленная порча, кража	Средняя	Ограничение доступа к устройствам ЛВС
Несанкционированный доступ к информации	Разглашение пользователями паролей учётных записей	Высокая	Введение мер административной ответственности, разъяснительная работа
	Оставление без присмотра рабочего места	Крайне высокая	Введение мер административной ответственности, разъяснительная работа,

			автоматическая блокировка рабочего стола.
	Хакерские действия	Несущественная	Применение сетевых экранов, политика стойких паролей
Утрата информации	Случайное удаление	Крайне высокая	Резервное копирование, ограничение прав пользователей
	Вирусное заражение	Средняя	Антивирусная программа
Крах системы	Вирусное заражение	Средняя	Антивирусная программа
	Неумелое администрирование	Средняя	Повышение квалификации администратора ЛВС
	Программная ошибка	Средняя	Средства восстановления системы

2.1. Доступ к рабочим станциям и в сеть Интернет осуществляется неперсонифицировано с учётными записями пользователей «ученик», «учитель», «администратор»
2.2. Контроль доступа в Интернет осуществляется программным обеспечением TrafficInspector (Сертификат соответствия ОС-1-СТ-0080).

3. Пользователям запрещается:

3.1. использовать компоненты программного и аппаратного обеспечения ЛВС в целях, не относящихся к образовательному процессу и функционалу;
3.2. получать и отправлять каким-либо способом программное обеспечение;
3.3. самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств РС;
3.4. записывать и хранить информацию для служебного пользования ДСП и персональные данные ПД на локальных жестких дисках РС;
3.5. оставлять РС включенным без присмотра, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
3.6. оставлять без личного присмотра, где бы то ни было переносные устройства памяти или документы, содержащие информацию ДСП и ПД;
3.7. умышленно использовать недокументированные свойства и ошибки в программном обеспечении или настройках средств защиты, которые могут привести к нарушению политики безопасности, а также не ставить в известность администратора при обнаружении такого рода ошибок;
3.8. предпринимать действия, направленные на несанкционированное получение прав доступа к программам, базам данных и иной информации, хранящейся в ЛВС;
3.9. посылать в электронном виде информацию ДСП и ПД без применения программного обеспечения для ее защиты.

4. Организация работы сети.

4.1. настройка профилей производится администратором;
4.2. все файлы пользователей, базы данных, публичная информация, а также информация служебного пользования (ДСП) и персональные данные (ПД) могут храниться только на отказоустойчивых носителях сервера, доступ к которому разрешен только администратору ЛВС; доступ к серверу иным лицам предоставляется в особых случаях приказом директора школы, в котором должны быть указаны: цель данного разрешения и срок его действия;
4.3. информация ДСП и ПД хранится на разделах дисков и в базах данных, логический доступ к которым защищен и разграничен между группами пользователей программными средствами;

4.4. на всех РС и серверах ЛВЛ установлено антивирусное ПО, которое настроено на ежесуточное автоматическое обновление;
4.5. все РС и серверы ЛВЛ с операционной системой Microsoft настроены на ежесуточную автоматическую установку обновлений ПО Microsoft;
4.6. на серверы и РС запрещается устанавливать программное обеспечение с использованием программ для снятия защиты от нелицензионного использования, а также программы, требующие для корректной работы права, превышающие стандартные права пользователя, установленные администратором;
4.7. контроль над соблюдением политики безопасности и установлением виновных в ее нарушении осуществляет администратор ЛВС; в спорных ситуациях на основании приказа Директора школы для установления причин нарушения политики безопасности и виновных лиц привлекается сторонняя компетентная организация, которой администратор обязан предоставить все необходимые для этого права доступа; выводы этой экспертизы являются окончательными и не подлежат пересмотру в каком бы то ни было порядке.
4.8. Поддержка функционирования локальной сети и доступа в Интернет осуществляется администратором сети (далее – «администратор»).
4.9. Разглашение данных учетной записи «учитель», «администратор» пользователем является нарушением политики безопасности. Если оно повлекло утрату важной информации или разглашение конфиденциальных сведений, пользователь несет ответственность в соответствии с действующим законодательством о защите информации и авторских прав, а для сотрудников школы, кроме того, положениями Трудового кодекса, трудовым договором и должностной инструкцией.
4.10. Техническая экспертиза причин на предмет нарушения политики безопасности и выявления виновных лицах осуществляется

- администратором локальной сети по записям в журналах регистрации событий системы (лог-файлах),
- либо, по решению администрации школы, сторонней компетентной организацией.

4.11. Выводы технической экспертизы оформляются протоколом, являются окончательными и не подлежат пересмотру кем-либо.
4.12. Каждый пользователь имеет право зарегистрировать у администратора персональный адрес электронной почты и своевременно сообщать о его изменения. Этот адрес используется для идентификации пользователя при запросах на восстановление пароля учётных записей при невозможности направить такой запрос через почту в информационной системе «Электронный дневник/журнал».
4.13. Все заявки о неисправности, жалобы на работу оборудования и сети, запросы на восстановление забытых паролей направляются пользователями администратору.

5. Ограничения на использование ресурсов локальной сети и Интернет.

5.1. Основной принцип ограничений: «разрешено всё, что не запрещено».
5.2. В локальной сети школы в персональных каталогах запрещается хранить данные, не имеющие отношение к образовательному процессу школы. При обнаружении таких данных каталог пользователя немедленно полностью очищается.
5.3. Запрещен доступ к следующим ресурсам сети Интернет:

- сайты сексуального, экстремистского содержания,
- сайты знакомств,
- игровые и развлекательные сайты,
- кроме того, для обучающихся: средства электронного общения, социальные сети, за исключением предусмотренных учебными программами в отведённое для этой цели время,
- сайты, доступ к которым ограничен в порядке, установленном действующим законодательством.

6. Контроль.

6.1. Фиксирование факта нарушения настоящего положения и отнесение информационного ресурса (включая ресурсы сети Интернет) к одному из

запрещённых осуществляет инженер и педагоги, организующие занятия с использованием компьютерной техники.

6.2. Поскольку не существует принципиальной возможности полностью ограничить доступность определённых видов контента, контроль использования сети Интернет осуществляется фактическим обнаружением умышленного обращений к неразрешенному ресурсу.

6.3. Нарушители сетевой политики подвергаются наказанию: сотрудники школы – в соответствии с положениями КЗОТ, трудовым договором и должностной инструкцией; обучающиеся– предупреждение.