МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«УРЗУФСКАЯ ШКОЛА»

СОГЛАСОВАНО
на педагогическом совете
МБОУ «Урзуфская школа»

Протокол заседания педагогического совета
МБОУ «Урзуфская школа»
от «25» августа 2022 г. № 4

УТВЕРЖДЕНО
И.о. директора МБОУ «Урзуфская школа »

_____Л.В. Котлубей
Приказ МБОУ «Урзуфская школа»
№51/1 от «12» сентября 2022 г.

ПОЛОЖЕНИЕ

об информационной безопасности школы (по обеспечению безопасного доступа обучающихся к ресурсам сети Интернет и определению методов контроля процесса работы в сети Интернет)

Урзуф – 2022

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

В настоящем положении - инструкции рассматриваются наиболее значимые направления организации безопасного использования ресурсов сети Интернет (РСИ) в образовательных учреждениях (ОУ): контентная фильтрация, техническое и административное ограничение доступа к опасным и вредоносным РСИ, антивирусная защита, обучение пользователей безопасной работе с РСИ, формирование пользовательской культуры, одним из показателей которой может служить навык предпочтительного обращения к доброкачественным ресурсам, что особенно важно в отношении обучающихся ОУ.

Предлагаемая инструкция адресована руководству ОУ и содержит предписания административного, организационного и технического характера, исполнение которых поможет существенно обезопасить образовательную среду ОУ, повысить эффективность и качество освоения обучающимися РСИ, современных информационных технологий и способствовать созданию психологически благоприятной обстановки на уроках, учебных занятиях, на переменах.

Все административные предписания снабжены приложениями, в них приведены примеры типовых локальных актов (приказы директора) и относящихся к ним текстов соответствующих положений и инструкций, которые легко могут быть адаптированы к условиям конкретного ОУ. Особо отмечены те случаи, в которых локальные акты рекомендуется основывать на решениях общественного или педагогического совета ОУ.

Исполнение инструкции предполагает распределение между работниками ОУ функционала ответственности за информационную безопасность ОУ, за точку доступа к Интернету, за антивирусную защиту компьютерной техники, за защиту персональных данных, функционала системного администратора локальной информационной сети, однако на практике в ОУ принято совмещать некоторые обязанности в исполнении одного должностного лица, что централизует организацию процесса пользования РСИ и не противоречит действующему законодательству.

1. МЕРОПРИЯТИЯ ПО КОНТЕНТНОЙ ФИЛЬТРАЦИИ

1.1. Ознакомить лицо, ответственное за информационную безопасность ОУ, с «Методическими и справочными материалами для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих исключение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания», подготовленными Экспертным педагогическим сообществом в соответствии с рекомендациями Министерства образования и науки РФ (http://www.skf.edu.ru/Help.aspx).

1.2. Установить наличие / отсутствие локальных контентных фильтров (ЛКФ) Единой системы контентной фильтрации — СКФ (техническое ограничение доступа к информации) на всех персональных компьютерах, находящихся в ОУ и имеющих доступ к сети Интернет.

1.3. В случае отсутствия СКФ необходимо предпринять меры по её установке и пройти регистрацию ОУ на сайте, рекомендованном Министерством образования и науки РФ: http://www.skf.edu.ru .

1.4. Уведомить Департамент образования города Москвы об установке СКФ в ОУ с указанием количества подключённых устройств, наименования и количества СКФ, используемых в ОУ.

1.5. Рекомендовать педагогическому совету ОУ обсудить и по итогам обсуждения принять Правила использования сети Интернет в ОУ, Положение об Общественном совете ОУ по вопросам регламентации доступа к информации в сети Интернет и Классификатор информации, несовместимой с задачами образования и воспитания обучающихся, рекомендуемый для применения в образовательном учреждении, которые

затем совместно с составом Общественного совета ОУ, Инструкцией для сотрудников ОУ по вопросам регламентации доступа к информации в сети Интернет, Должностной инструкцией ответственного за работу «точки доступа к Интернету» в ОУ утвердить приказом директора (Приложение 1) .

1.6. Рекомендовать Общественному совету ОУ по вопросам регламентации доступа к информации в сети Интернет обсудить и по итогам обсуждения принять Классификатор информации, несовместимой с задачами образования и воспитания обучающихся, рекомендуемый для применения в образовательном учреждении, который затем утвердить приказом директора (Приложение 1).

2. МЕРОПРИЯТИЯ ПО АНТИВИРУСНОЙ ЗАЩИТЕ КОМПЬЮТЕРНОЙ ТЕХНИКИ В ОУ

2.1. Приказом директора ОУ утвердить Инструкцию по организации антивирусной защиты компьютерной техники в ОУ; назначить ответственного за антивирусную защиту компьютерной техники ОУ (Приложение 2).

2.2. Установить соответствие автоматизированных рабочих мест в ОУ Спецификации автоматизированного рабочего места, предоставляемого субъектами Российской Федерации в образовательные учреждения, подключаемые к сети Интернет, утверждённой Приказом Минобрнауки России и Мининформсвязи России от 30 июня 2006 г. N 176/85: http://mon.gov.ru/pro/pnpo/int/2772/ .

2.3. Составить список используемого программного обеспечения (ПО) в ОУ.

2.4. Ознакомиться с комплектацией лицензионных программных продуктов на сайте Некоммерческого партнёрства поставщиков программных продуктов: http://www.npppp.ru/complect/spisok/soderzhanie.htm .

2.5. Проверить комплектацию ПО в ОУ по списку.

2.6. При обнаружении факта использования нелицензионного ПО необходимо прекратить его использование и предпринять действия по закупке необходимых лицензий или по согласованию с методическими центрами (в зависимости от подчинения ОУ) использовать аналогичные программные продукты, распространяемые бесплатно — на основании Распоряжения Правительства РФ от 17 декабря 2010 г. № 2299-р «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения».

3. РЕГЛАМЕНТАЦИЯ ПОЛЬЗОВАНИЯ ЛИЧНЫМИ СРЕДСТВАМИ КОММУНИКАЦИИ (МОБИЛЬНЫМИ ТЕЛЕФОНАМИ И Т.П. И ЛИЧНОЙ КОМПЬЮТЕРНОЙ ТЕХНИКОЙ В ОУ)

3.1. Рекомендовать педагогическому совету ОУ обсудить и по итогам обсуждения принять Положение о регламенте пользования личными средствами коммуникации (мобильными телефонами и т.п.) в ОУ (Приложение 3).

3.2. Приказом директора утвердить вышеуказанное Положение.

3.3. Ознакомить с Положением всех работников ОУ и через классных руководителей всех обучающихся и их родителей (законных представителей).

3.4. Не допускать использование в ОУ работниками и обучающимися личной компьютерной техники (ноутбуков, нетбуков и т.п.), предоставляющей доступ к сети Интернет, без личного согласования с ответственным за информационную безопасность; поручить ответственному за информационную безопасность составить список сотрудников, использующих в связи со служебной необходимостью в ОУ личную компьютерную технику, предоставляющую доступ к сети Интернет.

4. РЕГЛАМЕНТАЦИЯ РАБОТЫ В ЛОКАЛЬНОЙ ИНФОРМАЦИОННОЙ СЕТИ ОУ

4.1. Приказом директора утвердить Положение о локальной информационной сети образовательного учреждения; назначить системного администратора локальной информационной сети ОУ (Приложение 4).

5. МЕРОПРИЯТИЯ С ОБУЧАЮЩИМИСЯ ПО ОСНОВАМ КУЛЬТУРЫ РАБОТЫ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

5.1. Рекомендовать методическому объединению учителей информатики (при отсутствии такового — учителям информатики) составить и реализовать на учебных занятиях и во внеклассной работе План повышения уровня безопасности детей в сети Интернет при помощи технических и технологических средств.

5.2. Поручить ответственному за информационную безопасность совместно с заместителем директора по воспитательной работе организовать проведение классных часов по тематике, раскрывающей правила безопасного поведения детей в сети Интернет (в качестве примера — уроки безопасного Интернета, разработанные Фондом развития Интернета совместно с МГУ им. М.В. Ломоносова при поддержке МТС: http//www.detionline.com/mts/lessons)

5.3. В рамках внеклассной работы поручить классным руководителям организовать проведение тематических семинаров обучающихся по обмену информацией об интересных и полезных ресурсах сети Интернет.

5.4. Поручить заместителю директора по воспитательной работе по итогам проведения тематических семинаров обучающихся организовать

- составление и ведение школьного каталога «Мой интересный Интернет» (примером может служить материал выпусков каталога «Образовательные ресурсы сети Интернет» Федерального агентства по образованию Мин. образования науки РФ: http://catalog.iot.ru/index.php),
- проведение конкурсов на наиболее интересную и многостороннюю подборку веб-ссылок на полезные сайты сети Интернет.

5.5. Поручить ответственному за информационную безопасность и заместителю директора по воспитательной работе регулярно публиковать результаты вышеуказанной работы на официальном сайте ОУ.

5.6. Поручить ответственному за информационную безопасность совместно с заместителем директора по воспитательной работе составить памятку или информационную страницу по вопросам культуры работы и информационной безопасности обучающихся в сети Интернет и разместить её на официальном сайте ОУ.

5.7. По возможности организовать полиграфическое издание и распространение информационных буклетов по проблеме безопасности детей в Интернете с приложением каталога сайтов, интересных и полезных для обучающихся.

6. МЕРОПРИЯТИЯ С РОДИТЕЛЯМИ ПО ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ

6.1. С периодичностью не реже 1 раз в учебный год необходимо проводить общешкольное и/или классные тематические родительские собрания, посвящённые вопросам информационной безопасности детей в сети Интернет (по возможности с участием специалистов в области компьютерной коммуникации).

6.2. Рекомендовать классным руководителям проводить в рамках родительских собраний семинары по обмену опытом обеспечения безопасности ребенка в информационном обществе.

7. ОБ ИСПОЛЬЗОВАНИИ В ОУ ДОСТУПА К СЕТИ ИНТЕРНЕТ, ПРЕДОСТАВЛЯЕМОГО СТОРОННИМ ПРОВАЙДЕРОМ

7.1. По возможности отказаться от использования в ОУ доступа к сети Интернет, предоставляемого сторонним провайдером, в контракте с которым не предусмотрена организация безопасного трафика.

7.2. Установить личную ответственность директора за возможные нежелательные последствия использования в ОУ доступа к сети Интернет, предоставляемого сторонним провайдером, в контракте с которым не предусмотрена организация безопасного трафика.

8. МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Приказом директора утвердить Положение о порядке обработки персональных данных в образовательном учреждении; назначить сотрудника, ответственного за защиту персональных данных в ОУ; определить перечень лиц, допущенных к обработке персональных данных; ознакомить с вышеуказанным Положением лиц, допущенных к обработке персональных данных, с подписанием ими обязательства о неразглашении информации, содержащей персональные данные (Приложение 5).

8.2. Поручить ответственному за информационную безопасность взять на особый контроль порядок размещения персональных данных на официальном сайте ОУ и передачи их посредством сети Интернет.

9. МЕРОПРИЯТИЯ ПО ОСУЩЕСТВЛЕНИЮ КОНТРОЛЯ ЗА ИСПОЛЬЗОВАНИЕМ РЕСУРСОВ СЕТИ ИНТЕРНЕТ В ОУ

9.1. С периодичностью не реже 1 раза в полугодие заслушивать лиц, ответственных за использование РСИ, с публичным отчётом на заседаниях педагогического совета ОУ по вопросам:

- выявления случаев нарушения безопасности использования РСИ с анализом причин, предпринятых мер и их результатов;
- технической исправности компьютерной техники и аксессуаров;
- состояния воспитательной работы по формированию пользовательской культуры работы обучающихся в сети Интернет.

Список нормативно-правовых актов и материалов, на которых основываются положения Инструкции

– Методические и справочные материалы для реализации комплексных мер по внедрению и использованию программно-технических средств, обеспечивающих исключение доступа обучающихся образовательных учреждений к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания. — М.: ООО «МегаВерсия», 2006.

– Письмо Руководителя Федерального агентства по образованию № 15-51-46 ин/01-10.

– Правила подключения общеобразовательных учреждений к единой системе контент-фильтрации доступа к сети Интернет, реализованной Министерством образования и науки РФ (№ АФ-12/07 (вн) от 11.05.2011г.).

– Распоряжение Правительства РФ от 17 декабря 2010 г. №2299-р «О плане перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения».

– Федеральный закон РФ от 26.07.2006 № 152-ФЗ «О персональных данных».

Приложение 1

«Согласовано»
Профсоюзным комитетом
Председатель ПК
_____/ В.И. Обмачевская
«___»_____20____г.

УТВЕРЖДАЮ
И.о.директора МБОУ
«Урзуфская школа »
_____Л.В.Котлубей
от «___»_____2022 г.

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
лица ответственного за доступ к сети Интернет и внедрение системы контентной фильтрации в образовательном учреждении

Ответственный за доступ к сети Интернет и ограничение доступа назначается приказом директора. В качестве ответственного за организацию доступа к сети Интернет может быть назначен заместитель директора по информационным технологиям, преподаватель информатики, другой сотрудник образовательного учреждения.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за работу в сети Интернет и внедрение системы контентной фильтрации руководствуется в своей деятельности Конституцией и законами РФ и Конституцией Донецкой Народной Республики, государственными нормативными актами органов управления образования всех уровней; Правилами и нормами охраны труда, техники безопасности и противопожарной защиты; Уставом и локальными правовыми актами общеобразовательного учреждения, а также настоящей должностной инструкцией.

1.2. Должен знать:

– дидактические возможности использования ресурсов сети Интернет;
– правила безопасного использования сети Интернет.

2. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

2.1. Планирует использование ресурсов сети Интернет в образовательном учреждении на основании заявок учителей и других работников образовательного учреждения;

2.2. Разрабатывает, согласует с педагогическим коллективом, представляет на педагогическом совете образовательного учреждения регламент использования сети Интернет в образовательном учреждении, включая регламент определения доступа к ресурсам сети Интернет;

2.3. Организует получение сотрудниками образовательного учреждения электронных адресов и паролей для работы в сети Интернет и информационной среде образовательного учреждения;

2.4. Организует контроль над использованием сети Интернет в образовательном учреждении;

2.5. Организует контроль над работой оборудования и программных средств, обеспечивающих использование сети Интернет и ограничение доступа;

2.6. Систематически повышает свою профессиональную квалификацию, общепедагогическую и предметную компетентность, включая ИКТ-компетентность, компетентность в использовании возможностей Интернета в учебном процессе;

2.7. Обеспечивает информирование организаций, отвечающих за работу технических и программных средств, об ошибках в работе оборудования и программного обеспечения;

2.8. Соблюдает правила и нормы охраны труда, техники безопасности и

Противопожарной защиты, правила использования сети Интернет.

3. ПРАВА

Вправе определять ресурсы сети Интернет, используемые обучающимися вучебном процессе на основе запросов преподавателей.

4. ОТВЕТСТВЕННОСТЬ

Несет ответственность за выполнение правил использования Интернета и ограничения доступа, установленного в образовательном учреждении.

Ознакомлен:

«Согласовано»
Профсоюзным комитетом
Председатель ПК
_____/ В.И. Обмачевская
«____»_____20____г.

УТВЕРЖДАЮ
И.о. директора МБОУ
«Урзуфская школа»
_____Л.В. Котлубей
от «___»_____2022 г.

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
ответственного за точку доступа к сети Интернет

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за работу в сети Интернет и ограничение доступа к информационными интернет - ресурсами назначается на должность директором школы.

1.2. Ответственный за работу в сети Интернет и ограничение доступа к информационными интернет - ресурсами подчиняется непосредственно директору и заместителю директора.

1.3. Ответственный за работу в сети Интернет и ограничение доступа к информационными интернет - ресурсами руководствуется в своей деятельности Конституцией и законами РФ и Донецкой Народной Республики, государственными нормативными актами органов управления образования всех уровней, Правилами и нормами охраны труда, техники безопасности и противопожарной защиты; Уставом и локальными правовыми актами школы, а также настоящей должностной инструкцией.

2. ОСНОВНЫЕ ЗАДАЧИ И ОБЯЗАННОСТИ

Ответственный за работу в сети Интернет и ограничение доступа к информационным интернет ресурсам в школе обеспечивает доступ сотрудников школы и учащихся к Интернету, а именно:

2.1. Следит за состоянием компьютерной техники и Интернет-канала «точки доступа к Интернету». В случае необходимости инициирует обращение к поставщику Интернет услуг (оператору связи). Осуществляет контроль ремонтных работ.

2.2. На всех компьютерах, имеющих выход в Интернет, устанавливает систему контентной фильтрации.

2.3. Находится в помещении «точки доступа к сети Интернет» на протяжении всего времени ее работы.

2.4. Ведет учет пользователей «точки доступа к сети Интернет». В случае необходимости лимитирует время работы пользователя в Интернете.

2.5. Оказывает помощь пользователям «точки доступа к Интернету» во время сеансов работы в Сети.

2.6. Участвует в организации повышения квалификации сотрудников школы по использованию Интернета в профессиональной деятельности.

2.7. Осуществляет регулярное обновление антивирусного программного обеспечения. Контролирует проверку пользователями внешних электронных носителей информации(дискет, CD-ROM, флеш-накопителей) на отсутствие вирусов.

2.8. Принимает участие в создании (и актуализации) школьной веб-страницы.

3. ПРАВА

Ответственный за работу «точки доступа к сети Интернет» в школе имеет право:

3.1. Участвовать в административных совещаниях при обсуждении вопросов, связанных с использованием Интернета в образовательном процессе и управлении школой.

3.2. Отдавать распоряжения пользователям «точки доступа к сети Интернет» в рамках своей компетенции.

3.3. Ставить вопрос перед директором школы о нарушении пользователями «точки доступа к сети Интернет» правил техники безопасности, противопожарной безопасности, поведения, регламента работы в Интернете.

4. ОТВЕТСТВЕННОСТЬ

Ответственный за работу «точки доступа к сети Интернет» в школе несет полную ответственность за:

4.1. Надлежащее и своевременное выполнение обязанностей, возложенных на него настоящей должностной инструкцией.

4.2. Соблюдение Правил техники безопасности, противопожарной безопасности и норм охраны труда в школе.

4.3. Состояние делопроизводства по вверенному ему направлению работы.

Ознакомлен:

Приложение 2

ИНСТРУКЦИЯ
по организации антивирусной защиты компьютерной техники в МБОУ «Урзуфская школа»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. В ОУ используется только лицензионное антивирусное программное обеспечение.

1.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмный носитель).

1. 3. Файлы, помещаемые в электронный архив, в обязательном порядке должны подвергаться антивирусному контролю.

1.4. Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется на отсутствие вирусов.

1.5. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения регистрируется в специальном журнале за подписью лица, ответственного за антивирусную защиту.

2. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ МЕРОПРИЯТИЙ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

2.1. Ежедневно в начале работы при загрузке компьютера (для серверов локальной сети — при перезапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.

2. 2. Периодические проверки электронных архивов проводятся не реже одного раза в неделю.

2.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера выполняется:

- непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети); выполняется антивирусная проверка на серверах и персональных компьютерах образовательного учреждения. Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения регистрируется в специальном журнале за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего;
- при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

2.4. В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения заражённых вирусом файлов ответственного за обеспечение информационной безопасности в учреждении;
- совместно с владельцем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение заражённых файлов;

– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусную защиту направляет заражённый вирусом файл на гибком магнитном диске в организацию, с которой заключён договор на антивирусную поддержку для дальнейшего исследования.

3. ОТВЕТСТВЕННОСТЬ

3.1. Ответственность за организацию антивирусной защиты возлагается на ответственного за антивирусную защиту компьютерной техники, назначенного приказом директора ОУ.

3.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящего Положения возлагается на ответственного за антивирусную защиту компьютерной техники.

3.3. Периодический контроль за состоянием антивирусной защиты в гимназии осуществляется директором.

Приложение 3

СОГЛАСОВАНО
на Педагогическом совете
Протокол №4
от «25» августа 2022 г.

УТВЕРЖДАЮ
И.о.директора МБОУ
«Урзуфская школа»
_____Л.В. Котлубей
от «___»_____2022 г.

ПОЛОЖЕНИЕ

о регламенте пользования личными средствами коммуникации
(мобильными телефонами и т.п.)
в МБОУ «Урзуфская школа»

Урзуф – 2022

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в соответствии с Конституцией РФ, Федеральным законом РФ «Об образовании», федеральными законам и РФ от 29.12.10 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», «О персональных данных».

1.2. Настоящее положение распространяется на обучающихся, работников муниципального бюджетного общеобразовательного учреждения «Урзуфская школа» (*далее* - школа) с целью упорядочения и улучшения организации режима работы школы, защите личного достоинства и гражданских прав субъектов образовательного процесса: обучающихся, их родителей (законных представителей), работников школы.

1.3. Соблюдение настоящего Положения:

– содействует повышению качества и эффективности учебно-воспитательного процесса;

– способствует созданию психологически благоприятных условий проведения уроков и учебных занятий;

– обеспечивает защиту образовательного пространства от попыток пропаганды культа насилия, жестокости, порнографии и защиту обучающихся от информации, причиняющей вред их здоровью;

– обеспечивает повышение уровня дисциплины;

– гарантирует психологически комфортные условия образовательного процесса.

2. ОСНОВНЫЕ ПОНЯТИЯ

Личное средство коммуникации (далее ЛСК) — личное беспроводное мобильное средство сотовой связи, основным предназначением которого является вербальная (речевая) коммуникация: мобильный телефон, смартфон, iPod и т.п.

К ЛСК не относятся ноутбук, нетбук, планшетный компьютер, игровая приставка и т.д., т. к. они имеют другие основные предназначения.

Пользователь - работник ОУ или обучающийся, пользующиеся ЛСК.

3. ЦЕЛИ ИСПОЛЬЗОВАНИЯ ЛСК В ОУ

3.1. Цели использования ЛСК - установление и поддержания связи с абонентами сотовой сети в случае возникновения служебной необходимости у работников ОУ или в экстренных случаях у обучающихся и работников ОУ.

3.2. Нецелесообразным следует считать использование в ОУ не указанных выше возможностей ЛСК и сервисов, предоставляемых операторами мобильной связи: доступ к сети Интернет, видео- и фотосъѐмка,видеопросмотр, игра, аудиозапись.

4. УСЛОВИЯ ИСПОЛЬЗОВАНИЯ ЛСК В ГИМНАЗИИ

4.1. Каждый Пользователь обязан знать и соблюдать следующие условия и правила использования ЛСК в школе:

- в здании школы необходимо переводить ЛСК в беззвучный режим вызова (виброзвонок);
- во время проведения уроков и учебных занятий обучающимся и преподавателям необходимо отключать ЛСК, а обучающимся убирать ЛСК в портфели или в карманы одежды;
- прослушивание во время перемен радио и музыки посредством ЛСК не допускается;
- ответственность за сохранность ЛСК несѐт только его владелец (родители, законные представители владельца). Все случаи хищения имущества рассматриваются по заявлению и преследуются в соответствии с законодательством РФ.

4.2. Пользователям не рекомендуется нецелесообразное (см. п. 3.2.) использование ЛСК в школе.

4.3. Пользователям категорически запрещается:

- использовать ЛСК во время проведения уроков и учебных занятий в любом режиме (в том числе как калькулятор, записную книжку), за исключением случаев, специально разрешенных преподавателем;
- на территории школы использовать ЛСК для доступа к сети Интернет;
- распространять посредством ЛСК информацию, не совместимую с целями воспитания и образования обучающихся;
- сознательно наносить вред имиджу школы посредством ЛСК (съѐмка постановочных сцен насилия, актов вандализма, порчи имущества, личных вещей и т. п.).

5. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПОЛОЖЕНИЯ

5.1. За однократное нарушение Пользователем Положения, оформленное докладной запиской на имя директора школы, объявляется замечание, требующее объяснение поведения нарушителя в объяснительной записке.

5.2. При повторных фактах нарушения Положения со стороны работника Гимназии директором может быть наложено административное взыскание в виде выговора или, в зависимости от характера нарушения, осуществлено привлечение к ответственности через правоохранительные органы в порядке, предусмотренном законодательством РФ.

5.3. При повторных фактах нарушения Положения со стороны обучающегося проводится собеседование администрации школы с родителями обучающегося (законными представителями) с последующим дисциплинарным взысканием.

6. ИНЫЕ ПОЛОЖЕНИЯ

6.1. Родителям (законным представителям) не рекомендуется звонить своим детям (обучающимся) во время образовательного процесса. Следует ориентироваться на расписание звонков, размещѐнное на сайте школы и записанному в дневниках учащихся.

6.2. В случае форс-мажорных обстоятельств для связи со своими детьми во время образовательного процесса родителям (законным представителям) рекомендуется передавать сообщения через приемную по телефонам, размещѐнным на сайте и записанных в дневниках обучающихся.

6.3 При необходимости постоянного использования ЛСК во время образовательного процесса пользователь должен представить директору школы или дежурному администратору аргументированное объяснение (медицинское заключение, объяснительную записку и т.д.) и получить письменное разрешение.

6.4. При использовании ЛСК в здании школы соблюдать следующие этические нормы:

- не следует использовать в качестве звукового сигнала то, что может оскорбить или встревожить окружающих (нецензурная лексика, грубые резкие выражения и звуки и т.п.);
- разговаривать следует максимально тихим голосом;
- не вести приватные разговоры с использованием средств мобильной связи.

7. ПОРЯДОК ОБЕСПЕЧЕНИЯ СОХРАННОСТИ СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

7.1. Администрация МБОУ «Урзуфская школа» не несѐт материальной ответственности за утерянные средства мобильной связи и другие портативные электронные устройства.

7.2. В целях сохранности средств мобильной связи участники образовательного процесса обязаны: не оставлять свои средства мобильной связи и другие портативные электронные устройства без присмотра, в том числе в карманах верхней одежды.

Приложение 4

СОГЛАСОВАНО
на Педагогическом совете
Протокол №4
от «25» августа 2022 г.

УТВЕРЖДАЮ
И.о.директора МБОУ
«Урзуфская школа»
_____Л.В.Котлубей
от «__»_____2022 г.

ПОЛОЖЕНИЕ
о локальной информационной сети образовательного учреждения

Урзуф – 2022

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Локальная информационная сеть образовательного учреждения **(далее ЛС)** представляет собой организационно-технологический комплекс, созданный для взаимодействия информационных ресурсов гимназии, а также для интеграции локальных компьютерных сетей в единую сеть района.

1.2. ЛС обеспечивает возможность выхода пользователей во внешние сети и удалённый доступ для пользователей к общим информационным ресурсам гимназии и других учреждений системы образования.

1.3. ЛС является технической и технологической основой эффективного функционирования информационных узлов (серверов) школы, обеспечивающих информационную поддержку научной, методической и преподавательской деятельности сотрудников системы образования, включая систему документооборота, а также сферу административного управления.

1.4. Настоящее Положение определяет основные принципы и правила функционирования ЛС, а также права, обязанности и ответственность системных администраторов и пользователей сети.

2. ОСНОВНЫЕ ЗАДАЧИ ФУНКЦИОНИРОВАНИЯ ЛС И РАСПРЕДЕЛЕНИЕ ОБЯЗАННОСТЕЙ

2.1. Основными задачами формирования и эксплуатации ЛС являются: создание, развитие и обеспечение функционирования организационной, технической, программно-методической и технологической информационной инфраструктуры в целях использования глобальных телекоммуникационных сетей для информационного обеспечения научной, методической, преподавательской деятельности, а также административного управления; обеспечение информационного межсетевого взаимодействия в рамках выполняемых проектов.

2.2. Техническое и технологическое развитие ЛС с учётом потребностей школы осуществляются сетевым администратором ЛС на основании решений, утверждённых руководителем школы, а также силами сторонних организаций, привлекаемых на договорной основе.

3. ФУНКЦИОНАЛЬНАЯ СТРУКТУРА ЛС

3.1. ЛС – организационно-технологический комплекс, состоящий из следующих функциональных частей:

- средства доступа к глобальным сетям и передачи информации;
- средства защиты информации (межсетевые экраны как аппаратные, так и программные);
- средства коммутации (коммутаторы, хабы);
- серверное оборудование;
- рабочие места на базе персональных компьютеров.

3.2. Хранилища информационных ресурсов ЛС могут быть размещены на серверах информационных узлов.

4. УПРАВЛЕНИЕ РАБОТОЙ ЛС

4.1. Управление работой и обеспечение работоспособности сетевых, информационных, программных, информационных и технологических ресурсов ЛС осуществляются Системным администратором ЛС.

4.2. Управление работой сети включает в себя:

- обеспечение информационной безопасности;
- управление информационным обменом локальной сети с внешними сетями телекоммуникаций;

– управление информационными потоками внутри локальной сети;
– регистрацию информационных ресурсов и их разработчиков;
– управление доступом к информационным ресурсам;
– управление процессами размещения и модификации информационных ресурсов;
– регистрацию (подключение и отключение) рабочих мест;
– регистрацию Пользователей сети и Администраторов, определение их полномочий и прав по доступу к сетевым и информационным ресурсам данной сети;
– выбор используемых в локальной сети программных инструментальных средств;
– разрешение конфликтных ситуаций «Пользователь – сеть».

4.3. Для Пользователей локальной сети требования Системного администратора подразделений сети являются обязательными.

5. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛС

5.1. Обеспечение информационной безопасности ЛС необходимо в целях:
– защиты информационных, сетевых, технологических, программных и информационных ресурсов сети от попыток причинения вреда, ущерба (уничтожения, повреждения) или несанкционированного доступа;
– сохранности информационных ресурсов сети в случаях нарушений работоспособности сети и элементов её технического и технологического обеспечения;
– выполнения требований законов РФ и ДНР в сфере информационной безопасности, а также соответствия положениям, нормам и актам, предъявленным надзирательными органами.

5.2. Информационная безопасность сети обеспечивается путем:
– использования технических, технологических, программных и организационных средств защиты информационных программных и информационных ресурсов сети от попыток причинения вреда, ущерба или несанкционированного доступа,
– использования обязательной регистрации и документирования информационных ресурсов сети,
– использования резервного копирования информационных ресурсов сети в целях обеспечения их сохранности;
– осуществления Системными администраторами мер по разграничению доступа к информационным ресурсам Корпоративной сети, путем определения конфигураций и настроек программного, технического и сетевого обеспечения.

5.3. В целях обеспечения информационной безопасности Системный администратор сети обязан контролировать трафик, адресацию и источники сообщений, приходящих в сеть и исходящих из неё, выявлять и идентифицировать попытки несанкционированного доступа к ресурсам сети.

6. ФУНКЦИИ СИСТЕМНОГО АДМИНИСТРАТОРА ЛС

6.1. Системный администратор ЛС принимает меры к обеспечению работоспособности и информационной безопасности ЛС. Системный администратор обязан поддерживать заданные настройки программного обеспечения и технического оборудования, выполнять рекомендации по установке программного обеспечения на серверах и компьютерах ЛС.

6.2. Системные администраторы обеспечивают:
– работоспособность технических, сетевых ресурсов и информационную безопасность сети;
– регистрацию Пользователей сети;
– реализацию полномочий и прав доступа к сетевым, информационным

ресурсам сети.

– создание и поддержку единой технической, программно-методической и технологической инфраструктуры локальных сетей;

– документирование и регистрацию информационных ресурсов сети и разработчиков информационных ресурсов, размещение информационных ресурсов и прекращение доступа к ним;

– организационное и технологическое обеспечение выхода пользователей во внешние сети и доступа извне к информационным ресурсам других локальных сетей через информационные узлы;

– создание и модификацию баз информационных ресурсов;

– создание учетных записей пользователей; отключение и регистрацию рабочих мест пользователей; подключение, отключение и тестирование правильности настроек серверов и маршрутизаторов локальных сетей, входящих в состав ЛС;

– предотвращение несанкционированного доступа извне к ресурсам сети;

– проведение учебной и консультативной работы с пользователями ЛС;

– эксплуатацию программного обеспечения для регистрации, анализа, обработки и учёта данных о пользователях.

7. ПОЛЬЗОВАТЕЛИ ЛС, ИХ ПРАВА И ОБЯЗАННОСТИ

7.1. Пользователями сети являются сотрудники образовательного учреждения, прошедшие установленную процедуру регистрации в качестве Пользователей. В ходе регистрации за каждым Пользователем закрепляется имя, пароль и одно или несколько определенных рабочих мест.

7.2. Пользователь сети обязан:

– использовать доступ к локальным и глобальным сетям только в профессиональных и служебных целях;

– не использовать информационные и технические ресурсы сети в коммерческих целях и для явной или скрытой рекламы услуг, продукции и товаров любых организаций и физических лиц, за исключением образовательных услуг, а также продукции и товаров, предназначенных для обеспечения образовательного процесса;

– исключить возможность неосторожного причинения вреда (действием или бездействием) техническим и информационным ресурсам сети;

– не предпринимать попыток несанкционированного доступа к информационным ресурсам локальных и глобальных сетей, доступ к которым осуществляется через сеть (в том числе не пытаться бесплатно или за чужой счёт получить платную информацию);

– перед использованием или открытием файлов, полученных из других источников, проверять файлы на наличие вирусов;

– не использовать доступ к ЛС для распространения и тиражирования информации, распространение которой преследуется по закону, заведомо ложной информации и информации, порочащей организации и физические лица, а также служебной информации.

– не распространять ни в какой форме (в том числе в электронном или печатном виде) информацию, приравненную к служебной информации, полученную из информационных ресурсов сети.

7.3. Пользователи имеют право на:

– размещение своего почтового ящика на одном из почтовых серверов Корпоративной сети в установленном порядке;

– обращение к платной информации, имеющейся в глобальной сети, с разрешения руководителя гимназии. В этом случае пользователи оплачивают получаемые ими услуги самостоятельно и предоставляют документы, подтверждающие

оплату.

7.4. Пользователям сети запрещено:

– использование программ, осуществляющих сканирование сети (различные снифферы, сканеры портов) и тому подобные действия без письменного предупреждения системного администратора с объяснением служебной необходимости подобных действий;

– устанавливать дополнительные сетевые протоколы, вносить изменения в конфигурации настроек сетевых протоколов без ведома системного администратора;

– пользоваться просмотром видео, за исключением случаев, связанных со служебной необходимостью;

– отправлять по электронной почте объёмные файлы (музыку, видео) за исключением случаев, связанных со служебной необходимостью;

– открывать файлы и запускать программы на локальном компьютере из непроверенных источников или принесённых с собой на переносных носителях без предварительного сохранения на локальном жёстком диске и без последующей проверки антивирусной программой;

– хранить на публичных сетевых дисках файлы, не относящиеся к выполнению текущих задач работы в сети или к образовательному процессу в целом (игры, фото, видео, виртуальные CD и т.п.);

– просматривать и распространять в сети ссылки на сайты порнографической, развлекательной направленности и сайты, содержание которых не относится напрямую к текущим задачам работы в сети;

– использовать программы для зарабатывания денег в сети Интернет;

– скачивать и распространять в ЛС музыкальные и видео- и фотоматериалы, не имеющие отношения к текущим задачам работы в сети;

– открывать на локальном компьютере приложения к почте из непроверенных источников без предварительного сохранения на локальном жёстком диске и без последующей проверки антивирусной программой.

7.5. Пользователь сети может входить в сеть только под своими именем и паролем, полученными в ходе регистрации Пользователя в сети. Передача Пользователем имени и пароля другому лицу запрещена.

8. ПОРЯДОК РЕГИСТРАЦИИ И ПЕРЕРЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ ЛС

8.1. Регистрация Пользователя ЛС производится бессрочно.

8.2. В ходе регистрации определяются сетевое имя Пользователя и его пароль.

8.3. Регистрация Пользователя сети аннулируется:

– по представлению руководителя образовательного учреждения, в котором работает Пользователь;

– по представлению Системного администратора сети в случае нарушения Пользователем требований настоящего Положения;

– в связи с прекращением трудовых отношений.

8.4. В случае прекращения регистрации Пользователя в связи с прекращением трудовых отношений руководитель образовательного учреждения, в котором работает Пользователь, извещает об этом системного администратора не менее, чем за неделю до даты увольнения.

9. ПОРЯДОК ПОДКЛЮЧЕНИЯ И ОТКЛЮЧЕНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ ЛС

9.1. Документирование и регистрация конкретных информационных ресурсов ЛС производится Системным администратором по окончании работ по созданию или

модификации каждого ресурса, после передачи копии ресурса на магнитном носителе и предоставления заявки на регистрацию информационного ресурса.

9.2. Отключение ресурса и прекращение доступа к нему производится:

– в установленный в ходе регистрации срок,

– при нарушении установленных при регистрации сроков обязательной модификации ресурса,

– по представлению владельцев ресурса.

9.3. Перерегистрация информационных ресурсов и их владельцев производится планово, не реже одного раза в год.

10. ОТВЕТСТВЕННОСТЬ, ВОЗНИКАЮЩАЯ В СВЯЗИ С ФУНКЦИОНИРОВАНИЕМ ЛС

10.1. Ответственность, возникающая в связи с функционированием сети, определяется в соответствии с действующим законодательством РФ и настоящим Положением.

10.2. Ответственность может разделяться между руководителем образовательного учреждения и его заместителями, где нарушена работоспособность сети или её информационная безопасность, Системным администратором сети в пределах своей компетенции в соответствии с данным Положением.

10.3. Пользователь сети, за которым закреплено определённое рабочее место, несет ответственность за соблюдение установленных настоящим Положением требований.

10.4. Пользователь сети обязан при невозможности обеспечить выполнение требований данного Положения немедленно информировать об этом Системного администратора сети (по электронной почте, письменно, по телефону или лично).

10.5. Системный администратор обо всех случаях нарушения настоящего Положения обязан в письменном виде информировать руководителя гимназии.

10.6. При систематическом нарушении требований настоящего Положения Пользователями конкретного подразделения производится отключение зарегистрированного рабочего места (локальной сети) соответствующего подразделения (пользователя) от ЛС.

10.7. В случае возникновения ущерба или причинения вреда имуществу, правам, репутации в результате деятельности Пользователя (ей) сети возмещение ущерба является обязанностью пользователя (ей), чьи действия послужили причиной возникновения конкретного ущерба или вреда. Такое возмещение производится добровольно или по решению суда в соответствии с действующим законодательством РФ.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Действие настоящего Положения распространяется на лиц, работающих или обучающихся в образовательном учреждении, зарегистрированных в качестве Пользователей сети.

11.2. Все изменения и дополнения в настоящее Положение вносятся исходя из потребностей гимназии и изменений имеющихся материальных и информационных ресурсов, и утверждаются руководителем школы.

Приложение 5

СОГЛАСОВАНО
на Педагогическом совете
Протокол №4
от «25» августа 2022 г.

УТВЕРЖДАЮ
И.о.директора МБОУ
«Урзуфская школа»
_____Л.В. Котлубей
от «__»_____2022 г.

ПОЛОЖЕНИЕ

лиц, допущенных к обработке персональных данных, с подписанием ими обязательства о неразглашении информации, содержащей персональные данные

Урзуф – 2022

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет общие положения работы лиц (далее – пользователей), допущенных к обработке персональных данных (далее – ПДн), по вопросам обеспечения защиты информации при обработке конфиденциальных документов в ОмГУПС.

1.2. Допуск пользователей для работы с ПДн осуществляется ответственным за эксплуатацию и обеспечение безопасности информации в соответствии со списком сотрудников, допущенных к обработке ПДн.

1.3. ПДн, согласно Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», являются конфиденциальной информацией.

1.4. С учетом большого объема (массовости) документов, содержащих ПДн, и строго регламентированного порядка их хранения пометка конфиденциальности на них не ставится.

1.5. Допуск сотрудников к обработке ПДн, осуществляется ответственным за эксплуатацию и обеспечение безопасности информации, в соответствии со списком сотрудников, допущенных к обработке ПДн, утверждаемом приказом ректора.

1.6. Вскрытие и сдача под охрану помещений, где ведется обработка ПДн, осуществляется сотрудниками допущенными к обработке ПДн. и которым для выполнения своих должностных обязанностей необходим доступ в данное помещение.

1.7. Новый сотрудник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой ПДн, только после успешного прохождения первичного инструктажа по защите ПДн.

1.8. Лица, осуществляющие обработку ПДн, подписывают обязательство о неразглашении информации, содержащей ПДн.

1.9. Материальные носители, содержащие ПДн - это дела, книги и журналы учета, договоры, иные носители информации, содержащие ПДн с зафиксированной на нем в любой форме информацией, содержащей ПДн субъектов персональных данных в виде текста, фотографии и (или) их сочетания.

1.10. При хранении материальных носителей ПДн должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ, а также раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

1.11. Уничтожение или обезличивание части ПДн, если это допускается Носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе ПДн (удаление, вымарывание).

1.12. Уничтожение материальных носителей ПДн осуществляются путем шредирования (измельчение, гидрообработка) и (или) уничтожение через термическую обработку (сжигание).

1.13. Носители, не подлежащие уничтожению в соответствии с Федеральными

законами и иными нормативными правовыми актами, подлежат сдаче в архив. Хранение архивных документов, содержащих ПДн, в архивном фонде, осуществляется всоответствии с Федеральным законом «Об архивном деле в Российской Федерации» от 22.10.2004 г. № 125-ФЗ.

1.14. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в них ПДн, если иное не предусмотрено законодательством Российской Федерации. Не допускается отвечать на вопросы, связанные с передачей ПДн, по телефону или факсу.

2. ПОЛЬЗОВАТЕЛЬ ИМЕЕТ ПРАВО

2.1. Пользователи наделяются правом в отведенное им время решать поставленные задачи в соответствии с их должностной инструкцией, при этом указанным лицам предоставляется право обрабатывать только те ПДн, которые необходимы для выполнения их конкретных функций.

2.2. По всем вопросам, возникающим при работе с ПДн обращаться к ответственному за организацию обработки ПДн, администратору безопасности.

3. ПОЛЬЗОВАТЕЛЬ ОБЯЗАН

3.1. Вся информация, содержащая персональные данные должна вобязательном порядке хранится и обрабатываться в персональном компьютере в папке: D:\ CONFIDENTIALLY\, за исключением базы данных .

3.2. В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем самостоятельно. В случае отказа системы в идентификации пользователя, либо не подтверждения личного пароля следует немедленно обратиться к администратору безопасности.

3.3. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, владельца пароля хранилище.

3.4. При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами (видеокамерами и т.д.).

3.5. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, при работе на нижнем этаже шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

3.6. В случае компрометации паролей, т.е. при:

- физической утери носителя с информацией;
- передачи идентификационной информации по открытым каналам связи;
- визуальном осмотре носителя идентификационной информации посторонним лицом;
- перехвате пароля техническими средствами;
- сознательной передачи информации постороннему лицу,

необходимо сообщить ответственному за эксплуатацию информационной системы персональных данных и администратора безопасности информации.

3.7. Пользователи перед началом работы с отчуждаемыми носителями информации (USB-флэш-накопитель, CD\DVD диск) обязаны проверить их на наличие (отсутствие) компьютерных вирусов с использованием штатных антивирусных программ. Ярлык для запуска антивирусной программыдолжен быть вынесен в окно «Рабочий стол» системы Windows.

3.8. При обнаружении компьютерного вируса пользователь обязан немедленно поставить в известность администратора безопасности и прекратить какие-либо действия .

3.9. Пользователи, работающие с электронной цифровой подписью или

использующие шифрование, обязаны соблюдать Инструкцию по обращению со средствами криптографической защиты информации.

3.10. Пользователи, работающие с ПДн, обязаны использовать данную информацию исключительно для целей, связанных с выполнением своих должностных обязанностей.

3.11. Не передавать и не разглашать третьим лицам информацию, содержащую ПДн, в случае расторжения трудового договора, освобождения от замещаемой должности, увольнения, прекратить обработку ПДн, ставших известными в связи с исполнением должностных обязанностей. Все материальные носители (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении Пользователя в связи с выполнением должностных обязанностей, он должен передать ответственному за эксплуатацию и обеспечение безопасности информации;

3.12. При работе с документами, содержащими ПДн, пользователь обязан исключить возможность неправомерного или случайного доступа к ним, уничтожения, изменения, копирования, распространения ПДн, а также от иных неправомерных действий лицами, не допущенными к работе с ними (в том числе другими работниками ОмГУПС).

3.13. После подготовки и передачи документа файлы, копии, черновики документа переносятся подготовившим их пользователем на маркированные материальные носители, предназначенные для хранения ПДн, или уничтожаются установленным путем.

3.14. При выходе в течение рабочего дня из помещения убирать материальные носители ПДн и обеспечивать невозможность несанкционированного доступа к ПДн, также закрывать само помещение, в котором проводится обработка ПДн. Кроме того, в свое отсутствие пользователи обязаны выключать персональную электронно-вычислительную машину (ПЭВМ) или блокировать ее. После этого разблокировка ПЭВМ производится только после ввода своего пароляпользователем.

3.15. При выносе материальных носителей за пределы помещения, в котором проводится обработка ПДн, по служебной необходимости пользователь должен принять все возможные меры, исключающие утрату (утерю, хищение) их.

3.16. При утрате (утере, хищении) материальных носителей ПДн пользователь обязан немедленно доложить ответственному за эксплуатацию и обеспечение безопасности информации и (или) ответственному за организацию обработки ПДн о факте утраты (утере, хищении) материальных носителей. По каждому такому факту назначается служебное расследование.

3.17. Пользователь обязан немедленно сообщать ответственному за эксплуатацию и обеспечение безопасности информации и (или) ответственному за организацию обработки ПДн обо всех ставших ему известными фактах получения третьими лицами несанкционированного доступа, либо попытки получения доступа к ПДн, об утрате или недостаче материальных носителей ПДн, удостоверений, ключей от сейфов (хранилищ), личных печатей, и других фактах, которые могут привести к несанкционированному доступу к ПДн, а также о причинах и условиях возможной утечки этих сведений.

3.18. Устранять допущенные нарушения в случае выявления неправомерных действий с ПДн в срок, не превышающий трех рабочих днейс даты такого выявления.

3.19. Выполнять требования ответственного за эксплуатацию информационной системы персональных данных, администратора безопасности и ответственного за организацию обработки персональных данных.

4. В ПРОЦЕССЕ РАБОТЫ ПОЛЬЗОВАТЕЛЮЗАПРЕЩАЕТСЯ

4.1. Проводить обработку персональных данных при неисправно работающих средствах защиты информации.

4.2. При работе с парольной защитой:

- разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
- предоставлять доступ от своей учетной записи к информации,хранящейся в ИСПДн посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах, находящихся в свободном доступе.

4.3. Устанавливать на ОИ программное обеспечение, не связанное с выполнением функций, предусмотренных технологическим процессом обработки информации.

4.4. Сообщать ПДн Субъекта лицам, не имеющим права доступа к этим сведениям, за исключением случаев, установленных законодательством Российской Федерации.

4.5. Допускать к обработке ПДн лиц, не имеющих допуска к этим работам.

4.6. Передавать ПДн по телекоммуникационных каналам связи в открытом виде, в том числе международной информационно-телекоммуникационной сети Интернет, по телефону, телефаксу, электронной почте и т.п. (без использования средств шифрования).

4.7. Без согласования с ответственным за эксплуатацию и обеспечение безопасности информации формировать и хранить базы данных (картотеки, файловые архивы и др.), содержащие ПДн.

4.8. Делать неучтенные копии материальных носителей или документов, содержащих ПДн.

4.9. Покидать помещение, не убрав материальные носители или документы с ПДн в места препятствующие несанкционированному доступу кним.

4.10. Выносить материальные носители или документы, содержащие ПДн, из помещений Университета без служебной необходимости.

4.11. Использовать для хранения информации черновиков, с обратной стороны которых имеются ПДн субъектов персональных данных.

5. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ

5.1. Пользователи несут ответственность в полном объеме по действующему законодательству за разглашение ПДн, ставших известными им в соответствии с исполнением ими должностных обязанностей, а также утрату материальных носителей ПДн.

5.2. Пользователь отвечает за правильность обработки ПДн.

Прошнуровано и пронумеровано
26 (двадцать шесть) листов

И.о.директора школы *Л.В. Котлубей*