«ПРИНЯТО»
Решением
педагогического Совета
ГБОУ СОШ «ОЦ»
п.г.т. Рощинский
Протокол № 8 от 18.04.2023 г.

«УТВЕРЖДЕНО»
Приказом **№ – од от «21» 04. 2023 г.**
директор ГБОУ СОШ «ОЦ» п. г. т. Рощинский О.И. Рубина

«УЧТЕНО»
Мнение Профсоюзного комитета
(представительского органа работников)
ГБОУ СОШ «ОЦ» п. г. т. Рощинский
от «18» апреля 2023 г.
Председатель Н. М. Барашкина

«ПРИНЯТО»
С учетом мнения родителей
(Протокол совета родителей / законных представителей от 17.04.2023 г. № 3)

ЭП

C=RU, O="ГБОУ СОШ ""ОЦ"" п.г.т. Рощинский",
CN=Рубина О.И.,
E=roshinsky_sch_vlg@samara.edu.ru
00ea17aca4d591c1ca
2023.04.26 18:18:51+04'00'

ПОЛОЖЕНИЕ

«Об электронной информационно-образовательной среде в государственном бюджетном общеобразовательном учреждении Самарской области средней общеобразовательной школе «Образовательный центр» имени 81 гвардейского мотострелкового полка п. г. т. Рощинский муниципального района Волжский Самарской области»

1. Общие положения

1.1. Информатизация образования – один из приоритетов модернизации Российского образования, главной задачей которой является создание и функционирование единой информационно-образовательной среды (ИОС). ИОС рассматривается как одно из условий достижения нового качества образования.

1.2. Информационно-образовательная среда (ИОС) – система информационно-образовательных ресурсов и инструментов, обеспечивающих условия реализации основной образовательной программы образовательной организации.

1.3. ИОС образовательной организации включает в себя совокупность технологических средств (компьютеры, базы данных), культурные и организационные формы информационного взаимодействия, компетентность участников образовательного процесса в решении учебно-познавательных и профессиональных задач с применением информационно-коммуникационных технологий (ИКТ).

1.4. Основные характеристики ИОС, значимые для организации процесса обучения:

1.4.1. *Открытость*, которая обеспечивается за счет взаимодействия среды с информационно-образовательным пространством.

1.4.2. *Целостность*, за счет которой обеспечивается целесообразная логика развертывания процесса обучения: постановка целей обучения, связанные с нею деятельность учителя, деятельность учащихся и планируемый результат. Она конструируется с учетом инвариантного содержания учебного материала, оптимальных методов и способов обучения, содействующих достижению целей образования.

1.5. ИОС позволяет реализовать дидактические возможности инновационных технологий, эффективно организовать индивидуальную и коллективную работу обучающихся, обеспечивая тем самым целенаправленное развитие их самостоятельной познавательной деятельности.

2. Цели и задачи ИОС

2.1 Приоритетной, **ведущей целью ИОС** является создание единого образовательного пространства школы, повышение качества образования, создание условий для поэтапного перехода к новому уровню образования на основе информационных технологий, создание условий для возможности предоставления дистанционных образовательных услуг.

2.2 Основные задачи ИОС:

2.2.1. Планирование образовательного процесса, размещение и сохранение материалов образовательного процесса, фиксация результатов освоения основной образовательной программы, взаимодействие между участниками образовательного процесса, контролирование доступа участников образовательного процесса к информационным образовательным ресурсам в сети Интернет;

2.2.2. Предоставление возможности быстрого доступа к данным по важнейшим показателям образовательного учреждения за любой период времени.

2.3 Правильно организованная ИОС образовательной организации позволяет на новом уровне осуществить дифференциацию обучения, повысить мотивацию учащихся, обеспечить наглядность представления практически любого материала, обучать современным способам самостоятельного получения знаний.

3. Структура ИОС

3.1 Техническая инфраструктура ИОС образовательной организации: компьютерная техника, периферийное оборудование, локальная сеть, системное программное обеспечение.

3.2 Информационная инфраструктура ИОС образовательной организации: программное обеспечение общего назначения, программное обеспечение для автоматизации деятельности различных служб, программно-методическое обеспечение для организации учебно-воспитательного процесса, информационные ресурсы образовательного учреждения.

4. Права и обязанности пользователей ИОС

4.1 Пользователями ИОС образовательного учреждения являются: обучающиеся, педагогические работники образовательного учреждения, административно-управленческий аппарат, вспомогательный и технический персонал, родители или законные представители обучающихся.

4.2 Права пользователей ИОС образовательного учреждения разграничиваются в соответствии со спецификой статуса, должностных обязанностей и содержанием информационных запросов.

4.3 Обучающиеся имеют право:

4.3.1. Свободного доступа к необходимым образовательным информационным ресурсам;

4.3.2. Выполнять индивидуальную работу, участвовать в групповой, коллективной работе класса и размещать результаты своих достижений в ИОС (регистрация разработок, публикация на сайте); 4.3.3. Формировать портфолио в АСУ РСО РГО;

4.3.4. Запрашивать информационные ресурсы;

4.3.5. На научно-методическую и консультационную поддержку в освоении новейших информационных технологий.

4.4. Обучающиеся обязаны:

4.4.1. Соблюдать правила пользования информационными ресурсами;

4.5. Учитель имеет право:

4.6. Учитель обязан:

4.5.1. Готовить (создавать) учебные материалы (материалы для выступлений, задания учащимся, индивидуальные рекомендации) и делать их доступными в ИОС;
4.5.2. Получать и использовать материалы и результаты внешней экспертизы, направляемые органами управления образования, методическими службами, структурами независимого контроля;
4.5.3. Делать поурочное планирование с использованием ИКТ, АСУ РСО РГО;
4.5.4. Подбирать программное обеспечение для учебных целей;
4.5.5. Подбирать материал в электронной библиотеке с доступом к информационным образовательным ресурсам, в сети Интернет;
4.5.6. Ээффективно использовать ИКТ для объяснения нового материала;
4.5.7. На научно-методическую и консультационную поддержку в освоении новейших информационных технологий.
4.5.8. Получать консультационную помощь по вопросам поиска и выбора источников информации.

4.6.1. Использовать возможности ИКТ в урочной и воспитательной деятельности;
4.6.2. Соблюдать правила пользования ИОС;
4.6.3. Планировать и повышать профессиональную компетентность, включающую ИКТ-компетентность различных форм.

4.7. Администрация образовательной организации имеет право:

4.7.1. На общение посредством инструментов ИКТ с участниками образовательного процесса;
4.7.2. На размещение, обновление и удаление информации о деятельности образовательного учреждения;
4.7.3. На ввод, хранение, обработку и анализ персональных данных работников и учащихся в пределах объема должностных обязанностей;
4.7.4. На осуществление телекоммуникационного обмена в сети Интернет с использованием официальных адресов образовательного учреждения.

4.8. Администрация образовательной организации обязана

4.8.1. Организовывать взаимодействие всех участников образовательного процесса в рамках ИОС;
4.8.2. Разрабатывать и организовывать принятие локальных актов школы, регламентирующих сферу ИОС;
4.8.3. Осуществлять контроль над деятельностью пользователей ИОС образовательного учреждения;
4.8.4. Организовывать восстановление работоспособности программных и технических компонентов после аварийной ситуации в короткие сроки;
4.8.5. Организовывать непрерывное повышение ИКТ-компетентности всех работников школы;
4.8.6. Обеспечивать информационную безопасность.

4.9. Родители обучающихся (или законные представители) имеют право:

4.9.1. Получать информацию о важных и типичных моментов школьной жизни в ИОС (школьный сайт, региональный образовательный портал);
4.9.2. Знакомиться и обсуждать аналитические материалы по работе школы, в частности, публичного отчета школы.

4.10. Родители обучающихся (или законные представители) обязаны:

4.10.1. **Подписывать договор о сотрудничестве со школой;**
4.10.2. Размещать информацию о причинах отсутствия учащегося на занятии (информационное письмо на адрес электронной почты образовательного учреждения);
4.10.3. Получать направляемою школой

информацию;
4.10.4. Содействовать эффективному использованию ИКТ учащимися школы.

5. Информационные ресурсы ИОС образовательной организации

5.1. К информационным ресурсам ИОС образовательной организации относятся программные компоненты различного назначения (лицензионные операционные системы, прикладные программные средства, программные компоненты информационных сред; файлы баз данных), необходимые для обеспечения функционирования ГБОУ СОШ «ОЦ» п. г. т. Рощинский и удовлетворения информационных запросов и потребностей участников образовательного процесса: педагогические ресурсы, персональные данные работников и учащихся, информационные ресурсы структурных подразделений, служб и объектов инфраструктуры.
5.2 Педагогические ресурсы ИОС образовательного учреждения создаются и используются в соответствии с реализуемыми образовательными программами.
5.3 Обработка электронных ресурсов, содержащих персональные данные работников и учащихся, проводится строго в соответствии с нормами законодательства Российской Федерации на основании личного согласия работников и родителей учащихся.
5.4. Несанкционированное использование и копирование информационных ресурсов структурных подразделений, служб и объектов инфраструктуры не допускается.

6. Структура информационно-образовательной среды образовательной организации

6.1. Структура информационной среды образовательной организации включает следующие компоненты:
6.1.1. Организационно-управленческие компоненты: законодательные, нормативно-методические и распорядительные документы, должностные обязанности, инструкции и регламенты деятельности и управления ИОС ОО;
6.1.2. Программные компоненты: операционные системы; прикладные программные средства; программно-методические комплексы, цифровые образовательные ресурсы (ЦОР) и учебно-методические материалы (УММ, УМК), в том числе электронный журнал в АСУ РСО РГО и все его разделы (компоненты, материалы, возможности).

6.2. Основные элементы ИОС общеобразовательной организации

6.2.1. Информационно-обучающая составляющая:

- *официальный сайт ГБОУ СОШ «ОЦ» п. г. т. Рощинский в информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет) /* ***http://roshchaschool.minobr63.ru***
- *Государственная информационная система «Электронное образование»;*
- *Система обучения с применением ДОТ;*
- *Система видеоконференцсвязи для проведения видеоконференций, интернет-семинаров (вебинаров), трансляции учебных занятий и научных мероприятий образовательных организаций посредством сети Интернет обучающимся и участникам мероприятий;*
- *Открытые справочно-правовые системы;*
- *Информационно-образовательные ресурсы на сменных носителях и в сети Интернет;*
- *Виртуальные лаборатории, тренажеры, виртуальные экскурсии и приложения по виртуализации культурного наследия;*
- *Цифровой трехмерный, визуальный, интерактивный, мобильный образовательный контент и методики его применения;*
- *Иные компоненты, необходимые для организации учебного процесса и взаимодействия компонентов ИОС.*

6.2.2. Программно-техническая составляющая:

- *Предметные кабинеты, компьютерные классы, лингафонные кабинеты;*
- *Библиотека (в том числе цифровая (электронная) библиотека), музей, медиатека, актовый зал; кабинеты «Точки роста» / центр образования естественно-научной и технологической направленностей*

- *Сетевой центр (серверная);*
- *Вычислительная и информационно-телекоммуникационная инфраструктура;*
- *Лаборатории, издательский центр, видеостудия, студия робототехники, web-студия;*
- *Автоматизированные рабочие места администрации, педагогов, методической службы, медицинского работника, психолога, библиотекаря, службы охраны и других работников ГБОУ СОШ «ОЦ» п. г. т. Рощинский*
- *Системное и прикладное программное обеспечение, в том числе и сетевое;*
- *Мультимедийные образовательные программы;*
- *Прикладные программы, в том числе поддерживающие администрирование и фи-нансово-хозяйственную деятельность общеобразовательной организации (бухгалтерский учет, делопроизводство, кадры и т. д.).*

6.3. ИОС ГБОУ СОШ «ОЦ» п. г. т. Рощинский обеспечивает образовательный процесс учебно-методическими и информационными возможностями:

- *Реализация индивидуальных образовательных планов обучающихся, осуществления их самостоятельной образовательной деятельности;*
- *Ввода русского и иноязычного текста, распознавания сканированного текста; создания текста на основе расшифровки аудиозаписи; использования средств орфографического и синтаксического контроля русского текста и текста на иностранном языке; редактирования и структурирования текста средствами текстового редактора;*
- *Записи и обработки изображения (включая микроскопические, телескопические и спутниковые изображения) и звука при фиксации явлений в природе и обществе, хода образовательного процесса; переноса информации с нецифровых носителей (включая трех-мерные объекты) в цифровую среду (оцифровка, сканирование);*
- *Создания и использования диаграмм различных видов (алгоритмических, концептуальных, классификационных, организационных, хронологических, родства и др.), специализированных географических (в Географических информационных системах - ГИС) и исторических карт; создания виртуальных геометрических объектов, графических сообщений с проведением рукой произвольных линий;*
- *Организации сообщений в виде линейного или включающего ссылки сопровождения выступления, сообщения для самостоятельного просмотра, в том числе видеомонтажа и озвучивания видео сообщений;*
- *Выступления с аудио-, видео- и графическим экранным сопровождением;*
- *Вывода информации на бумагу и т. п. и в трехмерную материальную среду (печать);*
- *Информационного подключения к локальной сети и сети Интернет, входа в информационную среду организации, в том числе через сеть Интернет, размещения гипермедиа сообщений в ИОС общеобразовательной организации;*
- *Поиска и получения информации;*
- *Использования источников информации на бумажных и цифровых носителях (в том числе в справочниках, словарях, поисковых системах);*
- *Использования носимых аудио- видео- устройств для учебной деятельности на уроке и вне урока;*
- *Общения в сети Интернет, взаимодействия в социальных группах и сетях, участия в форумах, групповой работы над сообщениями (вики);*
- *Создания, заполнения и анализа баз данных, в том числе определителей; их наглядного представления;*
- *Включения обучающихся в проектную и учебно-исследовательскую деятельность, проведения наблюдений и экспериментов, в том числе с использованием: учебного лабораторного оборудования, цифрового (электронного) и традиционного измерения, включая определение местонахождения; виртуальных лабораторий, вещественных и виртуально-наглядных моделей и коллекций основных математических и естественнонаучных объектов и явлений;*

- *Исполнения, сочинения и аранжировки музыкальных произведений с применением традиционных народных и современных инструментов и цифровых технологий, использования звуковых и музыкальных редакторов, клавишных и кинестетических синтезаторов;*
- *Художественного творчества с использованием ручных, электрических и ИКТ-инструментов, реализации художественно-оформительских и издательских проектов, натурной и рисованной мультипликации;*
- *Проектирования и конструирования, в том числе моделей с цифровым управлением и обратной связью, с использованием конструкторов управления объектами программирования;*
- *Занятий по изучению правил дорожного движения с использованием игр, оборудования (автогородок), а также компьютерных тренажеров;*
- *Размещения продуктов познавательной, учебно-исследовательской и проектной деятельности обучающихся в ЭИОС общеобразовательной организации;*
- *Проектирования и организации индивидуальной и групповой деятельности, организации своего времени с использованием ИКТ; планирования учебного процесса, фиксирования его реализации в целом и отдельных этапов (выступлений, дискуссий, экспериментов);*
- *Обеспечения доступа в школьной библиотеке к информационным ресурсам сети Интернет, учебной и художественной литературе, коллекциям медиаресурсов на электронных носителях, множительной технике для тиражирования учебных и методических тексто - графических и аудио - видеоматериалов, результатов творческой, научно-исследовательской и проектной деятельности обучающихся;*
- *Проведения массовых мероприятий, собраний, представлений; досуга и общения обучающихся с возможностью для массового просмотра кино- и видеоматериалов, организации сценической работы, театрализованных представлений, обеспеченных озвучиванием, освещением и мультимедиа сопровождением;*
- *Выпуска школьных печатных изданий, работы школьного телевидения.*

7. **Сопровождение программных компонентов информационно-образовательной среды образовательной организации**

7.1. Сопровождению подлежат программные компоненты ИОС, находящееся на балансе образовательного учреждения.
7.2 Формами сопровождения программных компонентов ИОС являются:
7.2.1. Гарантийное обслуживание, осуществляемое поставщиком или производителем;
7.2.2. Обновление и замена версий;
7.2.3. Выполнение мероприятий антивирусной защиты;
7.2.4. Резервное копирование и восстановление файлов;
7.2.5. Аварийные и другие неотложные работы по восстановлению функций программного обеспечения;
7.2.6. Техническое консультирование.
7.3 Субъектами сопровождения являются:
7.3.1. Должностные лица образовательного учреждения – **системный администратор;**
7.3.2. Работники организаций, осуществляющих гарантийное и постгарантийное обслуживание на основании договоров.
7.4 Регламент профилактического обслуживания включает следующие виды работ:
7.4.1. Обновление антивирусного программного обеспечения, проверка устройств постоянного хранения информации;
7.4.2. Инсталляция программного обеспечения (кроме продуктов, инсталлируемых специалистами производителя или поставщика) по мере поступления программных продуктов;
7.4.3. Проверка и установка критических обновлений безопасности операционной системы;
7.4.4. Установка обновлений программного обеспечения;
7.4.5. Проверка и дефрагментация жестких дисков;
7.4.6. Приведение в стандартное состояние профиля пользователей;

7.4.7. Администрирование сети (регистрация и редактирование пользовательских учетных записей, сетевых прав и ограничений доступа);
7.4.8. Структурирование и оптимизация данных.

8. **Организация безопасной эксплуатации информационно-образовательной среды образовательной организации**

8.1 Безопасная эксплуатация компонентов ИОС включает следующие компоненты:
8.1.1. *Информационная безопасность:* обеспечение сохранности, целостности и работоспособности информационных ресурсов, профилактика несанкционированного доступа, использования, копирования или удаления информации, а также изменения структуры информационных ресурсов;
8.1.2. *Технологическая безопасность:* обеспечение стабильности функционирования технических компонентов ИОС, предупреждение нецелесообразного использования, нарушения работоспособности, преждевременного износа, повреждения или уничтожения оборудования;
8.1.3. *Техническая безопасность:* предупреждение или минимизация неблагоприятного воздействия оборудования на организм пользователя, нарушения правил техники безопасности при использовании оборудования, профилактика поражения пользователей электрическим током;
8.1.4. *Организационная безопасность:* предупреждение использования оборудования лицами, не владеющими необходимыми пользовательскими компетентностями, профилактика использования оборудования в целях, не соответствующих целям деятельности образовательного учреждения.
8.2 Безопасная эксплуатация компонентов ИОС обеспечивается организационными, программными и аппаратными средствами, человеческими ресурсами (материально ответственными лицами).
8.3 Организационными средствами обеспечения безопасности ИОС являются:
8.3.1. *Разработка нормативных документов*, регламентирующих вопросы безопасной эксплуатации ИОС;
8.3.2. *Проведение инструктажей* работников и учащихся по безопасному использованию компонентов ИОС;
8.3.3. *Упорядочивание форм* использования компонентов ИОС;
8 .3.4. *Регламентация учетной и контрольной деятельности*;
8.3. 5. *Нормативно-правовая документация*, регламентирующими условия размещения оборудования согласно требований СанПин.
8.4. Программными средствами обеспечения безопасности ИОС являются:
8.4.1. *Организация антивирусного мониторинга и защиты;*
8.4.2. *Обеспечение контроля входящего и исходящего трафика;*
8.4.3. *Администрирование доступа к информационным ресурсам* интрасети и Интернет.
8.5. Аппаратными средствами обеспечения безопасности ИОС являются:
8.5.1. Применение аппаратных средств маршрутизации;
8.5.2. Применение устройств бесперебойного питания;
8.5.3. Применение резервного копирования и создание копий информационных ресурсов;
8.6. В целях обеспечения безопасной эксплуатации ИОС всем категориям пользователей без получения соответствующего разрешения запрещается:
8.6.1. Размещение информационных ресурсов в Интернет;
8.6.2. Использование, копирование и удаление информационных ресурсов или их компонентов;
8.6.3. Обновление или изменение версии программного обеспечения;
8.6.4. Изменение имен и паролей для доступа к сетевым ресурсам;
8.6.5. Изменение системных настроек компьютеров и серверов;
8.6.6. Изменение политик безопасности.

9. **Ответственность пользователей информационно-образовательной среды образовательной организации**

9.1. Ответственность пользователей ИОС за совершение противоправных деяний наступает в соответствии с административным и уголовным кодексом РФ.
9.2. Возмещение вреда, причиненного имущественным и смежным правам, совершенное с использованием компонентов ИОС наступает в соответствии с гражданским кодексом РФ.
9.3. Дисциплинарная и материальная ответственность пользователей ИОС – работников образовательной организации, наступает в соответствии с трудовым кодексом, Законом Российской Федерации «Об образовании», коллективным договором, правилами внутреннего трудового распорядка, Уставом образовательной организации и настоящим Положением.
9.3.1. Основаниями для привлечения пользователей ИОС – работников образовательной организации к дисциплинарной ответственности являются нарушения эксплуатации компонентов ИОС, правил внутреннего трудового распорядка, должностных обязанностей и настоящего Положения.
9.3.2. Основаниями для привлечения пользователей ИОС – работников образовательной организации к материальной ответственности является причинение вреда программным или техническим компонентам ИОС ОУ.
9.4. Дисциплинарная ответственность пользователей ИОС – учащихся образовательной организации наступает в соответствии с Законом Российской Федерации «Об образовании», Уставом образовательного учреждения, Правилами внутреннего распорядка для учащихся и настоящим Положением.
9.5. Основаниями для привлечения пользователей ИОС образовательной организации – учащихся в образовательном учреждении к дисциплинарной ответственности являются нарушения работоспособности объектов ИОС, повреждение или несанкционированное использование информационных внутренних и внешних ресурсов ИОС, создание и (или) размещение информационных ресурсов, противоречащих общечеловеческим ценностям, призывающих к насилию, национализму, расизму и аморальному поведению.

Приложение № 1
к Положению «Об электронной информационно-образовательной среде»

Свод правил по безопасной работе сотрудников ГБОУ СОШ «ОЦ» п. г. т. Рощинский при использовании сети Интернет, осуществлении информационного взаимодействия с сервисами государственных информационных систем

Общие положения

1.1. Настоящий Свод правил по безопасной работе сотрудников ГБОУ ССОШ «ОЦ» п. г. т. Рощинский при использовании сети Интернет, осуществлении информационного взаимодействия с сервисами государственных информационных систем (далее – Свод правил, пользователи) основан на требованиях Федерального закона от 27.07.2006 № 149- ФЗ «Об информации, информационных технологиях и о защите информации», нормативных правовых актах Российской Федерации, регулирующих отношения в области защиты информации.
1.2. Целями Свода правил являются:
– регулирование работы пользователей при использовании сети Интернет и осуществлении информационного взаимодействия с сервисами государственных информационных систем;
– обеспечение целостности, конфиденциальности и доступности хранящейся и передаваемой информации, находящейся на автоматизированных рабочих местах (далее – АРМ) или локальной вычислительной сети (далее – ЛВС);
– соблюдение требований, предусмотренных законодательством Российской Федерации и нормативными правовыми актами в области защиты информации.
1.3. При работе в сети Интернет и информационных системах пользователи руководствуются законодательством Российской Федерации, нормативными правовыми актами, иными документами в области информационных технологий и безопасности информации, а также Сводом правил.

2. Общие правила пользования на АРМ

2.1. Пользователь отвечает за правильность включения (выключения) АРМ, вход в систему и все действия при работе на нем.
2.2. АРМ разрешается использовать исключительно в служебных целях.
2.3. Пользователь обязан исключить возможность неосторожного причинения вреда техническим и информационным ресурсам.
2.4. Систематически осуществлять резервное копирование важной информации, хранящейся на АРМ пользователя.
2.5. Систематически проверять обновление антивирусной базы (как правило, в настройках антивируса, установлено их автоматическое обновление).
2.6. Во время работы, не связанной с обучением детей, экран монитора компьютера располагать в помещении таким образом, чтобы исключить возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами. При работе со служебной, персональной, конфиденциальной информацией шторы на оконных проемах должны быть завешаны (жалюзи закрыты).
2.7. При временном отсутствии пользователя на рабочем месте экран монитора должен быть потушен или использована экранная заставка.
2.8. Соблюдать требования парольной политики (Раздел 8 Свода правил).
2.9. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получений консультаций по вопросам информационной безопасности, необходимо обращаться к системному **администратору информационной образовательной сети.**
2.10. Использовать электронную цифровую подпись (далее – ЭЦП) в соответствии с Руководством (правилам) по обеспечению использования ЭЦП и средств ЭЦП, выданным удостоверяющим центром.

Пользователям запрещается:

2.11. Открывать на АРМ файлы и запускать программы, полученные из непроверенных источников.
2.12. Передавать свои идентификационные данные (пароли, логины), атрибуты доступа к ресурсам информационной системы посторонним лицам.
2.13. Отключать (блокировать) средства защиты информации.
2.14. Привлекать посторонних лиц для производства ремонта или настройки АРМ.
2.15. Разглашать обрабатываемую информацию третьим лицам.
2.16. Копировать служебную информацию на внешние носители без разрешения руководства.
2.17. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
2.18. Несанкционированно открывать общий доступ к папкам на АРМ.
2.19. Осуществлять подключение к АРМ и ЛВС посторонних и личных устройств (например: смартфоны, телефоны, считыватели информации, излучающие устройства (Wi- Fi, Bluetooth, радиомодемы) и т.п.

3. Правила пользования в сети Интернет

3.1. Ресурсы сети Интернет предоставляются пользователям для получения информации необходимой для выполнения служебных обязанностей.
3.2. Пользователь обязан не предпринимать попыток несанкционированного доступа к информационным ресурсам, доступ к которым ему ограничен.
3.3. Пользователь может посещать только те ресурсы, содержание которых не противоречит законодательству Российской Федерации, а цель посещения должна быть связана с его служебной деятельностью.
3.4. Внимательно набирать имена сайтов, особенно на которых проводятся финансовые операции. Поддельные сайты могут иметь отличие даже одного знака или тот же вид, что и оригинальные. Такие сайты могут содержать невидимые области, нажатие на которые может привести к заражению АРМ вредоносными программами или перенаправление на зараженные сайты. Более

безопасно не набирать вручную наименование сайта, а пользоваться заранее сделанными закладками.
3.5. В настоящее время киберпреступники создают поддельные сайты якобы для оплаты штрафов ГИБДД или оформления заявки на кредит и других целей. На не проверенных сайтах ввод конфиденциальных данных не рекомендуется!
3.6. Категорически запрещено использование для служебной деятельности иностранных Интернет-сервисов систем обмена мгновенными сообщениями, голосовой и видеоинформацией (ICQ, QIP, Jabber, Whatsap, Skype и т.д.), облачных сервисов хранения информации (iCloud, Dropbox и т.д.).
3.7. Пользователям запрещается:
– использовать доступ к сети Интернет в личных целях;
– посещать досугово-развлекательные сайты не связанные с образовательным процессом;
– использовать доступ к сети Интернет для распространения и тиражирования информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

4. Правила работы с электронной почтой

4.1. Для служебной деятельности необходимо использовать электронную почту домена ГБОУ СОШ «ОЦ» п. г. т. Рощинский (ГБОУ СОШ "ОЦ" п.г.т. Рощинский samara.edu.ru).
Использование иных общедоступных почтовых сервисов должно быть исключено. Используя общедоступные почтовые сервисы Вы **сознательно** предоставляете передаваемую информацию этим сервисам, и она может быть доступна третьим лицам. **Категорически запрещено использование иностранных почтовых сервисов электронной почты** (Gmail, Yahoo и т.д.) для служебной деятельности.
4.2. При получении электронного письма с вложением необходимо внимательно посмотреть адрес отправителя. В случае, если этот адрес неизвестен, или отличается от реального хотя бы одним знаком, открытие вложений таких писем не безопасно, поскольку могут содержать вредоносные программы.
4.3. В последнее время зафиксирована рассылка на электронные адреса пользователей, а также на официальные почтовые ящики органов исполнительной власти Самарской области и органов местного самоуправления муниципальных образований в Самарской области, во вложении к которым содержатся вредоносные файлы типа «Акты сверки.zip», «Коммерческое предложение.zip», «Судебное производство.zip», с различными графическими изображениями. Такие вложения, как правило, содержат вирусы- шифровальщики (Trojan.Encoder), которые имитируют зависание операционной системы Windows компьютера и шифруют документы пользователей с расширениями *.doc, *.xls, *.pdf, *.txt, *.jpg, *.tif, *.rar, *.zip и другими, некоторые передают (воруют) информацию насторонние сервера.
Вирусы-шифровальщики не определяются антивирусными программами в момент заражения АРМ.
4.4. При получении письма от неизвестного адресата, необходимо связаться с исполнителем и уточнить происхождение файлов. В случае невозможности установить происхождение письма, необходимо его удалить, не сохраняя и не запуская приложенные файлы.
4.5. Запрещается передавать информацию ограниченного доступа через сеть Интернет (в том числе посредством электронной почты) без использования средств защиты информации.
4.6. Запрещается осуществлять массовые рассылки электронной почты неслужебного характера (СПАМа).
4.7. Необходимо своевременно очищать свой почтовый ящик.
4.8. Необходимо осуществлять ежедневную обработку писем.

5. Правила пользования государственными и муниципальными информационными системами

5.1. АРМ, используемые для работы с государственными и муниципальными информационными системами (далее – ГИС и МИС) должны соответствовать требованиям, изложенным в документации соответствующих ГИС и МИС.
5.2. Перед началом работы в ГИС и МИС пользователи должны ознакомиться с правилами работы в соответствующих ГИС и МИС (инструкциями пользователям).

6. Правила работы в автоматизированной информационной системе документооборота и делопроизводства в Администрации Губернатора Самарской области, секретариате Правительства Самарской области и органах исполнительной власти Самарской области

Работа в автоматизированной информационной системе документооборота и делопроизводства (далее – АИС ДД) Администрации Губернатора Самарской области, секретариате Правительства Самарской области и органах исполнительной власти Самарской области осуществляется с применением электронной подписи, в соответствии с приложением № 1 «Инструкции по делопроизводству в Администрации Губернатора Самарской области, секретариате Правительства Самарской области и органах исполнительной власти Самарской области», утвержденной распоряжением Губернатора Самарской области от 29.04.2013 № 234-р.

7. Правила антивирусной защиты

7.1. Для обеспечения антивирусной защиты должно использоваться сертифицированное лицензионное антивирусное программное обеспечение.
7.2. Ярлык антивирусной программы, как правило, находится в области уведомления или на вкладке «отображать скрытые значки» (нижний правый угол экрана).
7.3. Пользователи при работе с внешними носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.
7.4. Обновление антивирусной программы, как правило, производится автоматически, в противном случае необходимо обратиться к администратору ЛВС.
7.5. Периодическое тестирование всего установленного программного обеспечения на предмет компьютерных вирусов производится автоматически. Полную проверку АРМ необходимо проводить при установке антивирусной программы, в случаях подозрения заражением, периодически 1 – 2 раза в год.
7.6. В случае обнаружения подозрительных программ срабатывает антивирус и необходимо прекратить какие-либо действия на АРМ и обратиться к администратору ЛВС.
7.7. В случае обнаружения вируса, не поддающегося лечению, администратор ЛВС, ответственный за обеспечение безопасности информации, принимает меры по восстановлению работы системы.
7.8. Вирусы-шифровальщики не определяются антивирусными программами в момент заражения АРМ.
7.9. В тех случаях, когда заражение вирусом АРМ все-таки произошло, необходимо:

- *немедленно отключить компьютер для остановки действий вредоносной программы и не включать компьютер с зашифрованными данными, т.к. во время включений и перезагрузок происходят изменения файловой системы компьютера;*
- *не пытаться самостоятельно изменять расширения зараженных файлов, а также удалять любые файлы с рабочего компьютера и электронные сообщения;*
- *обратиться к должностному лицу, отвечающему за установку антивирусных программ, обеспечение безопасности информации в своем структурном подразделении;*
- *обратиться к инженеру обслуживающим Вашу вычислительную технику;*
- *обратиться в службу технической поддержки, установленной у Вас антивирусной программы и совместно с ними попытаться восстановить утраченную информацию.*

По информации производителей антивирусных программ возможность восстановления информации – минимальна, т.к. каждое вредоносное сообщение содержит индивидуальный файл-шифровальщик. Напоминаем о необходимости проведения регулярной процедуры резервного копирования всей важной рабочей информации АРМ, т.к. это позволит быстро восстановить Ваши данные в случае их повреждения (заражения)!

8. Парольная политика

8.1. Идентификация и проверка подлинности пользователя при входе в АРМ, информационную систему может осуществляться по паролю условно-постоянного действия, с использованием аппаратных средств (TouchMemory и др.), с использованием ЭП.
8.2. Полная плановая смена паролей пользователей должна проводиться регулярно (нереже 1 раза в 3 месяца).
8.3. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.
8.4. В случае компрометации (утраты, разглашения, кражи, взлома) личного пароля пользователь должен немедленно предпринять меры по смене пароля.
8.5. Хранение пользователем значений своих паролей на материальном носителе допускается только в личном, запираемом ящике (сейфе).
8.6. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).
8.7. Правила формирования пароля: 8.7.1. Пароль должен состоять не менее чем из восьми символов.
8.7.2. В пароле должны присутствовать символы трех категорий из числа следующих четырех:

- *прописные буквы английского алфавита от A до Z;*
- *строчные буквы английского алфавита от a до z;*
- *цифры (от 0 до 9);*
- *символы, не принадлежащие алфавитно-цифровому набору (например: !,$,#, %).*

8.7.3. Пароль не может содержать имя учетной записи Пользователя или какую- либо его часть.
8.7.4. Пароль не должен включать в себя легко вычисляемые сочетания символов, простые пароли типа «123», «111», «qwerty» и им подобные, а так же ФИО и даты рождения свои и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые могут быть подобраны, основываясь на информации о пользователе.
8.7.5. Не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «аааааааа»).
8.7.6. Не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).
8.7.7. Не использовать ранее использованные пароли.
8.7.8. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.
8.7.9. Во время ввода пароля необходимо убедиться, что клавиатура находится вне поля зрения посторонних лиц, а также технических средств (видеокамер, фотоаппаратов).
8.7.10. Не использовать один пароль в разных информационных ресурсах.

9. Ответственность Пользователя

Пользователи несут персональную ответственность за свои действия в период осуществления информационного взаимодействия с использованием АРМ, за нарушение настоящего Свода правил, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, нарушение работы государственных информационных систем и ресурсов, АРМ пользователя может быть отключен от ЛВС до выяснения обстоятельств нарушения.
Нарушение требований законодательства Российской Федерации об информации, информационных технологиях и о защите информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 2
к Положению «Об электронной информационно-образовательной среде»

ИНСТРУКЦИЯ

по организации парольной защиты при работе с информацией, содержащей данные ограниченного распространения, на автоматизированных рабочих местах сотрудников ГБОУ СОШ «ОЦ» п. г. т. Рощинский

1. Общие положения

1.1. Настоящая Инструкция предназначена для использования в работе сотрудниками ГБОУ СОШ «ОЦ» п. г. т. Рощинский и определяет порядок обеспечения защиты локальных ресурсов отдельных рабочих станций автоматизированных рабочих мест (далее по тексту настоящей Инструкции – АРМ), использующих подсистемы парольной защиты от несанкционированного доступа (далее по тексту настоящей Инструкции – НСД) в информационных системах (далее – ИС).

1.2. Парольная защита при работе на объекте информатизации осуществляется с целью предотвращения НСД к информации, содержащей данные ограниченного распространения.

1.3. Парольная защита объекта информатизации является составной частью подсистемы управления доступом общей системы защиты от НСД.

К основным видам (категориям) паролей относятся:

- *пароли доступа к локальным ресурсам отдельного компьютера (АРМ);*
- *пароли доступа к ресурсам АРМ;*
- *пароли доступа к прикладным программам, обеспечивающим доступ к конфиденциальной информации;*
- *пароли доступа средств защиты от НСД;*
- *пароли систем доступа, встроенные в используемые операционные системы.*

2. Требования к организации парольной защиты объекта информатизации

2.1. Личный пароль доступа к информационной системе выдается пользователю организации администратором информационной безопасности организации-оператора ИС.

2.2. Лица, использующие парольную защиту, обязаны:

- *знать и строго выполнять требования настоящей Инструкции и других документов, регламентирующих использование парольной защиты;*
- *своевременно сообщать администратору информационной безопасности министерства обо всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями;*
- *располагать в помещении экран видеомонитора во время работы так, чтобы исключить возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами;*
- *обеспечивать запирание помещения на ключ при выходе всех работников из помещения, в котором осуществляется работа с информационными системами;*
- *поддерживать постоянную работу (не отключать (блокировать) средства защиты информации;*
- *передавать в случае прекращения трудовых отношений.*

Ответственному за организацию обработки персональных данных в ИС все имеющиеся в пользовании материальные носители информации, содержащие информацию ограниченного доступа.

2.3. При организации парольной защиты запрещается:

- *записывать свои пароли в очевидных местах (на корпусе монитора, на обратной стороне клавиатуры и т.д.);*
- *хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги, а также в электронном виде на магнитных, оптических и электронных носителях информации;*
- *сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД; создавать и хранить документы, содержащие информацию ограниченного доступа, в папках, предназначенных для обмена открытыми документами;*

- *работать с информацией ограниченного доступа в общественных местах и на рабочих станциях, не оборудованных средствами защиты информации;*
- *осуществлять обработку информации на автоматизированном рабочем месте в присутствии лиц, не допущенных к данной информации;*
- *оставлять без личного контроля съемные и другие носители информации (в т. ч. и установленные на автоматизированном рабочем месте), распечатки, содержащие информацию ограниченного доступа;*
- *записывать на устройства, предназначенные для хранения информации ограниченного доступа, посторонние данные;*
- *использовать информацию ограниченного доступа в личных целях, в т. ч. в целях получения выгоды;*
- *выносить за пределы контролируемой зоны организации материальные носители с информацией ограниченного доступа;*
- *оставлять без личного контроля включенное автоматизированное рабочее место без активированной блокировки*

2.4. Руководители структурных подразделений организации несут персональную ответственность за организацию в своем подразделении работы по безусловному выполнению требований настоящей Инструкции и других документов, регламентирующих использование парольной защиты.

3. Порядок применения парольной защиты

3.1. Защита с применением паролей технических средств и программных продуктов осуществляется в соответствии с эксплуатационной документацией на эти технические средства и программные продукты.
3.2. Полная плановая смена паролей на АРМ проводится регулярно, не реже одного раза в год.
3.3. Внеплановая смена (удаление) личного пароля любого пользователя должна производиться в следующих случаях:

- *по окончании срока действия пароля;*
- *в случае увольнения, перехода на другую работу сотрудника организации, являвшегося пользователем АРМ (после окончания последнего сеанса работы данного пользователя с системой);*
- *при обнаружении факта успешной попытки НСД к ИС;*
- *при обнаружении факта компрометации базы данных (электронный или бумажный носитель, содержащей пароли пользователей). 3.4. Срок действия пароля в случае производственной необходимости определяется администратором информационной безопасности. Пароли для ИС хранятся в электронном виде у ответственного сотрудника оператора ИС.*

3.5. Для предотвращения доступа к информации, данным ограниченного распространения, находящейся в ИС, минуя ввод пароля, пользователь по окончании сеанса работы или во время перерыва в работе обязан осуществить выход из ИС либо произвести выключение ПЭВМ.
3.6. Пароли, используемые для локального доступа к программно-аппаратным средствам и доступа к ресурсам ИС вводятся пользователем с клавиатуры.
3.7. Информация о компрометации действующих паролей является чрезвычайным происшествием, доводится пользователем организации до непосредственного руководителя.
3.8. Под компрометацией понимается хищение, утрата действующих паролей, передача или сообщение их лицам, не имеющим на то право, несанкционированный доступ к данным пользователя, защищаемым паролем, другие действия ответственного исполнителя, приведшие к получению его пароля лицами, не имеющими на то право.
3.9. Скомпрометированные пароли выводятся из действия незамедлительно.
3.10. По каждому случаю, связанному с компрометацией действующих паролей, руководство организации организует и проводит в установленном порядке служебное расследование.

По результатам служебного расследования к лицам, допустившим разглашение паролей, могут быть применены меры дисциплинарного воздействия и иные меры, предусмотренные действующим законодательством.

4. Правила обращения со съемными носителями

Сотрудники организации используют съемные носители информации только в случаях, когда это необходимо для выполнения трудовых (служебных) обязанностей.

При использовании съемных носителей сотрудники организации обязаны:

- *использовать съемные носители исключительно для выполнения трудовых обязанностей и не использовать в личных целях;*
- *обеспечивать физическую безопасность съемных носителей;*
- *обеспечивать проверку отсутствия вредоносного программного обеспеченияна съемных носителях;*
- *извещать Ответственного за организацию обработки персональных данных в ИС о фактах утери съемных носителей, содержавших персональные данные работников и (или) обучающихся;*
- *не передавать съемные носители третьим лицам при отсутствии в этом производственной необходимости;*
- *не оставлять съемные носители без присмотра.*

5. Использование электронной почты и ресурсов сети Интернет

При использовании электронной почты сотрудникам организации запрещается:
пересылать информацию ограниченного доступа с использованием общедоступных почтовых сервисов (Яндекс, Рамблер,Mail.ru,Google и другие);

- *открывать вложения подозрительных электронных сообщений: сообщений от незнакомых отправителей; сообщений, содержащих исполняемые файлы (EXE, COM, BAT); сообщений рекламного, развлекательного, оскорбительного характера; переходить по ссылкам на сайты из подозрительных электронных сообщений, в том числе сообщений, содержащих приглашения «открыть», «запустить», «посетить», «нажать», «перейти»;*
- *отправлять электронные письма от имени других сотрудников организации, если иное не определено их служебными обязанностями;*
- *предпринимать попытки несанкционированного доступа к почтовым ящикам других сотрудников организации.*

При использовании ресурсов сети Интернет сотрудникам организации запрещается:

- *использовать для обмена информацией ограниченного доступа сайты представляющие услуги хранения и обмена информацией;*
- *размещать, публиковать информацию ограниченного доступа на общедоступных ресурсах;*
- *загружать из сети Интернет программное обеспечение и устанавливать его на автоматизированные рабочие места.*

6. Порядок действий в случае возникновения нештатных ситуаций

При возникновении нештатных ситуаций, связанных с использованием информационной системы, а также в случаях:

- *подозрения на компрометацию (утерю, разглашение, несанкционированное копирование или использование) личных паролей;*
- *подозрения на наличие вредоносных программ (нетипичная работа программ, появление*
- *графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.);*
- *обнаружения фактов совершения в отсутствие пользователя попыток несанкционированного доступа к техническим средствам и носителям информации (следов вскрытия, измененного состава подключенных устройств, кабелей, в том числе отводов кабелей);*

- *невозможности запуска средств защиты информации или при ошибках в процессе их выполнения;*
- *несанкционированных изменений в конфигурации программного обеспечения; отклонений в нормальной работе программного обеспечения, затрудняющих*
- *эксплуатацию автоматизированного рабочего места;*
- *обнаружения ошибок в программном обеспечении, сотрудник организации обязан обратиться с описанием проблемы к ответственному за обеспечение защиты информации лицу или ответственному за эксплуатацию ИС.*

7. Ответственность сотрудников организации

Сотрудники организации несут персональную ответственность за надлежащее исполнение своих обязанностей, а также сохранность технических средств автоматизированного рабочего места, съемных носителей информации, электронных идентификаторов и целостность установленного программного обеспечения. Пользователь, виновный в нарушениях, несет ответственность, предусмотренную действующим законодательством Российской Федерации.