Рассмотрено и принято:
на Общем собрании трудового коллектива
Протокол № 2 от 17.05.2021г.

Утверждено:
Заведующий
_____Н.Г. Кадочникова
Приказ № 214 от 20.05.2021г.

Согласовано:
Председатель первичной
профсоюзной организации
_____О.Н. Матрошилова
17.05.2021г.

Положение

о разрешительной системе допуска пользователей к информационным системам, используемым в МБДОУ «Детский сад №27 «Семицветик» г.Юрги», в которых обрабатывается конфиденциальная информация

1. Назначение

1.1. Настоящее Положение определяет разрешительный порядок доступа сотрудников МБДОУ «Детский сад №27 «Семицветик» г.Юрги» (далее – Учреждение) к информации, обрабатываемой в информационных системах Учреждения.

II. Область применения

2.1. Настоящее Положение применяется сотрудниками Учреждения, допущенными к обработке информации в информационных системах Учреждения.

III. Нормативные ссылки

3.1. Настоящее Положение разработано в соответствии со следующими документами:

– п.8 ч.2 ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– п. «в» ст.13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;

– п.15.1, п.16.3, п.18.1, п.18.2, п.20.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (Зарегистрировано в Минюсте России 31.05.2013 №28608), а также п. УПД.2, п. УПД.4, п.АНВЗ.5 Приложения 2 к указанным Требованиям;

– подпунктом а) п.8 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620);

– п.3.6 и п.3.15 ,п.5.1.3., п.5.2.7, п.5.3.6., п.5.4.2., п.5.6.3. и п.6.3.14. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;

– методическим документом «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);

– п. А.10.1.3 Таблицы А.1 - Цели и меры управления ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования;

– п. 10.1.3 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;

– Политики информационной безопасности в МБДОУ «Детский сад №27 «Семицветик» г.Юрги»;

– Положения о конфиденциальной информации МБДОУ «Детский сад №27 «Семицветик» г.Юрги».

IV. Термины, обозначения и сокращения

4.1. В настоящем Положении используются следующие термины и определения:

4.1.1. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

4.1.2. Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

4.1.3. Администратор безопасности информации - лицо, отвечающее за защиту информационных систем от несанкционированного доступа к информации, за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации.

4.1.4. Безопасность информации [данных] - 1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность; 2) состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

4.1.5. Должностное лицо – сотрудник Учреждения, правомочный от имени Учреждения исполнять определенные, предусмотренные должностными регламентами (должностными обязанностями) действия.

4.1.6. Информационная система (ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

4.1.7. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

4.1.8. Контрольная зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

4.1.9. Несанкционированный доступ (несанкционированные действия) (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или информационными системами.

4.1.10. Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

4.1.11. Оператор персональных данных (оператор ПДн) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

4.1.12. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

4.1.13. Пользователь (потребитель) информации – 1) субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею; 2) сотрудник Учреждения, или сотрудник иного органа (организации), допущенный в установленном порядке к работе с защищаемой информацией, полномочия которого регламентированы внутренними организационно - распорядительными актами Учреждения.

4.1.14. Регуляторы - Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [1], Федеральная служба безопасности (ФСБ России) [2], Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)[3].

4.1.15. Система защиты информации информационных систем (СЗИИС) – 1) система по обеспечению безопасности защищаемой информации, создаваемая в соответствии с нормативными правовыми актами с целью нейтрализации актуальных угроз безопасности защищаемой информации; 2) система защиты информации информационных систем включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности защищаемой информации и информационных технологий, используемых в информационных системах.

4.1.16. Субъект доступа - пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

4.1.17. Управление доступом - ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

4.1.18. Уязвимость информационной системы - недостаток (слабость) информационной системы, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

4.2. В настоящем Положении используются следующие сокращения:

4.2.1. АС - автоматизированная система;

4.2.2. ИС - информационная система;

4.2.3. ИСПДн - информационная система персональных данных;

4.2.4. ЛВС - локальная вычислительная сеть;

4.2.5. МНИ - машинный носитель информации;

4.2.6. ПДн - персональные данные;

4.2.7. СЗИИС - система защиты информации информационной системы;

4.2.8. СЗИ - средства защиты информации.

---

[1] Полномочия установлены в соответствии с:

- ч.9 ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ч.5 ст.16 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации";
- ст.1 Положения о Федеральной службе по техническому и экспертному контролю, утвержденному Указом Президента Российской Федерации от 16.08.2004 №1085.

[2] Полномочия установлены в соответствии с:

- ч.9 ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ст.11.2, п. «и.1» ст.12 Федерального закона от 03.04.1995 №40-ФЗ "О Федеральной службе безопасности";
- ст.5 Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденного Постановлением Правительства РФ от 16.04.2012 №313.

[3] Полномочия установлены в соответствии с:

- ст.23 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ст.1. и ст.5 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного Постановлением Правительства РФ от 16.03.2009 №228.

V. Общие положения

5.1. Настоящее Положение о разрешительной системе допуска пользователей к информационным системам Учреждения, в которых обрабатывается конфиденциальная информация (далее – Положение) устанавливает разрешительную систему допуска к информации в ИС Учреждения.

5.2. Вся информация, циркулирующая в Учреждении, подразделяется на:

– общедоступную информацию;

– информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

– информацию, в отношении которой установлено требование об обеспечении ее конфиденциальности.

5.3.Относить информацию к категории конфиденциальной, включать/исключать ее в/из Перечня имеет право заведующий ДОУ.

5.4. Контроль соблюдения требований по размещению и использованию компьютеров аттестованной ИС Учреждения (при наличии), указанных в паспорте информационной системы, возлагается на администраторов безопасности информации.

VI. Допуск к информации Учреждения

6.1. Доступ к общедоступной информации Учреждения:

Доступ к общедоступной информации Учреждения, обрабатываемой в информационных системах Учреждения, имеют все сотрудники Учреждения без ограничения, а также иные лица в порядке, определенном внутренними организационно-распорядительными актами Учреждения как оператора информационных систем[4].

6.2. Допуск к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности:

6.2.1. Допуск сотрудников Учреждения к конфиденциальной информации Учреждения, в том числе и обрабатываемой в информационных системах, регламентирован действующими нормативными правовыми актами федеральных органов власти, а также настоящим Положением и Положением о конфиденциальной информации МБДОУ «Детский сад №27 «Семицветик» г.Юрги».

6.2.2. Допуск сотрудников Учреждения к конфиденциальной информации, обрабатываемой в информационных системах Учреждения, осуществляется на основании приказа Учреждения в соответствии с занимаемой должностью в объеме, необходимом для выполнения должностных обязанностей.

6.2.3. Допуск администратора информационных систем, администратора безопасности информации и руководителя подразделения, ответственного за организацию обеспечения безопасности информации к архивным файлам, параметрам настройки средств защиты информации и программного обеспечения и иным данным, не подлежащим изменению в процессе обработки персональных данных, должен быть специально оговорен в приказе, указанном в п.6.2.2 настоящего Положения[5].

---

[4] См.: п.14.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608)

[5] Применяется только для ГИС «АС «АСП». См.:

– п. ЗИС.15 Приложения № 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных

6.2.4. Руководители структурных подразделений допускаются к конфиденциальной информации, обрабатываемой в информационных системах Учреждения, в объеме, необходимом для выполнения стоящих перед указанным подразделением задач.

6.2.5. Технический и обслуживающий персонал допускается к конфиденциальной информации, обрабатываемой в информационных системах Учреждения, в объеме, необходимом для функционирования обслуживаемых технических средств и программных продуктов.

6.2.6. Все сотрудники Учреждения, допущенные к работе в информационных системах, должны быть ознакомлены под подпись в ведомости ознакомления с настоящим Положением и Перечнем.

6.2.7. Допуск к конфиденциальной информации, обрабатываемой в информационных системах Учреждения, иных лиц:

– надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции, на законных основаниях и при наличии документов, на основании которых они проводят проверку;

– контрагенты на основании государственных контрактов или гражданско-правовых договоров, в которых в обязательном порядке оговорены условия соблюдения конфиденциальности полученной информации, допуск к конфиденциальной информации в данном случае предоставляется только в объеме, необходимом для выполнения работ, при этом допуск к персональным данным о частной жизни сотрудника осуществляется с его письменного согласия.

VII. Порядок допуска пользователей и администраторов к информационным ресурсам ИС Учреждения

7.1 Допуск к информационным ресурсам информационных систем Учреждения осуществляется на основании Списка [6] пользователей и администраторов информационных систем Учреждения (Приложение к настоящему Положению). Этот список может вестись в электронном виде.

7.2 Список (Приложение к настоящему Положению) ведет МБДОУ «Детский сад №27 «Семицветик» г.Юрги». В Список (Приложение к настоящему Положению) на основании приказов заведующего включаются сотрудники Учреждения (пользователи и администраторы информационных систем).

7.3 Допуск пользователей и администраторов к информационным ресурсам ИС Учреждения осуществляется только после инструктажа, проведенного администратором безопасности информации.

7.4 Администратор безопасности информации на основании приказов Учреждения регистрирует пользователей и назначает права доступа к информационным ресурсам.

7.5 При изменении статуса пользователя или администратора ИС (увольнении, переводе на другую должность и т.д.) администратор безопасности информации производит изменения в матрице доступа.

приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

– разд.3.13 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[6] Ведется в соответствии с п.5.7.6. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282

7.6 В целях разграничения доступа к информационным ресурсам ИС в Учреждении устанавливается единая система паролирования.

7.7 Действия пользователей, допущенных к информационным ресурсам ИС Учреждения, протоколируются. Ответственность за уничтожение, изменение информации несет пользователь, под чьим именем была проведена регистрация в ИС.

7.8 Все сотрудники Учреждения, допущенные к работе с информационными ресурсами ИС Учреждения, должны быть ознакомлены под подпись с перечисленными выше требованиями[7] и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, за разглашение парольной информации и сохранность конфиденциальной информации информационных систем.

VIII. Доступ к конфигурации информационных систем Учреждения

8.1 С целью пресечения несанкционированных действий пользователей должны выполняться необходимые мероприятия по защите конфигурации настроек компьютеров, входящих в информационные системы.

8.2 В программе начальной загрузки SETUP должна быть заблокирована возможность загрузки с системной дискеты или CD-ROM.

8.3 Для обеспечения безопасности функционирования информационных систем Учреждения и информационных ресурсов в указанных ИС должны быть установлены ограничения для программ настроек сети, защиты, системы, должна блокироваться возможность настройки ПЭВМ пользователем, должны скрываться кнопки организации доступа к файлам и принтерам, должны делаться недоступными средства редактирования реестра, должен быть запрещен запуск программ MS-DOS в монопольном режиме и т.д.

8.4 Реализация и усиление тех или иных ограничений по изменению конфигурационных настроек возлагается на администратора информационной безопасности, который имеют право изменения данных правил для осуществления политики информационной безопасности в ИС.

8.5 Заведующий МБДОУ «Детский сад №27 «Семицветик» г.Юрги», и _____ имеют право требовать от пользователей прекращения обработки информации в ИС Учреждения в случае установления несанкционированных действий пользователей по изменению конфигурации ИС.

IX. Контроль допуска лиц в помещения контролируемой зоны Учреждения

9.1 Контроль доступа лиц в помещения контрольной зоны Учреждения:

9.1.1 в рабочее время осуществляется самими сотрудниками и ответственным за помещение контрольной зоны:

- должен осуществляться контроль доступа посетителей в помещения контрольной зоны, контроль перемещения посетителей внутри помещения контрольной зоны, запрещается оставлять посетителей одних в помещениях контрольной зоны;
- должен осуществляться контроль условий невозможности считывания посетителями с мониторов компьютеров видовой информации, а также контроль блокирования компьютеров ИС сотрудниками Учреждения при временной отлучке с рабочего места и др.;

9.1.2 в нерабочее время:

- контроль доступа в контрольную зону заключается в осуществлении общего контроля исполнения сотрудниками Учреждения требований Инструкции по обеспечению физической защиты помещений контролируемой зоны МБДОУ «Детский сад №27

---

[7] См.:
п.8 ст.86 Трудового кодекса Российской Федерации.

«Семицветик» г.Юрги» и Порядка обращения с конфиденциальной информацией и средствами криптографической защиты в МБДОУ «Детский сад №27 «Семицветик» г.Юрги».

X. Ответственность персонала

10.1 Ответственность персонала

За нарушение требований настоящего Положения должностные лица Учреждения несут ответственность в соответствии с действующим законодательством.

8

Приложение

к Положению о разрешительной системе допуска пользователей

к информационным системам МБДОУ ДС №27 «Семицветик» г.Юрги

Утверждено:
Заведующий
_____ Н.Г. Кадочникова
Приказ № 214 от 20.05.2021г.

СПИСОК
пользователей и администраторов информационных систем, обрабатывающих конфиденциальную информацию Учреждения

Левый разворот

№п/п	Фамилия, имя, отчество	должность	Наименование ИС Учреждения
1	2	3	4
1.	Кадочникова Н.Г.	заведующий	АИС ДОУ
2.	Рослова Т.Ю.	старший воспитатель	АИС Образование Кемеровской области; Сайт МБДОУ «Детский сад №27 «Семицветик» г.Юрги»
3.	Коржуева Н.Б.	главный бухгалтер	Парус

Правый разворот

Наименование органа или учреждения (для внешних пользователей)	№ и дата приказа о допуске к конфиденциальной информации Учреждения	Примечания
5	6	7