МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ДЕТСКИЙ САД № 5»

ПРИКАЗ

г. Североуральск,
п.Черемухово

22.06.2022 № 180

Об утверждении Положения
о службе информационной безопасности

В целях обеспечения выполнения требований действующего законодательства, иных нормативных правых актов в сфере защиты персональных данных и иной конфиденциальной информации,

ПРИКАЗЫВАЮ

1. Утвердить:

1.1. Положение о службе информационной безопасности (далее Положение) (Приложение 1.);

1.2. Форму журнала регистрации выявленных нарушений в сфере защиты персональных данных и иной конфиденциальной информации (Приложение 2.);

1.3. Форму акта выявления нарушений в сфере защиты персональных данных и иной конфиденциальной информации (Приложение 3.).

2. Назначить Руководителем службы информационной безопасности Дик Марину Альбертовну.

3. Руководителю службы информационной безопасности Дик Марине Альбертовне:

3.1. Организовать деятельность службы информационной безопасности в соответствии с утверждённым Положением;

3.2. Разработать и представить на утверждение в срок до 01.07.2022г. план работы по обеспечению информационной безопасности учреждения на 2022-2023г.

4. Контроль за выполнением настоящего приказа возложить на заместителя по воспитательной и методической работе Митяшину Светлану Викторовну.

Заведующий
МАДОУ № 5 Н.Г. Хвалова

В дело 01-14

Муниципальное автономное дошкольное образовательное учреждение
«Детский сад № 5» (МАДОУ № 5)

Адрес: 624475, Свердловская область, г. Североуральск, п. Черемухово, ул. Калинина, д.5,
телефон: (34380) 4-77-29, 4-77-05;
624475 Свердловская область, г. Североуральск, п. Черемухово, ул. Калинина, д. 19а,
телефон: (34380) 4-72-32, 4-72-33, e-mail: mdou5@bk.ru адрес сайта: http://dou5.ru

СОГЛАСОВАНО
Председатель первичной профсоюзной
организации МАДОУ № 5
_____/ Завальная О.М./
(подпись) (Ф.И.О.)
Протокол заседания профкома
№ 3 от 20 июня 2022 г.

УТВЕРЖДАЮ:
Заведующий МАДОУ № 5
_____ Н.Г. Хвалова
Приказ № 180
« 22 » июня 2022 года.

Хвалова Наталья Георгиевна
Подписано цифровой подписью: Хвалова Наталья Георгиевна
Дата: 2022.06.27 14:48:20 +05'00'

Положение о службе информационной безопасности Муниципального автономного дошкольного образовательного учреждения «Детский сад № 5» (МАДОУ № 5)

п. Черемухово, 2022г.

1. Общие положения

Служба информационной безопасности (далее Служба) МАДОУ № 5 (далее Оператор) создаётся в целях выполнения требований действующего законодательства Российской Федерации, иных нормативно-правовых актов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных, а также обеспечение защиты и безопасности информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных.

2. Структура

Структура и штатная численность Службы определяются приказом руководителя учреждения. Служба является самостоятельным структурным подразделением Оператора *(в случае, если это определено соответствующим приказом Оператора, а в штатном расписании выделены штатные единицы специально для Службы)*. *Либо Служба создаётся на функциональной основе, т.е без выделения отдельных штатных единиц, и включает заместителя заведующего, руководителей (при их отсутствии специалистов) кадрового и юридического подразделений, бухгалтера, медицинского работника (кто конкретно указывается в соответствующем приказе заведующего).* Руководство Службой по приказу заведующего возлагается на заместителя заведующего *(если же Служба по каким-либо причинам не создаётся, то он назначается ответственным за информационную безопасность)*.

3. Задачи

Основные задачи Службы заключаются в следующем.

1. Разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
2. Обеспечение постоянного контроля в подразделениях Оператора за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных.
3. Разработка и внесение предложений руководству Оператора по совершенствованию и развитию корпоративной системы обеспечения безопасности и защиты информации, в том числе персональных данных.

4. Функции

Для выполнения поставленных задач Служба осуществляет следующие функции.

1. Готовит и представляет на рассмотрение руководству Оператора проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных.
2. Организует и проводит во взаимодействии с заинтересованными подразделениями классификацию информационных систем на этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в

эксплуатацию и (или) модернизируемых информационных систем) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных в соответствии с установленными требованиями.

3. Разрабатывает и реализует комплекс организационных и мер по обеспечению защиты информации от:

- неправомерного доступа;
- уничтожения;
- модифицирования;
- блокирования;
- копирования;
- предоставления;
- распространения;
- а также от иных неправомерных действий в отношении такой информации.

4. Для защиты информации, в том числе персональных данных от неправомерного доступа Служба обеспечивает:

- контроль за строгим соблюдением принятого Оператором Порядка доступа к конфиденциальной информации, в том числе к персональным данным;
- предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

5. Служба при создании и эксплуатации корпоративных информационных систем:

- самостоятельно разрабатывает и внедряет методы и способы защиты информации, соответствующие установленным требованиям;
- согласовывает исполнителю планируемые для использования в целях защиты информации методы и способы при условии их соответствия установленным требованиям.

6. Служба:

- разрабатывает и реализует меры организационного и технического по недопущению воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- организует и(или) проводит экспертизу технических средств, используемых при обработке информации на предмет соответствия возможностей защиты информации указанных средств установленным требованиям.

7. Служба разрабатывает и реализует меры по информированию и обучению персонала Оператора, в том числе вновь принимаемых на работу лиц, по вопросам защиты информации и персональных данных.

8. Служба контролирует выполнение установленных требований по:

- осуществлению обмена персональными данными при их обработке в информационных системах по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств:

- размещению информационных систем, специального оборудования и охране помещений, в которых ведется работа с персональными данными, организации режима обеспечения безопасности в этих помещениях в части обеспечения сохранности носителей персональных данных и средств защиты информации, а также исключения возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

- соблюдению парольной защиты;

- соблюдению установленного регламента работы с электронной почтой;

- соблюдению требований к программному обеспечению и его использованию.

9. В соответствии с установленными нормативно-правовыми актами требованиями Служба обеспечивает:

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с персональными данными в информационной системе;

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- разбор и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание системы защиты информации, в том числе персональных данных;

- ежегодное планирование работы по совершенствованию системы защиты информации, в том числе персональных данных;

- подготовку и предоставление отчётов заведующему, а также по требованию надзорных и иных уполномоченных органов об организационных и

технических мероприятиях по защите информации, в том числе персональных данных;

- постоянный контроль за обеспечением уровня защищенности информации.

5. Взаимодействие

Для решения поставленных задач и осуществления предусмотренных настоящим Положением функций Служба взаимодействует:

- с руководителем Оператора и его заместителями;
- с любыми иными подразделениями, сотрудниками Оператора;
- с государственными, муниципальными органами, учреждениями и организациями, с надзорными органами, а также с иными органами, предприятиями и организациями.

В ходе взаимодействия руководитель и сотрудники Службы:

- в установленном порядке, получают необходимую для осуществления деятельности Службы информацию, разъяснения, уточнения, нормативные и иные документы;
- готовит и в установленном порядке вносят заведующему предложения по проведению организационных и технических мероприятий, изданию локальных нормативных актов, принятию иных мер по установленным направлениям деятельности в сфере защиты информации, в том числе персональных данных;
- готовят и в установленном порядке предоставляют информацию по находящимся в их компетенции вопросам в сфере защиты информации, в том числе персональных данных, по запросам подразделений и должностных лиц Оператора, государственных, муниципальных органов, учреждений и организаций, надзорных органов, а также иных органов, предприятий и организаций.

6. Ответственность

Руководитель Службы несет ответственность перед руководством Оператора согласно действующему законодательству, нормативно-правовым и локальным нормативным правовым актам за обеспечение:

- выполнения поставленных перед подразделением задач и функций,
- работы с документами и их сохранности, своевременного и качественного исполнения поручений и обращений,
- выполнения требований правил внутреннего трудового распорядка,
- соблюдения в подразделении правил противопожарной безопасности.

Материальную ответственность за сохранность имущества Оператора несут сотрудники Службы, принявшие его на ответственное хранение, согласно действующему законодательству, локальным нормативным правовым актами и договором о материальной ответственности.

Ответственность перед руководителем подразделения за оперативную работу с поступающими документами и контроль за их исполнением в подразделении, несет сотрудник подразделения, назначенный заведующим.

Все сотрудники Службы несут ответственность перед руководителем Службы и заведующим за своевременное и качественное выполнение:

- требований выполнения действующего законодательства Российской Федерации, иных нормативно-правовых документов, регламентирующих обеспечение защиты информации, в том числе обеспечение безопасности при обработке персональных данных;
- обязанностей, предусмотренных Трудовым кодексом РФ, правилами внутреннего трудового распорядка, коллективным договором, настоящим Положением, трудовыми договорами и должностными инструкциями.

Приложение 2.

к приказу от 22.06.2022г. № 180

Форма

Начат «___» _____ 2022г.

Окончен «___» _____ 2022 г.

На _____ листах

ЖУРНАЛ
журнала регистрации выявленных нарушений в сфере защиты персональных данных и иной конфиденциальной информации

№	Дата выявления нарушения	Подразделение, где выявлено нарушение и допустившее нарушение лицо (ФИО, должность)	Кем и при каких обстоятельствах выявлено нарушение (жалоба, плановая проверка и т.д.)	Содержание нарушения	Требования, каких нормативных документов нарушены
1	2	3	4	5	6

Корректирующие и предупреждающие действия по устранению нарушения и предотвращению нарушения в дальнейшем	Ответственное за устранение лицо выявленного нарушения лицо (ФИО, должность и его подпись)	Срок устранения нарушения	Отметка о контроле за выполнением (дата, ФИО и должность проверяющего)
7	8	9	10

Приложение 3.

к приказу от 22.06.2022г. № 180

А К Т №

акта выявления нарушений в сфере защиты персональных данных и иной конфиденциальной информации

_____ «____» _____ 20___ г

Настоящий акт составлен в том, что в

_____

(наименование структурного подразделения, где выявлено нарушение)

ФИО и должность лица, допустившего нарушение_____

допущено нарушение установленных требований в сфере защиты персональных данных и иной конфиденциальной информации.

Содержание нарушения_____

_____

Требования каких нормативных документов нарушены_____

_____

_____

_____

_____

Комиссия (или уполномоченное лицо), выявившая нарушения

Подписи

_____	_____
(подпись)	(Ф. И. О.)
_____	_____
(подпись)	(Ф. И. О.)
_____	_____
(подпись)	(Ф. И. О.)

С актом ознакомлены:

подпись лица, допустившего нарушение_____(ФИО_____)

подпись руководителя структурного подразделения, где допущено нарушение_____(ФИО_____)