Принято на заседании
общего собрания работников
МОБУ «СОШ «Янинский ЦО»
Протокол от 28.12.2001 № 3

Введено в действие
приказом от 28.12.2020 № 368
Директор _____ А.Б. Зюзин

**Положение о службе (ответственном лице)
информационной безопасности**

I. Общие положения

1.1. Ответственный за информационную безопасность (далее - Служба) муниципального общеобразовательного бюджетного учреждения «Средняя общеобразовательная школа «Янинский центр образования» (далее по тексту - 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.

II. Структура

2.1. Структура и штатная численность Службы определяются приказом руководителя учреждения.

2.2. Служба является самостоятельным структурным подразделением Оператора (в случае, если что определено соответствующим приказом Оператора, а в штатном расписании выделены штатные единицы специально для Службы). Либо Служба создается на функциональной основе, т.е без выделения отдельных штатных единиц, и включает заместителей заведующего, медицинского работника (кто конкретно указывается в соответствующем приказе директора).

2.3 Руководство Службой по приказу директора возлагается на заместителя директора (если же Служба по каким-либо причинам не создается то он назначается ответственным за информационную безопасность).

III. Задачи

3.1. Основные задачи Службы заключаются в следующем:

разработка и реализация комплекса организационных и технических мер, направленных на выполнение установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных;

обеспечение постоянного контроля в подразделениях Оператора за выполнением установленных требований к обеспечению безопасности и защите информации, в том числе персональных данных;

разработка и внесение предложении руководству Оператора по совершенствованию и развитию корпоративной системы обеспечения безопасности и защиты информации, в том числе персональных данных.

IV. Функции

4.1. Для выполнения поставленных задач Служба осуществляет следующие функции.

4.1.1. Готовит и представляет на рассмотрение руководству Оператора проекты локальных нормативных актов по вопросам обеспечения защиты информации, в том числе персональных данных.

4.1.2 Организует и проводит во взаимодействии и 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.

4.1.3. 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.

4.1.4. 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.

4.1.5. 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.

4.1.6. 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

4.1.7. 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.

4.1.8. 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.

4.1.9. 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 н 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 к 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, о том числе персональных данных;
ежегодное планирование работы по совершенствованию системы защиты информации, в том числе персональных данных;

подготовку и предоставление отчетов 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.

V. Взаимодействие

5.1. 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.

5.2. 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

VI. Ответственность

6.1. 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 функции;

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.

6.2. 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.

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

6.4. 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.