УТВЕРЖДАЮ

Директор МАУ «МФЦ»
Зимовниковского района
Ростовской области

Н.А.Белякова

«01» декабря 2019 г.

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МАУ «МФЦ» Зимовниковского района Ростовской области

Зимовники
2019

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение документа

1.1.1 Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Положение) определяет содержание и порядок осуществления мероприятий по защите персональных данных в МАУ «МФЦ» Зимовниковского района Ростовской области (далее - Учреждение).

1.1.2 Настоящее Положение разработано в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и «Положением об обработке персональных данных».

1.1.3 Цель Положения – регулирование работ по защите персональных данных и обеспечение функционирования информационных систем персональных данных Учреждения в соответствии с требованиями действующего федерального законодательства в области информационной безопасности.

1.2 Область действия документа

1.2.1 Действие Положения распространяется на информационные системы персональных данных Учреждения, в которых осуществляется обработка персональных данных.

1.2.2 Все работники Учреждения, допущенные к работе с персональными данными, в обязательном порядке должны быть ознакомлены с настоящим Положением под подпись.

1.3 Вступление в силу документа

1.3.1 Настоящее Положение вступает в силу с момента его утверждения руководителем и действует бессрочно до замены его новым Положением.

1.3.2 Все изменения в Положение вносятся приказом руководителя.

2. Организация и проведение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

2.1 Планирование работ по обеспечению безопасности персональных данных

2.1.1 В целях исполнения настоящего Положения ответственный за защиту ПДн и администратор безопасности составляет и утверждает у руководителя план работ по обеспечению безопасности персональных данных, обрабатываемых в Учреждении.

Проводимые в Учреждении мероприятия по обеспечению безопасности персональных данных учитываются в плане мероприятий по защите персональных данных в Учреждении.

2.2 Выполнение работ по обеспечению безопасности персональных данных

2.2.1 В целях организации и проведения работ по обеспечению безопасности персональных данных в Учреждении приказом руководителя назначаются:

– лицо, ответственное за проведение мероприятий по обеспечению безопасности персональных данных и поддержание необходимого уровня информационной безопасности;

– администратор информационной безопасности, ответственный за установку, настройку и обслуживание средств защиты информации, применяемых в Учреждении для обеспечения безопасности персональных данных, а также за организацию и проведение инструктажа работников по основам информационной безопасности при работе с персональными данными;

– комиссия по проведению классификации информационных систем.

2.2.2 Указанные лица ответственны за проведение следующих мероприятий по обеспечению безопасности персональных данных:

– определение и описание информационных систем персональных данных;

– классификацию информационных систем персональных данных;

– определение актуальных угроз безопасности персональных данных;

– проектирование системы защиты персональных данных, включающей организационные, физические и технические меры и средства защиты;

– закупку, установку и настройку технических средств защиты информации;

– внедрение организационных мер и разработку соответствующих регламентов и положений;

– инструктаж и обучение лиц, которые будут использовать средства защиты информации.

2.2.3 Начальники отделов, в которых происходит обработка персональных данных, являются лицами, ответственными за соблюдение требований Положения об обработке персональных данных и других установленных в Учреждении требований.

2.2.4 Для обеспечения безопасности персональных данных в Учреждении применяются следующие меры безопасности:

– организационные меры безопасности:

- инструктаж работников по правилам обеспечения безопасности обрабатываемых персональных данных;
- учет и хранение съемных носителей информации и порядок их обращения, исключающие хищение, подмену и уничтожение;
- мониторинг и реагирование на инциденты информационной безопасности, связанные с персональными данными, включая проведение внутренних проверок, разбирательств и составление заключений;
- постоянный контроль за соблюдением требований по обеспечению безопасности персональных данных (реализуется путем внутренних аудитов);

– меры физической безопасности:

- ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Приказом руководителя устанавливается контролируемая зона, вводятся в действие Список помещений с ограниченным доступом и Список лиц, имеющих право посещать помещения Учреждения с ограниченным доступом. Лица, не указанные в Списке, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт

оборудования и технических средств), при наличии необходимости могут посещать помещения с ограниченным доступом в сопровождении ответственных лиц;

- размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;
- организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

– технические меры безопасности:

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- резервирование технических средств, дублирование массивов и носителей информации;
- использование защищенных каналов связи;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

2.2.5 Ремонтно-восстановительные работы технических средств обработки информации проводятся администратором безопасности. В случае необходимости ремонт технических средств может быть проведен с привлечением сторонних специалистов на договорной основе с составлением актов выполненных работ.

2.3 Контроль выполнения работ по обеспечению безопасности персональных данных

2.3.1 Контроль выполнения работ по обеспечению безопасности персональных данных в Учреждении (далее – Контроль) осуществляется путем проведения периодических контрольных мероприятий (в рамках внутренних аудитов) и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

2.3.2 В рамках проведения контрольных мероприятий выполняются:

– проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности персональных данных за истекший период;

– проверка осведомленности и соблюдения персоналом требований к обеспечению безопасности персональных данных;

– проверка соответствия перечня лиц, которым предоставлен доступ к персональным данным, фактическому состоянию;

– проверка наличия и исправности функционирования технических средств защиты информации, используемых для обеспечения безопасности персональных данных, в соответствии с требованиями эксплуатационной и технической документации;

– инструментальная проверка соответствия настроек технических средств защиты информации требованиям к обеспечению безопасности персональных данных (при необходимости);

– проверка соответствия моделей угроз для информационных систем персональных данных условиям функционирования данных систем;

– проверка соответствия организационно-распорядительной документации по обеспечению безопасности персональным данных действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

2.3.3 Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения должны быть зафиксированы документально.

2.3.4 Контрольные мероприятия проводятся как периодически в соответствии с планом и программой аудита, так и внепланово по решению руководителя и в случае возникновения инцидентов информационной безопасности.

2.3.5 Внутренние проверки в Учреждении в обязательном порядке проводятся в случае выявления следующих фактов:

– нарушение конфиденциальности, целостности, доступности персональных данных;

– халатность и несоблюдение требований к обеспечению безопасности персональных данных;

– несоблюдение условий хранения носителей персональных данных;

– использование средств защиты информации, которые могут привести к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

2.3.6 Задачами внутренней проверки являются:

– установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

– установление лиц, непосредственно виновных в данном нарушении;

– выявление причин и условий, способствовавших нарушению.

2.4 Совершенствование системы защиты персональных данных

2.4.1 Ежегодно ответственный за защиту персональных данных предоставляет руководителю отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности персональных данных вместе с перечнем предложений по совершенствованию системы защиты персональных данных.

2.4.2 Необходимость реализации мероприятий по совершенствованию системы защиты персональных данных может быть обусловлена:

– результатами проведенных аудитов и контрольных мероприятий;

– изменениями федерального законодательства в области персональных данных;

– изменениями структуры процессов обработки персональных данных в пенсионном фонде;

– результатами анализа инцидентов информационной безопасности;

– результатами мероприятий по контролю и надзору за обработкой персональных данных, проводимых уполномоченным органом;

– жалоб и запросов субъектов персональных данных.

2.4.3 На основании решения, принятого руководителем по результатам рассмотрения ежегодного отчета и предложений по совершенствованию системы защиты персональных данных, ответственный за защиту персональных данных составляет план работ по обеспечению безопасности персональных данных, обрабатываемых в Учреждении, на следующий год.

Лист ознакомления

работников МАУ «МФЦ Зимовниковского района» с Положением МАУ МФЦ Зимовниковского района от 03.12.2019г. «по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МАУ «МФЦ» Зимовниковского района Ростовской области»

Наименование должности	ФИО	Подпись	Дата
Директор	Белякова Наталья Андреевна		03.12.19.
Главный бухгалтер	Мальева Ольга Николаевна		03.12.19.
Начальник информационно-аналитического отдела, системный администратор	Косман Антон Борисович		03.12.19
Ведущий специалист информационно-аналитического отдела	Горбачева Анна Сергеевна		03. 12 19
Ведущий специалист информационно-аналитического отдела	Косман Ирина Валерьевна		03.12.2019г.
Начальник отдела консультирования, приема-выдачи документов	Винокурова Елена Владимировна		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Дьяченко Светлана Викторовна		03 12 2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Денисова Лилия Васильевна		03.12.2019.
Ведущий специалист отдела консультирования, приема-выдачи документов	Гайворонская Марина Георгиевна		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Грицай Екатерина Олеговна		03. 12. 2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Просвирова Наталья Владимировна		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Керимов Руслан Фикрет оглы		03.12.2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Тицкая Виктория Сергеевна		03. 12. 2019
Ведущий специалист отдела консультирования, приема-выдачи документов	Утянская Анастасия Павловна		03.12.2019
Ведущий специалист-консультант	Литвинов Андрей Николаевич		03.12.2019
Специалист ТОСП	Власенко Людмила Ивановна		03.12.2019
Специалист ТОСП	Землянская Татьяна Михайловна		03.12.2019
Специалист ТОСП	Кабан Галина Григорьевна		03.12.19
Специалист ТОСП	Моисеенко Алла Александровна		03.12.2019

Наименование должности	ФИО	Подпись	Дата
Специалист ТОСП	Раева Наталья Юрьевна	Раева	03.12.2019
Специалист ТОСП	Фурсова Наталья Пантелеевна	Фур.	03.12.2019
Вед. спец. отдела консульт. приёма - выдачи документов	Мельникова Маргарита Николаевна		15.07.2020г.
Специалист ТОСП	Самитова Светлана Надимовна	Самит	08.10.2020г.