БАШҠОРТОСТАН РЕСПУБЛИКАҺЫ
ҒАФУРИ РАЙОНЫ МУНИЦИПАЛЬ
РАЙОНЫ ИМӘНДӘШ АУЫЛЫНЫҢ
ТӨП ДӨЙӨМ БЕЛЕМ БИРЕҮ МӘКТӘБЕ
МУНИЦИПАЛЬ БЮДЖЕТ ДӨЙӨМ БЕЛЕМ
БИРЕҮ УЧРЕЖДЕНИЯҺЫ
453053, ИМӘНДӘШ АУЫЛЫ,
КОЛХОЗ урамы, 47

Телефон (факс) : 2-52-61
E-mail: school-imendysh
@yandex.ru

РЕСПУБЛИКА БАШКОРТОСТАН
ГАФУРИЙСКИЙ РАЙОН
МУНИЦИПАЛЬНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ОСНОВНАЯ
ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА
С. ИМЕНДЯШЕВО
453053, С.ИМЕНДЯШЕВО,
ул. Колхозная 47

Телефон (факс): 2-52-61
E-mail: school-imendysh
@yandex.ru

БОЙОРОК **ПРИКАЗ**

«15» январь 2025 й. № 1А «15» января 2025 г.

«О создании комиссии и проведении внутреннего контроля работы с персональными данными»

В соответствии с пунктом 4 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ, с требованиями законодательства в сфере обработки персональных данных

П Р И К А З Ы В А Ю:

1. Создать комиссию по проведению внутреннего контроля соответствия обработки персональных данных в составе

Махмутовой А.Ф. – и.о. директора школы;

Махмутовой А.А. – зам по УВР;

Муллашева С.И. – председатель первичной профсоюзной организации в школе.

2. Утвердить план-график мероприятий внутреннего контроля соответствия обработки персональных данных на 2024/2025 учебный год (приложение).

3. Утвердить перечень персональных данных, обрабатываемых в МОБУ ООШ с. Имендяшево, инструкцию об осуществлении контроля выполнения требований по защите персональных данных, инструкцию администратора безопасности средств криптографическом защите информации МОБУ ООШ с. Имендяшево.

4. Комиссии по проведению внутреннего контроля соответствия обработки персональных данных:

- провести мероприятия внутреннего контроля в соответствии с планом- графиком, указанным в пункте 2 настоящего приказа, Положением о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МОБУ ООШ с. Имендяшево МР Гафурийский район РБ и НОШ д. Таишево – филиала МОБУ ООШ с. Имендяшево требованиям законодательства в сфере обработки персональных данных и Политикой обработки персональных данных МОБУ ООШ с.Имендяшево МР Гафурийский район РБ;
- представить итоги внутреннего контроля в срок, указанный в плане- графике мероприятий внутреннего контроля соответствия обработки персональных данных на 2024/2025 учебный год.

5. Контроль исполнения настоящего приказа оставляю за собой.

И.о директора школы А.Ф. Махмутова

С приказом ознакомлены:

Приложение
к приказу
от 15.01.2025г № 1А

План-график мероприятий внутреннего контроля соответствия обработки персональных данных на 2024/2025 учебный год

Мероприятие	Ответственный	Срок исполнения
Проверка соблюдения правил доступа к персональным данным	Зам по УВР	01.02.2025, 01.03.2025, 01.04.2025, 13.05.2025, 03.06.2025
Проверка соблюдения режима защиты		
Проверка выполнения антивирусной политики	Учитель информатики и ИКТ –	25.03.2025, 21.06.2025
Проверка обновления ПО и единообразия применяемого ПО на всех устройствах, используемых при обработке персональных данных		
Проверка актуальности локальных нормативных актов в сфере обработки персональных данных	Зам по УВР	10.01.2025, 16.05.2025
Рассмотрение итогов мероприятий внутреннего контроля на совещании при директоре	Зам по УВР	

Утверждено
приказом и.о.
директора школы
№ 1А от 15.01.2025г

Перечень персональных данных, обрабатываемых в МОБУ ООШ с. Имендяшево МР Гафурийский район РБ

1. Перечень персональных данных, обрабатываемых и подлежащих защите в МОБУ ООШ с.Имендяшево МР Гафурийский район РБ (далее – МОБУ ООШ с.Имендяшево), разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Уставом МОБУ ООШ с.Имендяшево.

2. Сведениями, составляющими персональные данные, в МОБУ ООШ с.Имендяшево является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу.

3. Персональные данные, обрабатываемые в МОБУ ООШ с.Имендяшево подразделяются на три категории: персональные данные работников МОБУ ООШ с.Имендяшево, учащихся и выпускников МОБУ ООШ с.Имендяшево, персональные данные родителей (законных представителей) обучающихся МОБУ ООШ с.Имендяшево.

4. Персональные данные работников, обрабатываемые в МОБУ ООШ с.Имендяшево:

- фамилия, имя, отчество;
- дата и место рождения;
- паспортные данные и гражданство;
- адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;
- номера телефонов (мобильного и домашнего);
- сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения);
- сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения);
- сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации, а также реквизитов других организаций с полным наименование занимаемых ранее в них должностей и времени работы в этих организациях);
- сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и

записях в ней;

- содержание и реквизиты трудового договора с работником или гражданс правового договора с клиентом;

- сведения о заработной плате (номера счетов для расчета с работниками);

- сведения о воинском учете военнообязанных лиц и лиц, подлежащих призы на военную службу (серия, номер, дата выдачи, наименование органа, выдавше военный билет);

- сведения о семейном положении (состояние в браке, данные свидетельства заключении брака; фамилии, имена, отчества, даты рождения, место учеб иждивенцев);

- данные страхового свидетельства государственного пенсионного страхования;

- сведения об идентификационном номере налогоплательщика;

- данные страхового полиса обязательного медицинского страхования;

- адрес электронной почты;

- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

- прохождение аттестации, датах прохождения и принятых аттестационными комиссиями решениях и вынесенных рекомендациях.

- награждение государственными и ведомственными наградами, иными наградами

- фотографии.

5. Персональные данные учащихся и выпускников, обрабатываемые в МОБУ ООШ с.Имендяшево:

- фамилия, имя, отчество;
- дата рождения;
- СНИЛС;
- реквизиты свидетельства о рождении (серия и номер, дата выдачи, кем выдан) или реквизиты документа, удостоверяющего личность (тип документа, серия и номер, дата и место выдачи, кем выдан).
- адрес фактического места жительства;
- домашний телефон;
- номер полиса обязательного медицинского страхования;
- медицинские противопоказания, и рекомендации медицинского характера
- место учебы (работы);
- класс (если есть);
- дата зачисления (прибытия);
- дата и номер приказа о приеме;
- форма обучения;
- вид образовательной программы (дополнительная общеразвивающая программа);
- наименование образовательной программы;
- направленность образовательной программы

- результаты обучения по годам и курсам;
- участие в мероприятиях (олимпиадах, конкурсах, соревнованиях и т.д.): название мероприятия, тип мероприятия, дата участия, форма и результаты участия ребенка;
- дата окончания/отчисления (факт);
- приказ об окончании/отчислении;
- основание окончания/отчисления.

6. Персональные данные персональные данные родителей (законных представителей) обучающихся МОБУ ООШ с.Имендяшево:

- фамилия, имя, отчество, дата рождения;
- образование;
- место регистрации и место фактического проживания;
- номер домашнего и мобильного телефона;
- выполняемая работа, занимаемая должность;
- номер служебного телефона;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС)

БАШҠОРТОСТАН РЕСПУБЛИКАҺЫ
ҒАФУРИ РАЙОНЫ МУНИЦИПАЛЬ
РАЙОНЫ ИМӘНДӘШ АУЫЛЫНЫҢ
ТӨП ДӨЙӨМ БЕЛЕМ БИРЕҮ МӘКТӘБЕ
МУНИЦИПАЛЬ БЮДЖЕТ ДӨЙӨМ БЕЛЕМ
БИРЕҮ УЧРЕЖДЕНИЯҺЫ
453053, ИМӘНДӘШ АУЫЛЫ,
КОЛХОЗ урамы, 47

Телефон (факс) : 2-52-61
E-mail: school-imendysh
@yandex.ru

РЕСПУБЛИКА БАШКОРТОСТАН
ГАФУРИЙСКИЙ РАЙОН
МУНИЦИПАЛЬНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ОСНОВНАЯ
ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА
С. ИМЕНДЯШЕВО
453053, С.ИМЕНДЯШЕВО,
ул. Колхозная 47

Телефон (факс): 2-52-61
E-mail: school-imendysh
@yandex.ru

БОЙОРОК

«15» январь 2025 й. № 1Б

ПРИКАЗ

«15» января 2025 г.

«Об утверждении перечня программного обеспечения, разрешенного к установке в МОБУ ООШ с.Имендяшево МР Гафурийский район РБ»

В соответствии с защитой информации от утечки по техническим каналам,
п р и к а з ы в а ю :

1. Утвердить перечень программного обеспечения, разрешенного к установке в МОБУ ООШ с.Имендяшево МР Гафурийский район РБ (далее - Перечень) согласно приложению 1 к настоящему приказу.
2. Утвердить инструкции по установке, ремонту, модернизации, модификации и техническому обслуживанию программного обеспечения и аппаратных средств в ИСПДн МОБУ ООШ с.Имендяшево МР Гафурийский район РБ.
3. Сотрудникам МОБУ ООШ с.Имендяшево МР Гафурийский район РБ запретить использование на автоматизированных рабочих местах (далее - АРМ) программного обеспечения, не вошедшего в Перечень.
4. Специалисту по защите информации МОБУ ООШ с.Имендяшево МР Гафурийский район РБ Рашитовой М.З., ответственному за выполнение работ в области информационных технологий, не реже 1 раза в полугодие проводить мероприятия по выявлению и удалению на АРМ сотрудников МОБУ ООШ с.Имендяшево МР Гафурийский район РБ программного обеспечения, не вошедшего в Перечень.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Приложение 1
к приказу
от 15.01.2025 № 1Б

ПЕРЕЧЕНЬ
программного обеспечения, разрешенного к установке
в МОБУ ООШ с. Имендяшево, НОШ д. Таишево – филиала МОБУ ООШ с. Имендяшево

№ п/п	Тип программного обеспечения	Наименование программного обеспечения
1.	Операционные системы	Alt Linux
2.		Astra Linux
3.	Системы мониторинга управления	Kaspersky Security Center
4.		Сервер безопасности Dallas Lock
5.	Средства обеспечения информационной безопасности	VipNet Client
6.		VipNet CSP
7.		VipNet Coordinator
8.		КриптоПро CSP
9.		Dallas Lock
10.		Secret Net
11.		Средство криптографической защиты информации «Континент- АП»
12.		Крипто АРМ
13.		Kaspersky Endpoint Security
14.	Прикладное ПО общего назначения	ТЕЗИС Помощник
15.		СПО справки БК
16.		CorelDRAW Graphics Suite
17.		AutoCAD
18.		NanoCAD
19.		Renga X 3
20.		ArchiCad
21.		Photoshop
22.		MapInfo
23.		Автоматизированный Кадастровый Офис
24.		Autodesk 360 Arhicad
25.		Autodesk 3ds Max
26.		Vray for 3ds Max
27.		Zulu 7.0
28.		Архиватор WinRAR
29.		IBM Lotus Notes
30.		Nero
31.		ЕДДС-112
32.		Программа подготовки отчетных документов для ПФР "Spu orb"
33.		СБ «Лавина»
34.		K-Lite Codec Pack
35.	Офисные приложения	Microsoft Office
36.		Р7 Офис
37.		Libre Office
38.		Яндекс.Браузер
39.		Браузер chromium-gost
40.		Google Chrome
41.		Adobe Acrobat Reader
42.		Единая система коммуникаций на базе типового АРМ для

УТВЕРЖДЕНА
приказом
от 15.01.2025 г. № 1Б

ИНСТРУКЦИЯ
по установке, ремонту, модернизации, модификации и техническому обслуживанию программного обеспечения и аппаратных средств в ИСПДн МОБУ ООШ с.Имендяшево МР Гафурийский район РБ

1. Общие положения.

Инструкция по установке, ремонту, модернизации, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных (ИСПДн) МОБУ ООШ с.Имендяшево МР Гафурийский район РБ и НОШ д. Таишево – филиал МОБУ ООШ с. Имендяшево (далее – Учреждение), включает в себя описание полного комплекса организационно-технических мер по проведению работ по данной тематике.

Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников Учреждения, использующих в работе ИСПДн, в которых осуществляется обработка информации ограниченного доступа, не составляющей государственной тайны.

Должностные лица Учреждения, задействованные в обеспечении функционирования ИСПДн, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

Ознакомление с требованиями Инструкции пользователей ИСПДн осуществляется ответственным за организацию обработки персональных данных.

2. Порядок проведения работ

Право внесения изменений в конфигурацию автоматизированных рабочих мест и состава программного обеспечения средств вычислительной техники Учреждения предоставляется учителю информатики и ИКТ.

Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме учителя информатики и ИКТ ЗАПРЕЩЕНО.

Установка и настройка программного средства осуществляется учителем информатики и ИКТ согласно эксплуатационной документации.

Запрещается установка и использование на ПЭВМ (серверах) любого программного обеспечения (ПО), не входящего в перечень программного обеспечения, разрешенного к использованию в Учреждении.

Руководители структурных подразделений осуществляют контроль за отсутствием на ПЭВМ сотрудников подразделения программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

Установка (обновление) ПО (системного, тестового и т.п.) на рабочих станциях и серверах производится с эталонных копий программных средств, хранящихся у учителя информатики и ИКТ .

Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода.

После установки (обновления) программного обеспечения учитель информатики и ИКТ.), должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и, совместно с пользователем АРМ проверить правильность настройки средств защиты.

В случае обнаружения не декларированных (не описанных в документации) возможностей программного средства, сотрудники немедленно докладывают руководителю и учителю информатики и ИКТ . В этом случае использование программного средства до получения специальных указаний ЗАПРЕЩАЕТСЯ.

При изъятии ПЭВМ из состава рабочих станций, обрабатывающих информацию ограниченного распространения (защищаемая информация), её передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как учитель информатики и ИКТ снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации, которая хранилась на дисках компьютера.

Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью учителя информатики и ИКТ.

3. Порядок пересмотра инструкции

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Учреждения, приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности ПДн Учреждения.

Полный пересмотр данного документа проводится ответственным за организацию обработки персональных данных с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Учреждения.

Вносимые изменения не должны противоречить другим положениям Инструкции.

4. Ответственные за организацию и контроль выполнения инструкции

Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников Учреждения.

Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на учителя информатики и ИКТ и специалистов Учреждения.

Ответственность за общий контроль информационной безопасности возлагается на ответственного за организацию обработки персональных данных и администратора информационной безопасности.

7. Срок действия и порядок внесения изменений

7.1. Настоящая Инструкция вступает в силу с момента её утверждения и действует бессрочно.

7.2. По мере необходимости в настоящую Инструкцию могут быть внесены дополнения и изменения в соответствии с законодательством РФ.

7.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом директора Учреждения.

БАШҠОРТОСТАН РЕСПУБЛИКАҺЫ
ҒАФУРИ РАЙОНЫ МУНИЦИПАЛЬ
РАЙОНЫ ИМӘНДӘШ АУЫЛЫНЫҢ
ТӨП ДӨЙӨМ БЕЛЕМ БИРЕҮ МӘКТӘБЕ
МУНИЦИПАЛЬ БЮДЖЕТ ДӨЙӨМ БЕЛЕМ
БИРЕҮ УЧРЕЖДЕНИЯҺЫ
453053, ИМӘНДӘШ АУЫЛЫ,
КОЛХОЗ урамы, 47

Телефон (факс) : 2-52-61
E-mail: school-imendysh
@yandex.ru

РЕСПУБЛИКА БАШКОРТОСТАН
ГАФУРИЙСКИЙ РАЙОН
МУНИЦИПАЛЬНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ОСНОВНАЯ
ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА
С. ИМЕНДЯШЕВО
453053, С.ИМЕНДЯШЕВО,
ул. Колхозная 47

Телефон (факс): 2-52-61
E-mail: school-imendysh
@yandex.ru

БОЙОРОК **ПРИКАЗ**

«15» январь 2025 й. № 1В «15» января 2025 г.

«Об утверждении регламента реагирования на инциденты информационной безопасности в информационных системах персональных данных»

Во исполнение требований Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», и прочих нормативных документов по защите информации,

П Р И К А З Ы В А Ю:

1. Утвердить и ввести в действие Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных МОБУ ООШ с.Имендяшево МР Гафурийский район РБ (далее – Регламент) (Приложение к настоящему Приказу).
2. Требования прилагаемого Регламента довести до работников, непосредственно осуществляющих защиту персональных данных в информационных системах персональных данных.
3. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. директора А.Ф. Махмутова

Приложение
к приказу от 15.01.2025г № 1В

РЕГЛАМЕНТ

реагирования на инциденты информационной безопасности в информационных системах персональных данных МОБУ ООШ с.Имендяшево МР Гафурийский район РБ и НОШ д. Таишево – филиал МОБУ ООШ с. Имендяшево

1. Термины и определения

1.1. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.2. Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.3. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

1.5. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящий Регламент реагирования на инциденты информационной безопасности в информационных системах персональных данных МОБУ ООШ с.Имендяшево МР Гафурийский район РБ и НОШ д. Таишево – филиал МОБУ ООШ с. Имендяшево (далее – Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее –ПДн) и нормативно-методическими документами федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящий Регламент определяет:

- порядок регистрации событий безопасности;

- порядок выявления инцидентов информационной безопасности и реагированию на них;
- порядок проведения анализа инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов.

2.3. Регламент обязателен для исполнения всеми работниками МОБУ ООШ с.Имепндяшево МР Гафурийский район РБ (далее –Учреждение), непосредственно осуществляющими защиту ПДн в ИСПДн.

3. Инциденты информационной безопасности

3.1. К инцидентам ИБ относятся:

- несоблюдение требований по защите ПДн:
  - использование ЭВМ в целях, не связанных с выполнением трудовых (служебных, должностных, функциональных) обязанностей;
  - утрата носителя ПДн;
  - утрата ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков.
- попытки НСД к ПДн:
  - подбор чужого идентификатора и пароля, последующий доступ с использованием чужого пароля;
  - изменение настроек, состава, паролей технических средств ИСПДн;
  - изменение (увеличение) полномочий доступа;
  - нарушение целостности установленных защитных пломб;
  - копирование ПДн на неучтенные съемные носители ПДн;
  - заражение рабочего места и/или сервера ИСПДн вредоносной программой;
  - хищение носителей ПДн;
  - хищение технических средств ИСПДн;
  - умышленное нарушение работоспособности технических средств ИСПДн;
  - хищение криптосредств, ключевых документов, ключей от помещений и хранилищ, личных печатей, удостоверений, пропусков;
  - несанкционированное проникновение в помещения ИСПДн;
  - очистка электронных журналов мониторинга.
- сбои в работе технических средств ИСПДн Общества.

3.2. К инцидентам ИБ не относятся:

- неудачные попытки вторжений, которые были обнаружены и нейтрализованы с использованием СЗИ;
- неудачные попытки заражения рабочих мест и/или серверов ИСПДн вредоносной программой, которые были обнаружены и нейтрализованы с использованием СЗИ

4. Порядок регистрации событий безопасности

4.1. Регистрация событий безопасности в ИСПДн осуществляется в следующей последовательности:

1) Определение событий безопасности, подлежащих регистрации, и сроков их хранения.
2) Определение состава и содержания информации о событиях безопасности, подлежащих регистрации.

3) Сбор, запись и хранение информации о событиях безопасности.
4) Реагирование на сбои при регистрации событий безопасности.
5) Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.
6) Генерирование временных меток и (или) синхронизация системного времени в ИСПДн.
7) Защита информации о событиях безопасности.

4.2. События безопасности, подлежащие регистрации в ИСПДн, должны определяться с учетом способов реализации угроз безопасности ПДндля ИСПДн. К событиям безопасности, подлежащим регистрации в ИСПДн, должны быть отнесены любые проявления состояния ИСПДн и ее системы защиты, указывающие на возможность нарушения конфиденциальности, целостности или доступности ПДн, доступности компонентов ИСПДн, нарушения процедур, установленных организационно-распорядительными документами по защите ПДн, а также на нарушение штатного функционирования средств защиты информации (далее – СЗИ).

4.3. События безопасности, подлежащие регистрации в ИСПДн, и сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов информационной безопасности, возникших в ИСПДн.

4.4. В ИСПДн подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (остановка) операционной системы;
- подключение съемных машинных носителей ПДн и вывод ПДн на носители;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой ПДн;
- обновление или ошибки при обновлении программных средств ИСПДн и СЗИ;
- попытки доступа программных средств к определяемым защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

4.5. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъекта доступа (пользователя и (или) процесса), связанного с данным событием безопасности.

4.6. При регистрации входа (выхода) субъектов доступа в ИСПДн и загрузки (остановка) операционной системы состав и содержание информации должны, как минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (остановки) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

4.7. При регистрации подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители состав и содержание регистрационных записей должны, как

минимум, включать дату и время подключения съемных машинных носителей ПДн и вывода ПДн на съемные носители, логическое имя (номер) подключаемого съемного машинного носителя ПДн, идентификатор субъекта доступа, осуществляющего вывод ПДн на съемный носитель ПДн.

4.8. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой ПДнсостав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

4.9. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

4.10. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

4.11. При регистрации попыток удаленного доступа к ИСПДн состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к ИСПДн.

4.12. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

- возможность выбора Ответственным за обеспечение безопасности ПДн в ИСПДни (или) Администратором ИСПДн событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 4.4 настоящего Регламента;
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в соответствии с пунктами 4.6–4.11 настоящего Регламента;
- хранение информации о событиях безопасности в течение времени, установленного в пункте 4.3 настоящего Регламента.

4.13. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с пунктами 4.7 – 4.11настоящего Регламента, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

4.14. В ИСПДн должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

4.15. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

- предупреждение (сигнализация, индикация) о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения Ответственным за обеспечение безопасности ПДн в ИСПДн и (или) Администратором ИСПДн параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПДн, запись поверх устаревших хранимых записей событий безопасности.

4.16. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии и с периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов информационной безопасности в ИСПДн.

4.17. В случае выявление признаков инцидентов информационной безопасности в ИСПДн осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности в соответствии с порядком проведения разбирательств по фактам возникновения инцидентов в ИСПДн.

4.18. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИСПДн, достигается посредством применения внутренних системных часов ИСПДн.

4.19. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

4.20. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам:

- ответственному за обеспечение безопасности ПДн в ИСПДн;
- администратору ИСПДн.

5. Порядок выявления инцидентов информационной безопасности и реагирования на них

5.1. За выявление инцидентов информационной безопасности и реагирование на них отвечают:

- ответственный за обеспечение безопасности ПДн в ИСПДн;
- администратор ИСПДн.

5.2. Работники Учреждения, должны сообщать ответственным за выявление инцидентов информационной безопасности о любых инцидентах, в которые входят:

- факты попыток и успешной реализации несанкционированного доступа в ИСПДн, в помещения, в которых осуществляется обработка ПДн, и к хранилищам ПДн;
- факты сбоя или некорректной работы систем обработки информации;
- факты сбоя или некорректной работы СЗИ;
- факты разглашения ПДн;
- факты разглашения информации о методах и способах защиты и обработки ПДн.

5.3. Все нештатные ситуации, факты вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки ПДн в ИСПДн должны быть занесены ответственными за выявление инцидентов информационной безопасности в «Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки персональных данных в МОБУ ООШ с.Имендяшево МР Гафурийский район РБ, форма которого установлена в Приложении 1 к настоящему Регламенту или в электронные журналы операционной системы и СЗИ.

5.4. Анализ инцидентов информационной безопасности, в том числе определение источников и причин возникновения инцидентов, осуществляется согласно порядку проведения разбирательств по фактам возникновения инцидентов информационной безопасности в ИСПДн.

5.5. Меры по устранению последствий инцидентов информационной безопасности, планированию и принятию мер по предотвращению повторного возникновения инцидентов, возлагаются на ответственных за выявление инцидентовинформационной безопасности.

6. Основные этапы процесса реагирования на инциденты

6.1. Лица (администратор ИС), занимающиеся реагированием на инциденты должны обеспечить защиту ИСПДн и проинформировать пользователей, о важности мер по обеспечению информационной безопасности.

6.2. Лица, занимающиеся реагированием на инциденты, должны определить, является ли обнаруженное ими с помощью различных систем обеспечения информационной безопасности событие инцидентом или нет.

6.3. Лица, занимающиеся реагированием на инциденты, должны идентифицировать скомпрометированные компьютеры и настроить правила безопасности таким образом, чтобы заражение не распространилось дальше по сети. Кроме того, на этом этапе необходимо перенастроить сеть таким образом, чтобы ИСПДн могли продолжать работать без зараженных машин.

6.4. Далее лица, занимающиеся реагированием на инциденты, удаляют вредоносное программное обеспечение, а также все артефакты, которые оно могло оставить на зараженных компьютерах в ИСПДн.

6.5. Ранее скомпрометированные компьютеры вводятся обратно в сеть. При этом лица, занимающиеся реагированием на инциденты, некоторое время продолжают наблюдать за состоянием этих машин и ИСПДн в целом, чтобы убедиться в полном устранении угрозы.

6.6. Лица, занимающиеся реагированием на инциденты, анализируют произошедший инцидент, вносят необходимые изменения в конфигурацию программного обеспечения и оборудования, обеспечивающего информационной безопасности, и формируют рекомендации для того, чтобы в будущем предотвратить подобные инциденты. При невозможности полного предотвращения будущей атаки составленные рекомендации позволят ускорить реагирование на подобные инциденты.

7. Порядок проведения разбирательств по фактам возникновения инцидентов информационной безопасности

7.1. Для проведения разбирательств по фактам возникновения инцидентов информационной безопасности создаётся комиссия, состоящая не менее чем из трех человек с обязательным включением в её состав:

- ответственного за обеспечение безопасности ПДн в ИСПДн;
- администратора ИСПДн.

7.2. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками структурных подразделений организации, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам проведённого разбирательства, которое передается на рассмотрение Директору Учреждения.

7.3. При проведении разбирательства устанавливаются:

- наличие самого факта совершения инцидента информационной безопасности, служащего основанием для вынесения соответствующего решения;
- время, место и обстоятельства возникновения инцидента, а также оценка его последствий;
- конкретный работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента;
- наличие и степень вины работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновение инцидента;
- цели и мотивы, способствовавшие совершению инцидента информационной безопасности.

7.4. В целях проведения разбирательства все работники обязаны по первому требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения об известных им фактах по существу заданных им вопросов.

7.5. Работник, совершивший инцидент информационной безопасности или повлекший своими действиями возникновения инцидента, обязан по требованию комиссии представить объяснения в письменной форме не позднее трех рабочих дней с момента получения соответствующего требования. Комиссия вправе поставить перед

работником перечень вопросов, на которые работник обязан ответить. В случае отказа работника от письменных объяснений, комиссией составляется акт.

7.6. Работник имеет право, по согласованию с председателем комиссии, знакомиться с материалами разбирательства, касающимися лично его, и давать по поводу них свои комментарии, предоставлять дополнительную информацию и документы. По окончании разбирательства работнику для ознакомления предоставляется итоговый акт с выводами комиссии.

7.7. В случае давления на работника со стороны других лиц (не из состава комиссии) в виде просьб, угроз, шантажа и др., по вопросам, связанным с проведением разбирательства, работник обязан сообщить об этом председателю комиссии.

7.8. До окончания работы комиссии и вынесения решения членам комиссии запрещается разглашать сведения о ходе проведения разбирательства и ставшие известные им обстоятельства.

7.9. В процессе проведения разбирательства комиссией выясняются:

- перечень разглашенных сведений;
- причины разглашения сведений;
- лица, виновные в разглашении сведений;
- размер (экспертную оценку) причиненного ущерба;
- недостатки и нарушения, допущенные работниками при работе с ПДн;
- иные обстоятельства, необходимые для определения причин разглашения ПДн, степени виновности отдельных лиц, возможности применения к ним мер воздействия.

7.10. По завершении разбирательства комиссией составляется заключение. В заключении указываются:

- основание для проведения в разбирательства;
- состав комиссии и время проведения разбирательства;
- сведения о времени, месте и обстоятельствах возникновения инцидента информационной безопасности;
- сведения о работнике, совершившем инцидент информационной безопасности или повлекшем своими действиями возникновения инцидента (должность, фамилия, имя, отчество, год рождения, время работы в Учреждении, а также в занимаемая должность);
- цели и мотивы работника, способствовавшие совершению инцидента информационной безопасности;
- причины и условия возникновения инцидента информационной безопасности;
- данные о характере и размерах причиненного в результате инцидента ущерба;
- предложения о мере ответственности работника, совершившего инцидент информационной безопасности или повлекшего своими действиями возникновения инцидента.

7.11. На основании заключения выносится решение о применении мер ответственности к работнику, совершившему инцидент или повлекшему своими действиями возникновению инцидента, также о возмещении ущерба виновным работником (или его законным представителем), которое доводится до указанного работника в письменной форме под расписку.

7.12. Все материалы разбирательства относятся к информации ограниченного доступа и хранятся в течение 5 лет. Копии заключения и распоряжения по результатам разбирательства приобщаются к личному делу работника, в отношении которого оно проводилось.

8. Ответственность

8.1. Все работники, осуществляющие защиту ПДн, обязаны ознакомиться с данным Регламентом под подпись.

8.2. Работники несут персональную ответственность за выполнение требований настоящего Регламента.

9. Срок действия и порядок внесения изменений

9.1. Настоящий Регламент вступает в силу с момента его утверждения и действует бессрочно.

9.2. Настоящий Регламент подлежит пересмотру не реже одного раза в три года.

9.3. Изменения и дополнения в настоящий Регламент вносятся приказом Директора Учреждения.

Приложение 1
к Регламенту реагирования на
инциденты информационной
безопасности в информационных
системах персональных данных

ФОРМА

Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических работ, установки и модификации аппаратных и программных средств обработки информации
в МОБУ ООШ с.Имендяшево МР Гафурийский район РБ

№ /п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО Ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных, подпись	ФИО Администратора информационной системы, подпись	Примечание
1	2	3	4	5	6