

ПРИКАЗ

03.04.2019

№ 185

Об утверждении Положения
о комиссии по обеспечению защиты
персональных данных при их
обработке в информационных системах
персональных данных
в Отделе образования Администрации
Обливского района

В соответствии с Конституцией Российской Федерации раздел первый, ст.24., во исполнение ст.86 Трудового Кодекса РФ от 30.12.2001 №197-ФЗ, ст.13.11. КоАП РФ от 30.12.2001 № 195-ФЗ, Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями от 08.06.2020) Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (с изменениями и дополнениями от 24.04.2020г.), Постановления Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Национальный стандарт РФ ГОСТ Р 53114-2008 "Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 532-ст) и в целях упорядочения особенностей хранения, защиты и обработки персональных данных работников Отдела образования,

ПРИКАЗЫВАЮ:

1. Утвердить Положение о комиссии по обеспечению защиты персональных данных при их обработке в информационных системах персональных данных (Приложение № 1).
2. Утвердить состав комиссии по обеспечению защиты персональных данных при их обработке в информационных системах персональных данных (Приложение №2).

3. Утвердить Перечень регулярных мероприятий на 2021-2023г.г.
(Приложение №3).

4. Инспектору по кадрам Поповой Э.И. ознакомить членов состава комиссии с данным приказом в течение 3-х дней под роспись.

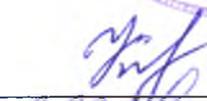
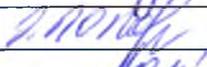
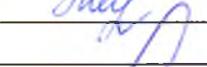
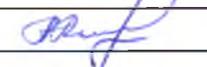
5. Контроль исполнения настоящего приказа оставляю за собой.

Заведующий Отделом образования
Администрации Обливского района



Н.А. Малахова

С приказом ознакомлены (н):

| | |
|---|-------------------|
|  | Колесникова Е.А. |
|  | Попова Э.И. |
|  | Лаптева Л.А. |
|  | Марянина Е.Ю. |
|  | Севастьянова М.Г. |
|  | Литовченко А.Н. |
|  | Некипилая Е.В. |

Эльвира Ивановна Попова
8 863 96 21 8 38

Положение

о комиссии по обеспечению защиты персональных данных при их обработке в информационных системах персональных данных

1. Общие положения

1.1. Настоящее Положение о комиссии по обеспечению защиты персональных данных при их обработке в информационных системах персональных данных в Отделе образования разработано в соответствии с Федеральным законом от 27 июля 2006 г. №152-ФЗ "О персональных данных", постановлением Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (далее - положение, организация) и определяет порядок и организацию работы комиссии по обеспечению защиты персональных данных (далее - комиссия).

1.2. Комиссия в своей работе руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, указами и приказами Президента Российской Федерации, постановлениями и приказами Правительства Российской Федерации, организационно-распорядительными документами организации и настоящим Положением.

Термины и определения:

База данных - совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимая от прикладных программ (ГОСТ 20886-85).

Безопасность информации - состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность (ГОСТ Р 50922-2006).

Выделенные помещения - помещения (кабинеты, актовые, конференц-залы и т.д.) специально предназначенные для обработки персональных данных.

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (ГОСТ Р 50922-2006).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922-2006).

Информационная безопасность (организации) - состояние защищенности интересов организации в условиях угроз в информационной сфере (ГОСТ Р 53114-2008).

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 152-ФЗ).

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (Федеральный закон от 27.07.2006 № 149-ФЗ).

Инцидент информационной безопасности - любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность (ГОСТ Р ИСО/МЭК 27001-2006).

Непреднамеренное воздействие на информацию - ошибка пользователя информацией, сбой технических и программных средств информационных систем, природные явления или иные нецеленаправленные на изменение информации действия, приводящие к искажению, уничтожению,

копированию, блокированию доступа к информации, а также утрате, уничтожению или сбою функционирования носителя информации (ГОСТ Р 51583-20001).

Несанкционированное воздействие на информацию - воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации (ГОСТ Р 50922-2006). 1 Заменен на ГОСТ Р 51583-2014 (с 1 сентября 2014 г.)

Несанкционированный доступ (к информации) - доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации (Р 50.1.053-2005).

Носитель информации - материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (ГОСТ Р 50922-2006).

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 (Федеральный закон от 27.07.2006 № 152-ФЗ).

Оператор (персональных данных) - 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 (Федеральный закон от 27.07.2006 № 152-ФЗ).

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ).

Правило доступа (к защищаемой информации) - совокупность правил, регламентирующих порядок и условия доступа субъекта к защищаемой информации и ее носителям (ГОСТ Р 50922-2006).

Право доступа (к защищаемой информации) - совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации (ГОСТ Р 50922-2006).

Разглашение информации - несанкционированное доведение защищаемой информации до лиц, не имеющих права доступа к этой информации (ГОСТ Р 53114-2008).

Система защиты персональных данных - совокупность организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах персональных данных (Постановление Правительства РФ от 01.11.2012 № 1119).

Угроза безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ).

Угроза информационной безопасности (организации) - совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации (ГОСТ Р 53114-2008).

Утечка информации - неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации иностранными разведками (ГОСТ Р 53114-2008).

2. Цели и задачи комиссии

2.1. Основной целью деятельности комиссии является проведение работ по совершенствованию контроля за соответствием информационных систем персональных данных организации обязательным требованиям законодательства Российской Федерации о защите персональных данных.

2.2. Основными задачами комиссии являются:

- организация и координация действий структурных подразделений организации по вопросам обеспечения безопасности персональных данных;

- обеспечение контроля за выполнением требований по защите персональных данных в организации.

2.3. Комиссия организует и координирует действия структурных подразделений организации по вопросам обеспечения безопасности персональных данных.

2.4. Комиссия вырабатывает рекомендации по вопросам:

- надежного и эффективного управления системой защиты персональных данных;

- своевременного выявления возможных каналов неправомерного распространения персональных данных;

- совершенствования системы защиты персональных данных.

3. Функции комиссии

3. Основными функциями комиссии являются:

3.1. Организация и проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к персональным данным.

3.2. Определение перечня информационных систем персональных данных и перечня персональных данных, подлежащих защите в информационных системах персональных данных.

3.3. Разработка планов мероприятий по обеспечению защиты персональных данных.

3.4. Формирование планов внутренних проверок режима защиты персональных данных и определение периодичности их проведения.

3.5. Выработка предложений об изменении и дополнении перечня персональных данных.

3.6. Разработка и внедрение в деятельность организации локальных нормативных актов, регламентирующих обработку персональных данных и устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации в этой сфере, а также на устранение последствий таких нарушений.

3.7. Проведение анализа обстоятельств и причин неправомерного распространения персональных данных.

3.8. Подготовка предложений по совершенствованию действующей системы защиты персональных данных.

3.9. Доведение до структурных подразделений организации рекомендаций по организации сбора, обработки, хранения, передачи и защиты персональных данных.

3.10. Осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами организации.

4. Порядок формирования комиссии

4.1. Комиссия является коллегиальным органом, строит свою деятельность

на принципах равноправия ее членов и гласности принимаемых решений.

4.2. Комиссия создается приказом руководителя организации, в котором определяется ее персональный состав, назначаются председатель комиссии, его заместитель и секретарь комиссии.

4.3. Председатель комиссии руководит деятельностью комиссии, определяет основные направления деятельности комиссии, организует ее работу и ведет заседания комиссии.

4.4. Срок полномочий комиссии – до особого распоряжения.

5. Организация и порядок работы комиссии

5.1. Деятельность комиссии организуется и проводится в соответствии с текущим планом работы комиссии. План работы комиссии формируются под руководством председателя комиссии.

5.2. План утверждается руководителем организации. При необходимости вопросы, не нашедшие отражения в планах работы комиссии, могут быть внесены на рассмотрение комиссии во внеплановом порядке.

5.3. Решения по вопросам, отнесенным к компетенции комиссии, принимаются на заседаниях комиссии.

5.4. Комиссия проводит заседания на основании плана-графика заседаний комиссии, но не реже одного раза в полгода. Внеплановые заседания проводятся по решению председателя комиссии.

5.5. Заседание комиссии созывается председателем комиссии.

5.6. Заседание комиссии считается правомочным, если на нем присутствует не менее половины ее членов.

5.7. Решения комиссии принимаются простым большинством голосов от числа присутствующих на заседании членов комиссии.

5.8. При голосовании каждый член комиссии имеет один голос.

5.9. Решения, принимаемые на заседании комиссии, оформляются протоколом, который подписывает председатель комиссии, в его отсутствие - заместитель председателя, и секретарь.

5.10. По результатам заседаний комиссии оформляются протоколы, которые подписываются председателем и членами комиссии.

5.11. Члены комиссии, в случае несогласия с принятым на заседании комиссии решением, имеют право письменно изложить свое особое мнение, которое подлежит обязательному приобщению к протоколу заседания.

6. Полномочия комиссии

6.1. Комиссия имеет право:

6.1.1. Знакомиться с документами и материалами, необходимыми для выполнения возложенных задач и функций.

6.1.2. Выступать с инициативой по разработке проектов нормативных документов (далее НД), регламентирующих обработку и защиту ПДн (персональных данных – далее ПДн) в учреждении.

6.1.3. Давать работникам учреждения обязательные для выполнения указания по защите ПДн, определяемые действующим законодательством РФ и НД учреждения.

6.1.4. Принимать мотивированные решения о привлечении сторонних специализированных организаций к проведению работ по технической защите ПДн.

6.1.5. Организовывать и координировать работу всех структурных подразделений учреждения в вопросах обработки и защиты ПДн.

6.1.6. Запрашивать и получать от всех структурных подразделений учреждения сведения или справочные материалы, необходимые для осуществления своей деятельности.

6.1.7. Привлекать в установленном порядке работников учреждения, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе своей работы, и выработки обоснованных рекомендаций и заключений.

6.1.8. Привлекать лицо, ответственное за обеспечение работоспособности программного обеспечения и технического сопровождения ПДн к выполнению работ по установке, настройке, администрированию и удалению средств защиты информации, а также к администрированию системы защиты ПДн.

6.1.9. Проводить проверки соблюдения установленного порядка защиты ПДн во всех структурных подразделениях Учреждения и докладывать об их результатах директору.

6.1.10. Взаимодействовать в соответствии с законодательством РФ с федеральными органами исполнительной власти, органами местного самоуправления, организациями по вопросам информационной безопасности и защиты ПДн.

6.1.11. Вносить руководителям структурных подразделений учреждения предложения о приостановке действий, противоречащих законодательству РФ в области ПДн, по направлениям, отнесенным к компетенции комиссии в соответствии с разделом 3 настоящего Положения.

6.1.12. Принимать необходимые меры в случае обнаружения нарушения установленного порядка защиты ПДн, вплоть до приостановки обработки ПДн в структурных подразделениях или в учреждении в целом.

6.1.13. Требовать от работников учреждения письменных объяснений необходимых обстоятельств и фактов при проведении служебных расследований.

6.1.14. Подготавливать и представлять в установленном порядке директору предложения о порядке определения размера ущерба, который может быть причинен учреждению, его работникам либо субъектам ПДн вследствие нарушения безопасности ПДн.

6.1.15. Вносить предложения директору об отстранении от выполнения служебных (трудовых) обязанностей работников учреждения, систематически нарушающих требования по защите ПДн.

6.1.16. Являться инициатором применения мер дисциплинарного взыскания по отношению к работникам, нарушающим установленный порядок защиты ПДн.

6.2. Членам Комиссии запрещается:

6.2.1. Доводить до работников учреждения сведения о системе защиты персональных данных в полном объеме.

6.2.2. При выводе из состава комиссии раскрывать объем работ и конкретные направления деятельности Комиссии, разглашать информацию, ставшую известной в ходе работы в составе комиссии.

7. Ответственность

7.1. Председатель комиссии несет персональную ответственность за деятельность комиссии, качество и своевременность исполнения обязанностей, возложенных на него в соответствии с настоящим положением и перечнем обязанностей членов комиссии.

7.2. Председатель и ответственный за техническое сопровождение в учреждении (инженер-электроник) комиссии несут персональную ответственность за поддержание установленных уровней защищенности ПДн при их обработке в системе защиты персональных данных учреждения, а также заданного уровня информационной безопасности учреждения.

7.3. Члены комиссии несут персональную ответственность за качество и своевременность исполнения обязанностей, возложенных на них в соответствии с настоящим положением и перечнем обязанностей членов комиссии.

Приложение №2
к Приказу Отдела образования
Администрации Обливского
района от 03.04.2019 № 185

СОСТАВ КОМИССИИ

по обеспечению защиты персональных данных при их обработке в
информационных системах персональных данных в Отделе образования
Администрации Обливского района

| | | |
|------------------------------------|------------------------------------|--------------------------------------|
| Малахова Нина Анатольевна | Заведующий Отделом образования | Председатель комиссии |
| Лаптева Любовь Александровна | Главный бухгалтер | Заместитель председателя комиссии |
| Попова Эльвира Ивановна | Инспектор по кадрам | Секретарь комиссии |
| Члены комиссии: | | |
| Литовченко Андрей Николаевич | Инженер-электроник | Член комиссии |
| Колесникова Елена Анатольевна | Заместитель главного бухгалтера | Член комиссии |
| Марянина Елена Юрьевна | Бухгалтер | Член комиссии |
| Севастьянова Марина Григорьевна | Бухгалтер | Член комиссии |
| Некипилая Елена Васильевна | Экономист | Член комиссии |

Приложение №3
к Приказу Отдела образования
Администрации Обливского
района от 03.04.2019 № 185

ПЕРЕЧЕНЬ

Мероприятий по обеспечению защиты персональных данных при их обработке
в информационных системах персональных данных в Отделе образования
Администрации Обливского района на 2021-2023г.г.

| Наименование мероприятия | Периодичность | Пункт | Ответственный |
|--|---|----------------|---|
| Заседания комиссии | 1 раз в полгода (по мере необходимости) | п.5.4. | Председатель комиссии |
| Контроль и оценка эффективности принимаемых мер защиты персональных данных и применяемых средств защиты информации | Ежегодно | п.3.3., п.3.4. | Члены комиссии (по назначению) |
| Организация и проведение учебно-методических мероприятий с работниками учреждения по вопросам защиты персональных данных | Ежегодно | п.2.1., п.2.4. | Инженер-электроник Инспектор по кадрам |
| Формирование резервного копирования ресурсов информационной системы персональных данных | Ежегодно | п.2.2. | Члены комиссии (по назначению) |
| Проведение мероприятий по очистке и (или) уничтожению машинных (информационных) носителей персональных данных | Ежегодно | п.2.1. | Инженер-электроник |
| Анализ возможных угроз безопасности персональным данным | Ежеквартально | п.2.1. | Инженер-электроник |
| Контроль наличия материальных носителей | Ежеквартально | п.2.1. | Инспектор по кадрам |

| | | | |
|--|---------------|--------|-----------------------------------|
| персональных данных (в части кадровых вопросов) | | | |
| Контроль наличия материальных носителей персональных данных (в части финансовых вопросов) | Ежеквартально | п.2.1. | Инженер-электроник |
| Контроль соблюдения требований технических условий, правил эксплуатации и сертификатов на эксплуатируемые средства защиты информации | Ежегодно | п.2.1. | Инженер-электроник |
| Планирование и организация Практических мероприятий по предотвращению попыток несанкционированного вмешательства в процесс нормального функционирования информационной системы персональных данных и попыток несанкционированного доступа к обрабатываемым персональным данным | Ежегодно | п.2.4. | Инженер-электроник |
| Контроль полноты и своевременности выполнения мероприятий по защите персональных данных | Ежемесячно | п.2.3. | Члены комиссии (по назначению) |
| Контроль функционирования системы защиты персональных данных | Ежедневно | п.2.3. | Инженер-электроник |