Приложение 2
к приказу от «22» ноября 2021г. № 187

ПОЛОЖЕНИЕ
о комиссии по защите информации

1. Общие положения

Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии по защите информации (далее - Комиссия).

2. Основные задачи комиссии по защите информации

Основными задачами Комиссии являются:

сбор и анализ исходных данных по информационным системам персональных данных (далее - ИСПДн) Муниципального автономного учреждения «Спортивная школа» (далее - Учреждение);

определение значений параметров для установления уровня защищенности персональных данных (далее - ПДн) 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»;

определение уровня защищенности ПДн при их обработке в ИСПДн;

принятие решения об уничтожении ПДн;

проведение внутренних проверок соответствия обработки ПДн в Учреждении требованиям законодательства в сфере защиты ПДн.

3. Порядок формирования комиссии по защите информации

Комиссия формируется из числа штатных сотрудников в Учреждения, участвующих в процессе обработки ПДн.

В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.

Члены Комиссии назначаются приказом директора Учреждения.

В случае изменения состава Комиссии, в приказ вносятся соответствующие изменения.

4. Полномочия комиссии по защите информации

Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:

получать необходимые сведения у всех сотрудников Учреждения, участвующих в обработке ПДн;

просматривать электронные базы данных и бумажные носители, содержащие ПДн, с целью выявления состава обрабатываемых ПДн;

отслеживать технологический процесс обработки ПДн;

выявлять или получать готовые сведения о структуре локальной вычислительной сети Учреждения;

определять или получать готовые сведения о наличии и способах доступа к информационно-телекоммуникационной сети;

определять или получать готовые сведения о технических и программных средствах обработки ПДн;

определять или получать готовые сведения об условиях, местах и способах передачи ПДн в сторонние организации.

5. Отчетность комиссии по защите информации

Комиссия при выполнении своих задач должна составить протокол заседания комиссии.

В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности ПДн при их обработке в ИСПДн /Акт уничтожения ПДн/Акт проведения внутренней проверки соответствия обработки ПДн в Учреждении требованиям законодательства в сфере защиты ПДн.

Приложение 3
к приказу от «22» ноября 2021г. № 187

Перечень лиц в МАУ «СШ», доступ которых к персональным данным, обрабатываемым в ИСПДн «ИАСПСР», необходим для выполнения ими трудовых обязанностей

№ п/п	ФИО	Должность	Способ обработки ПДн
1.	Табурцова Татьяна Алексеевна	Заместитель директора	смешанный
2.	Исаева Зимфира Абильфезовна	Заместитель директора	смешанный
3.	Алексеева Вероника Васильевна	Инструктор-методист	смешанный
4.	Горбунова Наталья Константиновна	Инструктор-методист	смешанный

Приложение 4
к приказу от «22» ноября 2021г. № 187

Для тренера

СОГЛАСИЕ
на обработку персональных данных

г. _____ «__» _____ г.

Я, _____,
(фамилия, имя, отчество)

_____ серия ____ № _____ выдан _____
(вид документа, удостоверяющего личность)

_____
(когда и кем)

проживающий(ая) по адресу: _____
_____

настоящим даю свое согласие на обработку моих персональных данных МАУ «СШ», расположенному по адресу: г.Покачи ул. Молодёжная 16, и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Согласие дается мною для целей обработки персональных данных при осуществлении подготовки спортивного резерва посредством использования единой базы данных по спортсменам, проходящим спортивную подготовку в учреждениях физической культуры и спорта Ханты-Мансийского автономного округа – Югры (Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе – Югре, далее - ИАСПСР), и распространяется на следующую информацию, полученную лично от меня:

- ФИО;
- СНИЛС;
- дата и место рождения;
- пол;
- год начала тренерской деятельности;
- данные документа, удостоверяющего личность;
- адрес проживания;
- телефон;
- электронный адрес;
- фотография.
- Сведения об образовании:
  - уровень образования;
  - наименование учебного заведения;
  - дата начала обучения;
  - дата окончания обучения;

- номер диплома, специальность;
- квалификация;
- документ (файл);
- дата начала тренерской деятельности;
- дополнительные сведения;

– Сведения о квалификации:
  - квалификационная категория;
  - дата и номер приказа ее получения;
  - файла приказа;
– Сведения о тренерской работе:
  - виды спорта и дисциплины;
  - специфика направления;
  - организация;
  - должность;
  - период работы;
  - список тренируемых спортсменов;
– Сведения о личных достижениях;
– Спортивные звания:
  - спортивное звание;
  - номер удостоверения о его присвоении,
  - дата присвоения.

Даю согласие на предоставление доступа к моим персональным данным, обрабатываемым в ИАСПСР:

Департаменту физической культуры и спорта Ханты-Мансийского автономного округа - Югры;

Администрации муниципального образования;

Физкультурно-спортивным и образовательным организациям Ханты-Мансийского автономного округа - Югры, осуществляющим подготовку спортивного резерва;

с целью реализации полномочий, возложенных на них законодательством Российской Федерации и Ханты-Мансийского автономного округа - Югры.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), удаление, уничтожение персональных данных.

Настоящее согласие дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

_____

(Ф.И.О., подпись лица, давшего согласие)

Для спортсмена

СОГЛАСИЕ
на обработку персональных данных

г. _____ «__» _____ г.

Я, _____,
(фамилия, имя, отчество)

_____ серия ____ № _____ выдан _____
(вид документа, удостоверяющего личность)

_____
(когда и кем)

проживающий(ая) по адресу: _____
_____

настоящим даю свое согласие на обработку моих персональных данных МАУ «СШ», расположенному по адресу: г.Покачи ул Молодежная 16, и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Согласие дается мною для целей обработки персональных данных при осуществлении подготовки спортивного резерва посредством использования единой базы данных по спортсменам, проходящим спортивную подготовку в учреждениях физической культуры и спорта Ханты-Мансийского автономного округа – Югры (Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе – Югре, далее - ИАСПСР), и распространяется на следующую информацию, полученную лично от меня:

- ФИО;
- СНИЛС;
- дата и место рождения;
- пол;
- данные документа, удостоверяющего личность;
- адрес проживания;
- телефон;
- электронный адрес;
- фотография;
- Антропометрические сведения:
  - рост;
  - вес;
  - размер обуви;
  - размер одежды;
  - обхват головы;
  - ведущая нога;
  - ведущая рука;
- Сведения о спортивном обучении:

- регион;
- вид спорта;
- организация;
- период обучения;
- дополнительные сведения;

– Сведения о разрядах и званиях:
  - разряд;
  - номер и дата удостоверения;
  - звание;
  - номер и дата удостоверения;
– Порог анаэробного обмена (ПАНО);
– Максимальное потребление кислорода (МПК);
– Сведения о соревновательной и тренировочной деятельности;
– Медицинские данные;
– Сведения о тренировках и учёт нагрузок;
– Система питания;
– Прогноз перспектив и рекомендации по нагрузкам;
– Рейтинг спортсмена;
– Сведения, содержащиеся в журнале посещаемости.

Даю согласие на предоставление доступа к моим персональным данным, обрабатываемым в ИАСПСР:

Департаменту физической культуры и спорта Ханты-Мансийского автономного округа - Югры;

Администрации муниципального образования;

Физкультурно-спортивным и образовательным организациям Ханты-Мансийского автономного округа - Югры, осуществляющим подготовку спортивного резерва;

с целью реализации полномочий, возложенных на них законодательством Российской Федерации и Ханты-Мансийского автономного округа - Югры.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), удаление, уничтожение персональных данных.

Настоящее согласие дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

_____

(Ф.И.О., подпись лица, давшего согласие)

Для представителя спортсмена

СОГЛАСИЕ
на обработку персональных данных

г. _____ «__» _____ г.

Я, _____,
(фамилия, имя, отчество)

_____ серия ____ № _____ выдан _____
(вид документа, удостоверяющего личность)

_____
(когда и кем)

проживающий(ая) по адресу: _____
_____

являясь законным представителем
_____,
(фамилия, имя, отчество)

проживающего(ей) по адресу: _____
_____

Данные документа, подтверждающего полномочия законного представителя
_____
(серия и номер)

_____
(когда и кем выдан)

настоящим даю свое согласие на обработку моих персональных данных, включенных в данное согласие (исключительно в целях получения согласия) и приведенных ниже, а также персональных данных моего ребенка
МАУ «СШ», расположенному по адресу:г.Покачи ул.Молодежная 16, и подтверждаю, что, давая такое согласие, я действую по своей воле и в интересах ребенка, законным представителем которого я являюсь.

Согласие дается мною для целей обработки персональных данных при осуществлении подготовки спортивного резерва посредством использования единой базы данных по спортсменам, проходящим спортивную подготовку в учреждениях физической культуры и спорта Ханты-Мансийского автономного округа – Югры (Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе – Югре, далее - ИАСПСР), и распространяется на следующую информацию, полученную лично от меня:

Персональные данные законного представителя:

- ФИО;

- СНИЛС;
- степень родства;
- данные документа, удостоверяющего личность;
- адрес проживания;
- телефон;
- электронный адрес.

Персональные данные ребенка:
- ФИО;
- СНИЛС;
- дата и место рождения;
- пол;
- данные документа, удостоверяющего личность;
- адрес проживания;
- телефон;
- электронный адрес;
- фотография;
- Антропометрические сведения:
  - рост;
  - вес;
  - размер обуви;
  - размер одежды;
  - обхват головы;
  - ведущая нога;
  - ведущая рука;
- Сведения о спортивном обучении:
  - регион;
  - вид спорта;
  - организация;
  - период обучения;
  - дополнительные сведения;
- Сведения о разрядах и званиях:
  - разряд;
  - номер и дата удостоверения;
  - звание;
  - номер и дата удостоверения;
- Порог анаэробного обмена (ПАНО);
- Максимальное потребление кислорода (МПК);
- Сведения о соревновательной и тренировочной деятельности;
- Медицинские данные;
- Сведения о тренировках и учёт нагрузок;
- Система питания;
- Прогноз перспектив и рекомендации по нагрузкам;
- Рейтинг спортсмена;

– Сведения, содержащиеся в журнале посещаемости.

Даю согласие на предоставление доступа к моим персональным данным, и персональным данным моего ребенка, обрабатываемым в ИАСПСР:

Департаменту физической культуры и спорта Ханты-Мансийского автономного округа - Югры;

Администрации муниципального образования;

Физкультурно-спортивным и образовательным организациям Ханты-Мансийского автономного округа - Югры, осуществляющим подготовку спортивного резерва;

с целью реализации полномочий, возложенных на них законодательством Российской Федерации и Ханты-Мансийского автономного округа - Югры.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), удаление, уничтожение персональных данных.

Настоящее согласие дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

_____

(Ф.И.О., подпись лица, давшего согласие)

Для медицинского работника

СОГЛАСИЕ
на обработку персональных данных

г. _____ «__» _____ г.

Я, _____,
(фамилия, имя, отчество)

_____ серия ____ № _____ выдан _____
(вид документа, удостоверяющего личность)

_____
(когда и кем)

проживающий(ая) по адресу: _____
_____

настоящим даю свое согласие на обработку моих персональных данных МАУ «СШ», расположенному по адресу: г.Покачи ул.Молодежная 16, и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Согласие дается мною для целей обработки персональных данных при осуществлении подготовки спортивного резерва посредством использования единой базы данных по спортсменам, проходящим спортивную подготовку в учреждениях физической культуры и спорта Ханты-Мансийского автономного округа – Югры (Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе – Югре, далее - ИАСПСР), и распространяется на следующую информацию, полученную лично от меня:

- ФИО;
- СНИЛС;
- дата и место рождения;
- пол;
- год начала работы;
- данные документа, удостоверяющего личность;
- адрес проживания;
- телефон;
- электронный адрес;
- фотография.
- Сведения об образовании:
  - уровень образования;
  - наименование учебного заведения;
  - дата начала обучения;
  - дата окончания обучения;
  - номер диплома, специальность;
  - документ (файл);
  - ученая степень;

- Сведения о квалификации:
  - квалификационная категория;
  - дата и номер приказа ее получения;
  - файла приказа;
- Сведения о работе в области физической культуры и спорта:
  - организация;
  - должность;
  - вид трудоустройства;
  - специализация;
  - период работы;
- Звания:
  - звание;
  - номер удостоверения о его присвоении,
  - дата присвоения.

Даю согласие на предоставление доступа к моим персональным данным, обрабатываемым в ИАСПСР:

Департаменту физической культуры и спорта Ханты-Мансийского автономного округа - Югры;

Администрации муниципального образования;

Физкультурно-спортивным и образовательным организациям Ханты-Мансийского автономного округа - Югры, осуществляющим подготовку спортивного резерва;

с целью реализации полномочий, возложенных на них законодательством Российской Федерации и Ханты-Мансийского автономного округа - Югры.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), удаление, уничтожение персональных данных.

Настоящее согласие дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

_____

(Ф.И.О., подпись лица, давшего согласие)

Для административного работника

СОГЛАСИЕ
на обработку персональных данных

г. _____ «__» _____ г.

Я, _____,
(фамилия, имя, отчество)

_____ серия ____ № _____ выдан _____
(вид документа, удостоверяющего личность)

_____
(когда и кем)

проживающий(ая) по адресу: _____
_____

настоящим даю свое согласие на обработку моих персональных данных МАУ СШ», расположенному по адресу:г.Покачи ул.Молодежная 16, и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Согласие дается мною для целей обработки персональных данных при осуществлении подготовки спортивного резерва посредством использования единой базы данных по спортсменам, проходящим спортивную подготовку в учреждениях физической культуры и спорта Ханты-Мансийского автономного округа – Югры (Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе – Югре, далее - ИАСПСР), и распространяется на следующую информацию, полученную лично от меня:

- ФИО;
- СНИЛС;
- дата и место рождения;
- пол;
- год начала работы;
- данные документа, удостоверяющего личность;
- адрес проживания;
- телефон;
- электронный адрес;
- фотография.
- Сведения об образовании:
  - уровень образования;
  - наименование учебного заведения;
  - дата начала обучения;
  - дата окончания обучения;
  - номер диплома, специальность;
  - документ (файл);
  - ученая степень;

- Сведения о квалификации:
  - квалификационная категория;
  - дата и номер приказа ее получения;
  - файла приказа;
- Сведения о работе в области физической культуры и спорта:
  - организация;
  - должность;
  - вид трудоустройства;
  - специализация;
  - период работы;
- Звания:
  - звание;
  - номер удостоверения о его присвоении,
  - дата присвоения.

Даю согласие на предоставление доступа к моим персональным данным, обрабатываемым в ИАСПСР:

Департаменту физической культуры и спорта Ханты-Мансийского автономного округа - Югры;

Администрации муниципального образования;

Физкультурно-спортивным и образовательным организациям Ханты-Мансийского автономного округа - Югры, осуществляющим подготовку спортивного резерва;

с целью реализации полномочий, возложенных на них законодательством Российской Федерации и Ханты-Мансийского автономного округа - Югры.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), удаление, уничтожение персональных данных.

Настоящее согласие дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

_____

(Ф.И.О., подпись лица, давшего согласие)

Приложение 5
к приказу от «22» ноября 2021г. № 187

Обязательство
о неразглашении информации, содержащей персональные данные

Я, _____,
(фамилия, имя, отчество полностью)

являясь сотрудником _____, в должности _____,
_____
(указать должность и наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____	_____	_____
дата	подпись	расшифровка

Приложение 6
к приказу от «22» ноября 2021г. № 187

ЖУРНАЛ
учета машинных носителей персональных данных (стационарные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Дата и место установки (использования)	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета машинных носителей персональных данных (съемные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета хранилищ

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатации	Примечание

ЖУРНАЛ
учета обращений субъектов персональных данных по вопросам обработки персональных данных

№ п/п	Дата обращения	ФИО обратившегося	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации	Подпись ответственного	Примечание

ЖУРНАЛ
учета выявленных инцидентов информационной безопасности

№ п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание

ЖУРНАЛ
ознакомления сотрудников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных

№ п/п	Ф. И. О. инструктируемого	Структурное подразделение, должность инструктируемого	Вид инструктажа	Дата	Ф. И. О. инструктирующего	Структурное подразделение, должность инструктирующего	Подпись инструктирующего	Подпись инструктируемого

Приложение 7
к приказу от «22» ноября 2021г. № 187

АКТ
определения уровня защищенности ПДн при их обработке в ИСПДн
«МАУ СШ»

Председатель комиссии Кузьмин Александр Александрович
Члены комиссии Пацук Марина Викторовна
Табурцова Татьяна Алексеевна
Исаева Зимфира Абильфезовна
Алексеева Вероника Васильевна

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

категории персональных данных обрабатываемых в ИСПДн: в информационной системе персональных данных обрабатываются _____ (биометрические, специальные, общедоступные, иные) категории персональных данных;

категории субъектов: субъектов персональных данных (субъектов персональных данных, являющихся сотрудниками оператора или субъектов персональных данных, не являющихся сотрудниками оператора);

объем обрабатываемых персональных данных: менее чем 100000 (менее чем 100000, более чем 100000);

тип актуальных угроз: для информационной системы персональных данных актуальны угрозы третьего (первого, второго, третьего) типа.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и на основании анализа исходных данных, требуется обеспечить 4 уровень защищенности (УЗ 4) персональных данных.

Результат оценки вреда:

Для информационной системы персональных данных актуальны угрозы 4 УЗ типа.

Председатель комиссии Кузьмин Александр Александрович
Члены комиссии Пацук Марина Викторовна
Табурцова Татьяна Алексеевна
Исаева Зимфира Абильфезовна
Алексеева Вероника Васильевна

«__»_____20___ г.

Приложение 8
к приказу от «22» ноября 2021г. № 187

АКТ
об уничтожении персональных данных субъектов персональных данных

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные:

№ п/п	Сведения, содержащие персональные данные	Место хранения	Кол-во ед. хранения	Примечание

Указанные персональные данные уничтожены путем _____
_____
(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель комиссии: _____ _____
подпись расшифровка

Члены комиссии: _____ _____
подпись расшифровка

_____ _____
подпись расшифровка

_____ _____
подпись расшифровка

Приложение 9
к приказу от «22» ноября 2021г. № 187

Перечень обрабатываемых в ИСПДн «ИАСПСР» персональных данных

Субъект персональных данных	Состав персональных данных	Цели обработки персональных данных	Правовое основание обработки персональных данных
Тренер	– ФИО; – СНИЛС; – дата и место рождения; – пол; – год начала тренерской деятельности; – данные документа, удостоверяющего личность; – адрес проживания; – телефон; – электронный адрес; – фотография. – Сведения об образовании: - уровень образования; - наименование учебного заведения; - дата начала обучения; - дата окончания обучения; - номер диплома, специальность; - квалификация; - документ (файл); - дата начала тренерской деятельности; - дополнительные сведения; – Сведения о квалификации: - квалификационная категория; - дата и номер приказа ее получения; - файла приказа; – Сведения о тренерской работе: - виды спорта и дисциплины; - специфика направления; - организация; - должность; - период работы; - список тренируемых спортсменов; – Сведения о личных достижениях; – Спортивные звания: - спортивное звание; - номер удостоверения о его	Обработка персональных данных при осуществлении подготовки спортивного резерва посредством использования единой базы данных по спортсменам, проходящим спортивную подготовку в учреждениях физической культуры и спорта Ханты-Мансийского автономного округа – Югры (Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе – Югре)	Федеральный закон от 04.12.2007 № 329-ФЗ «О физической культуре и спорте в Российской Федерации»; Распоряжение Правительства Российской Федерации от 17.10.2018 № 2245-р «Об утверждении Концепции подготовки спортивного резерва в Российской Федерации до 2025 года»; Приказ Министерства спорта Российской Федерации от 30.10.2015 № 999 «Об утверждении требований к обеспечению подготовки спортивного резерва для спортивных сборных команд Российской Федерации»; Постановление Правительства Ханты-Мансийского автономного округа – Югры от

Субъект персональных данных	Состав персональных данных	Цели обработки персональных данных	Правовое основание обработки персональных данных
	присвоении, - дата присвоения.		31.05.2019 № 166-п «Об утверждении Положения о государственной информационной системе Ханты-Мансийского автономного округа – Югры «Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе – Югре». Согласие субъекта персональных данных.
Спортсмен	– ФИО; – СНИЛС; – дата и место рождения; – пол; – данные документа, удостоверяющего личность; – адрес проживания; – телефон; – электронный адрес; – фотография; – Антропометрические сведения: - рост; - вес; - размер обуви; - размер одежды; - обхват головы; - ведущая нога; - ведущая рука; – Сведения о спортивном обучении: - регион; - вид спорта; - организация; - период обучения; - дополнительные сведения; – Сведения о разрядах и званиях: - разряд; - номер и дата удостоверения; - звание; - номер и дата удостоверения; – Порог анаэробного обмена (ПАНО); – Максимальное потребление кислорода (МПК); – Сведения о соревновательной и тренировочной деятельности; – Медицинские данные; – Сведения о тренировках и учёт нагрузок; – Система питания; – Прогноз перспектив и рекомендации по нагрузкам; – Рейтинг спортсмена; – Сведения, содержащиеся в журнале посещаемости.		
Представитель спортсмена	– ФИО; – СНИЛС; – степень родства;		

Субъект персональных данных	Состав персональных данных	Цели обработки персональных данных	Правовое основание обработки персональных данных
	– данные документа, удостоверяющего личность; – адрес проживания; – телефон; – электронный адрес.		
Медицинский работник	– ФИО; – СНИЛС; – дата и место рождения; – пол; – год начала работы; – данные документа, удостоверяющего личность; – адрес проживания; – телефон; – электронный адрес; – фотография. – Сведения об образовании: - уровень образования; - наименование учебного заведения; - дата начала обучения; - дата окончания обучения; - номер диплома, специальность; - документ (файл); - ученая степень; – Сведения о квалификации: - квалификационная категория; - дата и номер приказа ее получения; - файла приказа; – Сведения о работе в области физической культуры и спорта: - организация; - должность; - вид трудоустройства; - специализация; - период работы; – Звания: - звание; - номер удостоверения о его присвоении, - дата присвоения.		
Административный работник	– ФИО; – СНИЛС; – дата и место рождения; – пол; – год начала работы; – данные документа, удостоверяющего личность; – адрес проживания; – телефон; – электронный адрес;		

Субъект персональных данных	Состав персональных данных	Цели обработки персональных данных	Правовое основание обработки персональных данных
	– фотография. – Сведения об образовании: - уровень образования; - наименование учебного заведения; - дата начала обучения; - дата окончания обучения; - номер диплома, специальность; - документ (файл); - ученая степень; – Сведения о квалификации: - квалификационная категория; - дата и номер приказа ее получения; - файла приказа; – Сведения о работе в области физической культуры и спорта: - организация; - должность; - вид трудоустройства; - специализация; - период работы; – Звания: - звание; - номер удостоверения о его присвоении, - дата присвоения.		

Приложение 10
к приказу от «22» ноября 2021г. № 187

Порядок доступа сотрудников МАУ «СШ» в помещения, в которых ведется обработка персональных данных
(далее – Порядок доступа в помещения)

1. Общие положения

Порядок доступа в помещения разработан в соответствии с Постановлением правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 18.02.2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Обеспечение безопасности помещений муниципального автономного учреждения «Спортивная школа» (далее - Учреждение), где расположены информационные системы персональных данных (далее – ИСПДн), ведется обработка персональных данных (далее – ПДн), а также где расположено коммутационное оборудование, направлено на исключение возможности несанкционированного доступа к техническим средствам, входящим в состав ИСПДн, их хищения и нарушения работоспособности, хищения носителей информации.

Защита от проникновения посторонних лиц в помещения Учреждения обеспечивается организацией порядка доступа, а также соответствующей инженерно-технической защитой помещений, а именно охранной сигнализацией и системой контроля и управления доступом.

2. Предъявляемые требования к помещениям и порядок доступа к ним

Помещения Учреждения, в которых размещены ИСПДн и ведется обработка ПДн (далее – помещения), должны соответствовать следующим требованиям:

обеспечивать сохранность технических средств;

исключать возможность бесконтрольного проникновения в помещения;

исключать возможность визуального просмотра обрабатываемой информации посторонними лицами;

двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;

конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол. Стекла в рамах должны быть надежно закреплены в пазах. Рамы указанных оконных проемов оборудуются запорными устройствами. На окнах первого этажа, а также верхних этажей – при возможности прямого просмотра помещения с улицы, должны быть установлены жалюзи.

Перечень должностей в Учреждении, доступ которых в Помещения необходим для выполнения ими трудовых обязанностей приведен в приложении 1 к настоящему приказу.

Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в приложении 1 к настоящему приказу, разрешено в период рабочего времени в соответствии с утвержденным графиком работы Учреждения либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки ПДн или ответственного за обеспечение безопасности ПДн в ИСПДн.

Лица, не указанные в приложении 1 к настоящему приказу, допускаются в помещения в присутствии лиц, имеющих право пребывания в данных помещениях.

В случае отсутствия сотрудников в помещении в рабочее время, помещение должно быть закрыто на ключ.

Вскрытие и закрытие помещений осуществляется сотрудниками данной ИСПДн.

Перед закрытием помещения по окончании рабочего времени лица, непосредственно обрабатывающие ПДн, обязаны:

убрать бумажные и электронные носители, содержащие ПДн, в металлические шкафы (сейфы);

отключить технические средства обработки информации и электроприборы.

Сотрудник, последний покидающий помещение, обязан:

закрыть окна;

выключить освещение;

закрыть дверь помещения.

Перед открытием помещения первый прибывший сотрудник обязан:

провести внешний осмотр двери и дверного замка с целью установления их целостности;

открыть дверь и осмотреть помещение;

проверить наличие и целостность замков на металлических шкафах (сейфах) с целью установления их целостности.

При обнаружении факта взлома двери (дверного замка) помещения сотрудник обязан:

не вскрывая помещение, незамедлительно сообщить непосредственному руководителю;

в присутствии не менее двух лиц и непосредственного руководителя вскрыть помещение и осмотреть его;

составить акт о факте взлома двери (дверного замка) и направить его директору Учреждения.

3. Перечень помещений, в которых осуществляется обработка персональных данных

Перечень помещений, в которых осуществляется обработка ПДн, приведен в приложении 1 к настоящему Порядку.

4. Организация и порядок производства

ремонтно-строительных работ

Рабочие и специалисты ремонтно-строительных организаций допускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством. Работы проводятся только в присутствии контролирующего лица из числа сотрудников.

Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих.

5. Организация охраны

Для охраны помещений Учреждения используется охранная сигнализация.

Для исключения несанкционированного доступа к информации, содержащей ПДн, при покидании помещения необходимо закрывать его на ключ.

6. Уборка помещений

Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Во время уборки в помещении должна быть приостановлена работа с ПДн, должны быть заблокированы все АРМ, на которых хранятся ПДн, носители, содержащие ПДн, должны быть убраны в сейф.

Приложение 1

Перечень помещений, в которых осуществляется обработка персональных данных

№ п/п	Помещение	Наименование должностей, доступ которых в Помещения необходим для выполнения ими должностных обязанностей
1.	Каб. № 28	Заместитель директора
2.	Каб. № 12	Инструктор-методист
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		

Приложение 11
к приказу от «22» ноября 2021г. № 187

ПОЛИТИКА
в отношении обработки персональных данных в ИСПДн «ИАСПСР»

1. Общие положения

Настоящая Политика в отношении обработки персональных данных в ИСПДн «ИАСПСР» (далее – Политика) определяет принципы, порядок и условия обработки персональных данных (далее - ПДн) субъектов ПДн, чьи ПДн обрабатываются в Муниципальном автономном учреждении «Спортивная школа» (далее - Учреждение), с целью обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность сотрудников Учреждения, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн.

Политика разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологий и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и другими нормативными правовыми актами, регулирующими отношения, связанные с обработкой персональных данных.

Политика определяет порядок и условия обработки ПДн в Учреждении с использованием средств автоматизации и без использования таких средств.

Политика вступает в силу с момента подписания директором Учреждения.

Политика подлежит пересмотру в ходе периодического анализа со стороны руководства Учреждения, а также в случаях изменения законодательства Российской Федерации в области обеспечения безопасности ПДн.

Основные понятия, используемые в настоящей Политике

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

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.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Цели и правовые основания обработки персональных данных

Обработка ПДн в ИСПДн «ИАСПСР» осуществляется Учреждением в следующих целях:

− Обработка персональных данных при осуществлении подготовки спортивного резерва посредством использования единой базы данных по спортсменам, проходящим спортивную подготовку в учреждениях физической культуры и спорта Ханты-Мансийского автономного округа – Югры (Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе – Югре).

Правовые основания обработки ПДн:

− Федеральный закон от 04.12.2007 № 329-ФЗ «О физической культуре и спорте в Российской Федерации»;

− Распоряжение Правительства Российской Федерации от 17.10.2018 № 2245-р «Об утверждении Концепции подготовки спортивного резерва в Российской Федерации до 2025 года»;

− Приказ Министерства спорта Российской Федерации от 30.10.2015 № 999 «Об утверждении требований к обеспечению подготовки спортивного резерва для спортивных сборных команд Российской Федерации»;

− Постановление Правительства Ханты-Мансийского автономного округа – Югры от 31.05.2019 № 166-п «Об утверждении Положения о государственной информационной системе Ханты-Мансийского автономного округа – Югры «Информационно-аналитическая система подготовки спортивного резерва в Ханты-Мансийском автономном округе – Югре».

− Согласие субъекта персональных данных;

− Политика в отношении обработки персональных данных в ИСПДн «ИАСПСР».

3. Категории субъектов, персональные данные которых обрабатываются

В соответствии с целями обработки ПДн, указанными в п. 2. настоящей Политики, Учреждением осуществляется обработка следующих категорий субъектов ПДн:

− Тренер;
− Спортсмен;
− Представитель спортсмена;
− Медицинский работник;
− Административный работник.

Перечень обрабатываемых ПДн утвержден приказом Учреждения.

4. Принципы обработки персональных данных

Обработка ПДн осуществляется на законной основе.

Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только те ПДн, которые отвечают целям их обработки.

Содержание и объем ПДн соответствуют заявленным целям обработки. Обрабатываемые ПДн не являются избыточным по отношению к заявленным целям их обработки.

При обработке ПДн обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Учреждение обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.

Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5. Условия обработки персональных данных

Обработка специальных категорий ПДн осуществляется Учреждением в соответствии с требованиями действующего законодательства Российской Федерации в области подготовки спортивного резерва. Субъекты ПДн дают согласие в письменной форме на обработку своих ПДн.

Обработки иных категорий ПДн осуществляется Учреждением с соблюдением следующих условий:

− обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Учреждение функций, полномочий и обязанностей;

− обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн.

Учреждение вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

Лицо, осуществляющее обработку ПДн по договору с Учреждением, соблюдает принципы и правила обработки ПДн, предусмотренные настоящей Политикой. В договоре с Учреждением определены перечень действий (операций) с ПДн, которые будут совершаться лицом,

осуществляющим обработку ПДн, и цели обработки, установлена обязанность такого лица соблюдать конфиденциальность ПДн и обеспечивать безопасность ПДн при их обработке, а также указаны требования к защите обрабатываемых ПДн.

В случае, если Учреждение поручает обработку ПДн другому лицу, ответственность перед субъектом ПДн за действия указанного лица несет Учреждение. Лицо, осуществляющее обработку ПДн по поручению Учреждения, несет ответственность перед Учреждением.

Условием прекращения обработки ПДн являться достижение целей обработки ПДн, истечение срока действия согласия или отзыв согласия субъекта ПДн на обработку его ПДн, а также выявление неправомерной обработки ПДн.

6. Конфиденциальность персональных данных

Сотрудники Учреждения, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

7. Согласие субъекта персональных данных на обработку его персональных данных

При необходимости обеспечения условий обработки ПДн субъекта может предоставляться согласие субъекта ПДн на обработку его ПДн.

Субъект ПДн принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Учреждением.

Согласие на обработку ПДн может быть отозвано субъектом ПДн.

Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн возлагается на Учреждение.

В случаях, предусмотренных федеральным законом, обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя, в частности:

фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);

наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта ПДн;

цель обработки ПДн;

перечень ПДн, на обработку которых дается согласие субъекта ПДн;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;

перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;

подпись субъекта ПДн.

В случае недееспособности субъекта ПДн согласие на обработку его ПДн дает законный представитель субъекта ПДн.

В случае смерти субъекта ПДн согласие на обработку его ПДн дают наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.

8. Право субъекта персональных данных на доступ к его персональным данным

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

подтверждение факта обработки ПДн Учреждением;

правовые основания и цели обработки ПДн;

цели и применяемые Учреждением способы обработки ПДн;

наименование и место нахождения Учреждения, сведения о лицах (за исключением сотрудников Учреждения), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Учреждением или на основании федерального закона;

обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

сроки обработки ПДн, в том числе сроки их хранения;

порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

информацию об осуществленной или о предполагаемой трансграничной ПДн;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

Субъект ПДн имеет право на получение запрашиваемой субъектом информации, за исключением следующих случаев:

обработка ПДн, включая ПДн, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Субъект ПДн имеет право на получение сведений, указанных в абзаце 1 п. 9. настоящей Политики, за исключением случаев, при которых доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц. Субъект ПДн вправе требовать от Учреждения уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Сведения, указанные в абзаце 1 п. 9. настоящей Политики, должны быть предоставлены субъекту ПДн Учреждением в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

Сведения, указанные в абзаце 1 п. 9. настоящей Политики, предоставляются субъекту ПДн или его представителю Учреждением при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать номер основного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Учреждением (номер контракта (договора), дата заключения контракта (договора), условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Учреждением, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

В случае, если сведения, указанные в абзаце 1 п. 9. настоящей Политики, а также обрабатываемы ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к Учреждению или направить ему повторный запрос в целях получения сведений, указанных в абзаце 1 п. 9. настоящей Политики, и ознакомления с такими ПДн не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

Субъект ПДн вправе обратиться повторно к Учреждению или направить ему запрос в целях получения сведений, указанных в абзаце 1 п. 9. настоящей Политики, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в абзаце 6 п. 9. настоящей Политики, в случае, если такие сведения и (или) обрабатываемы ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимой для запроса информацией должен содержать основание направления повторного запроса.

Учреждение вправе отказать субъекту ПДн в выполнении повторного запроса, несоответствующего условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса возлагается на Учреждение.

10. Обязанности Учреждения

При сборе ПДн Учреждение обязано предоставить субъекту ПДн по его просьбе информацию, предусмотренную ч. 7 ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - 152-ФЗ).

Если предоставление ПДн является обязательным в соответствии с федеральным законом, Учреждение обязано разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн.

Если ПДн получены не от субъекта ПДн, Учреждение, за исключением случаев, предусмотренных ч. 4 ст. 18 152-ФЗ, до начала обработки таких ПДн обязан предоставить субъекту ПДн следующую информацию:

наименование либо фамилия, имя, отчество и адрес Учреждения или его представителя;

цель обработки ПДн и ее правовое основание;

предполагаемые пользователи ПДн;

установленные 152-ФЗ права субъекта ПДн;

источник получения ПДн.

Учреждение освобождается от обязанности предоставить субъекту ПДн сведения, предусмотренные ч. 3 ст. 18 152-ФЗ, в случаях, если:

субъект ПДн уведомлен об осуществлении обработки его ПДн Учреждение;

ПДн получены Учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;

Учреждение осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;

предоставление субъекту ПДн сведений, предусмотренных ч. 3 ст. 18 152-ФЗ, нарушает права и законные интересы третьих лиц.

При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети «Интернет», Учреждение обязано обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 152-ФЗ.

Учреждение обязано сообщить в порядке, предусмотренном ст. 14 152-ФЗ, субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение тридцати дней с даты получения запроса субъекта ПДн или его представителя.

В случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя Учреждение обязано дать в письменной форме

мотивированный ответ, содержащий ссылку на положение ч. 8 ст. 14 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

Учреждение обязано предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие ПДн. Оператор обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

Учреждение обязано сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов ПДн Учреждение обязано осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн Учреждение обязано осуществить блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

В случае подтверждения факта неточности ПДн Учреждение на основании сведений, представленных субъектом ПДн или его представителем либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов обязано уточнить ПДн либо обеспечить их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

В случае выявления неправомерной обработки ПДн, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки ПДн лицом, действующим по поручению Учреждения. В случае, если обеспечить правомерность обработки ПДн невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязано уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Учреждение обязано уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

В случае достижения цели обработки ПДн Учреждение обязано прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Учреждением и субъектом ПДн либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных 152-ФЗ или другими федеральными законами.

В случае отзыва субъектом ПДн согласия на обработку его ПДн орган власти обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению органа власти) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Учреждением и субъектом ПДн либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных 152-ФЗ или другими федеральными законами.

В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в ч. 3 - 5 ст. 21 152-ФЗ, Учреждение осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Учреждения) и

обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

11. Право на обжалование действий или бездействий Учреждения

Если субъект ПДн считает, что Учреждение осуществляет обработку его ПДн с нарушением требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействия Учреждения в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) или в судебном порядке.

Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

12. Меры направленные на обеспечение выполнения Учреждением обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»

Назначен ответственный за организацию обработки ПДн.

Изданы документы, определяющие политику Учреждения в отношении обработки ПДн, локальные акты по вопросам обработки ПДн, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

Применяются правовые, организационные и технические меры по обеспечению безопасности ПДн.

Утверждены правила проведения внутреннего контроля соответствия обработки ПДн требованиям Федерального закона от 27.07.2006№ 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, настоящей Политике, локальным актам.

Проведено ознакомление сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе, документами, определяющими политику Учреждения в отношении обработки ПДн, локальными актами по вопросам обработки ПДн.

13. Меры по обеспечению безопасности персональных данных при их обработке

Определены угрозы безопасности ПДн при их обработке в ИСПДн.

Применяются организационные и технические меры по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимые для выполнения требований к защите ПДн.

Применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.

Ведется учет машинных носителей ПДн.

Выполняются меры по обнаружению фактов несанкционированного доступа к ПДн и принятию соответствующих мер.

Определен комплекс мер по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Установлены правила доступа к ПДн, обрабатываемым в ИСПДн, обеспечена регистрация и учет всех действий, совершаемых с ПДн в ИСПДн.

При передаче (подготовке к передаче) ПДн по каналам связи, имеющим выход за пределы контролируемой зоны, защита от раскрытия, модификации или навязывания (ввода ложной информации) осуществляется путем применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации.

Для исключения несанкционированного просмотра ПДн на устройствах вывода (отображения, печати) информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны, их не размещают напротив оконных проемов, входных дверей, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

Осуществляется выявление, анализ и устранение уязвимостей ИСПДн на этапах создания и эксплуатации ИСПДн. Такие проверки проводятся с периодичностью один раз в месяц, с учетом того, что должны быть проведены обязательные проверки для критических уязвимостей в случае опубликования в общедоступных источниках персональных данных о новых уязвимостях в средствах ЗИ, ТС и ПО, применяемом в ИСПДн. При выявлении уязвимости составляется отчет и разрабатывается план по их устранению.

Осуществляется непрерывный контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ПДн.

Приложение 12
к приказу от «22» ноября 2021г. № 187

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

1. Общие положения

Ответственный за организацию обработки персональных данных в _____ (далее - Учреждение) назначается приказом директора Учреждения и отвечает за организацию обеспечения своевременного и квалифицированного выполнения сотрудниками Учреждения требований по организации обработки и обеспечения безопасности персональных данных (далее – ПДн).

Ответственный за организацию обработки персональных данных (далее – Ответственный) в своей деятельности руководствуется:

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;

приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

иными нормативными правовыми актами, регламентирующими вопросы обработки и защиты персональных данных;

политикой в отношении обработки персональных данных;

настоящей Инструкцией.

2. Основные функции и обязанности ответственного за организацию обработки персональных данных

Функции Ответственного:

доведение до сведения допущенных к обработке ПДн сотрудников положений законодательства о ПДн, локальных актов по вопросам обработки и защиты ПДн;

общий контроль за соблюдением сотрудниками законодательства о ПДн и мер по защите ПДн;

осуществление контроля за выполнением разовых и периодических мероприятий по обеспечению безопасности ПДн;

взаимодействие с субъектами ПДн по вопросам обработки и защиты ПДн;

взаимодействие с органами, контролирующими обработку и защиту ПДн, при проведении проверок;

поддержание локальных организационно-распорядительных документов по организации обработки и обеспечению безопасности ПДн в актуальном состоянии.

Ответственный обязан:

знать:

- перечень обрабатываемых в Учреждении ПДн;
- перечень ИСПДн;
- перечень должностей в Учреждении, доступ которых к ПДн либо осуществление доступа к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими трудовых обязанностей;
- условия и технологический процесс обработки ПДн в Учреждении;
- законодательство Российской Федерации о ПДн.

представлять по требованию директора Учреждения отчет о состоянии защиты ИСПДн и о нештатных ситуациях на объектах ИСПДн и допущенных сотрудниками нарушениях установленных требований по защите ПДн;

следить за изменениями законодательства Российской Федерации о ПДн, своевременно и точно отражать изменения в локальных организационных актах по управлению средствами защиты информации в ИСПДн и правилам обработки ПДн;

осуществлять внутренний контроль за соблюдением Учреждением и его сотрудниками законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн, а также локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и ПДн, машинными носителями ПДн;

доводить до сведения сотрудников Учреждения положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обеспечения и защиты обработки ПДн, требований к защите ПДн путем проведения занятий и инструктажа сотрудников с периодичностью один раз в год;

организовать прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов;

по запросу субъекта ПДн сообщать ему сведения об обработке его ПДн, в том числе ознакомить с Политикой обработки ПДн в Учреждении;

по запросу субъекта ПДн организовать уточнение, блокирование или уничтожение ПДн указанного субъекта;

вести журнал учета обращений субъектов ПДн по вопросам обработки ПДн;

осуществлять контроль и учет передачи ПДн по запросам третьих лиц/организаций;

осуществлять контроль за сбором с сотрудников, допущенных к обработке ПДн, письменного обязательства о соблюдении режима конфиденциальности ПДн и соблюдении правил их обработки (обязательство о неразглашении персональных данных);

участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения должностных обязанностей;

осуществлять контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн;

осуществлять сопровождение и решение вопросов проверочной комиссии надзорных органов в сфере обработки ПДн при проведении проверочных мероприятий;

принимать меры по реагированию в случае возникновения нештатных и аварийных ситуаций с целью ликвидации их последствий;

вносить свои предложения по совершенствованию мер защиты ПДн в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности ПДн вследствие неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с документами, содержащими ПДн, или по другим нарушениям, которые могут привести к снижению уровня защищенности ПДн.

3. Права ответственного за организацию обработки персональных данных

Ответственный имеет право:

иметь доступ к информации, касающейся обработки ПДн в Учреждении и включающей:

- цели обработки ПДн;
- категории обрабатываемых ПДн;
- категории субъектов, ПДн которых обрабатываются;
- правовые основания обработки ПДн;
- перечень действий с ПДн, общее описание используемых в Учреждении способов обработки ПДн;
- дату начала обработки ПДн;
- срок или условия прекращения обработки ПДн;
- сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки;
- сведения об обеспечении безопасности ПДн в соответствии с

требованиями к защите ПДн, установленными Правительством Российской Федерации.

требовать от сотрудников выполнения федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, а также локальных нормативно-правовых актов в части работы с ПДн;

требовать от сотрудников Учреждения письменных объяснений при нарушении требований по обработке и обеспечении безопасности ПДн;

не допускать сотрудников до обработки ПДн до подписания ими письменного обязательства о неразглашении информации, содержащей ПДн;

указывать сотрудникам, допущенным к обработке ПДн, на необходимость выполнения установленных мер по обеспечению безопасности ПДн;

указывать сотрудникам, участвующим в обработке ПДн, на необходимость осуществления уточнения, блокирования или уничтожения ПДн по запросу субъекта;

право доступа ко всем локальным нормативным актам в области обработки и защиты ПДн;

блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн;

запрашивать и получать от всех сотрудников сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного.

проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей ПДн, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищенности ПДн;

привлекать к реализации мер, направленных на выполнение требований законодательства о ПДн, иных сотрудников Учреждения с возложением на них соответствующих обязанностей и закреплением ответственности;

проходить обучение по защите ПДн в учебных центрах и центрах повышения квалификации;

выносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обеспечением безопасности ПДн.

4. Ответственность

Ответственный за организацию обработки ПДн несет ответственность за:

соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обработке и обеспечению безопасности ПДн;

осведомленность сотрудников, участвующих в обработке ПДн, в вопросах обеспечения безопасности ПДн;

комплектность и содержание локальных нормативных актов в области защиты ПДн;

выполнение обязанностей перед субъектами ПДн и уполномоченным органом по защите прав субъектов ПДн.

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, Ответственный несет персональную ответственность в соответствии с законодательством Российской Федерации.

Приложение 13
к приказу от «22» ноября 2021г. № 187

ИНСТРУКЦИЯ
ответственного за обеспечение
безопасности персональных данных в информационных системах
персональных данных

1. Общие положения

Настоящая инструкция определяет основные обязанности, права и ответственность ответственного за обеспечение безопасности персональных данных в ИСПДн «ИАСПСР» (далее – администратор информационной безопасности ИСПДн).

Администратор информационной безопасности ИСПДн назначается приказом директора _____ (далее - Учреждение) и отвечает за обеспечение безопасности заданных характеристик информации (конфиденциальность, целостность и доступность), содержащей персональные данные (далее – ПДн), в процессе их обработки в ИСПДн «ИАСПСР».

В своей деятельности администратор информационной безопасности ИСПДн руководствуется:

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

иными нормативными правовыми актами, регламентирующими вопросы обработки и защиты персональных данных;

политикой в отношении обработки персональных данных;

настоящей Инструкцией.

Администратор информационной безопасности ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности ПДн при их обработке в ИСПДн.

2. Основные функции и обязанности администратора информационной безопасности ИСПДн

Основными функциями администратора информационной безопасности ИСПДн являются:

обеспечение заданных характеристик информации, содержащей ПДн, (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн;

обеспечение выполнения и контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности ПДн при их обработке в ИСПДн;

администрирование системы защиты информации в составе следующих подсистем:

- идентификации и аутентификации субъектов доступа и объектов доступа (ИАФ);
- управления доступом пользователей ИСПДн к объектам доступа ИСПДн (УПД);
- защиты машинных носителей персональных данных (ЗНИ);
- регистрации событий безопасности (РСБ);
- антивирусной защиты (АВЗ);
- контроля (анализа) защищенности персональных данных (АНЗ);
- защиты информационных систем персональных данных, ее средств и систем связи и передачи данных (ЗИС);
- выявления инцидентов и реагирования на них (ИНЦ);
- управления конфигурацией информационной системы и системы защиты персональных данных (УКФ).

Администратор информационной безопасности ИСПДн обязан:

знать перечень обрабатываемых ПДн, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку ПДн;

знать эксплуатационную документацию на применяемые средства защиты информации (далее – СрЗИ), устанавливать и эксплуатировать СрЗИ в соответствии с документацией и поддерживать настройку СрЗИ, соответствующие требованиям нормативных документов по безопасности информации. При этом система должна реализовывать в совокупности на каждом автоматизированном рабочем месте ИСПДн функции, необходимые для выполнения требований по защите от несанкционированного доступа (далее – НСД);

исполнять и требовать исполнения от пользователей ИСПДн установленного комплекса мероприятий по обеспечению безопасности ПДн и соблюдения действующего законодательства в области информационной безопасности, в том числе иных организационно-распорядительных документов в части обеспечения безопасности ПДн;

проводить инструктаж пользователей ИСПДн по правилам обработки ПДн, правилам работы с используемыми техническими средствами и СрЗИ в соответствии с технической документацией на используемые СрЗИ;

фиксировать и пресекать невыполнение пользователями ИСПДн требований и норм нормативно-методических документов в области безопасности ПДн и организационно-распорядительных документов Учреждения, а также создания пользователями возможностей утечки ПДн. В случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации требовать прекращения обработки ПДн;

проверять соответствие прав доступа пользователей к объектам доступа ИСПДн в соответствии с задачами, решаемыми пользователями в ИСПДн и взаимодействующими с ней ИСПДн, Разрешительной системой доступа к ИСПДн;

администратор информационной безопасности ИСПДн оказывает методическую помощь и контролирует выполнение руководителем структурного подразделения, в котором эксплуатируется ИСПДн «ИАСПСР» следующих действий:

- при смене пользователя руководитель структурного подразделения инициирует внесение изменений в список сотрудников, допущенных к работе на данной ИСПДн, и в разрешительную систему доступа;

- при исключении пользователя ИСПДн из «Перечня лиц в Учреждении, доступ которых к ПДн, обрабатываемым в ИСПДн «ИАСПСР», необходим для выполнения ими трудовых обязанностей» руководителем структурного подразделения принимаются меры по исключению возможности нарушения данным пользователем характеристик безопасности ПДн ИСПДн.

Администратору информационной безопасности ИСПДн необходимо до момента доведения до сотрудника информации о прекращении его работы в ИСПДн лишить сотрудника возможности доступа к защищаемой информации.

поддерживать в актуальном состоянии Разрешительную систему доступа и Технический паспорт на ИСПДн;

участвовать при проведении внутреннего контроля соответствия обработки ПДн установленным требованиям;

обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания технических средств ИСПДн и отправке их в ремонт, в том числе разрешать проведение работ по обслуживанию технических средств ИСПДн и отправке их в ремонт в присутствии или в сопровождении администратора информационной безопасности ИСПДн;

проводить ежегодный анализ изменения угроз безопасности информации в ИСПДн, возникающих в ходе ее эксплуатации, и принимать меры защиты информации в случае возникновения новых угроз безопасности ПДн;

осуществлять учет средств защиты информации в «Журнале учета средств защиты информации»;

присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;

для безопасной работы в сети Интернет пользователями ИСПДн:

- отключить отслеживание местоположения;
- отключить поддержку JavaScript;
- включить блокировку всплывающих окон;
- включить защиту от фишинга;
- включить запрос на разрешение запуска плагинов.

осуществлять администрирование подсистемы идентификации и аутентификации субъектов доступа и объектов доступа:

- создание, присвоение и уничтожение идентификаторов внутренних пользователей и устройств;
- исключение повторного использования идентификатора пользователя в течение одного года;
- блокирование идентификатора пользователя через период времени неиспользования более 90 дней;
- хранение, выдача, инициализация, блокирование средств аутентификации (паролей) и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- при администрировании подсистемы идентификации и аутентификации субъектов доступа и объектов доступа руководствоваться Инструкцией по идентификации и аутентификации пользователей информационных систем персональных данных.

осуществлять администрирование подсистемы управления доступом субъектов доступа к объектам доступа:

- определять типы учетных записей (внутреннего пользователя, системная, приложения; иные типы записей);
- проверять должностные (функциональные) обязанности пользователя при заведении учетной записи, на соответствие заявке;
- осуществлять заведение, активирование, объединение учетных записей в группы (при необходимости), блокирование и уничтожение учетных записей пользователей;
- осуществлять периодический (один раз в месяц) пересмотр и, при необходимости, корректировку учетных записей пользователей (проверять отсутствие в ИСПДн учетных записей уволенных (отстраненных) сотрудников, своевременность удаления временных учетных записей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИСПДн);
- проверять соответствие прав доступа пользователей к объектам доступа ИСПДн в соответствии с задачами, решаемыми пользователями в ИСПДн и взаимодействующими с ней ИСПДн и Разрешительной системой доступа к ИСПДн;
- устанавливать права доступа пользователей к информационным и техническим ресурсам ИСПДн в соответствии с принятой и утвержденной Разрешительной системой доступа;

- назначать права и привилегии пользователям, администраторам и лицам, обеспечивающим функционирование ИСПДн, минимально необходимых для выполнения ими своих трудовых обязанностей (функций), и осуществление контроля доступа к объектам доступа в соответствии с минимально необходимыми правами;

- осуществлять контроль в части неизменности настроек СрЗИ, которые должны выполнять:

- препятствие передаче ПДн через сеть Интернет и (или) другие информационно-телекоммуникационные сети международного информационного обмена по незащищенным каналам связи;
- ограничение доступа к ИСПДн на 15 минут при 5 неудачных попытках входа в ИСПДн;
- запрет доступа к ИСПДн до прохождения процедур аутентификации и идентификации;
- обеспечение запрета удаленного доступа к ИСПДн.

осуществлять администрирование подсистемы защиты машинных носителей ПДн:

- осуществлять учет машинных носителей ПДн, используемых в ИСПДн для хранения и обработки информации в журнале;

- осуществлять выдачу и (или) прием машинных носителей ПДн должностным лицам, физический доступ которых к машинным носителям ПДн необходим для выполнения ими трудовых обязанностей с внесением соответствующей отметки в журнал;

- осуществлять контроль в части уничтожения (стирания) ПДн с машинных носителей ПДн при их передаче в сторонние организации для ремонта или утилизации.

осуществлять администрирование подсистемы регистрации событий:

- путем просмотра журналов операционной системы и средств защиты информации осуществлять еженедельный контроль регистрации событий безопасности, которые приведены в Инструкции по регистрации событий безопасности;

- осуществлять настройку СрЗИ (состав событий безопасности и срок их хранения), руководствуясь Инструкцией по регистрации событий безопасности;

- в случае выявления признаков инцидентов информационной безопасности в ИСПДн осуществить планирование и проведение мероприятий по реагированию на выявленные инциденты, согласно Инструкции по работе с инцидентами информационной безопасности.

осуществлять администрирование подсистемы антивирусной защиты:

- осуществлять еженедельные полные проверки АРМ на наличие вредоносных компьютерных программ (вирусов) средством антивирусной защиты, руководствуясь эксплуатационной документацией на данное СрЗИ;

- осуществлять настройку средства антивирусной защиты на ежедневную автоматическую проверку на наличие вредоносных

компьютерных программ (вирусов) в вечернее время и производить проверку результатов сканирования;

- в случае обнаружения не поддающегося лечению вируса, принять меры по удалению инфицированного файла и, в случае необходимости, провести мероприятия по восстановлению работоспособности ПО;

- осуществлять еженедельный контроль над процессом обновления антивирусных баз;

- при администрировании подсистемы антивирусной защиты руководствоваться Инструкцией по организации антивирусной защиты в информационных системах персональных данных.

осуществлять администрирование подсистемы контроля (анализа) защищенности персональных данных:

- с помощью средства анализа (контроля) защищенности (сканера безопасности) осуществлять периодический (один раз в три месяца или при опубликовании в общедоступных источниках информации о новых уязвимостях в СрЗИ, технических средствах и ПО, применяемом в ИСПДн) поиск уязвимостей в ИСПДн;

- осуществлять анализ отчета с описанием выявленных уязвимостей, разрабатывать план мероприятий по их устранению;

- осуществлять устранение выявленных уязвимостей с помощью установки обновления ПО СрЗИ, общесистемного ПО, прикладного ПО или настройки СрЗИ, изменения режима и порядка использования ИСПДн;

- осуществлять информирование ответственного за организацию обработки ПДн о выявленных уязвимостях и результатах их устранения;

- контролировать работоспособность параметров настройки и правильность функционирования ПО и СрЗИ с периодичностью один раз в квартал, путем осуществления:

- контроля работоспособности (неотключения) ПО и СрЗИ;
- проверки правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) ПО и СрЗИ;
- контроля соответствия настроек ПО и СрЗИ параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и СрЗИ;
- восстановления работоспособности (правильности функционирования) и параметров настройки ПО и СрЗИ (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

- хранить документацию и дистрибутивы СрЗИ в соответствии с техническими условиями (компакт-диск с ПО системы должен упаковываться согласно требованиям, предусмотренным для оптических носителей), производить, при необходимости, восстановление программной среды СрЗИ или настройки защитных механизмов операционной системы и привилегий пользователей по доступу к ресурсам ИСПДн;

- производить инвентаризацию технических средств, ПО и СрЗИ, применяемых в ИСПДн, не реже одного раза в шесть месяцев:

- осуществлять контроль соответствия состава технических средств, приведенного в техническом паспорте на ИСПДн, с целью поддержания актуальной конфигурации ИСПДн и принятие мер, направленных на устранение выявленных недостатков;

- осуществлять исключение (восстановление) из состава ИСПДн несанкционированно установленных (удаленных) технических средств;

- осуществлять контроль установленного (инсталлированного) в ИСПДн ПО на предмет его соответствия перечню ПО, определенному в Техническом паспорте на ИСПДн;

- осуществлять исключение (восстановление) из состава ИСПДн несанкционированно установленного (удаленного) ПО;

- осуществлять контроль соответствия состава СрЗИ, приведенных в техническом паспорте на ИСПДн, с целью поддержания актуальной конфигурации ИСПДн и принятие мер, направленных на устранение выявленных недостатков;

- осуществлять исключение (восстановление) из состава ИСПДн несанкционированно установленных (удаленных) СрЗИ.

- осуществлять учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения) в Техническом паспорте на ИСПДн;

- осуществлять контроль выполнения условий и сроков действия лицензий и сертификатов соответствия на СрЗИ и принятие мер, направленных на устранение выявленных недостатков;

- при установке обновлений ПО, включая ПО СрЗИ и ПО базовой системы ввода-вывода руководствоваться эксплуатационной документацией. После установки обновлений убедиться в работоспособности и правильности функционирования технических средств и СрЗИ, добавить отметки в формуляр;

- осуществлять еженедельный контроль за установкой обновлений ПО, включая ПО СрЗИ и ПО базовой системы ввода-вывода.

осуществлять администрирование подсистемы защиты ИСПДн, ее средств и систем связи и передачи данных:

- проводить ежегодный инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и СКЗИ в соответствии с технической документацией на используемые СКЗИ;

- осуществлять администрирование СКЗИ в соответствии с эксплуатационной документацией на данные средства;

- осуществлять периодический контроль (не реже 1 раза в месяц) сохранности и работоспособности установленных СКЗИ, а также всего используемого совместно с СКЗИ ПО для предотвращения внесения программно-аппаратных закладок и вирусов;

- осуществлять контроль в части отсутствия доступа к ИСПДн со стороны пользователей ИСПДн сторонних организаций;

- осуществлять контроль в части обеспечения запрета удаленного доступа к ИСПДн.

осуществлять администрирование подсистемы выявления инцидентов и реагирования на них:

- в случае получения от пользователей ИСПДн информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также о нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа (далее – НСД) к ИСПДн, незамедлительно проинформировать ответственного за организацию обработки ПДн (при нарушениях со стороны ответственного за организацию обработки ПДн докладывать необходимо непосредственно вышестоящему руководству) в Учреждении для принятия необходимых мер по устранению нарушений в порядке, установленном в Инструкции по работе с инцидентами информационной безопасности;

- при осуществлении администрирования подсистемы выявления инцидентов и реагирования на них руководствоваться Инструкцией по работе с инцидентами информационной безопасности.

осуществлять администрирование подсистемы управления конфигурацией информационной системы и системы защиты персональных данных:

- поддерживать базовую конфигурацию системы защиты информации в соответствии с эксплуатационной документацией на систему защиту информации, определять типы возможных изменений конфигурации системы защиты информации, анализировать потенциальное воздействие планируемых изменений на обеспечение защиты информации, на возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн;

- вносить изменения (при необходимости) в Технический паспорт на ИСПДн и Разрешительную систему доступа пользователей к сведениям конфиденциального характера в ИСПДн;

- принимать решения по результатам изменений о повторной аттестации ИСПДн или проведении дополнительных аттестационных испытаний;

- документировать информацию (данные) об изменениях в конфигурации ИСПДн и системы защиты ПДн в «Журнале учета выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн».

Администратору информационной безопасности ИСПДн запрещается раскрывать информацию об организации системы защиты ПДн в Учреждении и любую информацию, которая может создать предпосылки для возникновения канала утечки информации или создания угрозы безопасности информации.

3. Основные права администратора информационной безопасности ИСПДн

Администратор информационной безопасности ИСПДн имеет право:

знакомиться с нормативными актами Учреждения, регламентирующими процессы обработки ПДн;

вносить предложения своему непосредственному начальнику и (или) директору Учреждения по совершенствованию существующей системы защиты информации;

привлекать по согласованию с ответственным за организацию обработки ПДн и директором Учреждения к работе по созданию и совершенствованию системы защиты информации организации, имеющие лицензию ФСТЭК России на право осуществления деятельности по технической защите конфиденциальной информации и лицензию ФСБ России на право осуществления деятельности по предоставлению услуг в области шифрования информации, разработке, производству шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем, распространению шифровальных (криптографических) средств, техническому обслуживанию шифровальных (криптографических) средств. осуществления деятельности по разработке, производству, распространению шифровальных (криптографических) средств;

требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации, выполнения нормативно-методических документов в области безопасности информации и организационно-распорядительных документов в Учреждении;

инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн;

требовать прекращения работы в ИСПДн, как в целом, так и отдельных пользователей ИСПДн, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ИСПДн;

обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к ответственному за организацию обработки ПДн и/или ответственному за контроль выполнения требований по обработке ПДн в ИСПДн;

принимать участие в планировании мероприятий по защите информации в ИСПДн и планировании оснащения средствами защиты информации структурные подразделения.

4. Ответственность администратора информационной безопасности ИСПДн

На администратора информационной безопасности ИСПДн возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн.

Администратор информационной безопасности ИСПДн несет ответственность за разглашение ПДн, ставших известными ему по роду

деятельности, в соответствии с действующим законодательством Российской Федерации.

Приложение 14
к приказу от «22» ноября 2021г. № 187

ИНСТРУКЦИЯ
по идентификации и аутентификации пользователей

1. Общие положения

Настоящая инструкция определяет в _____ (далее - Учреждение) порядок действий ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – администратора информационной безопасности ИСПДн) и пользователей информационных систем персональных данных (далее – ИСПДн) при прохождении идентификации и аутентификации пользователями в ИСПДн «ИАСПСР».

Настоящая Инструкция разработана на основе следующих нормативных документов:

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Пользователи ИСПДн должны быть предупреждены об ответственности за действия с персональными идентификаторами и паролями доступа, нарушающие требования настоящей Инструкции.

Пользователи ИСПДн должны быть ознакомлены с настоящей Инструкцией до начала работы с ИСПДн под роспись. Обязанность ознакомления пользователей с настоящей инструкцией возлагается на ответственного за организацию обработки персональных данных (далее - ПДн).

Ответственным за создание, присвоение и уничтожение идентификаторов пользователей и устройств, хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации является администратор информационной безопасности ИСПДн.

2. Порядок идентификации и аутентификации внутренних пользователей

К внутренним пользователям относятся сотрудники Учреждения, допущенные в установленном порядке к работе в ИСПДн, а также должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИСПДн (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами Учреждения.

Порядок создания учетной записи пользователя, в том числе привилегированной учетной записи администратора (далее – учетная запись):

для создания учетной записи начальник соответствующего отдела инициирует заявку администратору информационной безопасности ИСПДн о создании учетной записи пользователя, в том числе временной (в виде персональных идентификаторов (логины, имена пользователей).

Временная учетная запись заводится для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования ИСПДн, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к ИСПДн).

Администратор информационной безопасности ИСПДн проверяет права доступа сотрудника к информационным ресурсам, определяет принадлежность к группе и незамедлительно, но в срок не более двух рабочих дней с момента подачи заявки, создает новую учетную запись, с указанными в заявке параметрами.

В момент создания учетной записи администратором информационной безопасности ИСПДн генерируется и выдается пользователю первичный пароль.

При первом доступе пользователь обязан изменить выданный ему первичный пароль, руководствуясь требованиями к сложности пароля, указанными в настоящей Инструкции.

Порядок блокирования учетной записи пользователя:

персональные идентификаторы должны быть заблокированы администратором информационной безопасности ИСПДн при превышении времени неиспользования более 90 дней. Персональные идентификаторы должны быть удалены из ИСПДн при увольнении сотрудника Учреждения немедленно по окончании последнего сеанса работы сотрудника, а уволенный сотрудник должен быть исключен из числа пользователей ИСПДн;

разблокировка учетной записи пользователя происходит по устному обращению начальника соответствующего отдела.

Порядок удаления учетной записи пользователя:

начальник соответствующего отдела инициирует заявку администратору информационной безопасности ИСПДн об удалении учетной записи увольняющегося пользователя;

администратор информационной безопасности ИСПДн удаляет учетную запись пользователя ИСПДн при увольнении немедленно по окончании последнего сеанса работы сотрудника, а уволенный сотрудник исключается из числа пользователей ИСПДн. Удаление временных учетных записей производятся, если:

- задача, требующая расширенного полномочия, для которого создавалась временная учетная запись, выполнена;
- произведена настройка и тестирование ИСПДн;
- по достижению даты, которая указывалась в заявке при создании временной учетной записи для организации гостевого доступа.

Порядок хранения исполненных заявок:

исполненные заявки подлежат хранению у администратора информационной безопасности ИСПДн, которые могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий в ИСПДн;
- для контроля правомерности наличия у конкретного пользователя прав доступа к информационному ресурсу;
- тем или иным ресурсам системы при разборе конфликтных ситуаций;
- для проверки правильности настройки средств разграничения доступа к ресурсам ИСПДн.

Требования к сложности пароля:

длина пароля должна быть не менее 6 символов;

алфавит пароля не менее 70 символов (буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

символы пароля должны вводиться в режиме латинской раскладки клавиатуры;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего на 3 символов;

при создании новых паролей пользователям запрещается использовать 3 последних использованных паролей;

пароль действует не более 90 дней, по истечении которых пользователь обязан заменить его новым.

Администратор информационной безопасности ИСПДн осуществляет настройку в ИСПДн параметров количества вводов неправильного пароля. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки технического средства или учетной записи пользователя устанавливается равным 5 попыткам. Время блокировки

программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации устанавливается равным 15 минутам. По истечении 15 минут блокировки пользователь может продолжить процедуру аутентификации.

Администратор информационной безопасности производит настройку в ИСПДн параметров блокирования сеанса доступа при времени бездействия пользователя более 15 минут или по запросу пользователя.

Администратором информационной безопасности ИСПДн должно быть исключено повторное использование идентификатора пользователя в течение не менее одного года.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности ИСПДн.

Администратору информационной безопасности ИСПДн разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИСПДн в случае сбоев в работе или выходе из строя отдельных технических средств (устройств). Пользователям запрещены любые действия в ИСПДн до процедуры идентификации и аутентификации.

Действия администратора информационной безопасности ИСПДн при компрометации паролей:

заблокировать доступ пользователя скомпрометированного пароля к ИСПДн;

выявить действия, произведенные в ИСПДн с использованием скомпрометированных персональных идентификаторов и паролей доступа;

доложить ответственному за организацию обработки ПДн об инциденте и предоставить результаты анализа инцидента;

совместно с ответственным за организацию обработки ПДн определить необходимость расследования инцидента;

создать и выдать пользователю новый персональный идентификатор и пароль доступа к ИСПДн.

Приложение 15
к приказу от «22» ноября 2021г. № 187

ИНСТРУКЦИЯ
по организации антивирусной защиты

1. Общие требования

Настоящая инструкция определяет требования к организации антивирусной защиты ИСПДн «ИАСПСР» от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководства и сотрудников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

Установка и настройка средств антивирусного контроля осуществляется администратором информационной безопасности ИСПДн.

2. Применение средств антивирусного контроля

При загрузке автоматизированного рабочего места (далее – АРМ) в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

Полному антивирусному контролю АРМ должны подвергаться не реже одного раза в неделю.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по информационно-телекоммуникационным сетям, а также информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения, администратором информационной безопасности в ИСПДн

должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ.

3. Порядок обновления антивирусных баз

Обновление антивирусных баз на АРМ, подключенных к локальной сети, осуществляется ежедневно в автоматическом режиме через сервер обновлений.

Контроль обновления антивирусных баз на АРМ, подключенных к локальной сети, должен осуществляться администратором информационной безопасности ИСПДн еженедельно. В случае возникновения ошибок при автоматическом обновлении средств антивирусной защиты (появлении диалоговых окон, сообщений об ошибке), необходимо принимать соответствующие меры, обновлять базу вручную в случае необходимости.

4. Действия при обнаружении вирусов

При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник отдела самостоятельно или вместе с администратором информационной безопасности ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

приостановить работу в ИСПДн;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за организацию обработки персональных данных и смежные подразделения, использующие эти файлы в работе;

совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

провести лечение или уничтожение зараженных файлов.

5. Ответственность

Ответственность за организацию антивирусной защиты возлагается на администратора информационной безопасности ИСПДн, который один раз в месяц осуществляет контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками _____.

Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на всех сотрудников, являющихся пользователями ИСПДн.

Приложение 16
к приказу от «22» ноября 2021г. № 187

ИНСТРУКЦИЯ
по регистрации событий безопасности

1. Общие положения

Настоящая инструкция разработана в соответствии с п. 8.5 приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Событие безопасности (информационной) – это идентифицированное возникновение состояния информационной системы персональных данных (далее – ИСПДн) (сегмента, компонента информационной системы персональных данных), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

Отслеживание событий (проверку), происходивших на автоматизированных рабочих местах (далее – АРМ), осуществляет ответственный за обеспечение безопасности персональных данных (далее – ПДн) в информационных системах персональных данных (далее – администратор информационной безопасности ИСПДн).

Общими задачами проверки являются:

контролирование состояния защищенности системы;

выявление причин произошедших изменений;

определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;

установление времени изменений.

2. Определение событий безопасности, подлежащих регистрации, их состава, содержания и сроков хранения

События, происходящие на АРМ, входящих в состав ИСПДн, регистрируются в журналах, приведенных в абзаце 1 п. 3. настоящей инструкции.

Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

В ИСПДн как минимум подлежат регистрации следующие события:

вход (выход), а также попытки входа субъектов доступа в ИСПДн и загрузки (останова) операционной системы;

подключение машинных носителей информации и вывод информации на носители информации;

запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;

попытки доступа программных средств к определяемым оператором 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.

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

При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей, как минимум, включают дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

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

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

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, как минимум, включают 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).

При регистрации попыток удаленного доступа к ИСПДн состав и содержание информации, как минимум, включают 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 информационной системе.

Срок хранения событий безопасности составляет 3 месяца для оперативного доступа, 12 месяцев - архивного хранения.

События безопасности подлежат защите, реализуемой организационным и техническими мерами, и соответствующим настройкам системы защиты информации на ограничение доступа пользователей к параметрам настройки средств защиты информации.

3. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

События безопасности регистрируются в:

штатных журналах операционной системы Windows;

журналах событий средств защиты информации.

Администратор информационной безопасности ИСПДн производит проверку электронных журналов не реже одного раза в неделю.

В случае сбоя при регистрации событий безопасности осуществляется предупреждение (сигнализация, индикация) администратора информационной безопасности ИСПДн о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности.

При обнаружении сбоя при регистрации событий безопасности администратор информационной безопасности ИСПДн обязан реагировать путем изменения 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.

Администратор информационной безопасности ИСПДн совместно с ответственным за организацию обработки ПДн принимают решение об определении события информационной безопасности к относящимся или не относящимся к инцидентам информационной безопасности. Инциденты информационной безопасности могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами. Их последствиями могут быть такие события, как несанкционированные раскрытие или изменение ПДн, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам _____ или их хищение.

В случае обнаружения инцидента информационной безопасности администратор информационной безопасности ИСПДн руководствуется Инструкцией по работе с инцидентами информационной безопасности.

Приложение 17
к приказу от «22» ноября 2021г. № 187

ИНСТРУКЦИЯ
о пропускном и внутриобъектовом режимах

1. Общие положения

Данная Инструкция регламентирует условия и порядок осуществления пропускного и внутриобъектового режимов в _____ (далее - Учреждение), в целях обеспечения предотвращения несанкционированного доступа к персональным данным (далее – ПДн).

Обеспечение доступа лиц на территорию Учреждения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности подразделений и определяет порядок пропуска сотрудников Учреждения, сотрудников иных организаций и учреждений и граждан.

Пропускной режим устанавливается в целях:

исключения фактов хищений собственности Учреждения;

исключение фактов вандализма со стороны недобросовестных посетителей;

исключения возможности несанкционированного доступа персонала и посетителей в помещения Учреждения.

Внутриобъектовый режим устанавливается в целях:

соблюдения сотрудниками и посетителями правил внутреннего распорядка и пожарной безопасности;

установления порядка допуска сотрудников в помещения ограниченного доступа Учреждения;

исключения возможности бесконтрольного передвижения посетителей по территории Учреждения.

Надежность пропускного и внутриобъектового режимов достигается:

осуществлением контроля за перемещением персонала с помощью системы видеонаблюдения;

осуществлением охраны помещений с помощью охранной сигнализации;

контролем за состоянием технических средств охраны.

Ответственным за организацию пропускного и внутриобъектового режимов в Учреждении является _директор Кузьмин А.А.

Ответственным за соблюдение правил внутреннего трудового распорядка, установленного режима функционирования, порядка содержания служебных помещений и мер противопожарной безопасности на объекте является Пацук М.В.

Ответственным за реализацию организационно-технических мероприятий, связанных с осуществлением пропускного и внутриобъектового режимов в Учреждении является администратор

информационной безопасности ИСПДн.

2. На территории Учреждения запрещено

На территории Учреждения запрещается:

проводить без разрешения руководства фото-, кино-, видеосъемки, в том числе с использованием мобильных телефонов;

курить;

пользоваться неисправными или самодельными электронагревательными и другими электробытовыми приборами;

загромождать территорию, основные и запасные входы (выходы), лестничные площадки материалами и предметами, которые создают помехи для системы видеонаблюдения, затрудняют эвакуацию людей, материальных ценностей, препятствуют ликвидации очагов возгорания;

совершать действия, нарушающие установленные режимы функционирования технических средств охраны и пожарной сигнализации;

заниматься торговой деятельностью.

вносить химические, взрывчатые и легковоспламеняющиеся вещества и иные предметы и средства, наличие либо применение (использования) которых может представлять угрозу для безопасности окружающих;

вносить боеприпасы, оружие всех видов и патроны к нему (кроме лиц, которым законодательством Российской Федерации разрешено ношение, хранение и применение оружия для исполнения возложенных на них обязанностей);

иметь при себе крупногабаритные предметы, в том числе хозяйственные сумки, рюкзаки, вещевые мешки, чемоданы (за исключением папок, портфелей, кейсов для документов).

При осуществлении гражданином попытки вноса предметов, перечисленных в абзаце 1 п. 2. настоящей Инструкции, они не пропускаются на территорию Учреждения.

3. Порядок вноса (выноса) материальных ценностей на (с) территорию (ии) Учреждения

Внос (вынос) материальных ценностей, замена мебели, оборудования, инвентаря осуществляется по согласованию с директором/заместителем директора Учреждения и осуществляется в присутствии ответственного лица Пацук М.В.

4. Порядок доставки (отправления) корреспонденции и посылок на территорию Учреждения

Доставка (отправление) специальной, а также почтовой корреспонденции осуществляется через центральный вход здания.

5. Порядок выдачи ключей от служебных помещений Учреждения

В ведении охраны находятся дубликаты ключей от служебных помещений, центрального входа и запасных выходов, электрощитовой, и выдаются ответственным лицам в экстренных случаях и чрезвычайных ситуациях (авариях, пожаре, срабатывании охранно-пожарной сигнализации), о чем делается запись в журнале учета выдачи ключей.

Охране запрещается выдача ключей от служебных помещений сотрудникам Учреждения, не имеющим допуск к ИСПДн.

В случае утраты ключей от служебного помещения или по другой причине об этом уведомляется руководство Учреждения, и выдача дубликата ключа охраной производится с его разрешения.

Приложение 18
к приказу от «22» ноября 2021г. № 187

ИНСТРУКЦИЯ
по обработке персональных данных без использования средств автоматизации

1. Общие положения

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в Муниципальное автономное учреждение «Спортивная школа» (далее - Учреждение), или сотруднику (далее – субъекту персональных данных) Учреждения.

Обработка персональных данных (далее – ПДн), содержащихся в информационных системах персональных данных (далее – ИСПДн) либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПДн, как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн, осуществляются при непосредственном участии человека.

Обработка ПДн не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что ПДн содержатся в ИСПДн либо были извлечены из нее.

Правила обработки ПДн, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти Ханты-Мансийского автономного округа – Югры.

2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

ПДн при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн,

осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку ПДн без использования средств автоматизации (в том числе сотрудники Учреждения или лица, осуществляющие такую обработку по договору с Учреждением), должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется Учреждением без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти Ханты-Мансийского автономного округа – Югры, а также локальными правовыми актами Учреждения.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), должны соблюдаться следующие условия:

типовая форма или связанные с ней документы должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, наименование и адрес Учреждения, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых Учреждением способов обработки ПДн;

типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку ПДн;

типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн.

При ведении журналов (журналов регистрации, журналов посещений), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн в помещения Учреждения или в иных аналогичных целях, должны соблюдаться следующие условия:

необходимость ведения такого журнала должна быть предусмотрена актом Учреждения, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способах фиксации и составе информации, запрашиваемой у субъектов ПДн, перечне лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроках обработки ПДн;

копирование содержащейся в таких журналах информации не допускается;

ПДн каждого субъекта ПДн могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта ПДн.

Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя,– путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

Обработка ПДн, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

Приложение 19
к приказу от «22» ноября 2021г. № 187

ИНСТРУКЦИЯ
по работе с инцидентами информационной безопасности

1. Общие положения

Настоящая инструкция устанавливает порядок действий по управлению инцидентами информационной безопасности (далее – ИБ) в МАУ «СШ» (далее - Учреждение»).

Ответственность за выявление инцидентов ИБ и реагирование на них в Учреждении возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн) (далее – администратор информационной безопасности ИСПДн).

В случае обнаружения инцидента ИБ администратор информационной безопасности ИСПДн руководствуется настоящей Инструкцией.

2. Порядок выявления инцидентов информационной безопасности

Администратор информационной безопасности ИСПДн совместно с ответственным за организацию обработки персональных данных (далее – ПДн) принимают решение об определении события ИБ к относящимся или не относящимся к инцидентам ИБ.

Инциденты ИБ могут быть преднамеренными или случайными (например, являться следствием какой-либо человеческой ошибки или природных явлений) и вызваны как техническими, так и нетехническими средствами. Их последствиями могут быть такие события, как несанкционированные раскрытие или изменение ПДн, ее уничтожение или другие события, которые делают ее недоступной, а также нанесение ущерба активам Учреждения или их хищение.

Внутренний инцидент – инцидент, источником которого является нарушитель, связанный с пострадавшей стороной непосредственным образом (трудовым договором или иным способом). Среди инцидентов такого типа можно выделить следующие наиболее распространенные:

утечка ПДн;
неправомерный доступ к ПДн;
удаление ПДн;
компрометация ПДн;
саботаж;
мошенничество;
использование ПДн в личных целях или в мошеннических операциях.

Внешний инцидент – инцидент, источником которого является нарушитель, не связанный с пострадавшей стороной непосредственным

образом. Среди инцидентов такого типа можно выделить следующие наиболее распространенные:

атаки типа «отказ в обслуживании» (DoS), в том числе распределенные (DDoS);

перехват и подмена трафика;

фишинг;

размещение конфиденциальной/провокационной информации в сети Интернет;

взлом, попытка взлома, сканирование портала;

сканирование сети, попытка взлома сетевых узлов;

вирусные атаки;

неправомерный доступ к ПДн.

Данный перечень не является исчерпывающим. В общем случае инцидентом является единичное, нежелательное или неожиданное событие информационной безопасности (или совокупность таких событий), которое угрожает информационной безопасности ИСПДн.

3. Анализ исходной информации и принятие решения о проведении разбирательства инцидента информационной безопасности

Администратор информационной безопасности ИСПДн совместно с ответственным за организацию обработки ПДн проводят анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий. Источниками и причинами возникновения инцидентов в ИСПДн могут являться:

действия организаций и отдельных лиц враждебные интересам Учреждения;

отсутствие персональной ответственности сотрудников оператора и их руководителей за обеспечение ИБ, в том числе ПДн;

недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе ПДн;

отсутствие моральной и материальной стимуляции за соблюдение правил и требований ИБ;

недостаточная техническая оснащенность подразделений, ответственных за обеспечение ИБ;

совмещение функций по разработке и сопровождению или сопровождению и контролю за ИСПДн;

наличие привилегированных бесконтрольных пользователей в ИСПДн;

пренебрежение правилами и требованиями ИБ сотрудниками Учреждения;

другие причины.

По усмотрению директора Учреждения инцидент ИБ, не приведший к негативным последствиям и совершенный впервые, фиксируется администратором информационной безопасности ИСПДн в «Журнале учета

выявленных инцидентов информационной безопасности» (приложение 7) с присвоением статуса «Разбирательство не требуется».

В случае нарушения прав субъекта ПДн разбирательство инцидента и реагирование на него происходит в порядке и сроки, предусмотренном в документе Учреждения «Правила рассмотрения запросов субъектов персональных данных или их представителей».

В случае наличия признаков инцидента ИБ в полученной информации, администратор информационной безопасности ИСПДн определяет предварительную степень важности инцидента ИБ и принимает решение о необходимости проведения разбирательства, информирует директора Учреждения об инциденте ИБ, производит запись в «Журнале учета выявленных инцидентов информационной безопасности» с присвоением ему статуса «В процессе разбирательства».

В срок не более 3 рабочих дней с момента поступления информации об инциденте ИБ, администратор информационной безопасности ИС, по согласованию с ответственным за организацию обработки ПДн, определяет и инициирует первоочередные меры, направленные на локализацию инцидента ИБ и на минимизацию его последствий.

4. Разбирательство инцидента информационной безопасности

Цели и этапы разбирательства инцидента ИБ:

Целями разбирательства инцидента ИБ являются:

выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;

защита репутации Учреждения и его ресурсов;

обеспечение безопасности ПДн;

обеспечение прав субъектов ПДн на обеспечение безопасности и конфиденциальности их ПДн, обрабатываемых Учреждением;

предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации.

Разбирательство инцидента ИБ, состоит из следующих этапов:

подтверждение/опровержение факта возникновения инцидента ИБ;

подтверждение/корректировка уровня значимости инцидента ИБ;

уточнение дополнительных обстоятельств (деталей) инцидента ИБ;

получение (сбор) доказательств возникновения инцидента ИБ, обеспечение их сохранности и целостности;

минимизация последствий инцидента ИБ;

информирование и консультирование сотрудников Учреждения по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;

разработка мероприятий по обнаружению и/или предупреждению инцидентов ИБ.

Порядок проведения разбирательства инцидента ИБ:

в процессе проведения разбирательства инцидента ИБ обязательными для установления являются:

- дата и время совершения инцидента ИБ;
- Ф.И.О, должность и подразделение Нарушителя ИБ (для внутреннего инцидента);
- уровень критичности инцидента ИБ;
- обстоятельства и мотивы совершения инцидента ИБ;
- информационные ресурсы, затронутые инцидентом ИБ;
- характер и размер реального и потенциального ущерба;
- обстоятельства, способствовавшие совершению инцидента ИБ.

Администратор информационной безопасности ИСПДн в процессе проведения расследования инцидента ИБ, при необходимости, запрашивает информацию в структурных подразделениях Учреждения. Запрос направляется на имя начальника отдела с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

После получения необходимой информации по инциденту ИБ администратор информационной безопасности ИСПДн проводит анализ полученных данных.

В течение 5 рабочих дней администратор информационной безопасности ИСПДн запрашивает у начальника отдела объяснительную записку Нарушителя ИБ. Объяснительная записка должна быть составлена, подписана Нарушителем ИБ в течение 2 рабочих дней и представлена его непосредственным руководителем администратору информационной безопасности ИСПДн в течение 3 рабочих дней с момента поступления запроса. В случае отказа Нарушителя ИБ предоставить объяснительную записку администратору информационной безопасности ИСПДн, составляется акт в соответствии с установленным в Учреждении порядке.

Администратор информационной безопасности ИСПДн проводит оценку негативных последствий от реализации инцидента ИБ. В ходе данной оценки учитываются:

прямой финансовый ущерб;

репутационный ущерб;

потенциальный ущерб;

косвенные потери, связанные с недоступностью сервисов, потерей информации;

другие виды ущерба или аспекты негативных последствий для Учреждения или субъектов ПДн.

С целью минимизации последствий инцидента ИБ возможно временное отключение прав доступа Нарушителя ИБ к информационным ресурсам (далее – ИР) на время проведения расследования, предварительно сделав заявку. Подобное отключение инициируется администратором информационной безопасности ИС с обязательным предварительным устным согласованием с руководителем Нарушителя ИБ.

В случае, если у Нарушителя ИБ были отключены права доступа к ИР на время проведения разбирательства, то по его результатам администратор информационной безопасности ИС по согласованию с руководителем Нарушителя ИБ принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имевшихся у Нарушителя ИБ прав доступа к ИР либо инициирует официальную процедуру отмены (изменения) прав доступа к ИР в соответствии с установленным порядком в Учреждении. Если нарушение ИБ было вызвано незнанием Нарушителем ИБ правил (технологии) работы с ИР высокого уровня безопасности, то основанием для возврата прав доступа является успешное прохождение повторного инструктажа ответственным за организацию обработки персональных данных, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами Учреждения.

Восстановление временно отключенных у Нарушителя ИБ прав доступа к ИР (разблокировка пользователя) может производиться только по заявке руководителя Нарушителя ИБ.

5. Оформление результатов проведенного разбирательства

Собранная в процессе разбирательства инцидента ИБ информация фиксируется администратором информационной безопасности ИС в «Журнале учета выявленных инцидентов информационной безопасности» и учитывается при подготовке итогового заключения по инциденту ИБ.

Администратор информационной безопасности ИСПДн формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение по расследованию инцидента ИБ.

Итоговое заключение по инциденту ИБ администратор информационной безопасности ИСПДн направляет директору, начальникам отделов, затронутых инцидентом ИБ, и ответственному за организацию обработки ПДн.

Администратор информационной безопасности ИСПДн фиксирует завершение разбирательства в «Журнале учета выявленных инцидентов информационной безопасности» и присваивает инциденту статус «Разбирательство завершено».

6. Завершение разбирательства инцидента информационной безопасности

По завершению разбирательства инцидента ИБ, администратор информационной безопасности ИСПДн передает имеющиеся материалы в объеме, достаточном для принятия решения, ответственному за организацию обработки ПДн для решения вопроса о целесообразности привлечения Нарушителя ИБ к дисциплинарной ответственности.

На основании полученных результатов разбирательства ответственный за организацию обработки ПДн в срок не более 3 рабочих дней

организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков ИБ в будущем:

повторное ознакомление Нарушителя ИБ с правилами по обеспечению безопасности ПДн;

просмотр и анализ имеющихся прав доступа к ИР у Нарушителя ИБ;

доведение до всех сотрудников Учреждения внутренних нормативных документов;

обсуждение инцидента ИБ на совещании руководителей;

отмена неактуальных прав доступа к ИР;

проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

и другие обоснованные мероприятия.

О результатах проведенного разбирательства инцидента ИБ ответственный за организацию обработки ПДн по необходимости инициирует подготовку сообщения об инциденте ИБ в адрес директора Учреждения.

7. Действия пользователей информационных систем персональных данных при возникновении инцидента информационной безопасности

Сбой программного обеспечения:

администратор информационной безопасности ИСПДн совместно с ответственным за организацию обработки ПДн выясняют причину сбоя программного обеспечения. Если привести систему в работоспособное состояние своими силами (в том числе после консультаций с разработчиками программного обеспечения) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику программного обеспечения для устранения причин, приведших к сбою. О произошедшем инциденте администратор информационной безопасности ИСПДн сообщает директору Учреждения для принятия решения по существу.

Отключение электропитания технических средств ИСПДн:

администратор информационной безопасности ИСПДн совместно с ответственным за организацию обработки ПДн проводят анализ на наличие потерь и (или) разрушения данных и программного обеспечения, а также проверяют работоспособность оборудования. В случае необходимости производится восстановление программного обеспечения и данных из последней резервной копии с составлением акта. О произошедшем инциденте администратор информационной безопасности ИСПДн сообщает директору Учреждения для принятия решения по существу.

Выход из строя технических средств ИСПДн (серверов, рабочих станций):

администратор информационной безопасности ИСПДн выполняют мероприятия по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы ИСПДн (замене рабочей станции);

о выходе из строя сервера (рабочей станции) администратор информационной безопасности ИСПДн сообщает директору Учреждения;

при необходимости производятся работы по восстановлению программного обеспечения и данных из резервных копий с составлением акта. О произошедшем инциденте администратор информационной безопасности ИСПДн сообщает директору Учреждения для принятия решения по существу.

Потеря данных:

при обнаружении потери данных администратор информационной безопасности ИСПДн проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность программного обеспечения, целостность и работоспособность оборудования);

при необходимости администратором информационной безопасности ИСПДн производится восстановление программного обеспечения и данных из резервных копий с составлением акта. Администратор информационной безопасности ИСПДн сообщает директору Учреждения для принятия решения по существу.

Обнаружение вредоносной программы в программной среде средств автоматизации ИСПДн:

при обнаружении вредоносной программы (далее - ВП) производится ее локализация с целью предотвращения ее дальнейшего распространения. При этом зараженная рабочая станция (сервер) физически отсоединяется от локальной вычислительной сети, и ответственным за антивирусную защиту и администратором информационной безопасности ИСПДн проводится анализ состояния рабочей станции;

в результате анализа может быть предпринята попытка сохранения данных, так как после перезагрузки рабочей станции данные могут быть потеряны. После успешной ликвидации ВП сохраненные данные подвергаются повторной проверке на наличие ВП. Кроме того, при обнаружении ВП следует руководствоваться инструкцией по эксплуатации применяемого антивирусного программного обеспечения;

после ликвидации ВП проводится внеочередная проверка на всех средствах локальной вычислительной системы с применением обновленных антивирусных баз. При необходимости производится восстановление программного обеспечения и данных из резервных копий с составлением акта;

по факту появления ВП в локальной вычислительной сети проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается директором Учреждения.

Утечка информации:

при обнаружении утечки информации ставится в известность ответственный за организацию обработки ПДн, администратор информационной безопасности ИСПДн и начальник отдела. По факту инициируется процедура служебного расследования. Если утечка информации произошла по техническим причинам, проводится анализ защищенности процессов ИСПДн и, если необходимо, принимаются меры по устранению каналов утечки и предотвращению их возникновения.

Взлом операционной системы средств автоматизации ИСПДн (несанкционированное получение доступа к ресурсам операционной системы):

при обнаружении взлома сервера ставится в известность директор Учреждения;

по возможности производится временное отключение сервера от локальной вычислительной сети для проверки на наличие ВП. Возможен временный переход на резервный сервер;

администратором информационной безопасности ИСПДн проверяется целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения. Администратором информационной безопасности ИСПДн проводится анализ состояния файлов - скриптов и журналов сервера, производится смена всех паролей, которые имели отношение к данному серверу;

в случае необходимости администратором информационной безопасности ИСПДн производится восстановление программного обеспечения и восстановление данных из эталонного архива и резервных копий с составлением акта;

по результатам анализа ситуации проверяется вероятность проникновения несанкционированных программ в локальную вычислительную сеть, после чего проводятся аналогичные работы по проверке и восстановлению программного обеспечения и данных на других информационных узлах ИСПДн.

Попытка несанкционированного доступа (далее - НСД):

при попытке НСД администратором информационной безопасности ИСПДн проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости (есть реальная угроза НСД), принимаются меры по предотвращению НСД;

Проводится внеплановая смена паролей. В случае появления обновлений программного обеспечения, устраняющих уязвимости системы безопасности, администратором информационной безопасности ИСПДн устанавливаются такие обновления;

по факту попытки НСД проводится служебное расследование. Решение о необходимости проведения служебного расследования принимается директором Учреждения.

в случае установления в ходе служебного расследования факта осуществления попытки НСД со стороны внешних по отношению к ИСПДн

субъектов, лицами, уполномоченными на проведение такого расследования, принимаются меры по фиксации и документированию факта инцидента и готовятся материалы для передачи в компетентные органы дознания для проведения предварительного расследования, установления субъекта-нарушителя, определения наличия состава преступления и принятия решения о возбуждении уголовного дела.

Компрометация ключевой информации (паролей доступа):

при компрометации ключевой информации (пароля доступа) администратором информационной безопасности ИСПДн проводится смена пароля, анализируется ситуация на наличие последствий компрометации и принимаются необходимые меры по минимизации возможного (или нанесенного) ущерба;

о произошедшем инциденте администратор информационной безопасности ИСПДн сообщает директору Учреждения для принятия решения по существу.

Физическое повреждение или хищение оборудования технических средств ИСПДн:

сотрудником, обнаружившим физическое повреждение элементов ИСПДн, ставятся в известность: непосредственный руководитель, администратор информационной безопасности ИСПДн и директор Учреждения.

администратором информационной безопасности ИСПДн проводится анализ с целью оценки возможности утечки или повреждения информации. Определяется причина повреждения элементов ИСПДн и возможные угрозы информационной безопасности;

в случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование;

администратором информационной безопасности ИСПДн проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов;

при необходимости администратором информационной безопасности ИСПДн проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта.

Невыполнение установленных правил ИБ (правил работы в ИСПДн), использование ИСПДн с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации:

сотрудником, обнаружившим невыполнение установленных правил ИБ, использование ИСПДн с нарушением требований, установленных в нормативно-технической и (или) конструкторской документации, ставятся в известность: непосредственный руководитель;

администратором информационной безопасности ИСПДн проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента;

об обнаруженном факте администратор информационной безопасности ИСПДн докладывает руководителю подразделения;

при необходимости по решению руководителя подразделения по фактам выявленных нарушений проводится служебное расследование.

Ошибки сотрудников:

в случае возникновения сбоя, связанного с ошибками сотрудников, руководитель подразделения, в котором произошел инцидент, ставит в известность администратора информационной безопасности ИСПДн;

администратором информационной безопасности ИСПДн проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы информационной безопасности в результате инцидента и необходимость восстановления программного обеспечения и данных;

при необходимости администратором информационной безопасности ИСПДн проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта;

в случае нанесения значительного ущерба вследствие ошибок сотрудников проводится служебное расследование.

Отказ в обслуживании:

сотрудником, обнаружившим отказ в обслуживании, ставятся в известность: непосредственный руководитель и администратор информационной безопасности ИСПДн;

администратором информационной безопасности ИСПДн проводится анализ с целью определения причин, вызвавших отказ в обслуживании;

администратором информационной безопасности ИСПДн проводится проверка программного обеспечения на целостность и на наличие ВП, а также проверка целостности данных и анализ электронных журналов;

при необходимости, администратором информационной безопасности ИСПДн проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта;

о причинах инцидента и принятых мерах администратор информационной безопасности ИСПДн информирует руководителя подразделения.

Несанкционированные изменения состава программных и аппаратных средств (конфигурации) ИСПДн:

в случае обнаружения несанкционированного изменения состава программных и аппаратных средств (конфигурации) ИСПДн администратором информационной безопасности ИСПДн проводится анализ с целью оценки возможности утечки или повреждения информации. Определяются возможные угрозы ИБ в результате инцидента;

администратором информационной безопасности ИСПДн проводятся мероприятия по восстановлению программного обеспечения и данных из резервных копий с составлением акта, а также (при необходимости) проверка на наличие компьютерных ВП;

об инциденте администратор информационной безопасности ИСПДн докладывает руководителю подразделения.

Техногенные и природные проявления нештатных ситуаций:

при стихийном бедствии, пожаре или наводнении, грозящем уничтожению или повреждению информации (данных), сотруднику, обнаружившему факт возникновения нештатной ситуации:

- немедленно оповестить других сотрудников и принять все меры для самостоятельной оперативной защиты помещения;
- немедленно позвонить в соответствующие службы помощи (пожарная охрана, служба спасения и т.д.);
- немедленно сообщить своему непосредственному руководителю и администратору информационной безопасности ИСПДн.

после оперативной ликвидации причин, вызвавших пожар или наводнение, назначается внутренняя комиссия по устранению последствий инцидента;

комиссия определяет ущерб (состав и объем уничтоженных оборудования и информации) и причины, по которым произошло происшествие, а также выявляет виновных.

8. Обязанности и права участников разбирательства инцидента информационной безопасности

Администратор информационной безопасности ИСПДн обязан:

объективно и основательно проводить разбирательство каждого инцидента ИБ;

определять первоочередные меры, направленные на локализацию инцидента ИБ и минимизацию негативных последствий;

фиксировать в «Журнале учета выявленных инцидентов информационной безопасности» всю исходную информацию об инциденте ИБ и результаты его расследования;

предоставлять отчеты и рекомендации по проведенным разбирательствам ответственному за организацию обработки ПДн и директору Учреждения;

проводить анализ обстоятельств, способствовавших совершению каждого инцидента ИБ, и на его основе, совместно с ответственным за организацию обработки ПДн, разрабатывать рекомендации и предложения по снижению ущерба от подобных инцидентов ИБ и минимизации возможности их повторения в будущем.

Администратор информационной безопасности ИСПДн имеет право:

по согласованию с непосредственным руководителем Нарушителя ИБ требовать предоставлений письменных объяснений по обстоятельствам инцидента ИБ у Нарушителя ИБ;

запрашивать и получать от руководителей и сотрудников Учреждения, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента ИБ;

инициировать отключение от ИР сотрудников Учреждения, нарушивших правила или требования ИБ, на период проведений расследования инцидента ИБ, в случае если имеется существенный риск того, что продолжение работы сотрудника с ИР может повлечь значительное увеличение ущерба или новые инциденты ИБ;

по результатам расследования инцидента ИБ инициировать изменения ИР Учреждения с целью повышения их защищенности и снижения рисков инцидентов ИБ;

инициировать процедуры привлечения Нарушителя ИБ к дисциплинарной или материальной ответственности, согласно внутренним нормативным документам Учреждения.

Начальник отдела и сотрудники Учреждения обязаны:

предоставлять по запросам администратора информационной безопасности ИСПДн устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента ИБ;

информировать администратора информационной безопасности ИСПДн о выявленных инцидентах ИБ.

Приложение 20
к приказу от «22» ноября 2021г. № 187

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей

1. Общие положения

Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее – Правила) в _____ (далее - Учреждение) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», и определяют права субъектов персональных данных (далее – ПДн), обязанности Учреждения при обращении субъекта ПДн или его представителя, а также сроки и последовательность действий сотрудников Учреждения при рассмотрении запросов субъектов ПДн или их представителей.

Представитель субъекта ПДн – лицо, действующее от имени субъекта ПДн в силу полномочий, основанных на доверенности, указании закона, либо акте уполномоченного на то государственного органа или органа местного самоуправления. При обращении представителя субъекта ПДн в орган власти представляется документ, подтверждающий полномочия законного представителя.

2. Права субъекта персональных данных

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

подтверждение факта обработки ПДн;

правовые основания и цели обработки ПДн;

цели и применяемые Учреждением способы обработки ПДн;

наименование и место нахождения Учреждения, сведения о лицах (за исключением сотрудников Учреждения), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Учреждением или на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон);

обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

сроки обработки ПДн, в том числе сроки их хранения;

порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом;

информация об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Учреждения, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные Федеральным законом или другими федеральными законами.

Сведения, указанные в абзаце 1 п. 2.1 настоящих Правил, должны быть предоставлены субъекту ПДн Учреждением в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

Сведения, указанные в абзаце 1 п. 2. настоящих Правил, предоставляются субъекту ПДн или его представителю Учреждением при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Учреждением (номер договора (контракта), дата заключения договора (контракта), условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Учреждением, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

В случае если сведения, указанные в абзаце 1 п. 2. настоящих Правил, а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к Учреждению или направить ему повторный запрос в целях ознакомления с такими ПДн не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной по которому является субъект ПДн.

Субъект ПДн вправе обратиться повторно к Учреждению или направить ему повторный запрос в целях получения сведений, указанные в абзаце 1 п. 2. настоящих Правил, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в абзаце 4 п. 2. настоящих правил, в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в абзаце 4 п. 2. настоящих правил, должен

содержать обоснование направления повторного запроса.

Субъект ПДн вправе требовать от Учреждения уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3. Обязанности Учреждения при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя

Учреждение обязано сообщить в порядке, предусмотренном настоящими Правилами, субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя либо в течение 30 дней с даты получения запроса субъекта ПДн или его представителя;

в случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн субъекту ПДн или его представителю при его обращении либо при получении запроса субъекта ПДн или его представителя Учреждение обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» или иного федерального закона, который является основанием для такого отказа, в срок, не превышающий 30 дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя;

Учреждение обязано предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту ПДн. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, орган власти обязан внести в них необходимые изменения. В срок, не превышающий 7 рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Учреждение обязано уничтожить такие ПДн. Учреждение обязано уведомить субъекта ПДн или его представителя о внесенных изменениях, предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы;

Учреждение обязано сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение 30 дней с даты получения такого запроса.

4. Права Учреждения

Учреждение вправе отказать субъекту в выполнении повторного запроса, не соответствующего условиям, предусмотренным абзацами 3 и 5 п. 2. настоящих Правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса возлагается на Учреждение.

5. Порядок рассмотрения запросов субъектов персональных данных или их представителей или уполномоченного органа по защите прав субъектов персональных данных

Действия Учреждения при обращении субъекта:

в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – 152-ФЗ) при личном устном приеме субъект ПДн предъявляет документ, удостоверяющий его личность;

в случае, если при личном приеме от имени субъекта ПДн действует его законный представитель, сотрудник Учреждение обязан удостовериться в наличии у такого лица законных полномочий;

содержание устного обращения регистрируется в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных». Ответ на обращение с согласия субъекта ПДн может быть дан устно в ходе личного приема, а также субъекту ПДн предоставляется возможность ознакомления с его ПДн, о чем делается запись в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных». При отсутствии возможности ознакомления субъекта с его ПДн немедленно при его личном обращении, такая возможность должна быть предоставлена субъекту ПДн в течение 30 рабочих дней с даты обращения;

в том случае, когда при личном приеме субъект ПДн изъявил желание получить ответ в письменной форме, сотрудник, ведущий прием, предлагает субъекту ПДн оформить письменный запрос и сообщает ему о сроках, в течение которых Учреждение обязано дать ответ на такой запрос в соответствии с 152-ФЗ;

если при рассмотрении обращения субъекта ПДн будет установлено, что предоставление ПДн нарушает права и законные интересы третьих лиц, сотрудник, осуществляющий личный прием субъекта ПДн, сообщает ему об отказе в предоставлении информации о ПДн, о чем делается запись в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных». Также в срок, не превышающий 30 дней со дня обращения, сотрудник направляет в адрес субъекта ПДн мотивированный ответ в письменной форме, содержащий ссылку на положение п. 4 ч. 8 ст. 14 152-ФЗ.

Действия Учреждения при получении запроса субъекта ПДн:

В соответствии с ч. 3 ст. 14 152-ФЗ запрос должен содержать:

сведения о номере основного документа, удостоверяющего личность субъекта ПДн или его представителя;

сведения о дате выдачи указанного документа и выдавшем его органе;

сведения, подтверждающие участие субъекта ПДн в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения) либо сведения, иным образом подтверждающие факт обработки ПДн Учреждением;

подпись субъекта ПДн или его представителя.

Регистрация запросов субъектов ПДн, а также регистрация ответов, направляемых субъектам ПДн, осуществляется в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных».

Сотрудниками Учреждение, осуществляющими прием обращений субъектов ПДн и регистрацию запросов субъектов ПДн и уполномоченного органа по защите прав субъектов ПДн (далее – сотрудник), является: Табурцова Т.А. заместитель директора.

Сотрудником Учреждение, осуществляющим рассмотрение запросов субъектов ПДн и контроль за подготовкой ответов на них, является ответственный за организацию обработки ПДн.

При получении запроса субъекта ПДн, сотрудник Учреждения непосредственно в день получения проверяет соответствие запроса требованиям к письменному обращению, установленным ст. 7 Федерального закона «О порядке рассмотрения обращений граждан Российской Федерации» от 02.05.2006 № 59-ФЗ (далее – 59-ФЗ), а именно:

наименование государственного органа, в который направлено письменное обращение, либо фамилию, имя, отчество соответствующего должностного лица, либо должность соответствующего лица;

наличие фамилии, имени, отчества (последнее - при наличии) субъекта ПДн;

наличие почтового адреса, по которому должен быть направлен ответ;

наличие личной подписи и даты;

наличие сведений о документе, удостоверяющем личность субъекта ПДн (номер документа, сведения о дате выдачи указанного документа и выдавшем его органе).

В случае соответствия запроса субъекта ПДн требованиям, перечисленным в п. 5.2.5 настоящего Порядка, такой запрос подлежит приему и регистрации в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных».

В случае если в запросе субъекта ПДн не указаны фамилия гражданина, направившего обращение, и почтовый адрес, по которому должен быть направлен ответ, в соответствии с ч. 1 ст. 11 59-ФЗ, ответ на такой запрос не дается, о чем делается отметка в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных».

В случае несоответствия запроса субъекта ПДн требованиям, перечисленным в п. 5.2.1 настоящего порядка, такой запрос подлежит приему и регистрации в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных» в тот же день. Также в срок, не превышающий 30 дней со дня обращения, сотрудник направляет в адрес субъекта ПДн мотивированный ответ в письменной форме о том, что сведения не могут быть предоставлены.

Зарегистрированные запросы субъектов ПДн в день регистрации подлежат передаче ответственному за организацию обработки ПДн.

Ответственный за организацию обработки ПДн обязан рассмотреть запрос субъекта ПДн и поручить подготовку ответа на него в письменной форме ответственному сотруднику Учреждения. Ответ на запрос должен быть подготовлен в течение 30 рабочих дней с даты получения указанного запроса.

В случае, если в запросе субъект ПДн изъявил желание ознакомиться со своими ПДн, возможность такого ознакомления должна быть предоставлена субъекту ПДн в течение 30 рабочих дней с даты получения указанного запроса.

Письменный ответ на запрос субъекта ПДн должен быть направлен по его адресу заказным письмом с уведомлением о вручении с соблюдением сроков, предусмотренных законодательством (приложение 1).

Если при рассмотрении запроса субъекта ПДн будет установлено, что предоставление ПДн нарушает права и законные интересы третьих лиц, Учреждение сообщает ему об отказе в предоставлении информации о ПДн, о чем в срок, не превышающий 7 рабочих дней со дня получения запроса субъекта ПДн, в адрес субъекта ПДн направляется мотивированный ответ в письменной форме, содержащий ссылку на положение п. 4 ч. 8 ст. 14 152-ФЗ.

Для обработки ПДн, содержащихся в обращении в письменной форме субъекта ПДн, дополнительного его согласия не требуется.

Действия Учреждения при получении запроса субъекта ПДн в электронной форме:

согласно п. 3 ст. 7 59-ФЗ обращение, поступившее в учреждение в форме электронного документа, подлежит рассмотрению в соответствии с порядком, установленным ст. 10 указанного закона;

в обращении субъект ПДн в обязательном порядке указывает свои фамилию, имя, отчество (последнее – при наличии), адрес электронной почты, если ответ должен быть направлен в форме электронного документа, и почтовый адрес, если ответ должен быть направлен в письменной форме. Субъект ПДн вправе приложить к такому обращению необходимые документы и материалы в электронной форме либо направить указанные документы и материалы или их копии в письменной форме;

прием и регистрация запросов субъектов ПДн в электронной форме подлежат регистрации в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных».

Действия Учреждения при получении запроса уполномоченного органа по защите прав субъектов ПДн:

прием и регистрация запросов уполномоченного органа по защите прав субъектов ПДн подлежат регистрации в «Журнал учета обращений субъектов персональных данных по вопросам обработки персональных данных»;

при получении запроса уполномоченного органа по защите прав субъектов ПДн сотрудник Учреждения, ответственный за прием и регистрацию входящей корреспонденции, в тот же день осуществляет регистрацию такого запроса и передает его ответственному за организацию обработки ПДн;

Учреждение, в лице ответственного за организацию обработки ПДн, сообщает в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, а также направляет запрошенные им документы в течение 30 дней с даты получения такого запроса;

в случае выявления уполномоченным органом по защите прав субъектов ПДн фактов недостоверности ПДн или неправомерных действий с ними, уточнение, блокирование или уничтожение таких ПДн осуществляется в порядке и сроки, предусмотренные законодательством (приложение 1) для соответствующих действий (операций) в отношении ПДн.

Формы запросов субъектов ПДн или их представителей и уполномоченного органа по защите прав субъектов ПДн представлены в приложении 2 к настоящим Правилам.

Формы ответов на запросы субъектов ПДн или их представителей и уполномоченного органа по защите прав субъектов ПДн представлены в приложении 3 к настоящим Правилам.

6. Ответственность

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение 1
к Правилам рассмотрения запросов
субъектов персональных данных или
их представителей

Сводная таблица
действий Учреждения в ответ на запросы субъекта персональных данных или его представителя

№ п/п	Запрос	Действия	Срок	Ответ
1. Запрос субъекта персональных данных или его представителя				
1.1.	Наличие персональных данных	подтверждение обработки персональных данных	30 дней (согласно п. 1 ст. 20 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – 152-ФЗ))	подтверждение обработки персональных данных
		отказ подтверждения обработки персональных данных	30 дней (согласно п. 2 ст. 20 152-ФЗ)	уведомление об отказе подтверждения обработки персональных данных
1.2.	Ознакомление с персональными данными	предоставление информации по персональным данным	30 дней (согласно п. 1 ст. 20 152-ФЗ)	подтверждение обработки персональных данных, а также правовые основания и цели такой обработки
				способы обработки персональных данных
				сведения о лицах, которые имеют доступ к персональным данным
				перечень обрабатываемых персональных данных и источник их получения
				сроки обработки персональных данных, в том числе сроки их хранения
				информация об осуществленной или о предполагаемой трансграничной передаче
		отказ предоставления информации по персональным данным	30 дней (согласно п. 2 ст. 20 152-ФЗ)	уведомление об отказе предоставления информации по персональным данным

1.3.	Уточнение персональных данных	изменение персональных данных	7 рабочих дней со дня предоставления уточняющих сведений (согласно п. 3 ст. 20 152-ФЗ)	уведомление о внесенных изменениях
		отказ изменения персональных данных	30 дней	уведомление об отказе изменений персональных данных
1.4.	Уничтожение персональных данных	уничтожение персональных данных	7 рабочих дней со дня предоставления сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки (согласно п. 3 ст. 20 152-ФЗ)	уведомление об уничтожении персональных данных
		отказ уничтожения персональных данных	30 дней	уведомление об отказе уничтожения персональных данных
1.5.	Отзыв согласия на обработку персональных данных	прекращение обработки и уничтожение персональных данных	30 дней (согласно п. 5 ст. 21 152-ФЗ)	уведомление о прекращении обработки и уничтожении персональных данных
		отказ прекращения обработки и уничтожения персональных данных	30 дней	уведомление об отказе прекращения обработки и уничтожения персональных данных
1.6.	Недостоверность персональных данных Субъекта	блокирование персональных данных	с момента получения запроса на период проверки (согласно п. 1 ст. 21 152-ФЗ)	уведомление о внесенных изменениях
		изменение персональных данных	7 рабочих дней со дня предоставления уточненных сведений (согласно п. 2 ст. 21 152-ФЗ)	
		снятие блокировки персональных данных		уведомление об отказе изменения персональных данных
		отказ изменения персональных данных	30 дней	

1.7.	Неправомерность действий с персональными данными Субъекта	прекращение неправомерной обработки персональных данных	3 рабочих дня (согласно п. 3 ст. 21 152-ФЗ)	уведомление об устранении нарушений
		уничтожение персональных данных в случае невозможности обеспечения правомерности обработки	10 рабочих дней(согласно п. 3 ст. 21 152-ФЗ)	уведомление об уничтожении персональных данных
1.8.	Достижение целей обработки персональных данных Субъекта	прекращение обработки персональных данных	30 дней (согласно п. 4 ст. 21 152-ФЗ)	уведомление об уничтожении персональных данных
		уничтожение персональных данных		
2. Запрос Уполномоченного органа по защите прав субъектов персональных данных				
2.1.	Информация для осуществления деятельности уполномоченного органа	предоставление затребованной информации по персональным данным	30 дней (согласно п. 4 ст. 20 152-ФЗ)	предоставление затребованной информации по персональным данным
2.2.	Неточность персональных данных Субъекта	блокирование персональных данных	с момента получения запроса на период проверки (согласно п. 1 ст. 21 152-ФЗ)	уведомление о внесенных изменениях
		изменение персональных данных	7 рабочих дней со дня предоставления уточненных сведений(согласно п. 2 ст. 21 152-ФЗ)	
		снятие блокировки персональных данных		уведомление об отказе изменения персональных данных
		отказ изменения персональных данных	30 дней	
2.3.	Неправомерность действий с персональными данными Субъекта	прекращение неправомерной обработки персональных данных	3 рабочих дня (согласно п. 3 ст. 21 152-ФЗ)	уведомление об устранении нарушений
		уничтожение персональных данных в случае невозможности обеспечения правомерности обработки	10 рабочих дней(согласно п. 3 ст. 21 152-ФЗ)	уведомление об уничтожении персональных данных
2.4.	Достижение целей обработки персональных данных Субъекта	прекращение обработки персональных данных	30 дней с даты достижения цели обработки	уведомление об уничтожении персональных данных

		уничтожение персональных данных	персональных данных (согласно п.4 ст. 21 152-ФЗ)	

Приложение 2

Форма запроса субъекта персональных данных о наличии и ознакомлении с ПДн

В _____
от _____
адрес:_____
_____
паспорт №_____ выдан _____
_____
_____

ЗАПРОС

Я *состою/не состою* в договорных отношениях с _____и со мной заключен договор № _____ от «___» _____ 20___г.

В соответствии со статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я имею право получить от вас сведения о наличии моих персональных данных, связанных с вышеуказанными данными.

Прошу вас предоставить мне следующую информацию:
1. осуществляется ли обработка моих персональных данных;
2. перечень обрабатываемых вами моих персональных данных и источник их получения;
3. какими способами эти данные обрабатываются;
4. какие лица имеют доступ или могут получить доступ к моим персональным данным;
5. срок хранения моих персональных данных;
6. осуществлялась ли трансграничная передача моих персональных данных, а, если нет, то предполагается ли такая передача;
7. какие юридические последствия для меня может повлечь обработка моих персональных данных.

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

С уважением, _____
«____» _____ 20___ года

Форма запроса субъекта персональных данных на уточнение ПДн

В _____
от _____
адрес:_____
_____
паспорт №_____ выдан _____
_____
_____

ЗАПРОС

Я *состою/не состою* в договорных отношениях с _____ и со мной заключен договор № _____ от «___» _____ 20__г.

В соответствии со статьей 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с _____
_____
прошу внести следующие изменения в мои персональные данные: _____
_____
_____
_____

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

С уважением, _____ «____» _____ 20___ года

Форма запроса субъекта персональных данных на уничтожение ПДн

В _____

от _____

адрес:_____

_____

паспорт №_____ выдан _____

_____

_____

ЗАПРОС

Я *состою/не состою* в договорных отношениях с _____ и со мной заключен договор № _____ от «___» _____ 20__г.

В соответствии со статьей 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с _____

_____

прошу Вас уничтожить мои персональные данные: _____

_____

_____

_____

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

С уважением, _____ «____» _____ 20___ года

Форма запроса субъекта персональных данных с отзывом согласия на обработку ПДн

В _____

от _____

адрес:_____

_____

паспорт №_____ выдан _____

_____

_____

ЗАПРОС

Я *состою/не состою* в договорных отношениях с _____ и со мной заключен договор № _____ от «___» _____ 20___г.

В соответствии со статьей 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с _____ прошу прекратить обработку следующих моих персональных данных: _____

_____

_____

Ответ на настоящий запрос прошу направить в письменной форме по вышеуказанному адресу в предусмотренный законом срок.

С уважением, _____

«____» _____ 20___ года

Приложение 3

Форма ответа на запрос субъекта персональных данных о наличии и ознакомлении с ПДн

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20___ г. относительно обработки Ваших персональных данных могу сообщить следующее.

_____ в период с «___» _____ 20___ г. по настоящее время с целью _____
_____
обрабатывает в рамках договора № _____ от «___» _____ 20___ г. следующие полученные от Вас персональные данные: _____
_____
_____
_____

Эта информация обрабатывается в соответствии с законодательством РФ о персональных данных, в Ваших интересах и с Вашего согласия. Обработка данных включает хранение, использование и, в случае необходимости, передачу данных третьим лицам. Обработкой Ваших персональных данных занимаются сотрудники _____, ознакомленные с обязанностями, возложенными на них в связи с обработкой Ваших персональных данных, и давшие подписку об их неразглашении. Никто другой к обработке Ваших персональных данных не допускается. Ваши персональные данные будут обрабатываться вплоть до достижения указанных целей, но не позже _____ лет с момента Вашего последнего обращения в _____ («_____» _____ 20___ г.).

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «____» _____ 20____ г. относительно обработки Ваших персональных данных могу сообщить следующее.

_____ не осуществляет обработки Ваших персональных данных.

С уважением, _____ М.П. _____ _____

(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Форма ответа на запрос субъекта персональных данных на уточнение ПДн

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20__ г. относительно уточнения Ваших персональных данных могу сообщить следующее.

_____ были внесены изменения в Ваши персональные данные:
_____
_____
_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «__» _____ 20__ г. относительно уточнения Ваших персональных данных могу сообщить следующее.

_____ не может внести изменения в Ваши персональные данные, так как Вами не было предоставлено необходимых документов, подтверждающих запрашиваемые Вами изменения.

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____

(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Форма ответа на запрос субъекта персональных данных на уничтожение ПДн

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20__ г. относительно уничтожения Ваших персональных данных могу сообщить следующее.

_____ были уничтожены Ваши персональные данные: _____
_____
_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20__ г. относительно уничтожения Ваших персональных данных могу сообщить следующее.

_____ не может уничтожить Ваши персональные данные, так как их обработка осуществляется согласно _____
_____
_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____

(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Форма ответа на запрос субъекта персональных данных с отзывом согласия на обработку ПДн

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20__ г. относительно отзыва согласия на обработку Ваших персональных данных могу сообщить следующее.

_____ была прекращена обработка и уничтожены Ваши персональные данные: _____
_____
_____
_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20__ г. относительно отзыва согласия на обработку Ваших персональных данных могу сообщить следующее.

_____ не может прекратить обработку и уничтожить Ваши персональные данные, так как их обработка осуществляется согласно _____
_____
_____

Если у Вас возникнут еще какие-либо вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____

(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Форма уведомления субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при выявлении недостоверности ПД

Г-ну/Г-же_____

В связи с выявлением недостоверности Ваших персональных данных могу сообщить следующее.

_____ были внесены изменения в Ваши персональные данные:
_____
_____
_____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

В связи с выявлением недостоверности персональных данных г-на/г-ки _____ могу сообщить следующее.

_____ были внесены изменения в персональные данные г-на/г-ки _____: _____
_____
_____

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) М.П. (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20___ г., относительно обработки Ваших персональных данных могу сообщить следующее.

_____ не может внести изменения в Ваши персональные данные, так как факт недостоверности не подтвержден и не были предоставлены необходимые документы, подтверждающие недостоверность ПДн.

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) М.П. (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

На Ваш запрос от «___» _____ 20___ г., относительно недостоверности обработки персональных данных г-на/г-ки _____ могу сообщить следующее.

_____ не может внести изменения в персональные данные г-на/г-ки _____, так как факт недостоверности не подтвержден и не были предоставлены необходимые документы, подтверждающие недостоверность ПДн.

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) М.П. (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Формы уведомления субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при выявлении неправомерности действий с ПДн

Г-ну/Г-ке_____

В связи с выявлением неправомерности действий с Вашими персональными данными могу сообщить следующее.

_____ были уничтожены Ваши персональные данные: _____
_____
_____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

В связи с выявлением неправомерности действий с персональных данными г-на/г-ки _____ могу сообщить следующее.

_____ были уничтожены персональные данные г-на/г-ки _____: _____
_____
_____

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) М.П. (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «____» _____ 20___ г., относительно неправомерности обработки Ваших персональных данных могу сообщить следующее.

_____ не может уничтожить Ваши персональные данные, так как факт неправомерности действий с Вашими персональными данными не подтвержден и Вами не были предоставлены необходимые документы, подтверждающие неправомерность действий с Вашими персональными данными.

_____ осуществляет обработку Ваших персональных данных согласно требованиям следующих законодательных актов: _____
_____
_____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) М.П. (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

На Ваш запрос от «____» _____ 20___ г., относительно неправомерности действий с персональными данными г-на/г-ки _____ могу сообщить следующее.

_____ не может уничтожить персональные данные г-на/г- ки _____, так как факт неправомерности действий с персональными данными г-на/г-ки _____ не подтвержден и Вами не были предоставлены необходимые документы, подтверждающие неправомерность действий с персональными данными г-на/г-ки _____.

_____ осуществляет обработку Ваших персональных данных согласно требованиям следующих законодательных актов: _____
_____
_____

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) М.П. (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Форма уведомления субъекта персональных данных, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных при достижении целей обработки ПДн

Г-ну/Г-ке_____

В связи с достижением целей обработки Ваших персональных данных могу сообщить следующее.

_____ была прекращена обработка и уничтожены Ваши персональные данные: _____
_____
_____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

В связи с достижением целей обработки персональных данных г-на/г-ки _____ могу сообщить следующее.

_____ была прекращена обработка и уничтожены персональные данные г-на/г-ки _____: _____
_____
_____

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) М.П. (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Г-ну/Г-ке_____

На Ваш запрос от «___» _____ 20___ г. относительно достижения целей обработки Ваших персональных данных могу сообщить следующее.

_____ не может прекратить обработку и уничтожить Ваши персональные данные, так как их обработка осуществляется согласно _____
_____
_____

Если у Вас есть вопросы, связанные с обработкой Ваших персональных данных, пожалуйста, обращайтесь.

С уважением, _____ _____ _____
(должность) М.П. (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Законному представителю г-на/г-ки
(Уполномоченному органу по защите прав
субъектов персональных данных)
(выбрать необходимое)

На Ваш запрос от «___» _____ 20___ г., относительно достижения целей обработки персональных данных г-на/г-ки _____ могу сообщить следующее.

_____ не может прекратить обработку и уничтожить персональные данные г-на/г-ки _____, так как их обработка осуществляется согласно _____
_____
_____

Если у Вас есть вопросы, связанные с обработкой персональных данных г-на/г-ки _____, пожалуйста, обращайтесь.

С уважением, _____ М.П. _____ _____
(должность) (подпись) (Фамилия, инициалы)

«____» _____ 20___ г.

Приложение 21
к приказу от «22» ноября 2021г. № 187

Правила
работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн «ИАСПСР», необходим для выполнения ими трудовых обязанностей

1. Общие положения

Лицами, участвующими в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн «ИАСПСР» являются сотрудники _____ (далее - Учреждение) в соответствии с утвержденным Перечнем лиц в Учреждении, доступ которых к персональным данным, обрабатываемым в ИСПДн «ИАСПСР», необходим для выполнения ими трудовых обязанностей (далее – Пользователи).

Пользователи должны принимать все необходимые меры по защите персональных данных (далее – ПДн) и контролю за соблюдением прав доступа к ней.

Пользователи ИСПДн в своих трудовых обязанностях обязаны руководствоваться настоящими Правилами и должны быть ознакомлены под роспись с настоящим документом и предупреждены об индивидуальной ответственности за его нарушение.

Основными задачами при обработке ПДн в ИСПДн являются:

обеспечение исполнения требований нормативных правовых актов, руководящих документов, регламентирующих защиту ПДн в Российской Федерации в процессе создания, хранения, передачи и удаления документов, содержащих ПДн в ИСПДн Учреждения;

обеспечение в ИСПДн необходимого уровня безопасности обработки, хранения и передачи ПДн;

обеспечение необходимого уровня безопасности носителей ПДн;

обеспечение безопасности ПДн при ее копировании, размножении.

2. Обязанности лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими трудовых обязанностей

При первичном допуске к работе в ИСПДн пользователь изучает требования настоящего документа, разрешительную систему доступа к ИСПДн, технологический процесс обработки информации в ИСПДн, руководящие, нормативно-методические и организационно-распорядительные документы по вопросам обеспечения безопасности ПДн.

Каждый пользователь ИСПДн, имеющий доступ к автоматизированному рабочему месту (далее – АРМ), программному

обеспечению (далее – ПО) и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

строго соблюдать установленные правила обеспечения безопасности ПДн при работе с программными и техническими средствами ИСПДн, в том числе положения настоящего документа;

знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

при работе в ИСПДн выполнять только те обязанности, которые прописаны в должностной инструкции;

не разглашать известные им ПДн лицам, не имеющим допуска к этим ПДн;

располагать во время работы экран монитора в помещении так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами, и основные технические средства и системы (далее – ОТСС) в соответствии с Техническим паспортом на ИСПДн;

помнить свой идентификатор и пароль;

держать свой пароль в тайне, а именно не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения (в том числе других сотрудников Учреждения, в т.ч. руководителей) личный пароль;

осуществлять ввод пароля только в условиях, исключающих его просмотр;

не хранить записки-памятки с личным паролем на видном и/или в легко доступном месте: на столе, на мониторе, под клавиатурой, в верхнем ящике стола и т.п.;

своевременно сообщать ответственному за обеспечение безопасности ПДн в ИСПДн (далее – администратор информационной безопасности ИСПДн) о фактах компрометации пароля (когда пароль стал или может быть известен еще кому – либо кроме его владельца), об утере или повреждении аппаратного идентификатора и в этих случаях не использовать ИСПДн до специального разрешения администратора информационной безопасности ИСПДн;

немедленно известить администратора информационной безопасности ИСПДн в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

при работе в ИСПДн использовать только учтенные съемные машинные носители ПДн, при обоснованной необходимости использования неучтенных носителей согласовывать использование с администратором информационной безопасности ИСПДн. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;

при работе со съемными машинными носителями ПДн каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями Инструкции по организации антивирусной защиты в ИСПДн;

выполнять требования Инструкции по организации антивирусной защиты в ИСПДн в полном объеме;

осуществлять установленным порядком уничтожение ПДн с машинных носителей ПДн (с помощью сертифицированного средства защиты информации от несанкционированного доступа (далее – НСД);

немедленно выполнять предписания администратора информационной безопасности ИСПДн в части обеспечения безопасности ПДн;

соблюдать установленный режим разграничения доступа к информационным ресурсам;

все изменения конфигурации технических и программных средств ИСПДн, ремонт, модификация и техническое обслуживание технических средств и систем, входящих в состав ИСПДн, производить только по согласованию с администратором информационной безопасности ИСПДн;

обеспечить сохранность оборудования и системных блоков компьютеров;

при отсутствии необходимости работы компьютера выключить (блокировать нажатием клавиш Windows+L) его;

при работе в сети Интернет:

обращать внимание на URL-адреса страниц, на которых он вводит учетные данные;

проверять наличие https-соединения для сайтов, на которых он собирается ввести учетные данные;

проверять реальные адреса гиперссылок, наводя на них курсор. Адрес, куда ведёт эта ссылка, будет отображён в левой нижней части браузера;

отвечать на письма и переходить по ссылкам, содержащимся в письмах от неизвестных отправителей только после проверки личности отправителя (организации) письма через поисковые системы или официальные сайты;

отключить функцию запоминания паролей;

использовать разные адреса электронной почты для деловой переписки, совершения финансовых операций и регистрации в различных социальных сетях и сайтах.

3. Права лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими трудовых обязанностей

Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для обработки, хранения и транспортировки ПДн разрешается использовать в ИСПДн только те машинные носители ПДн, которые учтены в «Журнале учета машинных носителей персональных данных».

Пользователь ИСПДн имеет право участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи ПДн и технических компонентов ИСПДн, если данное нарушение произошло под его идентификационными данными.

Своевременно получать доступ к информационным ресурсам ИСПДн, необходимым ему для выполнения своих должностных обязанностей.

Требовать от администратора информационной безопасности ИСПДн смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

4. Лицам, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими трудовых обязанностей, запрещается

Пользователю ИСПДн категорически запрещается:

самостоятельно устанавливать, тиражировать или модифицировать ПО, изменять установленный алгоритм функционирования технических и программных средств, устанавливать или удалять установленные администратором информационной безопасности ИСПДн сетевые программы на компьютерах, вскрывать компьютер, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование;

запускать любые системные или прикладные программы, не входящие в состав ПО;

использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного ПО АРМ;

записывать и хранить ПДн на неучтенных машинных носителях ПДн (гибких магнитных дисках, флэш-накопителях и т.п.);

оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители ПДн и распечатки, содержащие ПДн;

умышленно использовать недокументированные свойства и ошибки в ПО или в настройках средств защиты ПДн;

размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей ПДн;

осуществлять попытки НСД к ресурсам ИСПДН, проводить или участвовать в сетевых атаках и сетевом взломе;

производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов;

привлекать посторонних лиц для производства ремонта ОТСС без письменной заявки и согласования с администратором информационной безопасности ИСПДн;

отключать (блокировать) средства защиты информации;

сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ИСПДн;

хранить на учтенных носителях программы и данные, не относящиеся к рабочей информации;

выполнять работы с документами, содержащими ПДн, на дому, выносить их за пределы контролируемой зоны;

вводить в ОТСС ПДн под диктовку или с микрофона;

закрывать доступ к информации паролями без согласования с администратором информационной безопасности ИСПДн;

передавать свои учетные носители кому-либо;

запускать файлы-вложения, которые содержатся в спам-письмах;

сообщать приватную информацию, запрашиваемую в письмах, приходящих по электронной почте и сообщениях в электронных мессенджерах;

передавать защищаемую информацию с рабочего места, на котором установлено контрафактное ПО;

использовать в паролях даты, имена, номера телефонов и другой персональной информации, которая может быть угадана или найдена в открытых источниках.

5. Действия при обнаружении попыток несанкционированного доступа

К попыткам НСД относятся:

сеансы работы с ПДн незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к ПДн;

действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора информационной безопасности ИСПДн или другого

пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

При выявлении факта несанкционированного доступа (далее – НСД) лицо, выявившее факт НСД (пользователь, ответственный за организацию обработки ПДн, ответственный за контроль выполнения требования по обработке ПДн в ИСПДн, администратор информационной безопасности ИСПДн) обязан:

законными способами прекратить НСД к ПДн;

известить администратора информационной безопасности ИСПДн о факте НСД;

известить руководителя пользователя, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

известить директора Учреждения.

6. Порядок модификации конфигураций технических и программных средств ИСПДн

Право внесения изменений в конфигурацию аппаратно-программных средств защиты ИСПДн предоставляется администратору информационной безопасности ИСПДн:

в отношении системных и прикладных программных средств - по согласованию (в случае, если проводилась аттестация) с аттестационной комиссией, проводившей аттестацию данной ИСПДн;

в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты - по согласованию (в случае, если проводилась аттестация) с аттестационной комиссией, проводившей аттестацию данной ИСПДн.

Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных лиц, запрещено.

Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн, а также средств защиты информации инициируется заявкой начальника отдела.

В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн;

обновление (замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);

изменение настроек средств защиты информации;

удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

Также в заявке указывается условное наименование ИСПДн.

Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного ПО, которые можно решать с использованием указанного компьютера.

Заявку начальника отдела, в которой требуется произвести изменения конфигурации, рассматривает директор, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору информационной безопасности ИСПДн для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке ИСПДн.

Подготовка обновления, модификации общесистемного и прикладного ПО ИСПДн, тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного ПО, внесение необходимых изменений в настройки системы защиты информации от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором информационной безопасности ИСПДн по согласованию с аттестационной комиссией (в случае, если проводилась аттестация), проводившей аттестацию данной ИСПДн. Работы производятся в присутствии начальника отдела.

Установка и обновление ПО (системного, тестового и т.д.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком, прикладного ПО – с эталонных копий программных средств, полученных из архива дистрибутивов установленного ПО.

Все добавляемые программные и аппаратные компоненты должны быть предварительно установленным порядком проверены на работоспособность, а также отсутствие опасных функций.

После установки (обновления) ПО, администратор информационной безопасности ИСПДн должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО, правильность их настройки и произвести соответствующую запись в «Журнале учета выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн», сделать отметку о выполнении (на обратной стороне заявки) и в Техническом паспорте на ИСПДн.

При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, начальник отдела докладывает об этом администратору информационной безопасности ИСПДн, который в свою очередь связывается с аттестационной комиссией (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкций. В данном случае администратор информационной безопасности ИСПДн обязан предпринять необходимые меры для удаления ПДн с помощью сертифицированного средства защиты информации от НСД, которые

хранились на компьютере. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров, с отметками о внесении изменений в состав программных средств, должны храниться вместе с Техническим паспортом на ИСПДн и «Журналом учета выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у администратора информационной безопасности ИСПДн для:

восстановления конфигурации ИСПДн после аварий;

контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;

проверки правильности установки и настройки средств защиты информации, факта уничтожения ПДн, находившихся на компьютере, который оформляется актом и подписывается администратором информационной безопасности ИСПДн и начальником отдела.

7. Порядок учета, хранения и выдачи машинных носителей персональных данных

Порядок хранения и учета машинных носителей ПДн:

машинные носители, содержащие ПДн, подлежат обязательному учету администратором информационной безопасности ИСПДн. Учет осуществляется с помощью «Журнала учета машинных носителей ПДн»;

учет машинных носителей ПДн включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей, номер инвентарного учета и иные номера;

носители должны храниться в сейфе, расположенном в помещении Учреждения, и изыматься только для выполнения должностных обязанностей;

при поступлении нового машинного носителя, который будет использоваться для хранения или передачи ПДн, администратор информационной безопасности ИСПДн регистрирует его в «Журнале учета машинных носителей ПДн».

Порядок регистрации выдачи машинных носителей ПДн:

учет выдачи машинных носителей ПДн ведется в «Журнале учета машинных носителей ПДн», в котором указывается регистрационный (учетный) номер машинного носителя ПДн, дата, время, фамилия, имя и отчество должностного лица, получившего машинный носитель ПДн, его роспись;

в случае возврата должностным лицом машинного носителя ПДн в «Журнале учета машинных носителей ПДн» администратором информационной безопасности ИСПДн проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

Доступ к машинным носителям ПДн осуществляется в соответствии с перечнем должностей, физический доступ которых к машинным носителям ПДн необходим для выполнения ими трудовых обязанностей, который представлен в приложении 1 к настоящим правилам.

9. Порядок работы с файлами документов, внесение корректировок, уничтожение, хранение документов

№ п/п	Этап	Описание этапа
Подготовка к обработке информации		
1.	Получение допуска к работе	Допуск сотрудников к ИСПДн осуществляется в соответствии с Перечнем лиц в Учреждении, доступ которых к персональным данным, обрабатываемым в ИСПДн «ИАСПСР», необходим для выполнения ими трудовых обязанностей и Разрешительной системой доступа пользователей к сведениям конфиденциального характера ИСПДн. Права по доступу к информационным ресурсам должны быть определены утвержденной Разрешительной системой доступа пользователей к сведениям конфиденциального характера ИСПДн.
2.	Вход пользователя в систему	Пользователь авторизуется на своем рабочем месте средствами ОС. Для получения доступа в ИСПДн «ИАСПСР» проходит идентификацию и аутентификацию в ЕСИА или указывает логин и пароль действующей учетной записи. Пользователь получает доступ к информации в ИСПДн «ИАСПСР» в соответствии со своей ролью и соответствующими ей правами. Разграничение доступа обеспечивается средствами модуля авторизации и набором системных привилегий, средствами СУБД.
Обработка информации		
1.	Регистрация времени начала работы	Осуществляется штатными средствами прикладного ПО.
2.	Ввод обрабатываемых исходных данных в систему	Ввод в систему обрабатываемых ПДн производится вручную с клавиатуры.
3.	Обработка текстовой информации	Пользователь обязан принять меры по исключению возможности просмотра обрабатываемых ПДн с экрана монитора и с бумажных носителей (в том числе распечатываемых материалов) лицами, не допущенными к ПДн.
Сохранение результатов обработки информации		
1.	Распечатка документов	Распечатка документов (данных) производится на принтере, входящем в состав ОТСС объекта информатизации, при этом не ведется учет распечатанных документов.

№ п/п	Этап	Описание этапа
2.	Сохранение окончательных результатов работы	Готовые данные в электронном виде хранятся на АРМ пользователя и на учтенном съемном носителе ПДн. Готовые данные в бумажном виде хранятся в кабинетах здания.
3.	Передача носителей ПДн и распечатанных документов	В соответствии с требованиями организационно-распорядительных документов Учреждения.
4.	Очистка остаточной (удаленной) информации	Гарантированная очистка удаляемых ПДн с машинных носителей ПДн (без возможности ее восстановления) осуществляется сертифицированными средствами защиты информации от НСД.
5.	Регистрация времени работы и действий пользователя в системе	Осуществляется штатными средствами прикладного ПО.
6.	Завершение работы	После окончания работы с ИСПДн пользователь обязан на своем рабочем месте завершить работу всех программ, входящих в состав специализированного ПО и выключить компьютер (перегрузить). При необходимости оставить свое рабочее место на непродолжительное время пользователь обязан его заблокировать (дальнейшая работа может быть продолжена пользователем только после ввода его логина и пароля). После окончания рабочего дня необходимо закрыть окна и форточки, выключать электроприборы и запереть дверь.

10. Ответственность лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими трудовых обязанностей

Персональную ответственность за соблюдение установленных требований настоящего положения несут пользователи ИСПДн и администратор информационной безопасности ИСПДн.

За разглашение ПДн и нарушение порядка обращения с машинными носителями ПДн администратор информационной безопасности ИСПДн, а также пользователи ИСПДн, работающие с этими машинными носителями ПДн, могут быть привлечены к дисциплинарной и иной, предусмотренной законодательством Российской Федерации, ответственности.

Пользователи несут персональную ответственность за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование ПДн, нарушение работы компьютеров пользователей ИСПДн или ИСПДн в целом, может повлечь ответственность в соответствии с действующим законодательством.

Приложение 22
к приказу от «22» ноября 2021г. № 187

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Общие положения

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в _____ (далее - Учреждение) требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Правила), разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных (далее – ПДн), а также определяют основания, порядок и методы проведения внутреннего контроля соответствия обработки ПДн требованиям законодательства Российской Федерации.

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям защиты персональных данных

В целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям к защите ПДн в Учреждении организовывается проведение ежегодных проверок.

Проверки проводятся комиссией по защите информации с привлечением руководителя структурного подразделения, эксплуатирующего ИСПДн «ИАСПСР» (начальника отдела).

Плановые проверки условий обработки ПДн проводятся на основании приказа директора Учреждения.

Внеплановые проверки проводятся на основании поступившей информации о нарушениях правил обработки ПДн, по инициативе ответственного за организацию обработки ПДн, либо ответственного за обеспечение безопасности ПДн в ИСПДн. Проведение внеплановой проверки организуется в течение 3 рабочих дней со дня поступления информации о нарушениях правил обработки ПДн.

Проверки условий обработки ПДн осуществляются непосредственно на месте обработки ПДн путем опроса либо, при необходимости, путем осмотра служебных мест сотрудников Учреждения, участвующих в процессе обработки ПДн.

При проведении проверки должны быть полностью, объективно и всесторонне, установлены:

соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Учреждения;

соответствие объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;

достаточность (избыточность) ПДн для целей обработки ПДн, заявленных при сборе ПДн;

отсутствие (наличие) объединения, созданных для несовместимых между собой целей, баз данных информационных систем ПДн;

порядок и условия применения организационных и технических мер по обеспечению безопасности ПДн при их обработке, необходимых для выполнения требований к защите ПДн, исполнение которых обеспечивает установленные уровни защищенности ПДн;

порядок и условия соблюдения парольной защиты;

порядок и условия соблюдения антивирусной защиты;

эффективность принимаемых мер по обеспечению безопасности ПДн в ИСПДн;

условия соблюдения режима защиты при подключении к информационно-телекоммуникационным сетям;

порядок и условия обновления программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн;

порядок и условия применения средств защиты информации;

соблюдение учета носителей ПДн;

соблюдение правил доступа к ПДн;

соблюдение порядка доступа в помещения, в которых ведется обработка ПДн;

наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;

мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

осуществление мероприятий по обеспечению целостности ПДн.

Комиссия по защите информации, а также ответственные за контроль выполнения требований по обработке ПДн в ИСПДн в ходе проверки имеют право:

запрашивать у сотрудников информацию, необходимую для реализации своих полномочий;

требовать от уполномоченных на обработку ПДн сотрудников уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;

принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;

вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПДн при их обработке;

вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПДн.

Проверка условий обработки ПДн должна быть завершена не позднее чем через тридцать календарных дней со дня принятия решения о ее проведении.

По результатам проведенной проверки условий обработки ПДн оформляется Акт о результатах проведения плановой проверки состояния защиты персональных данных.

Приложение 23
к приказу от «22» ноября 2021г. № 187

ПОРЯДОК
уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

1. Общие положения

Настоящий документ устанавливает порядок уничтожения персональных данных (далее – ПДн) при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2. Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

Документы, дела, книги и журналы учета, содержащие ПДн, при достижении целей обработки или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Вопрос об уничтожении документов, содержащих ПДн, рассматривается на заседании Комиссии по защите информации.

Уничтожение документов производится в присутствии всех членов комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (проводится комиссией по классификации информационных систем и определению уровней защищенности ПДн). Результаты уничтожения документов оформляются актом (акт составляется в свободной форме).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста, или сжигаются.

После уничтожения материальных носителей членами комиссии подписывается акт в двух экземплярах, а также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с помощью сертифицированного средства защиты информации от несанкционированного доступа с гарантированной очисткой информации, установленной на АРМ.

Информация, содержащая ПДн, при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.