АДМИНИСТРАЦИЯ

КАРГОПОЛЬСКОГО МУНИЦИПАЛЬНОГО ОКРУГА

АРХАНГЕЛЬСКОЙ ОБЛАСТИ

П О С Т А Н О В Л Е Н И Е

от «1» июня 2021 года № 539

г. Каргополь

Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных администрации Каргопольского муниципального округа

В соответствии со статьей 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказами ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», администрация Каргопольского муниципального округа **п о с т а н о в л я е т**:

1. Утвердить прилагаемые:

- положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных администрации Каргопольского муниципального округа;
- инструкцию по организации парольной защиты в информационных системах персональных данных администрации Каргопольского муниципального округа;

– инструкцию по организации антивирусной защиты в информационных системах персональных данных администрации Каргопольского муниципального округа;

– инструкцию по безотказному функционированию, резервированию и восстановлению работоспособности технических средств и программного обеспечения в информационных системах персональных данных администрации Каргопольского муниципального округа;

– Положение о разрешительной системе допуска к информационным ресурсам информационных систем персональных данных администрации Каргопольского муниципального округа.

2. Настоящее постановление подлежит официальному опубликованию.

Глава Каргопольского
муниципального округа Н.В. Бубенщикова

Утверждено
постановлением
администрации Каргопольского
муниципального округа
Архангельской области
от 1 июня 2021 г. № 539

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных администрации Каргопольского муниципального округа

1. Общие положения

1.1. Настоящее Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных администрации Каргопольского муниципального округа (далее – Положение) определяет порядок выполнения мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации Каргопольского муниципального округа (далее – ИСПДн).

1.2. Безопасность персональных данных при их обработке в информационных системах администрации Каргопольского муниципального округа (далее-администрация) обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны соответствовать устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

1.3. Положение обязательно для исполнения всеми сотрудниками администрации, непосредственно осуществляющими обработку и защиту персональных данных в ИСПДн. Нарушение правил защиты персональных данных, определённых Положением, влечёт материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с нормами действующего законодательства Российской Федерации.

2. Основные понятия и определения

2.1. Администратор информационной безопасности (далее – администратор ИБ) - сотрудник администрации, ответственный за защиту информационных систем от несанкционированного доступа к информации.

2.2. Администратор ИСПДн – сотрудник администрации, ответственный за функционирование информационной системы в установленном штатном режиме работы.

2.3. Доступ к информации - возможность получения информации и ее использования.

2.4. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

2.5. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.6. Инцидент информационной безопасности - появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации технологического процесса и создания угрозы информационной безопасности (отказ в обслуживании, сбор информации, несанкционированный доступ и т.д.).

2.7. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

2.8. Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

2.9. Обладатель информации (информационного ресурса) - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

2.10. Обработка - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

2.11. Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие

обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

2.13. Событие информационной безопасности - идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

2.14. Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

2.15. Угроза безопасности информации - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при ее обработке в информационной системе.

2.16. Уничтожение информации - действия, в результате которых становится невозможным восстановить содержание информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации.

3. Возложение ответственности за обеспечение безопасности ПДн

3.1. Для каждой из ИСПДн, в отношении которой установлена необходимость обеспечения 3 уровня защищённости, распоряжением администрации назначается должностное лицо, ответственное за обеспечение безопасности персональных данных при их обработке в данной ИСПДн (далее – Ответственное лицо за ИСПДн). При этом одно должностное лицо может являться ответственным за обеспечение безопасности персональных данных при их обработке в нескольких ИСПДн.

3.2. Администрация определяет и осуществляет организационные и технические мероприятия, необходимые и достаточные в соответствии с требованиями действующего законодательства Российской Федерации для обеспечения безопасности персональных данных при их обработке в ИСПДн.

3.3. Администрация устанавливает требования к организационным и техническим мероприятиям, которые должна выполнять организация, осуществляющая доступ к ИСПДн.

4. Основные мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн

4.1. Администрация обязана определить необходимый уровень защищённости ПДн при их обработке в каждой из ИСПДн, оператором которой она является.

4.2. Администрация разрабатывает модель угроз безопасности персональных данных для каждой из ИСПДн.

4.3. Администрация определяет состав и содержание мер по обеспечению безопасности персональных данных при их обработке в ИСПДн на основании приказа ФСТЭК России от 18 февраля 2013 г. № 21 или приказа ФСТЭК России от 11 февраля 2013 г. № 17 (для муниципальных информационных систем), приказа ФСБ России от 10 июля 2014 г. № 378 (при использовании средств криптографической защиты информации), модели угроз безопасности персональных данных в ИСПДн и осуществляет организационные и технические мероприятия для реализации указанных мер.

4.4. Администрация самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации, проводит оценку эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных. Указанная оценка проводится не реже одного раза в 3 года.

Решение по форме оценки эффективности и документов, разрабатываемых по результатам (в процессе) оценки эффективности, принимается администрацией самостоятельно и (или) по соглашению с лицом, привлекаемым для проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных.

Оценка эффективности реализованных мер может быть проведена в рамках работ по аттестации ИСПДн в соответствии с национальным стандартом ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

4.5. Администрация должна обеспечить выполнение следующих мероприятий:

1) организация режима обеспечения безопасности помещений, в которых размещены ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

2) обеспечение сохранности носителей персональных данных;

3) актуальность утвержденного распоряжением главы Каргопольского муниципального округа документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей;

4) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз, при этом

сертификаты на средства защиты информации должны быть действительными;

5) назначение ответственного лица для каждой ИСПДн (для ИСПДн, для которой установлена необходимость обеспечения 3 уровня защищённости и выше).

4.6. Лицо, ответственное за организацию обработки персональных данных, получив информацию о факте нарушения действующих законодательных норм по обеспечению безопасности персональных данных в ИСПДн администрации, организует служебное расследование для выявления лиц, в результате действий или бездействия которых произошло нарушение законодательных норм по обеспечению безопасности персональных данных. К такому расследованию могут привлекаться сторонние организации, которым предоставлен доступ в ИСПДн.

Приложение № 1
к Положению об обеспечении безопасности
персональных данных при их обработке в информационных
системах персональных данных администрации
Каргопольского муниципального округа

Форма «Журнала учета средств защиты информации, эксплуатационной и технической документации к ним»

Левая сторона разворота журнала

N п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кого получены или Ф.И.О. сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении
1	2	3	4	5	6	7	8	9

Правая сторона разворота журнала

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
10	11	12	13	14	15	16

Приложение № 2
к Положению об обеспечении безопасности
персональных данных при их обработке в
информационных системах персональных данных
администрации Каргопольского муниципального
округа

Форма «Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (для обладателя конфиденциальной информации)»

Левая сторона разворота журнала

№ п.п	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографиические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
1	2	3	4	5	6	7	8

Правая сторона разворота журнала

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Утверждена
постановлением администрации
Каргопольского муниципального
округа от «___» июня 2020 года № _____

ИНСТРУКЦИЯ

по организации парольной защиты в информационных системах персональных данных администрации Каргопольского муниципального округа

1. Общие положения

1.1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных в администрации, а также контроль за действиями пользователей администраторами ИСПДн при работе с паролями.

1.2. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей в информационных системах ИСПДн и контроль за действиями пользователей и обслуживающего персонала систем при работе с паролями возлагается на администратора ИСПДн и администратора ИБ.

2. Правила формирования пароля

2.1. Персональные пароли должны создаваться администраторами ИСПДн с отметкой в журнале генерации (смены) паролей либо генерироваться специальными программными средствами с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в составе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (“ ~ # % ^ * ( ) - + = !);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- личный пароль пользователь не имеет права сообщать никому;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

2.2. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

2.3. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администраторов ИСПДн. Для генерации «стойких» значений паролей могут применяться специальные программные средства.

3. Ввод пароля

3.1. При вводе пароля пользователю необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам).

4. Порядок блокировки учетных записей при неуспешных попытках ввода пароля.

4.1. В зависимости от требуемого уровня защищенности (класса защищенности) персональных данных в ИСПДн устанавливаются следующие максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки учетной записи (программного обеспечения, программно-аппаратного средства) и время блокировки:

- для 4 уровня защищенности (класса защищенности) максимальное количество неуспешных попыток аутентификации от 3 до 10 попыток, время блокировки от 3 до 15 минут;
- для 3 уровня защищенности (класса защищенности) максимальное количество неуспешных попыток аутентификации от 3 до 10 попыток, время блокировки от 5 до 30 минут;

5. Порядок смены личных паролей пользователей ИС

5.1. Полная плановая смена паролей пользователей ИСПДн должна проводиться:

- для 4 уровня защищенности (класса защищенности) не более чем через 180 дней;
- для 3 уровня защищенности (класса защищенности) не более через 120 дней;

5.2. При возникновении нештатных ситуаций, форс-мажорных обстоятельств, производственной и технологической необходимости использования имен и паролей некоторых пользователей в их отсутствие, сменившие пароль сотрудники, обязаны сразу же после смены паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение администратору ИСПДн или администратору ИБ.

5.3. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри учреждения и т.п.) должна производиться администратором ИСПДн немедленно после окончания последнего сеанса работы данного пользователя с системой.

5.4. Срочная (внеплановая) полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри учреждения и другие обстоятельства) администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой информационной системы персональных данных в администрации.

5.5. Временный пароль, заданный администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

6. Хранение пароля и контроль за использованием пароля

6.1. Пользователям ИСПДн запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

6.2. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6.3. Хранение пользователями ИСПДн значений своих паролей на бумажном носителе допускается в запечатанном конверте или в журнале в запирающимся на ключ металлическом шкафу (сейфе) у администратора ИС или администратора ИБ.

6.5. Повседневный контроль за действиями пользователей ИСПДн и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора ИСПДн.

7. Действия в случае утери или компрометации пароля

7.1. В случае утери или компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п. 5.3. или п. 5.4. настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

8. Ответственность при организации парольной защиты

8.1. Владельцы паролей – пользователи ИСПДн должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

8.2. Периодический контроль за соблюдением требований настоящей Инструкции возлагается на администратора ИБ.

Приложение №1
к инструкции по организации парольной защиты в информационных системах персональных данных администрации Каргопольского муниципального округа

Форма журнала генерации (смены) паролей

№	Наименование ИСПДн	Ф.И.О. выдавшего пароль	Ф. И. О. владельца пароля	Персональный идентификатор	Содержание пароля	Дата выдачи	Подпись
1	2	3	4	5	6	7	8

Утверждена
постановлением администрации
Каргопольского муниципального округа
от «1» 06 2021 года № 539

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационных системах персональных данных администрации Каргопольского муниципального округа

1. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты ИСПДн от воздействия вредоносных компьютерных программ (вирусов), применению средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации) и устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих ИСПДн за их выполнение.

1.2. К использованию в ИСПДн допускаются только сертифицированные средства антивирусной защиты.

1.3. В случае необходимости использования новых антивирусных средств их применение необходимо согласовать с администраторами ИСПДн и администратором ИБ.

1.4. Установка средств антивирусной защиты на компьютере (сервере) ИСПДн осуществляется администратором ИСПДн, а настройка - администратором ИБ. Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств. Пользователи ИСПДн не должны иметь доступа к изменению настроек параметров средств антивирусной защиты.

2. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме должна запускаться проверка важных областей (содержимое системной памяти, объекты автозапуска, загрузочные сектора).

2.2. Обязательной антивирусной проверке подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, вложения электронной почты и т. п.), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях

-флэш-дисках, CD-DVD дисках и т.п.

2.3. Полная проверка компонентов ИСПДн (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных программ должна проводиться не реже одного раза в месяц.

2.4. Устанавливаемое программное обеспечение должно быть предварительно проверено администратором ИБ на отсутствие вредоносных программ. Непосредственно после установки или изменения программного обеспечения компьютера, должна быть выполнена антивирусная проверка.

2.5. При возникновении подозрения на наличие вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИСПДн должен провести внеочередную антивирусную проверку своей рабочей станции, а также обратиться к администратору ИБ или администратору ИСПДн.

2.6. В информационной системе при наличии технической возможности должно быть реализовано оповещение администратора ИБ в масштабе времени, близком к реальному, об обнаружении вредоносных программ (вирусов), неуспешном обновлении базы данных признаков вредоносных компьютерных программ (вирусов), сбоях в работе средств антивирусной защиты.

3. Действие пользователя в случае обнаружения вредоносных компьютерных программ (вирусов)

3.1. В случае обнаружения вредоносных программ (вирусов), зараженных файлов пользователи ИСПДн обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения администратора ИБ или администратора ИСПДн, владельца зараженных файлов (при возможности), а также сотрудников, использующих эти файлы в работе;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения вируса, не поддающегося лечению или удалению применяемыми средствами антивирусной защиты, обратиться к администратору ИБ или администратору ИСПДн.

4. Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

4.1. Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать:

1) получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);

2) получение из доверенных источников и установку обновлений базы

данных признаков вредоносных компьютерных программ (вирусов);

3) контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

4.2. При наличии технической возможности в ИСПДн должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов).

4.3. Обновление баз данных признаков вредоносных компьютерных программ (вирусов) должно проводиться каждый день автоматически или в ручном режиме пользователем ИСПДн при наличии источников обновлений в локально-вычислительной сети, в сети «Интернет», а при их отсутствии – администратором ИБ либо другими ответственными лицами учреждения с баз данных признаков вредоносных компьютерных программ (вирусов), записанных на внешние машинные носители информации, не реже 1 раза в неделю.

5. Ответственность

5.1. Ответственность за организацию антивирусного контроля в ИСПДн, в соответствии с требованиями настоящей Инструкции, возлагается на администратора ИСПДн.

5.2. Ответственность за проведение мероприятий антивирусного контроля на конкретном компьютере, имеющего доступ к информационным ресурсам ИСПДн и соблюдение требований настоящей Инструкции возлагается на пользователя ИСПДн.

5.3. Периодический контроль за состоянием антивирусной защиты ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется администратором ИБ.

Утверждена
постановлением администрации
Каргопольского муниципального округа»
от «___» _____ 2021 года № _____

ИНСТРУКЦИЯ

по безотказному функционированию, резервированию и восстановлению работоспособности технических средств и программного обеспечения в информационных системах персональных данных администрации Каргопольского муниципального округа

1. Общие положения

1.1. Инструкция по безотказному функционированию, резервированию и восстановлению работоспособности технических средств и программного обеспечения в ИСПДн (далее – Инструкция) определяет действия, связанные с безотказным функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящей Инструкции является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

1.3. Задачами данной Инструкции является:

- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных.

1.5. Ответственными сотрудниками за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор ИСПДн, пользователи ИСПДн.

1.6. Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов, приводящих к потере защищаемой информации, назначается далее – администратор ИБ.

2. Порядок реагирования на инцидент

2.1. В настоящей Инструкции под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.2. Все действия в процессе реагирования на инциденты должны документироваться администратором ИСПДн в Журнале учета инцидентов информационной безопасности.

2.3. Ответственные за реагирование на инциденты работники администрации (администратор ИСПДн, пользователь ИСПДн) предпринимают меры по восстановлению работоспособности.

3. Меры обеспечения непрерывности работы и восстановления информационных систем при возникновении инцидентов

3.1. Технические меры.

3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.1.2. Все помещения администрации, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами охранно-пожарной сигнализации.

3.1.3. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.1.4. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

- дублированные системы электропитания в устройствах;

- системы обеспечения отказоустойчивости.

3.1.5. Для обеспечения отказоустойчивости компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев могут использоваться методы кластеризации.

3.1.6. Для обеспечения требуемого времени восстановления информационных систем создается запас резервных технических средств (системные блоки, мониторы, сетевое оборудование, источники бесперебойного питания, жесткие диски)

3.1.7. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (CD/DVD-диск, съемный жесткий диск и т.п.).

3.2. Организационные меры

3.2.1. Резервное копирование и хранение данных должно осуществляться на периодической основе пользователем ИСПДн или администратором ИСПДн, либо автоматически по расписанию:

- для обрабатываемых персональных данных – не реже одного раза в неделю;

- для технологической информации – не реже одного раза в месяц;

- копии системного раздела серверов баз данных (операционная система, штатное и специальное программное обеспечение, программные средства защиты и т. п.) – не реже одного раза в месяц, и каждый раз перед установкой нового специального программного обеспечения, программных и программно-аппаратных средств защиты, внесением изменений в специальное программное обеспечение и средства защиты (обновление версий).

3.2.2. Носители, на которые произведено резервное копирование, должны быть пронумерованы, информация должная содержать дату проведения резервного копирования.

3.2.3. Резервное копирование информации, составляющей персональные данные, осуществляется на машинные носители информации, предназначенных для хранения персональных данных.

3.2.4. Информация о проведении резервного копирования заносится в Журнал резервного копирования по форме, приведенной в приложении к настоящей Инструкции.

3.2.5. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

3.2.6. В соответствии с настоящей Инструкцией для конкретных ИСПДн и средств резервирования и восстановления могут разрабатываться отдельные инструкции по резервированию и восстановлению (в том числе планы по действиям сотрудников при возникновении нештатных (аварийных)

ситуаций) с учетом работы и специфики программных средств, применяемых на данной ИСПДн.

4. Создание архива данных ИСПДн

4.1. Для обеспечения нормальной работы архива ИСПДн необходимо обеспечить следующее:

- пользователи ИСПДн совместно с администраторами ИСПДн обязаны определить часть информации подлежащей архивации;

- администратор ИСПДн определяют временной интервал проведения процесса архивации, исходя из технологических особенностей системы;

- для эффективного доступа к архивным данным информация, время доступа к которой является критичной величиной, записывается в соответствующую директорию (выделенную для хранения архивных копий) на диске сервера либо на учетный съемный машинный носитель информации (такой архив называется оперативным);

- с целью предотвращения переполнения диска сервера архив информации, потерявшей актуальность или время доступа к которой не является критичной величиной, переносится на учетный съемный машинный носитель информации, предназначенный для хранения персональных данных (такой архив называется основным);

- наиболее важная информация записывается одновременно как на диск сервера, так и на съемный машинный носитель.

- целостность и достоверность архивной информации проверяется администратором ИСПДн.

- архивная информация ИСПДн, размещенная на съемных машинных носителях, хранится в надежно запираемых шкафах либо в сейфе, причем копии хранятся отдельно от дубликатов.

4.2. Права на доступ к архиву должны быть определены в Матрице доступа пользователей к информационным ресурсам ИСПДн, постановлением администрации. Доступ иных лиц к данным хранящимся в архиве осуществляется на основании служебной записки главе Каргопольского муниципального округа.

4.3. Механизмы резервного копирования задействуются при модернизации и установке нового оборудования и прикладного программного обеспечения, обеспечивая перенос и резервирование данных на обновляемом рабочем месте.

4.4. Программные средства резервного копирования настраиваются таким образом, чтобы осуществлялось копирование открытых файлов, а также прав доступа на файлы и каталоги.

4.5. Процесс резервного копирования должен предусматривать перемещения и архивирования файлов локально на рабочих местах в дневное время, а операции по резервированию на постоянно включенных серверах – в нерабочее время вечером, ночью или в выходные дни.

5. Восстановление информации в случае аварийной ситуации

5.1. Выход из строя несистемных дисков (системных разделов) на сервере базы данных.

5.1.1. В случае выхода из строя дисков, не повлекшем за собой разрушения системного раздела или системного диска, на место неисправного диска вставляется новый или форматируется неисправный раздел (логический диск).

После этого производится восстановление данных, которые были на этом диске (разделе) с резервной копии.

5.1.2. В случае выхода из строя диска (раздела), которое повлекло за собой разрушение баз данных, следует:

- остановить работу сервера ИСПДн;
- заменить диск или отформатировать раздел;
- с резервной копии базы данных восстанавливаются последние архивные данные.

5.2. Выход из строя системных дисков на сервере базы данных ИСПДн.

Выполняются следующие действия:

- останавливается сервер;
- на место системных дисков на сервере вставляются новые диски;
- восстанавливается копия системного программного обеспечения данного сервера;
- запускается сервер баз данных (далее – БД).

5.3. При невозможности восстановления программного обеспечения (операционная система, специальное программного обеспечение, программные средства защиты) из резервных копий производится установка с дистрибутивов программного обеспечения и их настройка для обеспечения необходимого уровня защищенности информации. В случаях, когда восстановление работоспособности системы защиты информации невозможно, применяются компенсирующие меры защиты информации.

6. Ответственные за восстановление работоспособности ИС

6.1. Ответственность за организацию восстановительных работ несет администратор ИСПДн.

6.2. Восстановительными работами руководит администратор ИСПДн.

6.3. По окончанию восстановительных работ делается соответствующая запись в журнале регистрации работ технического паспорта ИСПДн (при необходимости).

Приложение № 1

к инструкции по безотказному функционированию, резервированию и восстановлению работоспособности технических средств и программного обеспечения в информационных системах персональных данных администрации Каргопольского муниципального округа

Журнал учета процедур резервного копирования

N п/п	Дата проведения резервного копирования	Наименование информационного массива информационной системы	Регистрационный (учетный, серийный) номер машинного носителя ин формации	Тип носителя	Подпись, Ф. И. О. специалиста
1	2	3	4	5	6

Приложение № 2

к инструкции по безотказному функционированию, резервированию и восстановлению работоспособности технических средств и программного обеспечения в информационных системах персональных данных администрации Каргопольского муниципального округа

Журнал учёта инцидентов информационной безопасности

Сведения об инцидентах					
Дата и время (инцидента)		Длительность (инцидента)	Наименование и характеристика отказавших: оборудования, Программного обеспечения, канала связи	Отказавший элемент	Краткая характеристика (инцидента)
Начало	Ликвидация				
1	2	3	4	5	6

Утверждено
постановлением администрации
Каргопольского муниципального округа
от «___» _____ 2021 года № _____

ПОЛОЖЕНИЕ
о разрешительной системе допуска к информационным ресурсам информационных систем персональных данных администрации Каргопольского муниципального округа

1. Общие положения

1.1. Настоящее Положение о разрешительной системе допуска к информационным ресурсам ИСПДн (далее - Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Разрешительная система доступа к информационным ресурсам ИСПДн представляет собой совокупность процедур оформления прав субъектов на доступ к информационным ресурсам (далее - ИР) администрации и обязанностей ответственных лиц, осуществляющих реализацию этих процедур.

1.3. Объектами доступа являются:

- ИР, обрабатываемые в ИСПДн (в том числе содержащие персональные данные), в виде баз данных, библиотек, архивов и на отдельных съемных носителях;

- технологическая информация системы защиты информации ИСПДн.

1.4. Субъектами доступа являются:

- уполномоченные работники администрации;

- уполномоченные органы государственной власти и юридические лица;

- физические лица - субъекты ПДн;

- уполномоченные представители субъектов ПДн;

- физические лица или представили юридических лиц, обслуживающие ИСПДн.

1.5 Субъекты доступа несут персональную ответственность за соблюдение ими установленного порядка обеспечения защиты ИР ИСПДн.

1.6. Ответственными лицами, осуществляющими реализацию процедур оформления и прав субъектов на доступ к ИР, являются:

- глава Каргопольского муниципального округа;
- ответственный за организацию обработки ПДн в администрации;
- начальники отделов администрации;
- администраторы ИСПДн администрации;
- администратор ИБ.

1.7. В ИСПДн выделяют следующие роли субъектов доступа

- пользователь ИСПДн;
- администратор ИСПДн;
- администратор ИБ.

1.8. Пользователям и администраторам назначаются минимально необходимые права и привилегии.

2. Порядок формирования информационных ресурсов ИСПДн администрации

2.1. Порядок формирования и использования информационных ресурсов ИСПДн администрации определяется ответственным за организацию обработки персональных данных в администрации.

2.2. Подлежащие защите информационные ресурсы ИСПДн включаются в перечень информационных ресурсов, подлежащих защите в ИСПДн администрации.

3. Допуск к информационным ресурсам ИСПДн администрации.

3.1. Наделение пользователей полномочиями доступа к информационным ресурсам ИСПДн администрации.

3.1.1. Необходимость доступа сотрудников к ИР ИСПДн администрации определяет начальник структурного подразделения пользователя ИСПДн на основании должностных (трудовых) обязанностей сотрудника. Допуск сотрудников к информации, содержащей персональные данные, осуществляется в объеме, необходимом для выполнения ими должностных обязанностей. Права доступа сотрудников к защищаемой информации определяются в Матрице доступа.

3.1.2. Основанием для предоставления (изменения либо прекращения) прав доступа пользователям ИСПДн администрации является письменная заявка, подписанная начальником структурного подразделения пользователя и согласованная с ответственным за организацию обработки персональных данных в администрации.

3.1.3. Согласованная заявка является разрешением на допуск и основанием для регистрации пользователя в ИСПДн администратором ИСПДн.

После получения заявки администратор ИСПДн производит необходимые

действия по созданию (изменению, удалению) учетной записи пользователя, присвоению ему пароля и заявленных прав доступа информационным ресурсам ИСПДн, включению его в соответствующие группы пользователей и другие необходимые действия.

Уникальное имя (учетная запись пользователя), под которым он регистрируется и осуществляет работу в системе, присваивается каждому пользователю ИСПДн для обеспечения персональной ответственности за свои действия. В случае производственной необходимости пользователю ИСПДн могут быть предоставлены несколько уникальных имен (учетных записей). Использование несколькими работниками при работе в ИСПДн одного и того же имени пользователя («группового имени») запрещается.

3.1.4. При изменении должностных обязанностей работника, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись пользователя на основании заявки начальника соответствующего структурного подразделения подлежит изменению (корректировке).

3.1.5. Администратор ИСПДн проводит регистрацию прав доступа к ИР, указанным в заявке, с отметкой изменений в Матрице доступа.

3.1.6. После внесения изменений в Матрицу доступа администратор ИБ производит настройку специализированных средств защиты рабочих станций (автоматизированных рабочих мест).

3.1.7. По результатам изменений в правах доступа администратор ИБ и администратор ИСПДн делают отметку об исполнении задания на бланке заявки.

3.1.8. Все изменения в правах доступа выполняются администраторами не позднее трех рабочих с момента получения заявки.

3.1.9. Блокирование учетных записей на время отпуска пользователей ИСПДн администрации осуществляется администратором ИСПДн по заявке начальника соответствующего структурного подразделения.

4. Отзыв прав доступа

4.1. При увольнении работников - пользователей ИСПДн и/или лишения их прав доступа к ресурсам ИСПДн начальник структурного подразделения, в котором работает пользователь, подает заявку на имя ответственного за организацию обработки персональных данных. Ответственный за организацию обработки персональных данных визирует заявку, утверждая тем самым лишение прав пользователя на доступ к ИР ИСПДн.

4.2. После визирования заявка поступает к соответствующему администратору ИСПДн и администратору ИБ.

4.3. Администратор ИСПДн удаляет учетные записи пользователя из всех указанных в заявке списков доступа, производит необходимые отметки в Матрице доступа.

Администратор ИБ:

- проводит смену (удаление) действующих настроек прав доступа на соответствующих средствах защиты в соответствии с изменившимися полномочиями;

- анализирует целостность данных, к которым имел доступ работник.

По результатам изменений в правах доступа администратор ИБ и администратор ИСПДн делают отметку об исполнении задания на бланке заявки.

Все изменения в правах доступа, связанные с увольнением пользователя ИСПДн, выполняются администраторами не позднее трех рабочих дней с момента получения заявки на внесение изменений.

5. Порядок и периодичность проверки прав пользователей

Проверка прав пользователей проводится администратором ИБ с периодичностью не реже одного раза в три месяца путем сравнения прав согласно утвержденной Матрице доступа с правами пользователей по доступу к ИР, указанными в Матрице доступа к ИР ИСПДн.

6. Допуск к информационным ресурсам ИСПДН администрации сторонних организаций

6.1. К организациям, деятельность которых не связана с выполнением функций ИСПДн, относятся в том числе:

- правоохранительные органы;
- судебные органы;
- органы статистики;
- органы исполнительной и законодательной власти субъектов Российской Федерации;
- подведомственные учреждения Каргопольского муниципального округа;
- средства массовой информации и др.

6.2. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций ИСПДн администрации, регламентируется законодательством Российской Федерации, приказами и распоряжениями министерств и служб, законодательно наделенных полномочиями на получение такой информации, а также настоящим Положением.

6.3. Доступ к информационным ресурсам ИСПДн администрации сторонних организаций осуществляется на основании письменных запросов, за исключением случаев, предусмотренных действующим законодательством.

В письменном запросе указывается:

- основание (с приведением ссылки на нормативный акт), в соответствии с которым предоставляется информация;

- для каких целей необходима информация;
- конкретное наименование предоставляемой информации и ее объем;
- способ доступа (предоставления).

6.4. Основанием для доступа (предоставления) информации служит резолюция главы Каргопольского муниципального округа на соответствующем документе (запросе).

7. Допуск к информационным ресурсам ИСПДН сторонних организаций, выполняющих работы на основании муниципального контракта (договора)

7.1. К организациям, выполняющим работы на основании муниципального контракта (договора), могут относиться:

- организации, оказывающие услуги связи;
- организации, осуществляющие монтаж и настройку ИСПДн, сопровождение программно-прикладного обеспечения и технических средств;
- организации, оказывающие услуги в области защиты информации (проведение обследований, монтаж и настройка средств защиты информации, контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);
- другие организации, оказывающие услуги по информационно-техническому обеспечению.

7.2. Порядок допуска определяется в муниципальном контракте на выполнение работ (оказание услуг) в соответствии с требованиями Федерального закона от 05 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Обязательным условием муниципального контракта является заключение соглашения о конфиденциальности (о неразглашении сведений, составляющих персональные данные, а также иной защищаемой информации, ставшей известной в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений).

7.3. Решением о допуске является подписанный в установленном порядке муниципальный контракт на выполнение работ или оказание услуг.

Приложение № 1
к Положению о разрешительной системе
допуска к информационным ресурсам
информационных систем персональных данных
администрации Каргопольского муниципального
округа

Матрица доступа пользователей к информационным ресурсам информационной системы

п/п	Фамилия, имя, отчество (идентификатор)	Должностные обязанности	Защищаемые информационные ресурсы и установленные права доступа				Примечание
			Наименование ресурса	Категория ресурса	Место хранения ресурса	Права по доступу к информации	
	2	3	4	5	6	7	9