АДМИНИСТРАЦИЯ
МУНИЦИПАЛЬНОГО РАЙОНА
ЧЕЛНО-ВЕРШИНСКИЙ
САМАРСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от 24.08.2020 № 92

Об обеспечении безопасности
персональных данных при их обработке
в информационных системах персональных данных
в администрации муниципального района
Челно-Вершинский Самарской области

С целью организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в администрации муниципального района Челно-Вершинский Самарской области, в соответствии с Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённым постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» :

1.Назначить лицом, ответственным за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в администрации муниципального района Челно-Вершинский Самарской области инженера-программиста администрации муниципального района Зотова Владимира Николаевича (далее – ответственный за обеспечение безопасности персональных данных).

2. Утвердить:

план мероприятий по защите персональных данных при их обработке в информационных системах персональных данных в администрации муниципального района Челно-Вершинский Самарской области (приложение № 1);

инструкцию администратора безопасности информационных систем персональных данных в администрации муниципального района Челно-Вершинский Самарской области (приложение № 2);

инструкцию пользователя информационных систем персональных данных в администрации муниципального района Челно-Вершинский Самарской области (приложение № 3);

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации информационной системе персональных данных в администрации муниципального района Челно-Вершинский Самарской области (приложение №4);

Форму журнала учета съемных носителей персональных данных (приложение №5);

3. Ответственному за выполнение работ по обеспечению безопасности персональных данных организовать учет носителей персональных данных.

4. Запретить сотрудникам, имеющим доступ к персональным данным, использовать для хранения и обработки персональных данных носители информации, не поставленные на учет в установленном порядке.

5. Распоряжение довести до сотрудников администрации муниципального района Челно-Вершинский Самарской области в части их касающейся.

6. Установить, что действие настоящего распоряжения не распространяется:

на муниципальные органы, являющимися структурными подразделениями администрации муниципального района Челно-Вершинский Самарской области и наделёнными статусом юридического лица;

на отношения, возникающие при обработке персональных данных, отнесённых в установленном порядке к сведениям, составляющим государственную тайну.

7. Контроль за исполнением данного распоряжения возлагаю на себя.

Глава муниципального района
Челно-Вершинский В.А. Князькин

Приложение N 1
к распоряжению администрации
муниципального района Челно-Вершинский
Самарской области
от 24.08.2020 N 92

План мероприятий по защите персональных данных при их обработке в информационных системах персональных данных в администрации муниципального района Челно-Вершинский Самарской области

Мероприятие	Периодичность	Ответственный
Организационные мероприятия		
Осуществление внутреннего контроля за соблюдением сотрудниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных	Согласно плана проведения внутреннего контроля	Комиссия по осуществлению внутреннего контроля соответствия обработки персональных данных в администрации муниципального района Челно-Вершинский Самарской области требованиям к защите персональных данных

Доведение до сведения положения законодательства РФ о персональных данных, разработанных внутренних локальных актов по вопросам обработки персональных данных, требований к защите персональных данных	По мере необходимости	Ответственный за организацию обработки персональных данных в администрации муниципального района Челно-Вершинский Самарской области
Организация приёма и обработки обращений и запросов субъектов персональных данных или их представителей	По мере необходимости	Работники, включенные в перечень должностей в администрации муниципального района Челно-Вершинский Самарской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

Определение уровней защищённости всех выявленных ИСПДн	Разовое	Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в администрации муниципального района Челно-Вершинский Самарской
Обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними	Ежемесячно, не позднее 25 числа месяца	Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в администрации муниципального Челно-Вершинский Самарской
Учет всех защищаемых носителей информации с помощью их маркировки и занесение учётных данных в Журнал учёта с отметкой об их выдаче (приеме)	Постоянно	Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в администрации муниципального Челно-Вершинский Самарской
Физические мероприятия		
Организация хранения материальных носителей ПДн в помещениях, установка дополнительных металлических шкафов (хранилищ) и замков	Разовое	Администрация района
Установка дополнительных замков на дверях в помещениях с аппаратными ИСПДн	Разовое	Администрация района
Установка систем бесперебойного питания на ключевые элементы ИСПДн	Разовое	Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в администрации муниципального Челно-Вершинский Самарской
Технические (аппаратные и программные) мероприятия		

Внедрение системы защиты от несанкционерного доступа и криптографической защиты	Разовое	Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в администрации муниципального Челно-Вершинский Самарской
Осуществление обновления системы антивирусной защиты	Ежегодно	Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в администрации муниципального Челно-Вершинский Самарской
Контролирующие мероприятия		
Проверка порядка использования технических средств защиты ПДн, в т.ч над соблюдением режима обработки ПДн, соблюдением режима защиты, над выполнением антивирусной защиты, над соблюдением режима защиты при подключении к сетям общего пользования, на предмет выявления изменений в режиме обработки и	Согласно плана проведения внутреннего контроля	Комиссия по осуществлению внутреннего контроля соответствия обработки персональных данных в администрации муниципального района Челно-Вершинский Самарской области требованиям к защите персональных данных

Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в администрации муниципального Челно-Вершинский Самарской
Контроль за обеспечением резервного копирования	Ежемесячно	Ответственный за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных в администрации муниципального Челно-Вершинский Самарской
Поддержание в актуальном состоянии нормативно-организационных документов		Ответственный за организацию обработки персональных данных в администрации муниципального района Челно-Вершинский Самарской области
Отслеживание объёмов обрабатываемых ПДн, состава обрабатываемых ПДн в различных ИСПДн, целей обработки ПДн	Согласно плана проведения внутреннего контроля	Комиссия по осуществлению внутреннего контроля соответствия обработки персональных данных в администрации муниципального района Челно-Вершинский Самарской области требованиям к защите персональных данных

Приложение N 2
к распоряжению администрации
муниципального района Челно-Вершинский
Самарской области
от 24.08.2020 N 92

Инструкция
администратора безопасности
информационных систем персональных данных
в администрации муниципального района Челно-Вершинский
Самарской области

1. Общие положения.

1.1. Настоящая Инструкция определяет обязанности должностного лица, ответственного за обеспечение безопасности информации (в том числе персональных данных (ПДн)), обрабатываемой в информационных системах ПДн (ИСПДн) администрации муниципального района Челно-Вершинский Самарской области (далее - администрации района), далее - администратора безопасности информации (администратора безопасности).

1.2. Действие настоящей Инструкции не распространяется на муниципальные органы, являющимися структурными подразделениями, наделёнными статусом юридического лица.

1.3. Администратор безопасности назначается распоряжением.

1.4.Администратор безопасности по вопросам обеспечения безопасности информации подчиняется уполномоченному за обработку персональных данных в администрации района.

1.5. Администратор безопасности отвечает за поддержание установленного уровня безопасности защищаемой информации, в том числе ПДн, при их обработке в ИСПДн администрации района.

1.6. Администратор безопасности осуществляет методическое руководство деятельностью пользователей ИСПДн администрации района в вопросах обеспечения безопасности информации.

1.7. Требования администратора безопасности, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИСПДн администрации района.

1.8. Администратор безопасности несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн администрации района, состояние и поддержание установленного уровня защиты информации, обрабатываемой в ИСПДн администрации района.

2. Задачи администратора безопасности

2.1. Основными задачами администратора безопасности являются:

- поддержание необходимого уровня защиты ИСПДн администрации района от несанкционированного доступа (НСД) к информации;
- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации;
- установка средств защиты информации и контроль выполнения правил их эксплуатации;
- сопровождение средств защиты информации (СЗИ) от НСД и основных технических средств и систем (ОТСС) ИСПДн администрации района;
- периодическое обновление СЗИ и комплекса мероприятий по предотвращению инцидентов ИБ;
- оперативное реагирование на нарушения требований по ИБ в ИСПДн администрации района и участие в их прекращении.

2.2. В рамках выполнения основных задач администратор безопасности осуществляет:

- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;
- текущий контроль технологического процесса автоматизированной обработки ПДн;
- участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности ПДн;
- контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации в администрации района;
- методическую помощь всем сотрудникам администрации района по вопросам обеспечения безопасности ПДн.

3. Обязанности администратора безопасности

Администратор безопасности обязан:

3.1. Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИСПДн администрации района.

3.2. Участвовать в установке, настройке и сопровождении программных средств защиты информации.

3.3. Участвовать в приемке новых программных средств обработки информации.

3.4. Обеспечить доступ к защищаемой информации пользователям ИСПДн администрации района согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).

3.5. Уточнять в установленном порядке обязанности пользователей ИСПДн администрации района при обработке ПДн.

3.6. Вести контроль осуществления резервного копирования информации.

3.7. Анализировать состояние защиты ИСПДн администрации района.

3.8. Контролировать правильность функционирования средств защиты информации и неизменность их настроек.

3.9. Контролировать физическую сохранность технических средств обработки информации.

3.10. Контролировать исполнение пользователями ИСПДн администрации района введенного режима безопасности, а также правильность работы с элементами ИСПДн и средствами защиты информации.

3.11. Контролировать исполнение пользователями правил парольной политики.

3.12. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений.

3.13. Не допускать установку, использование, хранение и размножение в ИСПДн администрации района программных средств, не связанных с выполнением функциональных задач.

3.14. Осуществлять периодические контрольные проверки автоматизированных рабочих мест (АРМ) ИСПДн администрации района.

3.15. Оказывать помощь пользователям ИСПДн администрации района в части применения средств защиты и консультировать по вопросам введенного режима защиты.

3.16. Периодически представлять руководству отчет о состоянии защиты ИСПДн администрации района и о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3.17. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн администрации района, в том числе средств защиты, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.18. В случае выявления нарушений режима безопасности информации (ПДн), а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.

3.19. Принимать участие в проведении работ по оценке соответствия ИСПДн администрации района требованиям безопасности информации.

4. Права администратора безопасности

Администратор безопасности имеет право:

4.1. Отключать от ресурсов ИСПДн администрации района сотрудников, осуществивших НСД к защищаемым ресурсам ИСПДн или нарушивших другие требования по ИБ.

4.2. Давать работникам обязательные для исполнения указания и рекомендации по вопросам ИБ.

4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ИСПДн администрации района.

4.4. Организовывать и участвовать в любых проверках по использованию пользователями администрации района телекоммуникационных ресурсов.

4.5. Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн администрации района при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

4.6. Осуществлять взаимодействие с руководством и персоналом администрации района по вопросам обеспечения ИБ.

4.7. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.

4.8. Запрашивать и получать от начальников и специалистов структурных подразделений администрации района информацию и материалы, необходимые для организации своей работы.

4.9. Вносить на рассмотрение руководства предложения по улучшению состояния ИБ ПДн, обрабатываемых в администрации района.

5. Ответственность администратора безопасности

Администратор безопасности несет ответственность:

5.1. За организацию защиты информационных ресурсов и технических средств ИСПДн администрации района.

5.2. За качество проводимых работ по контролю действий пользователей и администраторов ИСПДн, состояние и поддержание необходимого уровня защиты информационных и технических ресурсов ИСПДн администрации района.

5.3. За разглашение сведений ограниченного доступа (персональные данные и иная защищаемая информация), ставших известными ему по роду работы.

6. Действия администратора безопасности при обнаружении попыток НСД

6.1. К попыткам НСД относятся:

- сеансы работы с телекоммуникационными ресурсами администрации района незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими;

- действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ИСПДн администрации с

использованием учетной записи администратора или другого пользователя ИСПДн, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

6.2. При выявлении факта/попытки НСД администратор безопасности обязан:

- прекратить доступ к информационным ресурсам со стороны выявленного участка НСД:
- доложить руководству подразделения ИБ о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;
- известить начальника структурного подразделения администрации района, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;
- проанализировать характер НСД;
- по решению руководства подразделения ИБ осуществить действия по выяснению причин, приведших к НСД;
- предпринять меры по предотвращению подобных инцидентов в дальнейшем.

Приложение №3
к распоряжению администрации
муниципального района Челно-Вершинский
Самарской области

от 24.08.2020 N 92

Инструкция
пользователя информационных систем персональных данных в администрации муниципального района Челно-Вершинский Самарской области

1. Общие требования по обеспечению безопасности обработки информации в ИСПДН

1.1. К защищаемой информации, обрабатываемой в информационных системах персональных данных администрации муниципального района Челно-Вершинский (далее - ИСПДн администрации района), относятся персональные данные, служебная (технологическая) информация системы защиты, другая информация конфиденциального характера в соответствии с Перечнем информационных систем персональных данных администрации муниципального района Челно-Вершинский Самарской области

1.2. Действие настоящей Инструкции не распространяется на муниципальные органы, являющимися структурными подразделениями, наделёнными статусом юридического лица.

1.3. Ответственность за организацию защиты информации в ИСПДн администрации района и выполнение установленных условий ее функционирования возлагается на администратора безопасности информации в администрации района. Ответственность за выполнение мероприятий по обеспечению безопасности информации возлагается на лицо, производящее ее обработку (пользователя ИСПДн администрации района).

1.4. Допуск пользователей к работе в ИСПДн администрации района осуществляется в соответствии с Перечнем должностей муниципальной службы администрации муниципального района Челно-Вершинский Самарской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, необходим для выполнения служебных (трудовых) обязанностей", утверждённом постановлением администрации муниципального района Челно-Вершинский Самарской области «Об

обработке персональных данных в администрации муниципального района Челно-Вершинский Самарской области.

1.5. К самостоятельной работе на автоматизированных рабочих местах (АРМ), входящих в состав ИСПДн администрации района, допускаются лица, изучившие требования настоящей Инструкции и освоившие правила эксплуатации АРМ и технических средств защиты. Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

1.6. Помещения, в которых размещены технические средства ИСПДн администрации района, отвечают режимным требованиям и в нерабочее время сдаются под охрану установленным порядком.

1.7. Вход в помещения, в которых производится автоматизированная обработка защищаемой информации, разрешается постоянно работающим в нем работникам, а также лицам, привлекаемым к проведению ремонтных, наладочных и других работ и посетителей в сопровождении работников администрации района.

1.8. Техническое обслуживание АРМ, уборка помещения и т.п. проводятся только под контролем уполномоченного лица администрации района. При проведении этих работ обработка защищаемой информации (ПДн) запрещается.

1.9. По фактам и попыткам несанкционированного доступа к защищаемой информации, а также в случаях ее утечки и (или) модификации (уничтожения) проводятся служебные расследования.

2. Обязанности пользователя

2.1. При первичном допуске к работе в ИСПДн администрации района пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных (регламентирующих) документов по вопросам безопасности при автоматизированной обработке информации, изучает настоящую Инструкцию, получает личный текущий пароль у должностного лица, выполняющего функции администратора безопасности информации в ИСПДн администрации района (далее - администратор безопасности).

2.2. Каждый сотрудник администрации района , участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн администрации района, несет персональную ответственность (дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством Российской Федерации ответственность) за свои действия и обязан:

2.2.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн администрации района.

2.2.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн администрации района.

2.2.3. Хранить в тайне свой пароль.

2.2.4. Передавать для хранения установленным порядком при необходимости свои реквизиты разграничения доступа только администратору безопасности администрации района.

2.2.5. Выполнять требования по антивирусной защите в части, касающейся действий пользователей.

2.2.6. Немедленно ставить в известность администратора безопасности в следующих случаях:

- при подозрении компрометации личного пароля;

- обнаружения нарушения целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения в отсутствие пользователя попыток несанкционированного доступа (НСД) к ресурсам ИСПДн администрации района;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн администрации района;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн администрации района, выхода из строя или неустойчивого функционирования узлов или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных средств защиты;

- обнаружения непредусмотренных отводов кабелей и подключенных устройств;

- обнаружения фактов и попыток НСД и случаев нарушения установленного порядка обработки защищаемой информации.

2.3. Пользователю категорически запрещается:

2.3.1. Использовать компоненты программного и аппаратного обеспечения ИСПДн администрации района в неслужебных целях.

2.3.2. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн администрации района или устанавливать дополнительно любые программные и аппаратные средства.

2.3.3. Осуществлять обработку защищаемой информации в присутствии посторонних (не допущенных к данной информации) лиц.

2.3.4. Записывать и хранить защищаемую информацию на неучтенных носителях информации (гибких магнитных дисках и т.п.).

2.3.5. Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД.

2.3.6. Оставлять без личного присмотра на АРМ или где бы то ни было свои персональные реквизиты доступа, машинные носители и распечатки, содержащие защищаемую информацию.

2.3.7. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц. Об обнаружении такого рода ошибок ставить в известность администратора безопасности.

2.3.8. Производить перемещения технических средств АРМ без согласования с администратором безопасности.

2.3.9. Вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств, производить техническое обслуживание (ремонт) средств вычислительной техники без согласования с администратором безопасности и без оформления соответствующего Акта.

2.3.10. Подключать к АРМ нештатные устройства и самостоятельно вносить изменения в состав и конфигурацию.

2.3.11. Осуществлять ввод пароля в присутствии посторонних лиц.

2.3.12. Оставлять без контроля АРМ в процессе обработки конфиденциальной информации.

2.3.13. Привлекать посторонних лиц для производства ремонта (технического обслуживания) технических средств АРМ.

Приложение №4
к распоряжению администрации
муниципального района Челно-Вершинский
Самарской области

от 24.08.2020 N 92

Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, средств защиты информации и средств криптографической защиты информации информационной системе персональных данных в администрации муниципального района Челно-Вершинский

1. Общие положения

1.1. Настоящий порядок (далее - Порядок) по резервированию и восстановлению работоспособности технических средств (далее – ТС), программного обеспечения (далее – ПО), баз данных (далее – БД), средств защиты информации (далее – СЗИ) и средств криптографической защиты информации (далее – СКЗИ) информационной системы персональных данных (далее – АИС) в администрации муниципального района Челно-Вершинский определяет действия, связанные с функционированием технических и программных средств АИС и системы защиты персональных данных (далее – СЗПДн).

1.2. Порядок разработан в соответствии с руководящими и нормативными документами регуляторов Российской Федерации (Федеральные законы, ГОСТы, постановления Правительства, Нормативно-правовые акты ФСТЭК, НПА ФСБ, Роскомнадзора) в области защиты персональных данных.

1.3. Целью данного порядка является превентивная защита элементов АИС и СЗПДн от предотвращения потери защищаемой информации.

1.4. Задачами данного порядка являются:

- определение мер защиты от потери информации;
- определение действий восстановления технических и программных средств АИС и СЗПДн в случае потери информации.

1.5. Действие данного порядка распространяется на всех пользователей, имеющих доступ к ресурсам АИС, в том числе на ответственного за обеспечение безопасности персональных данных информационных систем персональных данных администрации муниципального района Челно-Вершинский и администратора АИС (далее – администратор системы), имеющих доступ к техническим и программным средствам СЗПДн в рамках своих полномочий, при возникновении аварийных ситуаций, в том числе:

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

1.6 Пользователем АИС (далее – Пользователь) является сотрудник администрации муниципального района Челно-Вершинский, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и СЗИ АИС.

1.7. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов АИС или СЗПДн, предоставляемых пользователям, а также потерей защищаемой информации.

2. Порядок реагирования на инцидент

2.1. 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 АИС и СЗПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.2. В кратчайшие сроки, не превышающие одного рабочего дня ответственный за обеспечение безопасности персональных данных в администрации муниципального района Челно-Вершинский и администратор системы предпринимают меры по восстановлению работоспособности.

2.3. Предпринимаемые меры, по возможности, согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Технические меры

3.1. 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 АИС;

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

3.2. Системы жизнеобеспечения АИС включают:
- пожарные сигнализации;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.3. Все критичные помещения администрации муниципального района Челно-Вершинский (помещения, в которых размещаются элементы АИС и СЗПДн) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

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

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы АИС и СЗПДн, сетевое и коммуникационное оборудование, а также наиболее критичные АРМ 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 (серверы, активное сетевое оборудование и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.6. Системы обеспечения отказоустойчивости:
- кластеризация;
- технология RAID.

3.7. Для обеспечения отказоустойчивости критичных компонентов АИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации.

3.8. Для наиболее критичных компонентов АИС должны использоваться территориально удаленные системы кластеров.

3.9. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.10. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

4. Организационные меры

4.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:

- для обрабатываемых ПДн – согласно инструкции по обеспечению безопасности ПДн;
- для технологической информации – не реже раза в месяц;
- эталонные копии программного обеспечения (ОС, штатное и специальное ПО, программные СЗИ), с которых осуществляется их установка на элементы АИС – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

4.2. Данные о проведении процедуры резервного копирования должны отражаться в специально созданном журнале учета.

4.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

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

4.5. Носители должны храниться не менее года для возможности восстановления данных.

Приложение №5
к распоряжению администрации
муниципального района Челно-Вершинский
Самарской области

от _____ N _____

ЖУРНАЛ
учета съемных носителей персональных данных

Администрации муниципального района Челно-Вершинский Самарской области
наименование структурного подразделения

Начат «___»_____2020 г. На ___ листах

Окончен «___»_____20__ г.

Ответственный за хранение _____
Должность, ФИО Подпись

№ п/п	Метка съемного носителя (учетный номер)	Фамилия исполнителя	Движение (Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Примечание*
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)