Приложение № 1
к постановлению администрации
города Кировска от 23.07.2020 № 643

ПОЛОЖЕНИЕ
О ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, СОДЕРЖАЩИХСЯ В АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ АДМИНИСТРАЦИИ ГОРОДА КИРОВСКА

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о защите конфиденциальной информации, в т.ч. персональных данных, содержащихся в автоматизированной информационной системе администрации города Кировска (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 г. № 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», приказом Федеральной службы по техническому и экспортному контролю 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», приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Цель разработки настоящего Положения –установление порядка организации и проведения работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация, информация), в автоматизированной информационной системе (далее – АИС) администрации города Кировска (далее – Администрация) на всех стадиях (этапах) создания АИС, в ходе ее эксплуатации и вывода из эксплуатации.

1.3. К защищаемой информации, обрабатываемой в АИС Администрации, относится следующая информация:

– персональные данные, содержащиеся в информационных системах персональных данных Администрации;

– информация, не содержащая сведения, составляющие государственную тайну, содержащаяся в государственных информационных системах Администрации;

– иная информация, обрабатываемая в информационных системах Администрации, обеспечение безопасности которой регулируется законодательством Российской Федерации.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем Положении используются следующие термины и их определения:

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

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

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Обработка информации – действия (операции) с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение информации.

Оператор – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных. В случае обработки персональных данных под оператором понимается 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.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

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

Пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Угрозы 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.

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

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. Под организацией обеспечения безопасности защищаемой информации при ее обработке в АИС понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на

минимизацию ущерба от возможной реализации угроз безопасности защищаемой информации, реализуемых в рамках создаваемой системы защиты информации (далее – СЗИ).

3.2. СЗИ включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности защищаемой информации, уровня защищенности персональных данных (далее – ПДн), который необходимо обеспечить и информационных технологий, используемых в АИС.

3.3. Безопасность защищаемой информации при ее обработке в АИС обеспечивает Администрация или лицо, осуществляющее обработку защищаемой информации по поручению Администрации на основании заключаемого с этим лицом договора (далее – уполномоченное лицо). Договор между Администрацией и уполномоченным лицом должен предусматривать обязанность уполномоченного лица обеспечить безопасность защищаемой информации при ее обработке в АИС.

3.4. Администрацией назначается лицо, ответственное за организацию обработки защищаемой информации при ее обработке в АИС администрации города Кировска.

3.5. Для обеспечения безопасности защищаемой информации, содержащейся в АИС, Администрацией назначается структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности защищаемой информации Администрации – Администратор информационной безопасности (далее – Администратор ИБ).

3.6. Для проведения работ по защите информации в ходе создания, эксплуатации и вывода из эксплуатации АИС Администрацией в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

3.7. Для обеспечения защиты информации, содержащейся в АИС, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

3.8. Защита информации, содержащейся в АИС, является составной частью работ по созданию и эксплуатации АИС и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках СЗИ.

3.9. Организационные и технические меры защиты информации, реализуемые в рамках СЗИ, должны быть направлены на исключение:

– неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

– неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

– неправомерного блокирования информации (обеспечение доступности информации).

3.10. Для обеспечения защиты информации, содержащейся в АИС, проводятся следующие мероприятия:

– формирование требований к защите информации, содержащейся в АИС;

– разработка СЗИ;

– внедрение СЗИ;

– аттестация АИС по требованиям защиты информации (далее – аттестация АИС);

– обеспечение защиты информации в ходе эксплуатации аттестованной АИС;

– обеспечение защиты информации при выводе из эксплуатации аттестованной АИС или после принятия решения об окончании обработки информации.

4. ПОРЯДОК РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ АДМИНИСТРАЦИИ

4.1. Настоящий порядок определяет правила проведения резервного копирования данных, обрабатываемых в АИС Администрации.

4.2. Целью резервного копирования является предотвращение потери информации при сбоях оборудования, программного обеспечения, в критических и кризисных ситуациях и т.д.

4.3. Резервному копированию подлежит информация, обрабатываемая в АИС Администрации.

4.4. В Администрации должна быть реализована централизованная система резервного копирования.

4.5. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации в установленные сроки и с заданной периодичностью.

4.6. Перед выполнением процедур резервного копирования или восстановления информации и ПО средств защиты необходимо провести проверку:

– доступности резервного носителя, достаточности свободного места в хранилище для записи или восстановления данных;

– работоспособности средств резервного копирования и восстановления;

– готовности информационных ресурсов к осуществлению их резервного копирования или восстановления;

– завершения работы ПО и процессов, способных повлиять на процесс создания или восстановления копий.

4.7. Расписание проведения резервного копирования определяется Администратором ИБ.

4.8. Резервное копирование проводится Администратором ИБ и регистрируется в Журнале резервного копирования и восстановления информации (Приложение № 1).

4.9. Перечень информационных ресурсов, подлежащих резервному копированию, время и дата создания копии, пометки об успешном/неуспешном завершении, а также, при необходимости, комментарии Администратора ИБ заносятся в Журнал резервного копирования и восстановления информации.

4.10. В случае выявления нарушений Администратору ИБ необходимо в кратчайшие сроки устранить неисправности в системе резервного копирования и восстановить работоспособность подсистем в штатный режим работы.

4.11. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, Администратор ИБ сообщает руководству Администрации немедленно.

4.12. Администратор ИБ должен контролировать проведение резервного копирования в целях выполнения требований по защите информации.

4.13. В случае обнаружения ошибки резервного копирования Администратор безопасности выполняет повторное копирование информации вручную в максимально сжатые сроки, не нарушая технологические процессы обработки информации пользователями Администрации, в Журнал резервного копирования и восстановления информации заносятся соответствующие отметки.

4.14. Хранение резервных копий данных осуществляется на сменных носителях информации (CD/DVD, внешние жесткие диски и т.п.), промаркированных Администратором ИБ в соответствие с расписанием резервного копирования. Маркировка должна содержать номер копии, дату ее создания, наименование АИС.

4.15. Использование носителей информации при резервном хранении должно подчиняться принципу ротации носителей, при котором для записи текущей копии используется носитель с самой ранней датой создания предыдущей копии.

4.16. Срок хранения резервных копий определяется Администратором ИБ.

4.17. Очистка устаревших резервных копий из хранилища должна производиться Администратором ИБ регулярно по мере заполнения выделенной области памяти или по истечении предусмотренного срока хранения.

4.18. Удаление резервных копий для повторного использования носителя информации, либо окончательное удаление производится Администратором ИБ.

4.19. Основанием для инициирования процедуры восстановления служит полная или частичная утрата информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях. Восстановление данных производится Администратором ИБ.

4.20. Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

4.21. В зависимости от характера и уровня повреждения информационных ресурсов, Администратор безопасности восстанавливает либо весь архив копии данных, либо отдельные потерянные части или технические средства из соответствующих хранилищ.

4.22. После завершения процесса восстановления Администратором ИБ проверяется целостность информационных ресурсов и корректная работа технических средств информационных систем.

4.23. Резервное копирование защищаемой информации, обрабатываемой в АИС Администрации может быть делегировано третьим лицам на договорной основе в рамках технической поддержки АИС Администрации.

4.24. Ведение журнала резервирования\восстановления информации ведется встроенными средствами системы резервного копирования информации.

5. ПОРЯДОК ДОПУСКА ПОЛЬЗОВАТЕЛЕЙ К РАБОТЕ В АИС АДМИНИСТРАЦИИ ГОРОДА КИРОВСКА

5.1 Разрешительная система доступа представляет собой совокупность процедур оформления прав субъектов на доступ к информационным ресурсам (ИР) (объектам доступа) АИС, а также прав и обязанностей ответственных лиц, осуществляющих реализацию этих процедур.

Объектами доступа являются:

-информационные ресурсы АИС.

Субъектами доступа являются:

- уполномоченные сотрудники администрации города Кировска.

Субъекты доступа несут персональную ответственность за соблюдение ими установленного на объекте информатизации порядка обеспечения защиты информационных ресурсов.

5.2 Лицом, осуществляющим реализацию процедур оформления прав субъектов на доступ к информационным ресурсам АИС, является Администратор ИБ.

5.3 Первоначальный допуск пользователей к работе в АИС осуществляется на основании «Перечня должностей служащих администрации города Кировска, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным»

5.4 Для обеспечения персональной ответственности за свои действия каждому пользователю АИС, допущенному к работе с защищаемой информацией, присваивается имя (учетная запись пользователя), под которым он регистрируется и осуществляет работу в системе. В случае производственной необходимости пользователю АИС могут быть сопоставлены несколько уникальных имен (учетных записей).

5.5 При регистрации и назначении прав доступа пользователей в АИС должны выполняться следующие требования:

- учетные записи всех пользователей привязываются к конкретным автоматизированным рабочим местам (АРМ), за исключением учетных записей технического персонала, обслуживающего компоненты АИС;

- при регистрации пользователей проводится проверка соответствия уровня доступа

возложенным на пользователя задачам (вмененным обязанностям);

- назначенные пользователю права доступа документируются;
- в АИС предусматривается разрешение доступа к сервисам только аутентифицированным пользователям;
- при внесении нового пользователя разрабатывается и обновляется формальный список всех пользователей, зарегистрированных для работы в АИС;
- при изменении должностных обязанностей (увольнении) пользователя проводится немедленное исправление (аннулирование) прав его доступа;
- Администратором безопасности проводится удаление всех неиспользуемых учетных записей. Предусмотренные в системе запасные идентификаторы недоступны другим пользователям.
- Права по установке и удалению программного обеспечения на АРМ предоставлены только сотрудникам, обладающим правами администратора безопасности.
- Процедура регистрации (создания учетной записи) пользователя и предоставления (или изменения) ему прав доступа к ресурсам АИС осуществляется с использованием сертифицированных средств защиты информации от несанкционированного доступа.

5.6 Для загрузки компьютера в АИС предусмотрены два типа учетных записей:

- учетная запись администратора безопасности - позволяет производить настройку средств защиты информации и добавлять/удалять пользователей в систему, производить установку и настройку программного обеспечения на АРМ АИС;
- учетная запись пользователя - наделена ограниченными правами.

После создания учетной записи, пользователь должен авторизоваться в системе.

5.7 Администратор безопасности обязан проверить наличие записей о входе пользователя в систему в журнале регистрации событий средств зашиты информации от несанкционированного доступа.

5.8 Для всех пользователей АИС устанавливается режим принудительного запроса смены пароля не реже одного раза в 90 дней, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки - 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации - 15 минут.

В случае производственной необходимости пользователю АИС могут быть сопоставлены несколько уникальных имен (учетных записей).

5.9 При изменении должностных обязанностей сотрудника, связанных с переводом в другое подразделение, переводом на другую должность и т.п., учетная запись пользователя подлежит изменению (корректировке), при этом старые полномочия аннулируются.

5.10 На время отпуска пользователей Администратором безопасности осуществляется блокирование их учетных записей.

5.11 Контроль выполнения требований разрешительной системы доступа к защищаемой информации) возлагается на Администратора безопасности.

6. ДОПУСК К ИНФОРМАЦИОННЫМ РЕСУРСАМ АИС СТОРОННИХ ОРГАНИЗАЦИЙ, ВЫПОЛНЯЮЩИХ РАБОТЫ В АДМИНИСТРАЦИИ ГОРОДА КИРОВСКА НА ДОГОВОРНОЙ ОСНОВЕ

6.1 К организациям, выполняющим работы на договорной основе, могут относиться:

-организации, осуществляющие монтаж и настройку технических средств АИС, сопровождение прикладного программного обеспечения;

-организации, оказывающие услуги в области защиты информации (проведение специальных проверок и исследований, монтаж и настройка средств защиты информации, контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);

-организации, осуществляющие поставку товаров для обеспечения повседневной

деятельности (мебели, канцтоваров, оргтехники, расходных материалов и т.п.).

6.2 Порядок допуска определяется в договоре на выполнение работ (оказание услуг). Кроме того, лицам, привлекаемым на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами оператора, на срок действия договора, должны быть присвоены учетные записи.

6.3 Решением о допуске является подписанный в установленном порядке договор на выполнение работ или оказание услуг. договор на оказание услуг включается условие о неразглашении сведений, содержащих персональные данные, а также служебной информации, ставшей известной в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений. Со всех работников сторонней организации, участвующих в выполнении работ, в этом случае берется подписка о неразглашении таких сведений.

7. ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

7.1 Формирование требований к защите информации, содержащейся в АИС, осуществляется Администрацией в соответствии с действующим законодательством РФ в соответствующей сфере деятельности.

7.2 Формирование требований к защите информации, содержащейся в АИС, включает:

– принятие решения о необходимости защиты информации, содержащейся в АИС;

– классификацию АИС по требованиям защиты информации, определение уровня защищенности ПДн, при их обработке в АИС;

– определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в АИС, и разработку на их основе модели угроз безопасности информации;

– определение требований к СЗИ.

7.3 При принятии решения о необходимости защиты информации, содержащейся в АИС, осуществляется:

– анализ целей создания АИС и задач, решаемых этой АИС;

– определение информации, подлежащей обработке в АИС;

– анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать АИС;

– принятие решения о необходимости создания СЗИ, а также определение целей и задач защиты информации в АИС, основных этапов создания СЗИ и функций по обеспечению защиты информации, содержащейся в АИС.

7.4 Результаты классификации АИС оформляются актом классификации.

7.5 Результаты определения уровня защищенности ПДн при их обработке в АИС оформляются актом определения уровня защищенности.

7.6 Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей АИС, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

7.7 В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России.

7.8 При определении угроз безопасности информации учитываются структурно-функциональные характеристики АИС, включающие структуру и состав АИС, физические, логические, функциональные и технологические взаимосвязи между сегментами АИС, с иными АИС и информационно-телекоммуникационными сетями, режимы обработки информации в АИС

и в ее отдельных сегментах, а также иные характеристики АИС, применяемые информационные технологии и особенности ее функционирования.

7.9 По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик АИС, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

7.10 Модель угроз безопасности информации должна содержать описание АИС и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей АИС, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

7.11 Требования к СЗИ определяются в зависимости от класса защищенности АИС, уровня защищенности ПДн при их обработке в АИС и угроз безопасности информации, включенных в модель угроз безопасности информации.

7.12 При определении требований к СЗИ учитываются положения политики Администрации в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну.

8. ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

8.1. Внедрение СЗИ организуется Администрацией.

8.2. Внедрение СЗИ осуществляется в соответствии с проектной и эксплуатационной документацией на СЗИ и, в том числе, включает:

– установку и настройку средств защиты информации в АИС;

– разработку документов, определяющих правила и процедуры, реализуемые Администрацией для обеспечения защиты информации в АИС в ходе ее эксплуатации (далее – организационно-распорядительные документы по защите информации);

– внедрение организационных мер защиты информации;

– предварительные испытания СЗИ (при необходимости);

– опытную эксплуатацию СЗИ (при необходимости);

– анализ уязвимостей АИС и принятие мер защиты информации по их устранению;

– приемочные испытания СЗИ (при необходимости).

8.3. Установка и настройка средств защиты информации в АИС должна проводиться в соответствии с эксплуатационной документацией на СЗИ и документацией на средства защиты информации.

8.4. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

– управления (администрирования) СЗИ;

– выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования АИС и (или) к возникновению угроз безопасности информации (далее – инциденты), и реагирования на них;

– управления конфигурацией аттестованной АИС и СЗИ;

– контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в АИС;

– защиты информации при выводе из эксплуатации АИС или после принятия решения об окончании обработки информации.

8.5. При внедрении организационных мер защиты информации осуществляются:

– реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного

обеспечения;

– проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов АИС по реализации организационных мер защиты информации;

– отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

8.6. Предварительные испытания СЗИ включают проверку работоспособности СЗИ, а также принятие решения о возможности опытной эксплуатации СЗИ.

8.7. Опытная эксплуатация СЗИ включает проверку функционирования СЗИ, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации СЗИ.

8.8. Анализ уязвимостей АИС проводится в целях оценки возможности преодоления нарушителем СЗИ и предотвращения реализации угроз безопасности информации. Анализ уязвимостей АИС включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения АИС. При анализе уязвимостей АИС проверяется отсутствие известных уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением. В случае выявления уязвимостей АИС, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителем выявленных уязвимостей. По результатам анализа уязвимостей должно быть подтверждено, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России, а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

8.9. Приемочные испытания СЗИ включают проверку выполнения требований к СЗИ в соответствии с техническим заданием на создание СЗИ.

9. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ХОДЕ ЭКСПЛУАТАЦИИ АТТЕСТОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

9.1. Обеспечение защиты информации в ходе эксплуатации аттестованной АИС осуществляется Администрацией в соответствии с эксплуатационной документацией на СЗИ и организационно-распорядительными документами по защите информации и в том числе включает:

– управление (администрирование) СЗИ;

– выявление инцидентов и реагирование на них;

– управление конфигурацией аттестованной АИС и СЗИ;

– контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в АИС.

9.2. В ходе управления (администрирования) СЗИ осуществляются:

– заведение и удаление учетных записей пользователей, управление полномочиями пользователей АИС и поддержание правил разграничения доступа в АИС;

– управление средствами защиты информации в АИС, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

– установка обновлений программного обеспечения, включая программное обеспечение

средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;

– централизованное управление СЗИ (при необходимости);

– регистрация и анализ событий в АИС, связанных с защитой информации (далее – события безопасности);

– информирование пользователей об угрозах безопасности информации, о правилах эксплуатации СЗИ и отдельных средств защиты информации, а также их обучение;

– сопровождение функционирования СЗИ в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации;

9.3. В ходе выявления инцидентов и реагирования на них осуществляются:

– определение лиц, ответственных за выявление инцидентов и реагирование на них;

– обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в АИС пользователями и администраторами;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению АИС и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

9.4. В ходе управления конфигурацией аттестованной АИС и ее СЗИ осуществляются:

– поддержание конфигурации АИС и ее СЗИ (структуры СЗИ, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на СЗИ (поддержание базовой конфигурации АИС и ее СЗИ);

– определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию АИС и СЗИ;

– управление изменениями базовой конфигурации АИС и СЗИ, в том числе определение типов возможных изменений базовой конфигурации АИС и СЗИ, санкционирование внесения изменений в базовую конфигурацию АИС и СЗИ, документирование действий по внесению изменений в базовую конфигурацию АИС и СЗИ, сохранение данных об изменениях базовой конфигурации АИС и СЗИ, контроль действий по внесению изменений в базовую конфигурацию АИС и ее СЗИ;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации АИС и СЗИ на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность АИС;

– определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию АИС и СЗИ;

– внесение информации (данных) об изменениях в базовой конфигурации АИС и СЗИ в эксплуатационную документацию на СЗИ;

– принятие решения по результатам управления конфигурацией о повторной аттестации

АИС или проведении дополнительных аттестационных испытаний.

9.5. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в АИС, осуществляются:

– контроль за событиями безопасности и действиями пользователей в АИС;

– контроль (анализ) защищенности информации, содержащейся в АИС;

– анализ и оценка функционирования СЗИ, включая выявление, анализ и устранение недостатков в функционировании СЗИ;

– периодический анализ изменения угроз безопасности информации в АИС, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в АИС;

– принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) СЗИ, повторной аттестации АИС или проведении дополнительных аттестационных испытаний.

9.6. Регулярные мероприятия по обеспечению безопасности защищаемой информации проводятся в соответствии с Планом мероприятий по защите информации (Приложение № 2). Внутренние проверки режима защиты информации проводятся в соответствии с Планом внутренних проверок режима защиты информации (Приложение № 3). По результатам проведения внутренней проверки составляется Отчет о результатах внутренней проверки режима защиты информации в администрации города Кировска (Приложение № 4).

10. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ВЫВОДЕ ИЗ ЭКСПЛУАТАЦИИ АТТЕСТОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ИЛИ ПОСЛЕ ПРИНЯТИЯ РЕШЕНИЯ ОБ ОКОНЧАНИИ ОБРАБОТКИ ИНФОРМАЦИИ

10.1. Обеспечение защиты информации при выводе из эксплуатации аттестованной АИС или после принятия решения об окончании обработки информации осуществляется Администрацией в соответствии с эксплуатационной документацией на СЗИ и организационно-распорядительными документами по защите информации и, в том числе, включает:

– архивирование информации, содержащейся в АИС;

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

10.2. Архивирование информации, содержащейся в АИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности Администрации.

10.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю АИС или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

Приложение № 1 к Положению

Журнал резервного копирования/восстановления данных

№ п/п	Схема резервного копирования/восстановления данных	Копируемые/восстанавливаемые ресурсы	Хранилище	Дата/время создания копии/восстановления	Фамилия Администратора ИБ	Подпись Администратора ИБ	Результат резервного копирования/восстановления данных	Комментарий
1	2	3	4	5	6	7	8	9

Приложение № 2 к Положению

План (типовой) мероприятий по обеспечению безопасности защищаемой информации в администрации города Кировска

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
1.	Документальное регламентирование работы с информацией	При необходимости	Разработка и (или) актуализация организационно-распорядительных документов по защите информации
2.	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необходимости	В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных»
3.	Ограничение доступа сотрудников к защищаемой информации	При необходимости	В случае создания АИС, а также приведения имеющихся АИСв соответствие с требованиями по безопасности информации необходимо разграничить доступ сотрудников Администрации к защищаемой информации
4.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передачи ПДн, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц
5.	Повышение квалификации сотрудников в области защиты информации	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, повышение осведомленности сотрудников – постоянно (данное обучение проводит Администратор безопасности за обеспечение безопасности персональных данных и за защиту информации, не содержащей сведения, составляющие государственную тайну, в информационных системах Администрации)
6.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия защищаемой информации
7.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для ПДн Администрацией устанавливаются сроки обработки, которые документально подтверждаются в нормативных документах Администрации. При пересмотре сроков необходимые изменения вносятся в соответствующие документы
8.	Уничтожение электронных (бумажных) носителей информации при достижении целей	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации производится с оформлением Акта на списание

№ п\п	Наименование мероприятия	Срок выполнения	Примечание
	обработки защищаемой информации		и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Приказе «О комиссии по уничтожению защищаемой информации, не содержащей сведения, составляющие государственную тайну»
9.	Определение класса защищенности АИС	При необходимости	Определение класса защищенности АИС осуществляется при создании АИС, при изменении состава АИС, масштаба АИС, степеней ущерба для характеристик АИС (конфиденциальности, целостности, доступности)
10.	Определение уровня защищенности ПДн при их обработке в АИС	При необходимости	Определение уровня защищенности ПДн при их обработке в АИС осуществляется при создании АИС, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн
11.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании СЗИ
12.	Аттестация АИС на соответствие требованиям по обеспечению безопасности информации	При необходимости	
13.	Эксплуатация АИС и контроль безопасности защищаемой информации	Постоянно	

Приложение№ 3к Положению

План (типовой) внутренних проверок режима защиты информации в администрации города Кировска

№	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ-152 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Раз в полгода	
2.	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн	Раз в полгода	
3.	Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство	Раз в полгода	
4.	Проверка уничтожения материальных носителей ПДн с составлением соответствующего акта	Ежегодно	
5.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	
6.	Проверка соблюдения условий хранения материальных носителей ПДн	Раз в полгода	
7.	Проверка состояния актуальности Уведомления об обработке (намерении осуществлять обработку) ПДн	Раз в полгода	
8.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн	Раз в полгода	
9.	Организация анализа и пересмотра имеющихся угроз безопасности информации, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно	
10.	Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ-152 «О персональных данных»	Ежегодно	
11.	Проверка применения для обеспечения безопасности информации средств защиты информации, прошедших в установленном порядке процедуру соответствия	Раз в полгода	
12.	Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию АИС	При необходимости	
13.	Контроль учета машинных носителей информации	Раз в полгода	

№	Мероприятие	Периодичность	Дата, подпись исполнителя
14.	Контроль за принимаемыми мерами по обеспечению безопасности информации, класса защищенности АИС и уровня защищенности ПДн в АИС	Раз в полгода	
15.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в АИС	Ежеквартально	
16.	Контроль внесения изменений в структурно-функциональные характеристики АИС	Ежеквартально	
17.	Контроль корректности настроек средств защиты информации	Раз в полгода	
18.	Контроль за обеспечением резервного копирования	Ежеквартально	
19.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам защиты информации	Раз в полгода	

Приложение№ 4к Положению

Отчет о результатах внутренней проверки режима защиты информации в администрации города Кировска

1.1 Внутренняя проверка произведена на основании Положения по организации и проведению работ по обеспечению безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, при ее обработке в информационных системах администрации города Кировска от «__» _____20__г.

1.2 Проверка проводилась «___»_____20__ г. по адресу:

_____

_____

1.3 В ходе проверки были проведены следующие мероприятия:

1) _____

2) _____

3) _____

4) _____

5) _____

1.4 Результаты проведения проверки:

1) _____

2) _____

3) _____

4) _____

5) _____

1.5 Необходимые мероприятия.

На основании проведения внутренней проверки режима защиты информации рекомендуется осуществить следующие мероприятия:

1) _____

2) _____

3) _____

4) _____

5) _____

Подписи ответственных лиц, проводивших внутреннюю проверку режима защиты информации:

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)
_____		
(дата)	(подпись)	(расшифровка подписи)
_____		
(дата)	(подпись)	(расшифровка подписи)

Приложение № 2
к постановлению администрации
города Кировска от 23.07.2020 № 643

Инструкция ответственного за организацию обработки персональных данных в автоматизированной информационной системе администрации города Кировска

1. Общие положения

1.1 Ответственным за организацию обработки персональных данных (далее - Ответственный) является штатный сотрудник администрации города Кировска, который осуществляет информационно-программное обслуживание Администрации.

1.2 Ответственный назначается оператором автоматизированной информационной системы (далее – АИС) персональных данных распоряжением главы администрации города Кировска.

1.3 Ответственный в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России, ФСБ России и регламентирующими документами администрации города Кировска, в том числе «Положением по организации и проведению работ, связанных с обработкой конфиденциальной информации, в т.ч. персональных данных, содержащихся в автоматизированной информационной системе администрации города Кировска» и отвечает за поддержание необходимого уровня безопасности обработки персональных данных (далее - ПДн).

1.4 Ответственный осуществляет методическое руководство муниципальными служащими и служащими, замещающими должности, не отнесенные к должностям муниципальной службы структурных подразделений администрации города Кировска, допущенными к обработке ПДн, в вопросах обеспечения безопасности персональных данных и несет персональную ответственность за качество проводимых им работ по контролю действий сотрудников, имеющих санкционированный доступ к ПДн, состояние и поддержание установленного уровня защиты информационных систем, обрабатывающих ПДн.

1.5 Требования Ответственного обязательны для исполнения всеми сотрудниками, допущенными к обработке ПДн.

2. Права ответственного за организацию обработки ПДн

Ответственный за организацию обработки ПДн имеет право:

2.1 Подать прошение руководителю о прохождении обучения по защите персональных данных в учебных центрах и курсах повышения квалификации;

2.2 Вносить руководителю предложения о наказании отдельных муниципальных служащих, служащих, замещающих должности, не отнесенные к должностям муниципальной службы структурных подразделений администрации города Кировска, допустивших нарушения в области безопасности и защиты ПДн.

3. Обязанности ответственного за организацию обработки ПДн

Ответственный за организацию обработки ПДн обязан:

3.1 Знать и выполнять требования законов Российской Федерации, Мурманской области и иных нормативных правовых актов Российской Федерации, Мурманской области, а также настоящего Положения и иных нормативных правовых актов органов местного самоуправления города Кировска в области защиты ПДн;

3.2 Предоставлять доступ муниципальным служащим, служащим, замещающим должности не отнесенные к должностям муниципальной службы структурных подразделений администрации города Кировска, допущенным к обработке персональных

данных, к операционной системе и автоматизированным системам обработки ПДн форме личной учетной записи (логин) и пароля доступа;

3.3 Участвовать в установке и настройке средств защиты, в контрольных и тестовых испытаниях и проверках элементов АИС, вести их учет;

3.4 Участвовать в приемке новых программных средств;

3.5 Обеспечить доступ к защищаемым ПДн пользователей АИС согласно их правам и полномочиям, к подсистемам АИС;

3.6 Уточнять в установленном порядке обязанности пользователей АИС по обработке объектов защиты;

3.7 Вести контроль над процессом осуществления резервного копирования объектов защиты;

3.8 Анализировать состояние защиты АИС и ее отдельных подсистем;

3.9 Контролировать неизменность состояния средств защиты, их параметров и режимов защиты;

3.10 Контролировать физическую сохранность средств и оборудования АИС;

3.11 Контролировать исполнение пользователями АИС введенного режима безопасности, а также правильность работы с элементами АИС и средствами защиты;

3.12 Контролировать исполнение пользователями парольной политики;

3.13 Контролировать работу пользователей АИС в сетях общего пользования в соответствии с Инструкцией по работе с Интернет и Инструкцией по работе с электронной почтой, утверждаемыми постановлением Администрации;

3.14 Не допускать установку, использование, хранение и размножение в АИС программных средств, не связанных с выполнением функциональных задач;

3.15 Не допускать к работе на элементах АИС посторонних лиц;

3.16 Осуществлять периодические контрольные проверки рабочих станций и тестирование правильности функционирования средств защиты АИС;

3.17 Оказывать помощь пользователям АИС в части применения средств защиты и консультировать по вопросам введенного режима защиты;

3.18 Представлять по требованию главы администрации города Кировска отчет о состоянии защиты АИС и о нештатных ситуациях на объектах АИС и допущенных пользователями АИС нарушениях установленных требований по защите информации;

3.19 В случае отказа работоспособности технических средств и программного обеспечения АИС, в том числе средств защиты принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

3.20 Принимать меры по реагированию, в случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий;

Приложение № 3
к постановлению администрации
города Кировска от 23.07.2020 № 643

Инструкция Администратора информационной безопасности автоматизированной информационной системы администрации города Кировска

1. Общие положения

1.1 Настоящая Инструкция определяет функции, права и обязанности Администратора информационной безопасности автоматизированной информационной системе администрации города Кировска (далее – АИС администрации) по вопросам обеспечения информационной безопасности при обработке персональных данных (далее – ПДн).

1.2 Администратор информационной безопасности (далее – Администратор ИБ) назначается из числа сотрудников администрации города Кировска (далее – Администрации) и является ответственным должностным лицом, уполномоченным на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты АИС и её ресурсов на этапах промышленной эксплуатации и модернизации.

1.3 Администратор ИБ в своей работе руководствуется законодательством Российской Федерации, настоящей Инструкцией, Положением о защите ПДн, руководящими и нормативными документами ФСТЭК России, внутренними документами Правительства Мурманской области, администрации города Кировска.

1.4 Администратор ИБ осуществляет методическое руководство Пользователей в вопросах обеспечения безопасности при обработке ПДн и иной информации ограниченного доступа.

1.5 Требования Администратора ИБ, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми Пользователями АИС администрации.

1.6 Администратор ИБ несет персональную ответственность за качество проводимых им работ по контролю действий Пользователей при работе в АИС администрации, состояние и поддержание установленного уровня защиты АИС администрации.

2. Обязанности Администратора ИБ

Администратор ИБ обязан:

2.1 Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2 Осуществлять установку, настройку и сопровождение технических средств защиты информации в АИС администрации.

2.3 Инициировать контрольные и тестовые испытания и проверки элементов АИС администрации.

2.4 Участвовать в приёмке новых программных и технических средств АИС администрации.

2.5 Осуществлять настройку и сопровождение в процессе эксплуатации подсистемы управления доступом:

- реализация полномочий доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);
- ввод описаний пользователей в информационную базу системы защиты информации (далее – СЗИ) от несанкционированного доступа (далее – НСД);
- своевременное удаление описаний пользователей из базы данных СЗИ при изменении списка допущенных к работе на объектах АИС администрации лиц;
- осуществлять контроль за исполнение парольной политики;

2.6 Осуществлять настройку и сопровождение подсистемы регистрации и учёта действий пользователей:

- настройка аудита событий;

- регулярное проведение анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;

- своевременное информирование руководства о несанкционированных действиях персонала и проведение расследования попыток НСД;

2.7 Осуществлять сопровождение подсистемы обеспечения целостности информации:

периодическое тестирование функций средств защиты информации, особенно при изменении программной среды и полномочий исполнителей;

- восстановление программной среды, программных средств и настроек СЗИ при сбоях;

- ведение двух копий программных средств и контроль их работоспособности;

- поддержание установленного порядка и правил антивирусной защиты информации;

- контроль за отсутствием на магнитных носителях остаточной информации по окончании работы пользователей;

- регулярная (при необходимости) актуализация (обновление) состава программного и аппаратного обеспечения АИС администрации;

- осуществлять контроль над процессом осуществления резервного копирования объектов защиты.

2.8 Анализировать состояние защиты АИС администрации и её отдельных подсистем.

2.9 Контролировать неизменность состояния средств защиты их параметров и режимов защиты.

2.10 Контролировать физическую сохранность средств и оборудования АИС администрации.

2.11 Контролировать исполнение пользователями АИС администрации введённого режима безопасности, а также правильность работы с элементами АИС администрации и средствами защиты.

2.12 Контролировать работу пользователей в сетях общего пользования и (или) международного обмена.

2.13 Осуществлять документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных – при наличии таких изменений.

2.14 Не допускать установку, использование, хранение и размножение в АИС администрации программных средств, не связанных с выполнением функциональных задач.

2.15 Не допускать к работе на элементах АИС администрации посторонних лиц.

2.16 Оказывать помощь пользователям АИС администрации в части применения средств защиты и консультировать по вопросам введенного режима защиты.

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

2.18 Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3. Права и ответственность Администратора ИБ

3.1 Администратор ИБ имеет право в отведённое ему время решать поставленные задачи в соответствии с его полномочиями в отношениях ресурсов ИБ и вверенным ему техническим и программным средствам. В частности, Администратор ИБ имеет право:

- вносить изменения в конфигурацию аппаратно-программных средств;

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

3.2 Несоблюдение требований Федерального закона от 27.07.2006 г. № 152-ФЗ (ред. от 25.07.2011 г.) «О персональных данных», настоящей Инструкции, иных нормативно-правовых документов в области персональных данных, Администратором ИБ влечёт за собой гражданскую, административную, дисциплинарную или иную предусмотренную законодательством Российской Федерации ответственность.

Приложение № 4
к постановлению администрации
города Кировска от 23.07.2020 № 643

Технологическая инструкция пользователя автоматизированной информационной системы администрации города Кировска

1. Общие положения

1.1 Пользователь автоматизированной информационной системы (далее – АИС) администрации города Кировска (далее – Пользователь АИС, Пользователь) и подсистем осуществляет обработку персональных данных (далее - ПДн) и иной информации ограниченного доступа.

1.2 Пользователем является сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и иной информации ограниченного доступа и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3 Пользователь несет персональную ответственность за свои действия.

1.4 Пользователь в своей работе руководствуется настоящей Инструкцией, Положением о защите ПДн, законодательством Российской Федерации, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Правительства Мурманской области, прочими организационно-распорядительными документами.

1.5 Методическое руководство работой пользователя осуществляется Администратором безопасности АИС.

2. Обязанности Пользователя

Пользователь обязан:

2.1 Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2 Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены для него установленными правами доступа.

2.3 Знать и соблюдать установленные требования по режиму обработки информации, учету, хранению и пересылке носителей информации, обеспечению безопасности информации, а также руководящих и организационно-распорядительных документов.

2.4 Соблюдать требования парольной политики.

2.5 Соблюдать требования антивирусной политики.

2.6 Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7 При передаче персональных данных и иной защищаемой информации в уполномоченные органы по каналам связи, пользователь обязан выполнять все необходимые процедуры подготовки и преобразования электронных документов (с использованием функций шифрования, электронной подписи) согласно установленным процедурам каждого уполномоченного органа, осуществляющего прием данных ограниченного доступа.

2.8 Обо всех выявленных нарушениях, связанных с информационной безопасностью ИС, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к Администратору безопасности.

2.9 Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам.
- несанкционированно копировать защищаемую информацию на внешние носители.

- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

- несанкционированно открывать общий доступ к папкам на своей рабочей станции.

- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

- несанкционированно отключать (блокировать) средства защиты информации и иные штатные технические средства.

- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к АИС.

- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам АИС.

- привлекать посторонних лиц для производства, ремонта или настройки АРМ, без согласования с Администратором АИС.

2.10 При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

2.11 Принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций под руководством Администратора безопасности АИС или руководителя подразделения, с целью ликвидации их последствий, в пределах возложенных на него полномочий и функций.

3. Права и ответственность пользователей АИС

3.1 Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам АИС.

3.2 Ответственность за выполнение требований настоящей Инструкции возлагается на всех Пользователей.

3.3 Пользователи несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность за несоблюдение требований настоящей Инструкции, иных нормативно-правовых документов, регламентирующих вопросы обработки и защиты информации ограниченного доступа.

Приложение № 5
к постановлению администрации
города Кировска от 23.07.2020 № 643

Инструкция об антивирусной защите информации в автоматизированной информационной системе администрации города Кировска

1. Общие положения

1.1 Настоящая Инструкция определяет требования к организации защиты автоматизированной информационной системы администрации города Кировска (далее – АИС) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников администрации города Кировска, эксплуатирующих и обслуживающих АИС, за их выполнение.

1.2 К использованию в АИС допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, рекомендованные к применению отделоминформационно-программного обеспечения администрации города Кировска.

1.3 Установка и настройка средств антивирусного контроля на компьютерах на серверах и рабочих станциях АИС осуществляется уполномоченными сотрудниками администрации города Кировска в соответствии руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1 Антивирусный контроль всех дисков и файлов рабочих станций должен проводиться ежедневно в начале работы при загрузке компьютера (для серверов - при перезапуске) в автоматическом режиме.

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

2.3 Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станциях занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

2.4 Необходимо организовать регулярное обновление антивирусных баз на всех рабочих станциях и серверах

2.5 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка;

3. Действия при обнаружении вирусов

3.1 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник самостоятельно или вместе с ответственным по информационной безопасности и технической защите информации и персональных данных в АИС администрации или лицом, им уполномоченным должен провести внеочередной антивирусный контроль своей рабочей станции.

3.2 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя своего подразделения и ответственного по информационной безопасности и технической защите информации и персональных данных в АИС администрации или сотрудника, им уполномоченного, а также 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 (при необходимости для выполнения требований данного пункта привлечь уполномоченных сотрудников Администрации);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на гибком магнитном диске уполномоченным сотрудникам Администрации;
- по факту обнаружения зараженных вирусом файлов составить служебную записку уполномоченному сотруднику Администрации, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

Приложение № 6 к постановлению
администрации города Кировска
от 23.07.2020 №643

Инструкция по организации парольной защиты
в автоматизированной информационной системе администрации города Кировска

1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной информационной системе администрации города Кировска (далее - АИС администрации), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с личными паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей и контроль за действиями пользователей при работе с паролями возлагается на ответственного по информационной безопасности и технической защите информации и персональных данных в АИС.

3. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 6 (шести) буквенно-цифровых символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АИС и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 (шести) позициях;
- личный пароль пользователь не имеет права сообщать никому.

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

4. В случае утечки информации о зарегистрированном пользователе необходимо немедленно удалить данные об этом пользователе и зарегистрировать заново.

5. Пользователи зарегистрированные для работы в АИС должны быть ознакомлены и предупреждены об ответственности за использование, хранение и потерю присвоенных логина и пароля.

6. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода.

7. Внеплановая смена личного пароля или удаление учетной записи пользователя, в случае прекращения его полномочий (увольнение, переход на другую работу, в другое подразделение организации и т.п.) должно немедленно производиться стирание ответственным по информационной безопасности и технической защите информации и персональных данных или лицом, им уполномоченным, информации о пользователе после окончания последнего сеанса работы данного пользователя в АИС.

8. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) ответственного по информационной безопасности и технической защите информации и персональных данных в АИС.

9. В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры в соответствии с п.7 или п.8 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

10. Хранение пользователем зарегистрированных логинов и значений своих паролей на бумажном носителе допускается только в сейфе у ответственного по информационной безопасности и технической защите информации и персональных данных в АИС.

11. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного по информационной безопасности и технической защите информации и персональных данных в АИС.

Приложение № 7
к постановлению администрации
города Кировска от 23.07.2020 № 643

Инструкция по работе в информационно-телекоммуникационной сети «Интернет»

1. Данная инструкция определяет полномочия, обязанности и ответственность сотрудников Администрации города Кировска при использовании ресурсов информационно-телекоммуникационной сети «Интернет» (далее - Интернет).

2. Доступ к сети Интернет осуществляется с автоматизированного рабочего места сотрудника (пользователя).

3. Пользователю разрешается использовать ресурсы сети Интернет только целях:

- доступа к специализированным (правовым и др.) базам данных;
- контактов с официальными лицами государственных структур, с сотрудниками структурных подразделений Администрации, с получателями государственных и муниципальных услуг;
- повышения квалификации, необходимой для выполнения работником своих должностных обязанностей;
- поиска и сбора информации по управленческим, производственным, финансовым, юридическим вопросам, если эти вопросы напрямую связаны с выполнением работником его должностных обязанностей;
- и др., связанных с выполнением работником его должностных обязанностей.

4. Пользователю запрещается:

- загружать, самостоятельно устанавливать прикладное, операционное, сетевое и другие виды программного обеспечения, а также осуществлять обновления операционной системы и прикладного ПО, если эти обновления не предоставляются сервером обновлений Администрации г. Кировска и если эта работа не входит в его должностные обязанности;
- использовать ресурсы Интернет в неслужебных целях;
- подключаться к ресурсам Интернет, используя автоматизированное рабочее место через не служебный канал доступа –сотовый телефон, модем, и др. устройства.
- посещение ресурсов с непристойным содержанием (эротико-порнографические ресурсы, нацистские или националистические ресурсы, ресурсы, призывающие к насилию);
- посещение игровых, развлекательных и прочих сайтов, не имеющих отношения к служебной деятельности пользователя;
- использовать в работе браузеры отличные от следующих:
- Internet Explorer;
- Mozilla Firefox;
- Google Chrome;
- Yandex браузер.
- Запускать на своих компьютерах программы, обеспечивающие удаленный доступ к рабочему столу.

5. Пользователь обязан:

- знать Инструкцию по антивирусной защите и уметь пользоваться антивирусным программным обеспечением.
- информировать ответственного по технической защите информации и персональных данных или лицо, им уполномоченное, (Администратора) о любых нарушениях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

6. Администратор безопасности обязан:

- производить подключение к сети Интернет только через специализированное устройство (межсетевой экран) для обеспечения защиты информационной сети

- знать и правильно использовать средства защиты информации и обеспечивать сохранность информационных ресурсов с помощью этих средств;

- информировать руководителей структурных подразделений о любых нарушениях требований настоящей инструкции и других негативных ситуациях, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе сети.

7. Администратор безопасности имеет право:

- при обнаружении доступа к сайтам развлекательного характера, запретить доступ к сайту;

- при обнаружении использования пользователем программных продуктов, которые могут привести к несанкционированному доступу, модификации, разрушению, удалению информационных ресурсов или сбоям в работе, запретить доступ к сети Интернет.

Приложение № 8
к постановлению администрации
города Кировска от 23.07.2020 №643

Инструкция по работе со съемными носителями информации

1. Данная инструкция определяет полномочия, обязанности и ответственность сотрудников администрации города Кировска при использовании съемных носителей информации.

2. Съемными носителями информации являются:

- USB-накопители (флэш-диски);
- съемные накопители на жестких магнитных дисках (НЖМД);
- дискеты;
- др.

3. Все находящиеся на хранении и в обращении в Администрации города Кировска съемные носители (диски, дискеты, USB флеш-накопители, пр.), содержащие конфиденциальную информацию и персональные данные, подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

4. Учет и выдачу съемных носителей осуществляют работники отдела информационно-программного обеспечения Администрации. Учет съемных носителей должен вестись в Журнале учета.

5. Хранение съемных носителей должно осуществляться в местах не доступных для посторонних лиц, также для должностных лиц, не имеющих полномочий на обработку персональных данных и конфиденциальной информации для выполнения должностных обязанностей.

6. При отправке или передаче информации адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка информации адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

7. Запрещается использовать учтенные съемные носители в личных целях.

8. О фактах утраты съемных носителей, содержащих персональные данные и конфиденциальную информацию, либо разглашения содержащихся в них сведений должно быть немедленно сообщено ответственному по информационной безопасности и технической защите информации и персональных данных.

Приложение № 9
к постановлению администрации
города Кировска от 23.07.2020 № 643

Инструкция по обеспечению безопасности информации, обрабатываемой в автоматизированной информационной системе администрации города Кировска при возникновении внештатных ситуаций

1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием автоматизированной информационной системы администрации города Кировска (далее - АИС), меры и средства поддержания непрерывности работы и восстановления работоспособности АИС после аварийных ситуаций.

2. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов АИС. Аварийная ситуация становится возможной в результате реализации одной из угроз:

2.3 Технологические угрозы:

- пожар в здании;
- повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения);
- взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением);
- химический выброс в атмосферу;

2.4 Стихийные бедствия:

- удар молнии;
- сильные морозы;
- просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания;
- подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод);

2.5 Телеком и ИТ угрозы:

- сбой системы кондиционирования;
- сбой ИТ – систем;

2.6 Угроза, связанная с человеческим фактором:

- ошибка персонала, имеющего доступ к серверной;
- нарушение конфиденциальности, целостности и доступности конфиденциальной информации;

2.7 Угрозы, связанные с внешними поставщиками:

- отключение электроэнергии;
- сбой в работе интернет-провайдера;
- физически разрыв внешних каналов связи;

3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством.

4. Для обеспечения восстановления работоспособности АИС в кратчайшие сроки при возникновении аварийных ситуаций необходимо выполнение следующих мер:

4.1 Ответственный за организацию обработки персональных данных, ответственный по информационной безопасности и технической защите информации и персональных данных, Администратор безопасности АИС должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов АИС.

4.2 Организационные меры:

- регулярные проверки навыков и знаний по реагированию на аварийные ситуации;

- дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации: оказание первой медицинской помощи, пожаротушение, эвакуация людей, защита материальных и информационных ресурсов, методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию, выключение оборудования, электричества, водоснабжения, газоснабжения.

4.3 Технические меры обеспечения непрерывной работы и восстановления:

- обеспечение резервного копирования и хранения данных;
- контроль физического доступа;
- наличие пожарные сигнализации и системы пожаротушения;
- наличие системы резервного питания.

Приложение № 10
к постановлению администрации
города Кировска от 23.07.2020 № 643

Регламент оценки вреда, который может быть причинен субъекту персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер

1. Определение возможного вреда субъектам ПДн производится коллегиально комиссией или рабочей группой.

2. В комиссию должны включатся следующие лица:

- лицо, ответственное за организацию обработки ПДн;
- администратор безопасности АИС.

3. При оценке вреда субъекту персональных данных необходимо учитывать присвоенный класс государственной информационной системы и уровень защищенности персональных данных, а также возможные юридические последствия и моральный вред субъекту персональных данных.

4. Актом классификации №1 от 30.09.2019 АИС администрации присвоен класс государственной информационной системы К3. В соответствии с присвоенным классом в результате нарушения свойств безопасности АИС администрации возможны лишь незначительные негативные последствия.

5. К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы. Возможные юридические последствия и моральный вред определяется членами комиссии в соответствии с законодательством РФ, Мурманской области, города Кировска, нормативными документами Администрации и другими документами.

6. По результатам оценки составляется Акт.

Приложение № 11 к постановлению
администрации города Кировска
от 23.07.2020 № 643

Перечень помещений, предназначенных для обработки конфиденциальной информации, в том числе персональных данных, содержащихся в автоматизированной информационной системе администрации города Кировска

№	Наименование помещения	Адрес местонахождения
1	Кабинет №101 комитет по управлению муниципальной собственностью администрации города Кировска	г. Кировск, пр. Ленина, 16
2	Кабинет №204 отдел муниципальной службы и противодействия коррупции администрации города Кировска	г. Кировск, пр. Ленина, 16
3	Кабинет №205 отдел муниципальной службы и противодействия коррупции администрации города Кировска	г. Кировск, пр. Ленина, 16
4	Кабинет №301 комитет по управлению муниципальной собственностью администрации города Кировска	г. Кировск, пр. Ленина, 16
5	Кабинет №302 комитет по управлению муниципальной собственностью администрации города Кировска	г. Кировск, пр. Ленина, 16
6	Кабинет №308 комитет по управлению муниципальной собственностью администрации города Кировска	г. Кировск, пр. Ленина, 16
7	Кабинет №310 комитет по управлению муниципальной собственностью администрации города Кировска	г. Кировск, пр. Ленина, 16
8	Кабинет №311 комитет по управлению муниципальной собственностью администрации города Кировска	г. Кировск, пр. Ленина, 16
9	Кабинет №312 комитет по управлению муниципальной собственностью администрации города Кировска	г. Кировск, пр. Ленина, 16
10	Кабинет №3 комиссия по делам несовершеннолетних и защите их прав, административная комиссия	г. Кировск, пр. Ленина, 18, 4-й этаж
11	Кабинет №1 отдел опеки и попечительства администрации города Кировска	г. Кировск, пр. Ленина, 18, 2-й этаж
12	Кабинет №2 отдел опеки и попечительства администрации города Кировска	г. Кировск, пр. Ленина, 18, 2-й этаж
13	Кабинет №3 отдел опеки и попечительства администрации города Кировска	г. Кировск, пр. Ленина, 18, 2-й этаж
14	Кабинет специалистов отдела ЗАГС администрации города Кировска	г. Кировск, пр. Ленина, 27, ЗАГС
15	Архив отдела ЗАГС администрации города Кировска	г. Кировск, пр. Ленина, 27, ЗАГС