ПРИЛОЖЕНИЕ 14

к распоряжению администрации

Белоярского района

от 30 сентября 2019 года № 274-р

**РУКОВОДСТВО**

**по защите информации в администрации Белоярского района**

Руководство по защите информации в администрации Белоярского района (далее - Руководство) на объектах информатизации администрации Белоярского района, разработано в соответствии с требованиями Федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных» и приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Настоящее Руководство определяет содержание и порядок осуществления мероприятий по защите информации, не составляющей государственную тайну, содержащейся в информационных системах, от угроз безопасности информации.

Защита информации информационной системы (далее – ИС) осуществляется в соответствии с требованиями законодательства РФ по защите информации.

Требования Руководства являются обязательными для исполнения всеми должностными лицами и работниками администрации Белоярского района при проведении ими работ, связанных с использованием информации, не составляющей государственную тайну, содержащейся в ИС, а также представителями сторонних организаций, выполняющих работы на объектах защиты.

Изменения в Руководство вносятся, согласовываются и утверждаются в том же порядке и на том же уровне, что и основной документ.

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

1.1. Обработка информации, не составляющей государственную тайну, содержащейся в ИС, в администрации Белоярского района осуществляется на основании Правил обработки персональных данных.

1.2. Проведение в администрации Белоярского района любых мероприятий и работ с использованием информации, содержащейся в ИС, без принятия необходимых мер по защите информации не допускается.

1.3. Главными направлениями работ по защите информации являются:

1) обеспечение эффективного управления системой защиты информации;

2) анализ и оценка угроз безопасности информации, реальной опасности несанкционированного доступа, разрушения (уничтожения) или искажения информации путем преднамеренных программно-технических воздействий в процессе ее обработки, передачи и хранения в ИС;

3) разработка организационно-технических мероприятий по защите информации и их реализация;

4) обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

5) организация и проведение контроля состояния защиты информации.

1.4. В состав объектов защиты входят защищаемые объекты информатизации:

1) автоматизированные системы на базе средств вычислительной техники (автоматизированные рабочие места, входящие в состав локальных вычислительных сетей; локальные вычислительные сети; системы связи и передачи данных; средства изготовления и тиражирования документов), используемые для обработки информации, не составляющей государственную тайну, содержащейся в ИС;

2) помещения, размещающие объекты ИС.

Перечень конкретных защищаемых объектов ИС в администрации Белоярского района определен в Техническом паспорте ИС.

1.5. Информация, содержащаяся в ИС, обрабатывается с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств защиты, сертифицированных в установленном порядке.

Обработка информации, содержащейся в ИС, с помощью технических средств производится на объектах информатизации, аттестованных на предмет соответствия применяемых методов, мер и средств защиты.

**2. СВЕДЕНИЯ, ПОДЛЕЖАЩИЕ ОГРАНИЧЕНИЮ ПО ДОСТУПУ**

2.1. В интересах обеспечения защиты информации от ее утечки, разрушения, блокирования, несанкционированного копирования и модификации, защите подлежат информационные ресурсы, содержащие сведения:

1) составляющие защищаемую информацию;

2) об организации защиты информации в администрации Белоярского района;

3) составляющие тайну физических лиц, в том числе персональные данные;

4) общедоступная информация, являющаяся ценной как информационный ресурс и требующая защиты от уничтожения, искажения, подделки, блокирования.

2.2. Сведениями об организации защиты информации в администрации Белоярского района являются:

1) перечень объектов информатизации;

2) перечень защищаемой информации;

3) руководство по защите информации ИС;

4) акты классификации государственных информационных систем и определения уровня защищенности персональных данных в информационных системах;

5) технические паспорта ИС;

6) эксплуатационно-техническая документация объектов информатизации и средств связи;

7) логины и пароли доступа к информационным ресурсам;

8) результаты контроля эффективности средств защиты информации;

9) материалы аттестационных испытаний объектов информатизации;

10) сведения о фактическом состоянии защиты ИС;

11) иные сведения, раскрывающие структуру, содержание и эффективность системы защиты информации на объектах.

2.3. Обеспечение защиты информации определяется Техническим заданием на создание системы защиты ИС.

2.3.1. Также определяется следующими нормативно-техническими документами:

а) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

б) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

в) Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

г) Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

д) Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

е) Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

ж) Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

з) Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

и) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. заместителем директора ФСТЭК России 15 февраля 2008 г.);

к) «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» №149/7/2/6-432 от 31.03.2015 г;

л) Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

м) Методический документ ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»;

н) «Методический документ. Методика. Определения угроз безопасности информации. В информационных системах.» Проект ФСТЭК России;

защищенном исполнении. Общие требования» (далее - ГОСТ Р 51624).

2.4. Администрации Белоярского района как собственник (обладатель информации) ИС:

1) устанавливает порядок предоставления в пользование информации с указанием ответственных должностных лиц, а также необходимых процедур и обеспечивает условия доступа пользователей к информации;

2) назначает лиц, осуществляющих оперативным управлением и защиту ИС;

3) устанавливает в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;

4) определяет условия распоряжения документами при их копировании и распространении.

**3. ЗАЩИТА ИНФОРМАЦИИ, ПОДЛЕЖАЩЕЙ   
ОГРАНИЧЕНИЮ ПО ДОСТУПУ**

3.1. Целями защиты информации являются:

1. обеспечение защищенности ИС в процессе обработки и хранения защищаемой информации;
2. обеспечение конфиденциальности защищаемой информации при ее обработке, а также других необходимых характеристик защищенности информации;
3. предотвращение несанкционированного уничтожения, искажения, копирования и блокирования информации в ИС;
4. соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах обработки;
5. сохранение возможности управления процессом обработки и пользования информацией.

3.2. Защита информации осуществляется путем:

1) исключения несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации;

2) предотвращения программных воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации.

3.3. Исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации достигается применением программных и программно-аппаратных средств защиты, использованием криптографических способов защиты, а также организационными и режимными мероприятиями.

3.4. Предотвращение программных воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации, достигается применением специальных программных средств защиты (антивирусные программы), организацией системы контроля безопасности программного обеспечения.

**4.** **ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ   
ПО ЗАЩИТЕ ИНФОРМАЦИИ**

4.1 К основным мероприятиям по защите информации в ИС относятся:

1. выделение и обеспечение контролируемой зоны;
2. организация и контроль доступа в помещения ИС;
3. инструктирование работников, работающих в помещениях ИС, по правилам эксплуатации технических средств обработки информации;
4. обеспечение защиты информации в ходе эксплуатации ИС;
5. инструктирование работников, работающих с ИС, по правилам эксплуатации и защиты ИС;
6. использование сертифицированных программно-аппаратных средств защиты от НСД;
7. назначение работников, ответственных за соблюдение требований по обработке информации и по защите информации;
8. классификация ИС;
9. использование в ИС источников бесперебойного питания;
10. использование лицензионных антивирусных программ в процессе эксплуатации АС;
11. использование в ИС средств резервного копирования информации;
12. аттестация ИС по требованиям безопасности информации;
13. реагирование на инциденты информационной безопасности в ходе эксплуатации ИС;
14. управление конфигурацией информационной системы и систем защиты персональных данных в ходе эксплуатации ИС;
15. контроль (анализ) состояния защищенности ИС.

**5. ДОСТУП К ИСПОЛЬЗОВАНИЮ РЕСУРСОВ ИС**

5.1. Допуск к работе с защищаемой информацией ИС имеют работники администрации Белоярского района, в том числе и находящиеся на испытательном сроке, которые:

1) ознакомлены под подпись с настоящим Руководством;

2) ознакомлены под подпись с иными организационно-распорядительными документами по защите информации;

3) подписали Соглашение о неразглашении конфиденциальной информации;

4) занимают должности, указанные в Списке лиц, допущенных к работе с персональными данными в администрации Белоярского района. (Запрещается допускать к работе с защищаемой информацией ИС других лиц без письменного разрешения главы Белоярского района.)

5.2. Под допуском подразумевается официальное присвоение работнику администрации Белоярского района конкретного уровня доступа (группы в ИС), дающего ему возможность использовать ресурсы ИС и обмена данными на заданном четко категорированном уровне и в ограниченном должностными обязанностями (не превышающем его непосредственные задачи) объеме.

5.3. Обязанности по присвоению уровня доступа возлагаются на руководителя органа администрации Белоярского района или администратора ИС. При этом необходимо руководствоваться принципами разумного ограничения возможностей и разграничения доступа к различным сведениям. Администратор ИС несет ответственность за регистрацию и предоставление (изменение) полномочий.

5.4. Все пользователи ИС подлежат учету по категориям установленного допуска и другим системным параметрам.

5.5. Привилегии системного администратора, кроме тех работников, которым должностными обязанностями предписано выполнять работы по эксплуатации и ремонту информационных ресурсов, имеют право получать работники отдела по информационным ресурсам и защите информации и другие должностные лица по согласованию с администратором безопасности информационной системы персональных данных (далее – ИСПДн) и с разрешения начальника отдела по информационным ресурсам и защите информации. Все лица, имеющие права системного администратора, подлежат отдельному учету.

**6. ХРАНЕНИЕ НОСИТЕЛЕЙ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ**

6.1. Съемные машинные носители защищаемой информации хранятся в недоступном для посторонних лиц месте (сейф, металлический шкаф, файл-бокс), исключающем несанкционированный доступ и пользование ими.

Сейф (несгораемый металлический шкаф) должен быть постоянно закрыт на ключ, а в нерабочее время опечатан.

В отделе должен быть один комплект ключей от сейфов — у руководителя органа администрации Белоярского района (ответственного работника администрации Белоярского района). Остальные комплекты должны храниться в сейфе в опечатанном пенале.

**7.** **ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ И РЕАГИРОВАНИЕ НА НИХ**

7.1. При получении информации об инцидентах информационной безопасности работники администрации Белоярского района обязаны своевременно проинформировать администратора безопасности администрации Белоярского района.

7.2. Администратором безопасности при получении информации об инцидентах информационной безопасности принимаются следующие меры:

1. обнаружение, идентификация и регистрация инцидентов;
2. при необходимости прекращение или ограничение в администрации Белоярского района работы технических средств и систем обработки информации ИС;
3. анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
4. принятие мер по устранению последствий инцидентов;
5. планирование и принятие мер по предотвращению повторного возникновения инцидентов.

**8.** **ОБЯЗАННОСТИ И ПРАВА ДОЛЖНОСТНЫХ ЛИЦ**

**8.1.** **Глава Белоярского района несет ответственность:**

1. за сохранность защищаемых информационных ресурсов администрации Белоярского района;
2. за осуществление общего контроля за руководством защиты информации в администрации Белоярского района;
3. утверждает документы в области защиты информации.

**8.2. Начальник отдела по информационным ресурсам и защиты информации** непосредственно организует работы по защите информации в администрации Белоярского района и несет ответственность:

1. за сохранность защищаемой информации, находящейся в его ведении;
2. за создание условий, при которых работники знакомятся только с теми сведениями и в таких объемах, которые необходимы для выполнения ими должностных обязанностей;
3. обеспечивает доступ к документам и работам по направлениям деятельности администрации Белоярского района и распорядительным документам, адресованным ему, а при наличии специального распоряжения - ко всем видам и категориям документов и работ всех исполнителей администрации Белоярского района и командированных из сторонних организаций, которым они необходимы для выполнения служебных обязанностей;
4. решает вопрос о привлечении к проведению работ по защите информации на договорной основе учреждений и организаций, имеющих лицензии на соответствующие виды деятельности.

8.3. **Администратор безопасности** назначается распоряжением главы Белоярского района. Администратор безопасности должен обладать достаточными навыками для выполнения функциональных обязанностей по защите информации.

**Администратор безопасности несет ответственность** согласно обязанностям должностной инструкции, включая обязанности:

1. за сохранность защищаемой информации, находящейся во владении и пользовании администрации Белоярского района;
2. за сохранность личных идентификаторов доступа в ИС, на АРМ управления средствами защиты и сохранение конфиденциальности личных паролей;
3. за эксплуатацию средств защиты информации ИС в соответствии с эксплуатационно-технической документацией ИС;
4. за неизменность состава, структуры и конфигурации аттестованной ИС по требованиям безопасности информации;
5. за организацию резервного копирования информации;
6. за ведение эксплуатационно-технической документации на ИС;
7. за уровень подготовки работников администрации Белоярского района в части защиты информации ИС;
8. полноту и качество выполнения им своих функциональных обязанностей по защите информации.

8.4. **Администраторы ИС** определяются согласно функциональным обязанностям занимаемой должности.

Администратор ИС должен обладать достаточными навыками для выполнения функциональных обязанностей по сопровождению ИС и защите информации.

Администраторы ИС допускаются к обработке защищаемых информационных ресурсов ИС после ознакомления с организационно-распорядительной документацией по защите информации ИС.

**Администратор ИС несет ответственность** согласно обязанностям должностной инструкции и организационно-распорядительной документацией по защите информации, включая обязанности:

1. за сохранность защищаемой информации, находящейся в его владении и пользовании;
2. за сохранность личных идентификаторов доступа в ИС и сохранение конфиденциальности личных паролей;
3. за эксплуатацию программных средств защиты информации, установленных на АРМ и серверах, в соответствии с эксплуатационно-технической документацией ИС;
4. за оперативное принятие мер по изменению учетных данных пользователей ИС при нарушении конфиденциальности личного идентификатора/пароля доступа в ИС.

8.5. **Работник (пользователь ИС)** **допускается** к обработке защищаемых информационных ресурсов ИС в соответствии с режимом доступа работников к ресурсам ИС и после ознакомления с организационно-распорядительной документацией по защите информации ИС.

**Работник (пользователь ИС) несет ответственность**:

1. за сохранность защищаемой информации, находящейся в его владении и пользовании;
2. за сохранность личного идентификатора доступа в ИС и сохранение конфиденциальности личного пароля;
3. за эксплуатацию программных средств защиты информации, установленных на АРМ, в соответствии с эксплуатационно-технической документацией ИС.

**Работник (пользователь ИС) обязан:**

1. знать свои полномочия, правила безопасной обработки информации и основы эксплуатации средств защиты информации;
2. проверять перед началом работы наличие печатей на корпусах АРМ и при выявлении нарушения целостности печатей проинформировать об этом администратора безопасности;
3. контролировать перед началом работы функционирование средств защиты информации и при выявлении нарушения функционирования проинформировать об этом администратора безопасности;
4. осуществлять обработку информации в соответствии с заданием и предоставленными полномочиями;
5. по окончании рабочего дня выключать АРМ;
6. при обнаружении инцидентов информационной безопасности проинформировать об этом администратора безопасности;
7. при нарушении конфиденциальности личного идентификатора/пароля доступа в ИС незамедлительно проинформировать Администраторов ИС.

**9**. **ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ХОДЕ ЭКСПЛУАТАЦИИ АТТЕСТОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ**

9.1. Обеспечение защиты информации в ходе эксплуатации аттестованной ИС осуществляется работниками администрации Белоярского района в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает:

1. управление (администрирование) системой защиты информации информационной системы;
2. выявление инцидентов и реагирование на них;
3. управление конфигурацией аттестованной информационной системы и ее системы защиты информации;
4. контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

9.2. Контроль за выполнением мероприятий по обеспечению защиты информации осуществляет администратор безопасности администрации Белоярского района, в том числе в соответствии с должностной инструкцией.

9.3. Выявление инцидентов и реагирование на них осуществляется работниками администрации Белоярского района, входящих в перечень лиц, осуществляющих работу в ИС, обеспечивающих функционирование ИС и защиту информации ИС.

9.4. Управление конфигурацией ИС осуществляют администраторы ИС, в том числе в соответствии с их должностной инструкцией.

9.5. Управление системой защиты информации ИС на уровне пользовательской части ИС, осуществляется только администратором безопасности.

9.6. Мероприятия по управлению (администрированию) системы защиты информации ИС и контроль (мониторинг) за обеспечением уровня защищенности информации ИС осуществляются только администратором безопасности, в том числе в соответствии с должностной инструкцией.

**10. ПЛАНИРОВАНИЕ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ И КОНТРОЛЮ**

10.1. Планирование работ по защите информации осуществляется на год.

10.2. Основными руководящими документами для планирования работ по защите информации являются:

1. техническое задание и технический проект на создание системы защиты ИС;
2. приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
3. методический документ ФСТЭК России от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах»;
4. эксплуатационно-техническая документация на программные, программно-аппаратные и технические средства защиты информации;
5. перспективные планы развития материально-технической базы.

10.3. **В план работы по защите информации включаются:**

1. мероприятия по выполнению законодательных актов, решений ФСТЭК России;
2. подготовка проектов распорядительных документов по вопросам организации защиты информации в администрации Белоярского района (постановлений, инструкций, методических рекомендаций, памяток по обеспечению безопасности информации), конкретных подразделений, технических средств обработки информации и выделенных помещений;
3. мероприятия по подготовке и аттестации объектов на соответствие требованиям по защите информации;
4. мероприятия по проведению контроля эффективности защиты информации;
5. мероприятия по совершенствованию защиты информации в администрации Белоярского района;
6. мероприятия по организации устранения выявленных нарушений и недостатков в организации защиты информации.

Организация и контроль выполнения планов и отчетность по ним возлагаются на заместителя руководителя департамента правового и информационного обеспечения.

10.4. Проекты планов разрабатываются отделом по информационным ресурсам и защиты информации (администратором безопасности ИСПДн) и утверждаются главой Белоярского района. Сроки разработки, представления и утверждения планов определяются регламентом работы администрации Белоярского района.

**11. КОНТРОЛЬ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ И СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ИС**

11.1. Контроль состояния защиты информации и состояния защищенности ИС осуществляется с целью своевременного выявления и предотвращения нарушения безопасности информации, несанкционированного доступа к ней, преднамеренных программных воздействий на информацию и оценки защиты ее от угроз безопасности информации.

Контроль заключается в проверке выполнения актов законодательства Российской Федерации по вопросам защиты информации, решений ФСТЭК Российской Федерации, а также в оценке обоснованности и эффективности принятых мер защиты для обеспечения выполнения утвержденных требований и норм по защите информации.

11.2. Контроль состояния защитыорганизуется:

1) контролирующими органами в сфере защиты информации (ФСТЭК России, ФСБ России);

2) действующей рабочей группой администрации Белоярского района;

3) органом по аттестации, выдавшим аттестат соответствия.

Контролирующие органы осуществляют контроль объектов информатизации в соответствии со своей компетенцией.

12.3. Контроль состояния защиты информации в государственных информационных системах осуществляется ФСТЭК России в установленном порядке по предъявлении специального удостоверения представителя ФСТЭК России и предписания на право проведения проверки данного объекта.

Контроль безопасности информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией в соответствии с Положением по аттестации объектов информатизации по требованиям безопасности информации осуществляется представителями Органа по аттестации, выдавшего аттестат соответствия на данный объект, по предъявлении Предписаний на право проведения проверки данного объекта и документа, удостоверяющего личность.

Контроль состояния защиты информации по вопросам, относящимся к компетенции Федеральной службы безопасности Российской Федерации осуществляется в порядке, установленном ФСБ России.

11.4. Контроль состояния защищенности ИС осуществляется администратором безопасности.

11.5. Защита информации считается эффективной, если принимаемые меры соответствуют установленным требованиям или нормам.

Несоответствие мер установленным требованиям или нормам по защите информации является нарушением.

Нарушения по степени важности делятся на три категории:

***первая* -** невыполнение требований или норм по защите информации, в результате чего имелась или имеется реальная возможность нарушение безопасности информации ИС;

***вторая*** - невыполнение требований по защите информации, в результате чего создаются предпосылки к нарушению безопасности информации ИС;

***третья* -** невыполнение других требований по защите информации.

11.6. **При обнаружении нарушений первой категории администратор безопасности ИСПДн:**

1) немедленно прекращает работы на рабочем месте или сервере, где обнаружены нарушения, и принимает меры по их устранению;

2) организует расследование причин и условий появления нарушений с целью недопущения их в дальнейшем и привлечения к ответственности виновных лиц;

3) сообщает начальнику отдела по информационным ресурсам и защите информации о вскрытых нарушениях и принятых мерах.

Возобновление работ разрешается после устранения нарушений и проверки достаточности и эффективности принятых мер.

11.7. При обнаружении нарушений второй и третьей категорий администратор безопасности принимает необходимые меры по их устранению в ближайшие сроки.

11.8. При организации контроля состояния защищенности ИС, эффективности средств защиты информации должностными лицами администрации Белоярского района разрабатывается план контроля состояния защищенности информации администрации Белоярского района и утверждается главой Белоярского района. Планирование осуществляется на один год.

**Периодичность контроля:**

1) работоспособности программно-аппаратных и технических средств защиты, опечатывания корпусов АРМ - постоянно (при включении);

2) эффективности технических средств защиты (аппаратурный контроль) - не менее 1 раза в год силами организаций, имеющих лицензию ФСТЭК России;

3) смены паролей пользователей, соответствия настройки ПАК защиты от НСД, содержимого машинных носителей и их учета, наличия оригиналов программных средств - с периодичностью, определяемой объемами и интенсивностью обработки информации.

Контроль отдельных средств и их параметров может осуществляться внезапно.

Обязательным является аппаратурный контроль эффективности средств защиты при вводе их в эксплуатацию и после проведения их ремонта.

**12**. **Взаимодействие с другими учреждениями**

**(органами власти, организациями)**

12.1. При проведении совместных работ администрации Белоярского района с иными органами власти, учреждениями и организациями должна быть обеспечена защита информации независимо от места проведения работ.

12.2. В технических заданиях (договорах) на выполнение совместных работ с использованием информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, должны быть предусмотрены обязанности и меры по защите этих сведений от угроз безопасности информации, которые должны выполняться каждой из сторон.

12.3. Организация защиты информации возлагается на руководителей совместных работ и администратора безопасности, ответственность за обеспечение защиты информации - на исполнителей работ при использовании ими технических средств для обработки и передачи информации, подлежащей защите.

**13**. **Обеспечение защиты информации при выводе из эксплуатации, аттестованной ИС или после принятия решения об окончании обработки информации**

13.1. Обеспечение защиты информации при выводе из эксплуатации, аттестованной ИС или после принятия решения об окончании обработки информации осуществляется администрацией Белоярского района в соответствии с эксплуатационной документацией на систему защиты информации ИС и организационно-распорядительными документами по защите информации и в том числе включает:

1. архивирование информации, содержащейся в информационной системе;
2. уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

13.2. Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности администрации Белоярского района.

13.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

13.4. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

13.5. Контроль за выполнением мероприятий по обеспечению защиты информации при выводе из эксплуатации, аттестованной ИС, или после принятия решения об окончании обработки информации осуществляет администратор безопасности, в том числе в соответствии с должностной инструкцией.