**Периодическое печатное издание
органов местного самоуправления
Баганского района Новосибирской области**

30 августа 2024 г.

Бюллетень органов местного самоуправления Баганского района

№ 21(348)
Издаётся с марта 2012 года

с. Баган

Периодическое печатное издание
органов местного самоуправления
Баганского района Новосибирской области

30 августа 2024 г.

Бюллетень органов местного самоуправления Баганского района

№ 21(348)
Издается с марта 2012 года

Бюллетень органов местного самоуправления Баганского района Новосибирской области издается в соответствии с решением восемнадцатой сессии Совета депутатов Баганского района Новосибирской области от 20 декабря 2011 года № 161 «Об учреждении периодического печатного издания «Бюллетень органов местного самоуправления Баганского района»»

Бюллетень состоит из четырех разделов:

- в первом разделе – правовые акты, принятые на местном референдуме; решения Совета депутатов Баганского района;

- во втором – правовые акты администрации района, иных органов местного самоуправления и должностных лиц местного самоуправления района;

- в третьем – официальные сообщения и материалы органов местного самоуправления Баганского района;

- в четвертом – иная информация в случаях, установленных федеральными законами и иными нормативными правовыми актами Российской Федерации, нормативными правовыми актами Новосибирской области, муниципальными правовыми актами Баганского района.

Редакционный совет

Артёменко Наталья Александровна – начальник отдела организационно-контрольной работы администрации района, председатель Редакционного совета.

Члены Редакционного совета:

Пупкова Наталья Александровна - главный специалист по работе с представительным органом отдела общественных связей, информации и работы с населением администрации района;

Кусь Татьяна Александровна – начальник отдела правовой и кадровой работы администрации района;

Нестерова Людмила Александровна, депутат Совета депутатов Баганского района от избирательного округа № 7;

Алтухова Светлана Юрьевна, депутат Совета депутатов Баганского района от избирательного округа № 4.

Адрес редакции и издателя:
ул. М. Горького, 28, с. Баган, Новосибирская область, 632770
Телефоны: 21-109, 21-984, 21-742
E-mail: admbagan@nso.ru
Тираж 37

Первый раздел.

ГЛАВА
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

20.08.2024 № 38

О назначении общественных обсуждений по проекту генерального плана Кузнецовского сельсовета Баганского района Новосибирской области

В целях выявления и учета мнения интересов жителей сельский поселений Баганского района Новосибирской области по проекту генеральных планов сельских поселений Баганского района Новосибирской области, в соответствии с Градостроительным кодексом Российской Федерации, Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», «Положение о порядке проведения общественных обсуждений по вопросам, предусмотренным Градостроительным кодексом Российской Федерации на территории Баганского района Новосибирской области», утвержденным решением сорок первой сессии Совета депутатов Баганского района Новосибирской области третьего созыва от 23.06.2020 года. №335, Законом Новосибирской области от 18.12.2015 № 27-ОЗ «О перераспределении полномочий между органами местного самоуправления муниципальных образований Новосибирской области и органами государственной власти Новосибирской области и внесении изменения в статью 3 Закона Новосибирской области «Об отдельных вопросах организации местного самоуправления в Новосибирской области»,

ПОСТАНОВЛЯЮ:

1.Назначить проведение общественных обсуждений по проекту генерального плана Кузнецовского сельсовета Баганского района Новосибирской области с 26.08.2024 по 20.09.2024 года

2.Отделу строительства и дорожного комплекса администрации Баганского района Новосибирской области обеспечить проведение общественных обсуждений на сайте Баганского района Новосибирской области.

3.Предложить гражданам, проживающим на территории, применительно к которой осуществляется подготовка генерального плана, правообладателям земельных участков и объектов капитального строительства, расположенных на указанной территории, лицам, законные интересы которых могут быть нарушены в связи с реализацией такого генерального плана принять участие в проведение общественных обсуждений по проекту генерального плана Кузнецовского сельсовета Баганского района Новосибирской области. Опубликовать настоящее постановление в периодическом издании «Бюллетень» органов местного самоуправления и разместить на официальном сайте администрации Баганского района Новосибирской области.

4.Контроль за исполнением постановления возложить на заместителя главы администрации Баганского района А.О. Бреус.

Глава Баганского района
Новосибирской области А.А. Воличенко

ГЛАВА
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 39

О назначении общественных обсуждений по проекту генерального плана Казанского сельсовета Баганского района Новосибирской области

В целях выявления и учета мнения интересов жителей сельский поселений Баганского района Новосибирской области по проекту генеральных планов сельских поселений Баганского района Новосибирской области, в соответствии с Градостроительным кодексом Российской Федерации, Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», «Положение о порядке проведения общественных обсуждений по вопросам, предусмотренным Градостроительным кодексом Российской Федерации на территории Баганского района Новосибирской области», утвержденным решением сорок первой сессии Совета депутатов Баганского района Новосибирской области третьего созыва от 23.06.2020 года. №335, Законом Новосибирской области от 18.12.2015 № 27-ОЗ «О перераспределении полномочий между органами местного самоуправления муниципальных образований Новосибирской области и органами государственной власти Новосибирской области и внесении изменения в статью 3 Закона Новосибирской области «Об отдельных вопросах организации местного самоуправления в Новосибирской области»,

ПОСТАНОВЛЯЮ:

1.Назначить проведение общественных обсуждений по проекту генерального плана Казанского сельсовета Баганского района Новосибирской области с 26.08.2024 по 20.09.2024 года

2.Отделу строительства и дорожного комплекса администрации Баганского района Новосибирской области обеспечить проведение общественных обсуждений на сайте Баганского района Новосибирской области.

3.Предложить гражданам, проживающим на территории, применительно к которой осуществляется подготовка генерального плана, правообладателям земельных участков и объектов капитального строительства, расположенных на указанной территории, лицам, законные интересы которых могут быть нарушены в связи с реализацией такого генерального плана принять участие в проведение общественных обсуждений по проекту генерального

плана Казанского сельсовета Баганского района Новосибирской области. Опубликовать настоящее постановление в периодическом издании «Бюллетень» органов местного самоуправления и разместить на официальном сайте администрации Баганского района Новосибирской области.

4.Контроль за исполнением постановления возложить на заместителя главы администрации Баганского района А.О. Бреус.

Глава Баганского района
Новосибирской области А.А. Воличенко

ГЛАВА
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 40

О назначении общественных обсуждений по проекту генерального плана Савкинского сельсовета Баганского района Новосибирской области

В целях выявления и учета мнения интересов жителей сельский поселений Баганского района Новосибирской области по проекту генеральных планов сельских поселений Баганского района Новосибирской области, в соответствии с Градостроительным кодексом Российской Федерации, Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», «Положение о порядке проведения общественных обсуждений по вопросам, предусмотренным Градостроительным кодексом Российской Федерации на территории Баганского района Новосибирской области», утвержденным решением сорок первой сессии Совета депутатов Баганского района Новосибирской области третьего созыва от 23.06.2020 года. №335, Законом Новосибирской области от 18.12.2015 № 27-ОЗ «О перераспределении полномочий между органами местного самоуправления муниципальных образований Новосибирской области и органами государственной власти Новосибирской области и внесении изменения в статью 3 Закона Новосибирской области «Об отдельных вопросах организации местного самоуправления в Новосибирской области»,

ПОСТАНОВЛЯЮ:

1.Назначить проведение общественных обсуждений по проекту генерального плана Савкинского сельсовета Баганского района Новосибирской области с 26.08.2024 по 20.09.2024 года

2.Отделу строительства и дорожного комплекса администрации Баганского района Новосибирской области обеспечить проведение общественных обсуждений на сайте Баганского района Новосибирской области.

3.Предложить гражданам, проживающим на территории, применительно к которой осуществляется подготовка генерального плана, правообладателям земельных участков и объектов капитального строительства, расположенных на указанной территории, лицам, законные интересы которых могут быть нарушены в связи с реализацией такого

генерального плана принять участие в проведение общественных обсуждений по проекту генерального плана Савкинского сельсовета Баганского района Новосибирской области. Опубликовать настоящее постановление в периодическом издании «Бюллетень» органов местного самоуправления и разместить на официальном сайте администрации Баганского района Новосибирской области.

4.Контроль за исполнением постановления возложить на заместителя главы администрации Баганского района А.О. Бреус.

Глава Баганского района
Новосибирской области А.А. Воличенко

Глава
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

26.08.2024 № 42а

О назначении общественных обсуждений по проекту планировки и проекту межевания территории по объекту «Реконструкция водопровода в с. Гнедухино Баганского района Новосибирской области»

В целях выявления и учета мнения интересов жителей сельский поселений Баганского района Новосибирской области по проекту правил землепользования и застройки сельских поселений Баганского района Новосибирской области, в соответствии с Градостроительным кодексом Российской Федерации, Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», «Положение о порядке проведения общественных обсуждений по вопросам, предусмотренным Градостроительным кодексом Российской Федерации на территории Баганского района Новосибирской области», утвержденным решением сорок первой сессии Совета депутатов Баганского района Новосибирской области третьего созыва от 23.06.2020 года. №335, Законом Новосибирской области от 18.12.2015 № 27-ОЗ «О перераспределении полномочий между органами местного самоуправления муниципальных образований Новосибирской области и органами государственной власти Новосибирской области и внесении изменения в статью 3 Закона Новосибирской области «Об отдельных вопросах организации местного самоуправления в Новосибирской области»,

ПОСТАНОВЛЯЮ:

1.Установить сроки проведения общественных обсуждений по проекту планировки и проекту межевания территории по объекту «Реконструкция водопровода в с. Гнедухино Баганского района Новосибирской области» с 28.08.2024 года до 13.09.2024 года.

2.Опубликовать оповещение о начале общественных обсуждений на официальном сайте администрации Баганского района Новосибирской области в сети «Интернет» по адресу: https://bagan.nso.ru/

3.Назначить отдел строительства и дорожного комплекса администрации Баганского района Новосибирской области уполномоченным поорганизации и проведению общественных обсуждений.

3.1.Организовать экспозицию материалов в кабинете №15 здания администрации Баганского района Новосибирской области по адресу с. Баган ул. М. Горького,21.

3.2.Организовать учет предложений и замечаний общественных обсуждений для включения их в протокол и заключение о результатахобщественных обсуждений.

3.3. Подготовить протокол и заключение о результатах общественных обсуждений;

3.4. Заключение о результатах общественных обсуждений разместить на официальном сайте администрации Баганского района в сети «Интернет» по адресу: https://bagan.nso.ru/ в срок до 18.09.2024 года;

4.Контроль за исполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области А.О.Бреус.

Глава Баганского района
Новосибирской области А.А. Воличенко

Второй раздел.

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

20.08.2024 № 735

Об отмене постановления администрации Баганского района Новосибирской области от 10.04.2024 №275 «Об определении Порядка и условий предоставления организациям федеральной почтовой связи соответствующих технологическим нормам нежилых помещений, находящихся в муниципальной собственности Баганского района Новосибирской области, в существующих (или строящихся) жилых или иных зданиях»

Руководствуясь экспертным заключением министерства юстиции Новосибирской области от 20.05.2024 №1847-02-02-03/9, в целях приведения нормативного правового акта в соответствие с действующим законодательством, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Постановление администрации Баганского района Новосибирской области от 10.04.2024 № 275 «Об определении Порядка и условий предоставления организациям федеральной почтовой связи соответствующих технологическим нормам нежилых помещений, находящихся в муниципальной собственности Баганского района Новосибирской области, в существующих (или строящихся) жилых или иных зданиях» отменить.

2.Данное постановление подлежит размещению на официальном сайте администрации Баганского района Новосибирской области, опубликованию в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района».

3.Настоящее постановление вступает в силу с момента опубликования в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района».

4.Контроль по исполнению настоящего постановления оставляю за собой.

Главы Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 736

Об утверждении схемы теплоснабжения муниципального образования Андреевского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025 года)

В соответствии с Федеральным законом от 27.07.2010 № 190 «О теплоснабжении», Постановлением Правительства Российской Федерации от 22.02.2012 № 154 «О требованиях к схемам теплоснабжения, порядку их разработки и утверждения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему теплоснабжения муниципального образования Андреевского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025года), согласно приложению №1.

2.Постановление от 16.08.2023 № 750 администрации Баганского района «Об утверждении схемы теплоснабжения муниципального образования Андреевского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024г.), признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 737

Об утверждении схемы теплоснабжения муниципального образования Баганского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025года)

В соответствии с Федеральным законом от 27.07.2010 № 190 «О теплоснабжении», Постановлением Правительства Российской Федерации от 22.02.2012 № 154 «О требованиях к схемам теплоснабжения, порядку их разработки и утверждения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему теплоснабжения муниципального образования Баганского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.), согласно приложению №1.

2.Постановление от 16.08.2024 № 751 администрации Баганского района «Об утверждении схемы теплоснабжения муниципального образования Баганского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024г.)», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 738

Об утверждении схемы теплоснабжения муниципального образования Ивановского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025года).

В соответствии с Федеральным законом от 27.07.2010 № 190 «О теплоснабжении», Постановлением Правительства Российской Федерации от 22.02.2012 № 154 «О требованиях к схемам теплоснабжения, порядку их разработки и утверждения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему теплоснабжения муниципального образования Ивановского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.), согласно приложению №1.

2.Постановление от 16.08.2023 № 752 администрации Баганского района «Об утверждении схемы теплоснабжения муниципального образования Ивановского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализированную по состоянию на 2024 г.)», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О..

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 739

Об утверждении схемы теплоснабжения муниципального образования Казанского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.)

В соответствии с Федеральным законом от 27.07.2010 № 190 «О теплоснабжении», Постановлением Правительства Российской Федерации от 22.02.2012 № 154 «О требованиях к схемам теплоснабжения, порядку их разработки и утверждения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему теплоснабжения муниципального образования Казанского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.), согласно приложению №1.

2.Постановление от 16.08.2023 № 753 администрации Баганского района «Об утверждении схемы теплоснабжения муниципального образования Казанского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024г.).», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О..

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 740

Об утверждении схемы теплоснабжения муниципального образования Кузнецовского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.).

В соответствии с Федеральным законом от 27.07.2010 № 190 «О теплоснабжении», Постановлением Правительства Российской Федерации от 22.02.2012 № 154 «О требованиях к схемам теплоснабжения, порядку их разработки и утверждения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему теплоснабжения муниципального образования Кузнецовского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.), согласно приложению № 1.

2.Постановление от 16.08.2023 № 754 администрации Баганского района «Об утверждении схемы теплоснабжения муниципального образования Кузнецовского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024г.)», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О..

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 741

Об утверждении схемы теплоснабжения муниципального образования Лозовского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.)

В соответствии с Федеральным законом от 27.07.2010 № 190 «О теплоснабжении», Постановлением Правительства Российской Федерации от 22.02.2012 № 154 «О требованиях к схемам теплоснабжения, порядку их разработки и утверждения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему теплоснабжения муниципального образования Лозовского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.), согласно приложению № 1.

2.Постановление от 16.08.2023 № 756 администрации Баганского района «Об утверждении схемы теплоснабжения муниципального образования Лозовского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024г.)», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О..

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

20.08.2024 № 742

Об утверждении схемы теплоснабжения муниципального образования Мироновского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.)

В соответствии с Федеральным законом от 27.07.2010 № 190 «О теплоснабжении» Постановлением Правительства Российской Федерации от 22.02.2012 № 154 «О требованиях к схемам теплоснабжения, порядку их разработки и утверждения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему теплоснабжения муниципального образования Мироновского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.), согласно приложению №1.

2.Постановление от 16.08.2023 № 755 администрации Баганского района «Об утверждении схемы теплоснабжения муниципального образования Мироновского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024г.).», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О..

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

от 20.08.2024 № 743

Об утверждении схемы теплоснабжения муниципального образования Палецкого сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.)

В соответствии с Федеральным законом от 27.07.2010 № 190 «О теплоснабжении», Постановлением Правительства Российской Федерации от 22.02.2012 № 154 «О требованиях к схемам теплоснабжения, порядку их разработки и утверждения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему теплоснабжения муниципального образования Палецкого сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.), согласно приложению №1.

2.Постановление от 16.08.2023 № 757 администрации Баганского района «Об утверждении схемы теплоснабжения муниципального образования Палецкого сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024г.)», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О..

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

от 20.08.2024 № 744

Об утверждении схемы теплоснабжения муниципального образования Савкинского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.)

В соответствии с Федеральным законом от 27.07.2010 № 190 «О теплоснабжении», Постановлением Правительства Российской Федерации от 22.02.2012 № 154 «О требованиях к схемам теплоснабжения, порядку их разработки и утверждения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему теплоснабжения муниципального образования Савкинского сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025г.), согласно приложению №1.

2.Постановление от 16.08.2023 № 758 администрации Баганского района «Об утверждении схемы теплоснабжения муниципального образования Савкинского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024г.)», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О..

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 745

Об утверждении схемы водоснабжения и водоотведения Андреевского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год)

В соответствии с Федеральным законом от 07.12.2011 года №416-ФЗ «О водоснабжении и водоотведении», постановлением Правительства Российской Федерации от 05.09.2013 года №782 «О схемах водоснабжении и водоотведения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему водоснабжения и водоотведения Андреевского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год), согласно приложению №1.

2.Постановление от 24.06.2022 № 700 администрации Баганского района «Об утверждении схемы водоснабжения и водоотведения муниципального образования Андреевского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024 год)», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 746

Об утверждении схемы водоснабжения и водоотведения Баганского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год)

В соответствии с Федеральным законом от 07.12.2011 года №416-ФЗ «О водоснабжении и водоотведении», постановлением Правительства Российской Федерации от 05.09.2013 года №782 «О схемах водоснабжении и водоотведения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему водоснабжения и водоотведения Баганского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год), согласно приложению №1.

2. Постановление от 16.08.2023 № 759 администрации Баганского района «Об утверждении схемы водоснабжения и водоотведения муниципального образования Баганского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024 год)», признать утратившим силу.

3. Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 747

Об утверждении схемы водоснабжения и водоотведения Ивановского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год)

В соответствии с Федеральным законом от 07.12.2011 года № 416-ФЗ «О водоснабжении и водоотведении», постановлением Правительства Российской Федерации от 05.09.2013 года № 782 «О схемах водоснабжении и водоотведения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему водоснабжения и водоотведения Ивановского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год), согласно приложению №1.

2.Постановление от 16.08.2023 № 761 администрации Баганского района «Об утверждении схемы водоснабжения и водоотведения муниципального образования Ивановского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024 год)», признать утратившим силу.

3. Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 748

Об утверждении схемы водоснабжения и водоотведения Казанского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год)

В соответствии с Федеральным законом от 07.12.2011 года №416-ФЗ «О водоснабжении и водоотведении», постановлением Правительства Российской Федерации от 05.09.2013 года №782 «О схемах водоснабжении и водоотведения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему водоснабжения и водоотведения Казанского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год), согласно приложению №1.

2.Постановление от 16.08.2023 № 762 администрации Баганского района «Об утверждении схемы водоснабжения и водоотведения муниципального образования Казанского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024 год)», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 749

Об утверждении схемы водоснабжения и водоотведения Кузнецовского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год).

В соответствии с Федеральным законом от 07.12.2011 года № 416-ФЗ «О водоснабжении и водоотведении», постановлением Правительства Российской Федерации от 05.09.2013 г. №782 «О схемах водоснабжении и водоотведения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему водоснабжения и водоотведения Кузнецовского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год), согласно приложению №1.

2.Постановление от 16.08.2023 № 763 администрации Баганского района «Об утверждении схемы водоснабжения и водоотведения муниципального образования Кузнецовского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024 год)», признать утратившим силу.

3. Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 750

Об утверждении схемы водоснабжения и водоотведения Лозовского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год)

В соответствии с Федеральным законом от 07.12.2011 года №416-ФЗ «О водоснабжении и водоотведении», постановлением Правительства Российской Федерации от 05.09.2013 года №782 «О схемах водоснабжении и водоотведения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему водоснабжения и водоотведения Лозовского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год), согласно приложению № 1.

2.Постановление от 16.08.2023 № 765 администрации Баганского района «Об утверждении схемы водоснабжения и водоотведения муниципального образования Лозовского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024 год)», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 751

Об утверждении схемы водоснабжения и водоотведения Мироновского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год)

В соответствии с Федеральным законом от 07.12.2011 года №416-ФЗ «О водоснабжении и водоотведении», постановлением Правительства Российской Федерации от 05.09.2013 года №782 «О схемах водоснабжении и водоотведения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему водоснабжения и водоотведения Мироновского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год), согласно приложению №1.

2.Постановление от 16.08.2023 № 764 администрации Баганского района «Об утверждении схемы водоснабжения и водоотведения муниципального образования Мироновского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024 год)», признать утратившим силу.

3. Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 752

Об утверждении схемы водоснабжения и водоотведения Палецкого сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год)

В соответствии с Федеральным законом от 07.12.2011 года № 416-ФЗ «О водоснабжении и водоотведении», постановлением Правительства Российской Федерации от 05.09.2013 года № 782 «О схемах водоснабжении и водоотведения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему водоснабжения и водоотведения Палецкого сельсовета Баганского района Новосибирской области на период до 2040 года (актуализация по состоянию на 2025 год), согласно приложению №1.

2.Постановление от 16.08.2023 № 766 администрации Баганского района «Об утверждении схемы водоснабжения и водоотведения муниципального образования Палецкого сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024 год)», признать утратившим силу.

3.Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

20.08.2024 № 753

Об утверждении схемы водоснабжения и водоотведения Савкинского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год)

В соответствии с Федеральным законом от 07.12.2011 года № 416-ФЗ «О водоснабжении и водоотведении», постановлением Правительства Российской Федерации от 05.09.2013 года №782 «О схемах водоснабжении и водоотведения», с Правилами организации теплоснабжения в Российской Федерации, утвержденными Постановлением Правительства Российской Федерации от 08.08.2012 № 808, с Федеральным законом от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации», руководствуясь Уставом Баганского района, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Утвердить схему водоснабжения и водоотведения Савкинского сельсовета Баганского района Новосибирской области на перспективу до 2040 года (актуализация по состоянию на 2025 год), согласно приложению №1.

2.Постановление от 16.08.2023 № 767 администрации Баганского района «Об утверждении схемы водоснабжения и водоотведения муниципального образования Савкинского сельсовета Баганского района Новосибирской области на период до 2039 года (актуализация по состоянию на 2024 год)», признать утратившим силу.

3. Настоящее постановление опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области» и на официальном сайте в сети интернет.

4.Постановление вступает в силу со дня его официального опубликования.

5.Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

29.08.2024 № 781

О создании комиссии по классификации информационных систем администрации Баганского района Новосибирской области

В целях выполнения требований постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», администрация Баганского района Новосибирской области

П О С Т А Н О В Л Я Е Т :

1. Создать комиссию по классификации информационных систем администрации Баганского района Новосибирской области (далее – Комиссия) в составе:

Бреус А.О.- заместитель главы администрации Баганского района Новосибирской области;

Колобова Е.В.-начальник отдела строительства и дорожного комплекса администрации Баганского района Новосибирской области;

Кусь Т.А. – начальник отдела правовой и кадровой работы администрации Баганского района Новосибирской области;

Удалов А.А. – инженер 1 категории МКУ «Центра бухгалтерского, информационного обеспечения муниципальных закупок Баганского района».

2.Комиссии обеспечить проведение работ по определению уровня защищенности персональных данных при их обработке в информационных системах администрации Баганского района Новосибирской области в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

3.Комиссии обеспечить проведение работ по классификации государственных информационных систем администрации Баганского района Новосибирской области (далее – администрация) в соответствии с Приложением № 1 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17.

4.В случае обработки в государственных информационных системах администрации информации, содержащей персональные данные, проведение работ по классификации государственных информационных систем администрации осуществляется с учетом определенного согласно п. 2 настоящего приказа уровня защищенности персональных данных в соответствии с нижеследующим:

-меры защиты информации, реализуемые для информационной системы первого класса защищенности, обеспечивают 1, 2, 3 и 4 уровни защищенности персональных данных;

-меры защиты информации, реализуемые для информационной системы второго класса защищенности, обеспечивают 2, 3 и 4 уровни защищенности персональных данных;

-меры защиты информации, реализуемые для информационной системы третьего класса защищенности, обеспечивают 3 и 4 уровни защищенности персональных данных.

5.Комиссии по результатам проведения работ по определению уровня защищенности персональных данных при их обработке в информационных системах администрации и классификации государственных информационных систем администрации подготовить соответствующие акты по форме согласно Приложению № 1 и Приложению № 2 к настоящему постановлению.

6.Опубликовать настоящее постановление на официальном сайте органов местного самоуправления Баганского района Новосибирской области и в периодическом печатном издании органов местного самоуправления «Бюллетень органов местного самоуправления Баганского района».

7.Данное постановление вступает в силу после его публикации в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области».

8.Контроль за исполнением настоящего возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

ПРИЛОЖЕНИЕ № 1

к постановлению администрации
Баганского района
Новосибирской области
от 29.08.2024 № 781

ФОРМА

АКТ
определения уровня защищенности персональных данных, обрабатываемых в администрации Баганского района Новосибирской области

Комиссия, назначенная постановлением от _____ № _____ «О создании комиссии по классификации информационных систем администрации Баганского района Новосибирской области», определила уровень защищенности персональных данных, обрабатываемых в Государственной информационной системе обеспечения градостроительной деятельности Новосибирской области».

В соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства Российской Федерации от 01.11.2012 № 1119, комиссия установила:

1. Категория обрабатываемых персональных данных: _____.
2. Категория субъектов персональных данных: _____.
3. Количество субъектов персональных данных: _____.
4. Тип актуальных угроз безопасности информации: _____.
5. Уровень защищенности персональных данных: _____.

Члены комиссии:

_____	_____	_____
(Должность)	(Подпись)	(И.О. Фамилия)
_____	_____	_____
(Должность)	(Подпись)	(И.О. Фамилия)
_____	_____	_____
(Должность)	(Подпись)	(И.О. Фамилия)

ПРИЛОЖЕНИЕ № 2
к постановлению администрации
Баганского района
Новосибирской области
от 29.08.2024 № 781

ФОРМА
АКТ
классификации Государственной информационной системе обеспечения градостроительной деятельности Новосибирской области администрации Баганского района Новосибирской области

Комиссия, назначенная постановлением от _____ № _____ «О создании комиссии по классификации информационных систем администрации Баганского района Новосибирской области», провела классификацию Государственной информационной системе обеспечения градостроительной деятельности Новосибирской области (далее – ГИСОГД НСО).

В соответствии с порядком определения класса защищенности согласно Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17, комиссия установила:

1. Масштаб ГИСОГД НСО: _____.
2. Уровень значимости информации, содержащейся в ГИСОГД НСО: _____.
3. Уровень защищенности персональных данных, обрабатываемых в ГИСОГД НСО: _____.
4. Класс защищенности ГИСОГД НСО: _____.

Члены комиссии:

_____	_____	_____
(Должность)	(Подпись)	(И.О. Фамилия)
_____	_____	_____
(Должность)	(Подпись)	(И.О. Фамилия)
_____	_____	_____
(Должность)	(Подпись)	(И.О. Фамилия)

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

29.08.2024 №782

Об утверждении политики в отношении обработки персональных данных администрации Баганского района Новосибирской области

В целях выполнения требований Федерального закона от 26.07.2006 № 152-ФЗ «О персональных данных», администрация Баганского района Новосибирской области

ПОСТАНОВЛЯЕТ:

1. Утвердить Политику в отношении обработки персональных данных администрации Баганского района Новосибирской области согласно Приложению № 1 к настоящему постановлению.
2. Опубликовать Политику на официальном сайте органов местного самоуправления Баганского района Новосибирской области и в периодическом печатном издании органов местного самоуправления «Бюллетень органов местного самоуправления Баганского района".
3. Данная Политика вступает в силу после его публикации в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области».
4. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации Баганского района Бреус А.О..

Главы Баганского района
Новосибирской области А.А. Воличенко

ПРИЛОЖЕНИЕ
к постановлению администрации
Баганского района
Новосибирской области
от 29.08.2024 № 782

ПОЛИТИКА
в отношении обработки персональных данных администрации Баганского района Новосибирской области

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных администрация Баганского района Новосибирской области (далее – Политика) определяет права и обязанности

сторон, цели и основные принципы обработки персональных данных, а также меры, направленные на защиту персональных данных при их обработке в администрации Баганского района Новосибирской области

1.2. Настоящая Политика разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»).

1.3. Политика вступает в силу с момента ее утверждения.

1.4. Политика подлежит пересмотру в ходе периодического анализа со стороны администрации Баганского района Новосибирской области (далее администрация)

1.5. Основные понятия, используемые в Политике:

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

– оператор – 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;

– обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

– автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

– распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

– предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

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

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

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

1.6. Основные права и обязанности субъектов персональных данных

1.6.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных Оператором;

– правовые основания и цели обработки персональных данных;

– применяемые Оператором способы обработки персональных данных;

– наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть

раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;

– информацию о способах исполнения Оператором обязанностей, установленных статьей 18.1 ФЗ «О персональных данных»;

– иные сведения, предусмотренные ФЗ «О персональных данных» или другими федеральными законами.

1.6.2. Сведения, указанные в пункте 1.5.1 настоящей Политики, предоставляются субъекту персональных данных или его представителю Оператором в течение десяти рабочих дней с момента обращения либо получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен не более чем на пять рабочих дней в случае направления в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя.

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

1.6.4. Субъект персональных данных вправе требовать исключить или исправить неверные или неполные персональные данные, а также данные, обрабатываемые с нарушением требованием ФЗ «О персональных данных».

1.6.5. Субъект персональных данных имеет право требовать об извещении всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта персональных данных, обо всех произведенных в них исключениях, исправлениях или дополнениях.

1.6.6. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

1.6.8. Субъект персональных данных вправе отозвать данное Оператору согласие на обработку своих персональных данных.

1.6.9. Субъект персональных данных вправе осуществлять иные права в соответствии с законодательством Российской Федерации.

1.6.10. Субъект персональных данных обязан предоставлять Оператору достоверные сведения о себе и своевременно информировать об их изменении.

1.7. Основные права и обязанности Оператора

1.7.1. Оператор обязан обрабатывать ПДн в соответствии с действующим законодательством Российской Федерации.

1.7.2. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного контракта, либо путем принятия соответствующего акта[1]. При этом лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные ФЗ «О персональных данных», соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных»;

1.7.3. Оператор обязан не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

1.7.4. Оператор вправе ограничить право субъекта ПДн на доступ к его ПДн/мотивированно отказать субъекту ПДн в предоставлении сведений, касающихся обработки его ПДн, в случаях, установленных законодательством Российской Федерации, в том числе при нарушении субъектом ПДн своих обязанностей по подаче такого запроса или если доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц.

1.7.5. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

1.7.6. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, указанную в пункте 1.5.1 настоящей Политики.

1.7.7. В случае достижения цели обработки ПДн или отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в ФЗ «О персональных данных».

1.7.8. Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации.

1.7.9. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

1.7.10. Оператору запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы. Решение, порождающее юридические последствия в отношении

[1] Лицо, осуществляющее обработку ПДн по поручению оператора, несет ответственность перед Оператором. Оператор несет ответственность перед субъектом ПДн за действия лица, осуществляющего обработку ПДн.

субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

2. Цели сбора персональных данных

2.1. Обработка персональных данных осуществляется на законной и справедливой основе.

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

2.3. Целью обработки персональных данных субъектов является реализация полномочий администрации, а именно:

- кадровое обеспечение деятельности;
- ведение бухгалтерского учета;
- осуществление образовательной деятельности;
- учет обращений граждан;
- исполнение обязанностей, предусмотренных договорами гражданско-правового характера.

2.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Категории субъектов ПДн и состав обрабатываемых ПДн определены настоящей Политикой и соответствуют заявленным целям обработки.

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

2.6. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

3. Правовые основания обработки персональных данных

3.1. Правовым основанием обработки персональных данных является следующая совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных:

- Трудовой кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе»;
- Федеральный закон от 15.12.2001 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Федеральный закон от 16.07.1999 № 165-ФЗ «Об основах обязательного социального страхования»;

– Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

– Постановление Правительства РФ от 27.11.2006 № 719 «Об утверждении Положения о воинском учете»;

– Постановление Правительства РФ от 16.04.2003 № 225 «О трудовых книжках»;

– Постановление Минтруда России от 10.10.2003 № 69 «Об утверждении Инструкции по заполнению трудовых книжек»;

– Приказ Минобрнауки России от 30.08.2013 № 1014 «Об утверждении Порядка организации и осуществления образовательной деятельности по основным общеобразовательным программам - образовательным программам дошкольного образования»;

– Приказ Минобрнауки России от 30.08.2013 № 1015 «Об утверждении Порядка организации и осуществления образовательной деятельности по основным общеобразовательным программам - образовательным программам начального общего, основного общего и среднего общего образования»;

– Устав администрации Баганского района Новосибирской области;

– договоры, заключаемые между Оператором и субъектом персональных данных;

– согласие на обработку персональных данных субъектов персональных данных.

4. Состав и категории обрабатываемых персональных данных, категории субъектов персональных данных

4.1. Сведения о категориях субъектов, персональные данные которых обрабатываются администрацией Баганского района Новосибирской области, категориях и перечне обрабатываемых персональных данных, способах, сроках их обработки и хранения представлены в Приложении № 1 к настоящей Политике.

4.2. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн) и которые используются для установления личности субъекта ПДн, Оператором не обрабатываются.

4.3. Обработка специальных категорий персональных данных Оператором не осуществляется.

5. Порядок и условия обработки персональных данных

5.1. При обработке персональных данных Оператором возможно осуществление следующего перечня действий, совершаемых с персональными данными субъектов: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ, распространение), обезличивание, блокирование, удаление, уничтожение персональных данных.

5.1 Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения[2]

Распространение персональных данных субъектов ПДн допускается при наличии согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, а также в иных случаях, предусмотренных законодательством Российской Федерации, в том числе в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей.

Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, оформляется отдельно от иных согласий субъекта ПДн на обработку его ПДн.

[2] Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения, не применяются в случае обработки персональных данных в целях выполнения возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей

Согласие на обработку ПДн, разрешенных субъектом ПДн для распространения, предоставляется субъектом ПДн непосредственно Оператору в письменной форме.

В случае, если из предоставленного субъектом ПДн согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, не следует, что субъект ПДн согласился с распространением ПДн, такие ПДн обрабатываются Оператором, без права распространения.

В случае, если из предоставленного субъектом ПДн согласия на обработку ПДн, разрешенных субъектом ПДн для распространения, не следует, что субъект ПДн не установил запреты и условия на обработку ПДн, или если в предоставленном субъектом ПДн таком согласии не указаны категории и перечень ПДн, для обработки которых субъект ПДн устанавливает условия и запреты в соответствии с ФЗ «О персональных данных», такие ПДн обрабатываются Оператором без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с ПДн неограниченному кругу лиц.

Молчание или бездействие субъекта ПДн ни при каких обстоятельствах не может считаться согласием на обработку ПДн, разрешенных субъектом ПДн для распространения.

В согласии на обработку ПДн, разрешенных субъектом ПДн для распространения, субъект ПДн вправе установить запреты на передачу (кроме предоставления доступа) этих ПДн Оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих ПДн неограниченным кругом лиц. Отказ Оператора в установлении субъектом ПДн запретов и условий, не допускается.

Оператор обязуется в срок не позднее трех рабочих дней с момента получения соответствующего согласия субъекта ПДн опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц ПДн, разрешенных субъектом ПДн для распространения.

Установленные субъектом ПДн запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) ПДн, разрешенных субъектом ПДн для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

Передача (распространение, предоставление, доступ) ПДн, разрешенных субъектом ПДн для распространения, должна быть прекращена в любое время по требованию субъекта ПДн. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта ПДн, а также перечень ПДн, обработка которых подлежит прекращению. Указанные в данном требовании ПДн могут обрабатываться только Оператором.

Оператор обязуется прекратить передачу (распространение, предоставление, доступ) ПДн в течение трех рабочих дней с момента получения требования субъекта ПДн.

5.2. Оператором осуществляется обработка персональных данных как с использованием средств автоматизации, так и без использования таких средств.

5.3. Взаимодействие с третьими лицами в рамках достижения целей обработки персональных данных, если иное не предусмотрено законодательством Российской Федерации, осуществляется при следующих условиях:

– наличие договора (соглашения) об информационном взаимодействии и (или) договора поручения на обработку персональных данных;

– наличие согласия субъекта персональных данных на передачу его персональных данных третьим лицам.

5.4. Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

5.5. Оператором не осуществляется трансграничная передача персональных данных.

5.6. Оператор и иные лица, получившие доступ к персональным данным на законном основании, с целью обеспечения конфиденциальности ПДн в соответствии со ст. 7 ФЗ «О персональных данных» обязуются не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

5.7. В администрации приняты следующие меры, направленные на обеспечение выполнения Оператором обязанностей, предусмотренных ФЗ «О персональных данных», в том числе меры по обеспечению безопасности ПДн:

– назначены лица, ответственные за организацию обработки персональных данных и защиту информации в администрации Баганского района Новосибирской области;

– разработаны локальные акты по вопросам обработки персональных данных, определяющие для каждой цели обработки ПДн категории и перечень обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, способы, сроки обработки и хранения, порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

– осуществляется внутренний контроль соответствия обработки персональных данных ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, локальным актам Оператора;

– ведется периодическое ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;

– Оператор оценивает вред, который может быть причинен субъектам ПДн в соответствии с Требованиями к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», утвержденными приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178;

– определены угрозы безопасности персональных данных при их обработке в информационных системах;

– с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных определены уровни защищенности персональных данных при их обработке в информационных системах администрации;

5.8. Оператором принимаются необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.9. Для обеспечения безопасности персональных данных в администрации принимаются следующие меры:,

– определены угрозы безопасности персональных данных при их обработке в информационных системах;

– применяются прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– проведена оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;

– осуществляется учет машинных носителей персональных данных;

– приняты меры, направленные на обнаружение фактов несанкционированного доступа к персональным данным и принятие соответствующих мер;

– приняты меры, позволяющие осуществлять восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлены правила доступа к персональным данным, обрабатываемым в информационных системах ;

– осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем администрации Баганского района Новосибирской области;

– организован режим обеспечения безопасности помещений, в которых обрабатываются персональные данные, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

5.10. Условием прекращения обработки персональных данных является:

– достижение целей обработки персональных данных;

– отзыв согласия субъекта персональных данных (или его представителя) на обработку его персональных данных;

– выявление неправомерной обработки персональных данных;

– истечение установленного срока хранения персональных данных;

– ликвидация Оператора;

– прекращение деятельности Оператора в результате его реорганизации.

5.11. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.12. Для организации хранения персональных данных в случае автоматизированной обработки Оператор в соответствии ФЗ «О персональных данных» использует технические устройства хранения данных, находящиеся на территории Российской Федерации.

5.13. При осуществлении хранения персональных данных с использованием средств автоматизации Оператор персональных данных использует базы данных, находящиеся на территории Российской Федерации, в соответствии с частью 5 статьи 18 ФЗ «О персональных данных».

5.14. Обработка персональных данных, осуществляемая без использования средств автоматизации, организована в соответствии с постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5.15. Оператором приняты следующие меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации:

– определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

– обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

– при хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

6. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

6.1. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

6.2. В случае выявления неправомерной обработки персональных данных Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) на период проверки.

6.3. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, Оператор обязан уничтожить такие персональные данные или обеспечить их уничтожение.

6.4. В случае выявления неточных персональных данных Оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.5. В случае подтверждения факта неточности персональных данных Оператор обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

6.6. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, а также в случае отзыва субъектом персональных данных согласия на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, или соглашением между Оператором и субъектом персональных данных.

6.7. Оператор обязуется осуществлять подтверждение факта уничтожения ПДн в указанных выше случаях в соответствии с Требованиями к подтверждению уничтожения персональных данных, утвержденными приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179.

6.8. Оператор обязан сообщить в порядке, предусмотренном ФЗ «О персональных данных», субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя, либо при получении запроса субъекта персональных данных или его представителя.

6.9. Правила рассмотрения запросов, обращений субъектов персональных данных и их представителей, уполномоченных органов по поводу неточности персональных данных, неправомерности их обработки, отзыва согласия и доступа субъекта персональных данных к

своим данным, а также соответствующие формы запросов, обращений предоставляются по запросу не позднее тридцати рабочих дней со дня получения запроса и (или) обращения.

7. Заключительные положения

7.1. В соответствии с требованиями ФЗ «О персональных данных» Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

7.2. Оператор оставляет за собой право в любой момент изменить положения настоящей Политики и обязуется опубликовать обновленную Политику и предоставить к ней доступ для ознакомления путем размещения в информационно-телекоммуникационной сети Интернет на официальном сайте Баганского района по адресу: https://bagan.nso.ru/.

Приложение № 1
к Политике в отношении обработки
персональных данных в администрации
Баганского района
Новосибирской области

Сведения о персональных данных, обрабатываемых в
администрации Баганского района Новосибирской области

Категория субъектов, чьи ПДн обрабатываются	Категория персональных данных		Перечень обрабатываемых ПДн	Способы обработки ПДн	Срок хранения ПДн или условие прекращении обработки ПДн
	Оформление и регулирование трудовых отношений, ведение кадрового учета (в том числе содействие работникам в обучении и должностном росте, организация профессиональной переподготовки и повышения квалификации работников учреждения, а также обеспечение личной безопасности работников, условий их труда, гарантий и компенсаций, сохранности имущества, контроля количества и качества выполняемой работы)				
Работники администрации Баганского района Новосибирской области	Иные		Фамилия, имя, отчество; дата и место рождения; контактный телефон; адрес прописки; адрес фактического места жительства; паспортные данные; ИНН; СНИЛС; данные о месте рождения; данные о браке; данные об изменении имени, фамилии, отчества; данные о родственниках; гражданство;	Смешанный (как с использованием, так и без использования средств автоматизации)	– Достижение целей обработки персональных данных; – отзыв согласия субъекта персональных данных (или его представителей) на обработку его персональных данных;

Категория субъектов, чьи ПДн обрабатываются	Категория персональных данных		Перечень обрабатываемых ПДн	Способы обработки ПДн	Срок хранения ПДн или условие прекращении обработки ПДн
			информация об образовании; информация о трудовом стаже; сведения о доходах, имуществе, обязательствах имущественного характера; данные об отношении к судимости; данные о пребывании за границей; данные о трудовом договоре; сведения о воинском учете; данные об аттестации работников; данные о повышении квалификации, профессиональной переподготовке; данные о наградах, медалях, поощрениях, почетных званиях; информация о приеме на работу перемещении по должности, увольнении; информация об отпусках; информация о командировках;		– выявление неправомерной обработки персональных данных; – ликвидация оператора; – прекращение осуществления деятельности оператора; – истечение установленного срока хранения ПДн (50 лет)

Категория субъектов, чьи ПДн обрабатываются	Категория персональных данных		Перечень обрабатываемых ПДн	Способы обработки ПДн	Срок хранения ПДн или условие прекращении обработки ПДн
			информация о медицинском страховании; банковские реквизиты		
Близкие родственники работников администрации Баганского района Новосибирской области	Иные		Фамилия, имя, отчество, дата рождения, место рождения, место работы и домашний адрес	Смешанный (как с использованием, так и без использования средств автоматизации)	– Достижение целей обработки персональных данных; – отзыв согласия субъекта персональных данных (или его представителей) на обработку его персональных данных; – выявление неправомерной обработки персональных данных; – ликвидация оператора; – прекращение осуществления деятельности оператора;

Категория субъектов, чьи ПДн обрабатываются	Категория персональных данных		Перечень обрабатываемых ПДн	Способы обработки ПДн	Срок хранения ПДн или условие прекращении обработки ПДн
					– истечение установленного срока хранения ПДн 50 лет)

Лист ознакомления
с постановлением от _____ № _____
«Об утверждении политики в отношении обработки персональных данных администрации Баганского района Новосибирской области

№ п/п	ФИО	Дата ознакомления	Подпись
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			
25.			
26.			
27.			
28.			
29.			
30.			
31.			
32.			
33.			
34.			
35.			

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

29.08.2024 № 783

О назначении ответственных лиц
в администрации Баганского района Новосибирской области

В целях обеспечения защиты информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – информация), обрабатываемой в администрации Баганского района Новосибирской области (далее – администрация), администрация Баганского района Новосибирской области

ПОСТАНОВЛЯЕТ:

1. Назначить ответственным за организацию обработки персональных данных в администрации Колобову Елену Владимировну, начальника отдела строительства и дорожного комплекса администрации Баганского района Новосибирской области
2. Утвердить Инструкцию ответственного за организацию обработки персональных данных в администрации согласно Приложению № 1.
3. Назначить ответственным за защиту информации, содержащейся в информационных системах администрации, Колобову Елену Владимировну, начальника отдела строительства и дорожного комплекса администрации Баганского района Новосибирской области
4. Возложить на ответственного за защиту информации в администрации обязанности по обеспечению безопасности персональных данных, обрабатываемых в информационных системах администрации Баганского района Новосибирской области.
5. Утвердить Инструкцию ответственного за защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, содержащейся в информационных системах администрации Баганского района Новосибирской области, согласно Приложению № 2.
6. Назначить администратором информационных систем администрации Удалова Андрея Анатольевича, инженера 1 категории МКУ «Центра бухгалтерского, информационного обеспечения муниципальных закупок Баганского района».
7. Утвердить Инструкцию администратора информационных систем администрации Баганского района Новосибирской области согласно Приложению № 3.
8. Опубликовать настоящее постановление на официальном сайте органов местного самоуправления Баганского района Новосибирской области и в периодическом печатном издании органов местного самоуправления «Бюллетень органов местного самоуправления Баганского района».
9. Данное постановление вступает в силу после его публикации в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области».
10. Контроль за исполнением настоящего возложить на заместителя главы администрации Баганского района Новосибирской области Бреус А.О..

Главы Баганского района
Новосибирской области А.А. Воличенко

ПРИЛОЖЕНИЕ №1
к постановлению администрации
Баганского района

Новосибирской области

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных
в администрации Баганского района Новосибирской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая Инструкция определяет основные права и обязанности ответственного за организацию обработки персональных данных в администрации Баганского района Новосибирской области (далее – администрация).

1.2 Лицо, ответственное за организацию обработки персональных данных, назначается постановлением Главы администрации Баганского района Новосибирской области из числа сотрудников администрации.

1.3 Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от заместителя главы администрации или иного уполномоченного лица и подотчетно ему.

1.4 Ответственный за организацию обработки персональных данных отвечает за организацию, обеспечение выполнения сотрудниками администрации требований законодательства Российской Федерации в области персональных данных, в том числе требований к обработке и обеспечению безопасности персональных данных.

1.5 Ответственный за организацию обработки персональных данных в своей деятельности руководствуется настоящей Инструкцией, законодательством Российской Федерации, нормативными правовыми актами, методическими и иными документами Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России), Федеральной службы безопасности Российской Федерации (далее - ФСБ России), Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор), а также локальными актами администрации, регламентирующими вопросы обработки и защиты персональных данных (далее также – ПДн).

2. ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Ответственный за организацию обработки персональных данных обязан:

2.1.1 Знать и соблюдать требования действующих нормативных правовых актов Российской Федерации, нормативных правовых актов методических и иных документов ФСТЭК России, ФСБ России и Роскомнадзора, а также локальных актов администрации, регламентирующих вопросы в области обработки и обеспечения безопасности персональных данных.

2.1.2 Обеспечить доведение до сведения работников администрации положений законодательства Российской Федерации о ПДн, локальных актов администрации по вопросам обработки ПДн, требований к защите ПДн (в случае изменения нормативной правовой базы, локальных актов администрации в области обработки и защиты ПДн обучение

(информирование) сотрудников должно быть проведено не позднее одного месяца с момента изменений).

2.1.3 Осуществлять внутренний контроль за соблюдением администрацией и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

2.1.4 Осуществлять ведение журнала обучения и проверок осведомленности сотрудников администрации в области обработки и защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

2.1.5 Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.1.6 Осуществлять ведение журнала учета обращений субъектов персональных данных по вопросам обработки их персональных данных в администрации

2.1.7 Обеспечивать проведение работ по определению и пересмотру (при необходимости) уровня защищенности персональных данных, обрабатываемых в информационных системах администрации в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

2.1.8 Обеспечивать поддержание в актуальном состоянии организационно-распорядительных документов, регламентирующих вопросы в области обработки и обеспечения безопасности персональных данных в администрации.

2.1.9 Обеспечивать допуск к персональным данным и учет сотрудников администрации, допущенных к обработке персональных данных (как в программных комплексах, используемых для обработки персональных данных в администрации, так и на бумажных носителях).

2.1.10 Сообщать обо всех зафиксированных попытках посторонних лиц получить несанкционированный доступ к персональным данным своему непосредственному руководителю и ответственному за защиту информации в администрации.

2.1.11 Принимать участие в расследовании нарушений по вопросам обработки и защиты персональных данных в администрации, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений.

2.1.12 Обеспечивать контроль за поддержанием в актуальном состоянии уведомления об обработке персональных данных уполномоченного органа по защите прав субъектов персональных данных.

2.1.13 Принимать участие в мероприятиях при проведении государственного контроля и надзора за соответствием обработки ПДн, выполнением организационных и технических мер по обеспечению безопасности ПДн.

2.1.14 Осуществлять в пределах своей компетенции иные функции в соответствии с целями и задачами администрации.

3. ПРАВА ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Ответственный за организацию обработки персональных данных имеет право:

3.1.1 Знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на него задач.

3.1.2 Проходить обучение (переподготовку) по вопросам организации работы с персональными данными в специализированных учебных центрах.

3.1.3 Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения своих обязанностей.

3.1.4 Получать доступ к информации, материалам, техническим средствам, помещениям, необходимым для надлежащего исполнения своих прав и обязанностей.

3.1.5 Обращаться за необходимыми разъяснениями по вопросам функционирования программных и технических средств (в том числе средств защиты информации) информационных систем администрации и обеспечения безопасности персональных данных к администратору информационных систем администрации, ответственному за защиту информации, содержащейся в информационных системах администрации, в пределах их компетенций.

3.1.6 Требовать от сотрудников [администрации соблюдения требований действующего законодательства Российской Федерации, локальных актов администрации в области обработки и обеспечения безопасности персональных данных.

3.1.7 Проводить проверки соблюдения режима обеспечения безопасности персональных данных в структурных подразделениях администрации.

3.1.8 Инициировать проведение и принимать участие в служебных расследованиях по фактам нарушения сотрудниками администрации установленных требований в области обработки и обеспечения безопасности персональных данных.

3.1.9 Требовать прекращения обработки персональных данных в случае нарушения правил обработки и требований по защите персональных данных.

3.1.10 Привлекать в случае необходимости при проведении служебных расследований сотрудников администрации, имеющих непосредственное отношение к рассматриваемым в ходе служебного расследования вопросам.

3.1.11 Вносить предложения по устранению выявленных инцидентов и предупреждению подобного рода нарушений.

3.1.12 Вносить предложения об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по обработке и защите ПДн.

4. ОТВЕТСТВЕННОСТЬ

4.1 Ответственный за организацию обработки персональных данных несет предусмотренную законодательством Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

– неисполнение либо ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией;

– нарушения в работе информационных систем администрации, вызванные его неправомерными действиями или неправильным использованием предоставленных прав;

– нарушение законодательства Российской Федерации, локальных актов администрации, устанавливающих порядок работы с персональными данными;

– превышение должностных полномочий и злоупотребление ими;

– применение к администрации штрафных санкций по вине ответственного за организацию обработки персональных данных;

– совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.

ПРИЛОЖЕНИЕ № 2
к постановлению администрации
Баганского района

Новосибирской области

ИНСТРУКЦИЯ
ответственного за защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, содержащейся в информационных системах администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящая Инструкция определяет основные права и обязанности ответственного за защиту информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – информация), содержащейся в информационных системах администрации Баганского района Новосибирской области (далее – администрация).

1.2 Ответственный за защиту информации, содержащейся в информационных системах администрации (далее – ответственный за защиту информации), назначается приказом администрации из числа сотрудников администрации.

1.3 Ответственный за защиту информации получает указания непосредственно от Главы Баганского района Новосибирской области или иного уполномоченного лица и подотчетно ему.

1.4 Ответственный за защиту информации отвечает за организацию и обеспечение выполнения требований по защите информации, в процессе ее обработки в информационных системах администрации.

1.5 Ответственный за защиту информации в своей работе руководствуется настоящей Инструкцией, нормативными правовыми актами Российской Федерации, нормативными правовыми актами, методическими и иными документами Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России), Федеральной службы безопасности Российской Федерации (далее – ФСБ России) и локальными актами администрации, регламентирующими вопросы обработки и защиты информации.

2. Обязанности ответственного за защиту информации

2.1 Ответственный за защиту информации обязан:

2.1.1 Знать и соблюдать требования действующих нормативных правовых актов Российской Федерации, нормативных правовых актов, методических и иных документов ФСТЭК России, ФСБ России, а также локальных актов администрации, регламентирующих вопросы в сфере (области) обеспечения безопасности информации.

2.1.2 Осуществлять планирование мероприятий по защите информации, обрабатываемой в информационных системах (далее – ИС) администрации, осуществлять пересмотр и корректировку (при необходимости) плана мероприятий по защите информации в ИС администрации.

2.1.3 Обеспечивать информирование пользователей ИС о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС.

2.1.4 Обеспечивать доведение до пользователей ИС администрации требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений.

2.1.5 Организовывать обучение пользователей ИС администрации правилам безопасной эксплуатации ИС не реже 1 раза в два года.

2.1.6 Осуществлять контроль осведомленности пользователей ИС администрации об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации с периодичностью не реже 1 раза в два года.

2.1.7 Осуществлять ведение Журнала обучения и проверок осведомленности сотрудников администрации в области обработки и защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну.

2.1.8 Осуществлять контроль выполнения пользователями ИС администрации требований Инструкции пользователя информационных систем администрации.

2.1.9 Обеспечивать проведение контроля за обеспечением уровня защищенности информации, содержащейся в ИС администрации, с периодичностью не реже 1 раза в два года.

2.1.10 Осуществлять мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС.

2.1.11 Обеспечивать поддержание в актуальном состоянии (пересмотр и доработку) эксплуатационной документации на систему защиты информации ИС администрации и организационно-распорядительной документации администрации в области защиты информации.

2.1.12 Обеспечивать контроль состава применяемых в ИС администрации средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков.

2.1.13 Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на применяемые в администрации средства защиты информации (далее – СЗИ) и принятие мер, направленных на устранение выявленных недостатков.

2.1.14 Обеспечивать учет и сохранность применяемых СЗИ, эксплуатационной и технической документации к ним, порядок обращения с СЗИ, направленный на исключение несанкционированного доступа к СЗИ.

2.1.15 Обеспечивать контроль работоспособности, параметров настройки и правильности функционирования СЗИ.

2.1.16 Обеспечивать ведение документации в области защиты информации, предусмотренной локальными актами администрации.

2.1.17 Осуществлять ведение Журнала учета машинных носителей персональных данных в администрации.

2.1.18 Обеспечивать регистрацию и контроль действий по удалению защищаемой информации и уничтожению машинных и иных материальных носителей персональных данных путем составления соответствующих актов, и занесение соответствующих записей в Журнал учета машинных носителей персональных данных.

2.1.19 Сообщать обо всех зафиксированных попытках посторонних лиц получить несанкционированный доступ к защищаемой информации и техническим средствам ИС администрации, и иных инцидентах информационной безопасности своему непосредственному руководителю или иному уполномоченному лицу в зависимости от характера инцидента.

2.1.20 Обеспечивать обнаружение инцидентов информационной безопасности и реагирование на них.

2.1.21 Принимать участие в расследовании нарушений по вопросам защиты информации (в том числе выявлении инцидентов), принимать меры по их устранению и предупреждению подобного рода нарушений.

2.1.22 Обеспечивать выявление (поиск), анализ и устранение уязвимостей в ИС администрации.

2.1.23 Принимать участие в устранении выявленных уязвимостей в соответствии с характером выявленных уязвимостей.

2.1.24 В случае возникновения нештатных и аварийных ситуаций, а также при выявлении нарушений, приводящих к снижению уровня защищенности информации, принимать меры по реагированию в пределах своих полномочий с целью предупреждения и ликвидации

неблагоприятных последствий, известить своего непосредственного руководителя и ответственных лиц, исходя из характера возникшего инцидента.

2.1.25 Участвовать в мероприятиях при проведении государственного контроля и надзора за соответствием обработки персональных данных, выполнением организационных и технических мер по обеспечению безопасности информации в администрации.

2.1.26 Присутствовать при выполнении технического обслуживания элементов ИС администрации представителями сторонних организаций.

2.1.27 Осуществлять в пределах своей компетенции иные функции в соответствии с целями и задачами администрации.

3. Права ответственного за защиту информации

3.1 Ответственный за защиту информации имеет право:

3.1.1 Знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на него задач.

3.1.2 Проходить обучение (переподготовку) по защите информации в специализированных учебных центрах.

3.1.3 Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения своих обязанностей.

3.1.4 Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей.

3.1.5 Требовать от сотрудников администрации соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности информации, локальных актов администрации по вопросам обработки информации и требований по защите информации в части их касающейся.

3.1.6 Проводить проверки соблюдения режима обеспечения безопасности информации в администрации.

3.1.7 Инициировать проведение и принимать участие в служебных расследованиях по фактам нарушения сотрудниками администрации установленных требований обработки и защиты информации.

3.1.8 Требовать прекращения обработки информации в случае нарушения правил обработки и требований по защите информации.

3.1.9 Привлекать в случае необходимости при проведении служебных расследований сотрудников администрации, имеющих непосредственное отношение к рассматриваемым в ходе служебного расследования вопросам.

3.1.10 Вносить предложения об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по защите информации.

4. Ответственность

4.1 Ответственный за защиту информации, содержащейся в ИС администрации, несет предусмотренную законодательством Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

– неисполнение либо ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией;

– нарушения в работе ИС администрации, вызванные его неправомерными действиями или неправильным использованием предоставленных прав;

– нарушение законодательства Российской Федерации, локальных актов администрации в области защиты информации;

– превышение должностных полномочий и злоупотребление ими;

– применение к администрации штрафных санкций по вине ответственного за защиту информации;

– совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в

отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.

ПРИЛОЖЕНИЕ №3
к постановлению администрации
Баганского района

Новосибирской области

ИНСТРУКЦИЯ
администратора информационных систем администрации Баганского района
Новосибирской области

1. Общие положения

1.1 Настоящая Инструкция определяет основные права и обязанности администратора информационных систем (далее – ИС) администрации Баганского района Новосибирской области (далее – администрация).

1.1 Администратор ИС назначается постановлением администрации из числа сотрудников администрации.

1.2 Администратор ИС получает указания непосредственно от Главы администрации или иного уполномоченного лица и подотчетно ему.

1.3 Администратор ИС отвечает за обеспечение работоспособности программных и технических средств, входящих в состав информационных систем администрации.

1.4 Администратор ИС в своей деятельности руководствуется настоящей Инструкций, законодательством Российской Федерации, включая нормативные правовые акты и методические документы Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России), Федеральной службы безопасности Российской Федерации (далее – ФСБ России) и иными локальными актами администрации, регламентирующими вопросы обработки и защиты информации.

1.5 Администратор ИС отвечает за обеспечение работоспособности ИС администрации (поддержание работоспособности оборудования и программного обеспечения).

2. Обязанности администратора ИС

2.1 Администратор ИС администрации обязан:

2.1.1 Знать и выполнять требования действующих нормативных правовых актов Российской Федерации, нормативных правовых актов, методических и иных документов ФСТЭК России, ФСБ России, а также локальных актов администрации в области обработки и обеспечения безопасности защищаемой информации (в том числе персональных данных).

2.1.2 Знать состав, структуру, назначение и задачи ИС администрации, владеть информацией о системном и прикладном программном обеспечении, о составе информационных технологий и технических средств, позволяющих осуществлять обработку информации, а также о конфигурации ИС администрации и выполнять свои обязанности в соответствии с эксплуатационной и технической документацией на применяемые в ИС администрации технические и программные средства.

2.1.3 Осуществлять общее техническое сопровождение ИС администрации:

– обеспечивать (организовывать) замену, установку, настройку и своевременное обновление элементов ИС;

– обеспечивать работоспособность элементов ИС;

– обеспечивать конфигурирование и административную настройку технических средств ИС, программного обеспечения (ПО) и оборудования, включая оборудование, отвечающее за безопасность защищаемого объекта;

– осуществлять контроль состава технических средств и программного обеспечения, а также параметров настройки и правильности их функционирования;

– обеспечивать размещение стационарных технических средств, обрабатывающих защищаемую информацию, а также средств обеспечения функционирования ИС в пределах контролируемой зоны;

– контролировать обеспечение размещения устройств вывода (отображения) информации, исключающего ее несанкционированный просмотр;

– обеспечить совместимость применяемых в информационных системах информационных технологий, технических и программных средств;

– контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств;

– в случае отказа работоспособности технических средств и программного обеспечения элементов ИС принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.1.4 Обеспечивать создание, присвоение и уничтожение идентификаторов пользователей и устройств в ИС.

2.1.5 Проводить инструктаж сотрудников – пользователей ИС правилам работы в ИС.

2.1.6 Осуществлять получение из доверенных источников и установку обновлений общесистемного, прикладного, специального программного (микропрограммного) обеспечения.

2.1.7 Проводить не реже одного раза в полгода контроль установленного (инсталлированного) в ИС программного обеспечения в соответствии с Перечнем разрешенного к использованию программного обеспечения и его компонентов.

2.1.8 Регулярно проводить анализ содержимого журналов регистрации событий (системных журналов средств вычислительной техники, программных средств, используемых для обработки защищаемой информации) и реагировать на возникающие нештатные ситуации.

2.1.9 Участвовать в проведении периодического поиска (выявлении), анализа и устранении выявленных уязвимостей в соответствии с характером выявленных уязвимостей в ИС.

2.1.10 Участвовать в анализе ситуаций, касающихся функционирования ИС, и служебных расследований фактов несанкционированного доступа.

2.1.11 Участвовать в выявлении инцидентов (одного события или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации), и принимать меры по их устранению.

2.1.12 Участвовать в проведении внутреннего контроля соответствия обработки ПДн требованиям законодательства Российской Федерации о персональных данных, в том числе требований к защите ПДн.

2.1.13 В кратчайшие сроки принимать меры по реагированию и восстановлению программного обеспечения в случае возникновения нештатных и аварийных ситуаций с целью ликвидации их последствий, включающие:

– восстановление программного обеспечения из резервных копий (дистрибутивов) программного обеспечения;

– возврат ИС в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей ИС, позволяющих решать задачи по обработке информации.

2.1.14 Контролировать выполнение пользователями ИС установленных правил работы с программными и техническими средствами ИС.

2.1.15 Регулярно проводить анализ системных журналов для выявления инцидентов информационной безопасности и своевременного реагирования на них.

2.1.16 Организовывать проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий.

2.1.17 Организовывать контроль безотказного функционирования технических средств, обнаружение и локализацию отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

2.1.18 Оперативно докладывать вышестоящему руководству о случаях возникновения нештатных и аварийных ситуаций.

2.1.19 Информировать ответственного за защиту информации о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИС администрации.

2.1.20 Присутствовать при выполнении технического обслуживания элементов ИС представителями сторонних организаций.

2.1.21 Обеспечивать выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт.

2.1.22 Участвовать в мероприятиях при проведении государственного контроля и надзора за соответствием обработки персональных данных, выполнением организационных и технических мер по обеспечению безопасности персональных данных.

2.1.23 Проводить анализ проектов технических заданий, нормативных актов и указаний, договоров на выполнение работ, отчетной документации, с целью определения достаточности предусмотренных в них требований и мероприятий по комплексной совместимости применяемых в ИС программных и аппаратных средств и технологий обработки информации с предполагаемыми к внедрению решениями.

3. Права администратора ИС

3.1 Администратор ИС администрации имеет право:

3.1.1 Знакомиться с локальными актами администрации, регламентирующими процессы обработки и защиты ПДн.

3.1.2 Проходить обучение (повышение квалификации) в специализированных учебных центрах.

3.1.3 Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.4 Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей (в т.ч. вести мониторинг действий пользователей и обслуживающего персонала ИС администрации).

3.1.5 Привлекать сотрудников администрации к работе по поддержанию функционирования и совершенствованию программной и технической оснащенности ИС администрации или специалистов сторонних организаций, компетентных в вопросах проводимых работ.

3.1.6 Требовать от пользователей ИС администрации соблюдения правил и руководств пользования программными и техническими средствами ИС, а также соблюдения требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности ПДн в части их касающейся.

3.1.7 Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность информации, вносить свои предложения по совершенствованию программной и технической оснащенности ИС администрации с целью обеспечения и поддержания устойчивого функционирования и оптимизации работы применяемых в ИС программных и технических средств.

3.1.8 Инициировать проведение и принимать участие в служебных расследованиях по фактам нарушения установленных требований обеспечения устойчивого функционирования ИС и безопасности ПДн.

3.1.9 Требовать прекращения работы в ИС администрации как в целом, так и отдельных пользователей ИС, в связи с нарушением функционирования ИС, в случае выявления нарушений

установленной технологии обработки информации или нарушения функционирования средств и систем защиты ИС.

3.1.10 Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к ответственному за организацию обработки персональных данных в администрации и ответственному за защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, содержащейся в ИС администрации.

4. Ответственность

4.1 Администратор ИС администрации несет предусмотренную законодательством Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

– неисполнение либо ненадлежащее исполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией;

– нарушения в работе ИС администрации, вызванные его неправомерными действиями или неправильным использованием предоставленных прав;

– нарушение законодательства Российской Федерации, локальных актов администрации в области защиты информации;

– превышение должностных полномочий и злоупотребление ими;

– применение к администрации штрафных санкций по вине администратора ИС;

– совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.

Лист ознакомления
с постановлением от _____ № _____
«О назначении ответственных лиц в администрации Баганского района Новосибирской области»

№ п/п	ФИО	Дата ознакомления	Подпись
36.			
37.			
38.			
39.			
40.			
41.			
42.			
43.			
44.			
45.			
46.			
47.			
48.			
49.			
50.			
51.			
52.			
53.			
54.			

55.			
56.			
57.			
58.			
59.			
60.			
61.			
62.			
63.			
64.			
65.			
66.			
67.			
68.			
69.			
70.			
71.			
72.			
73.			
74.			
75.			
76.			
77.			
78.			
79.			

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

29.08.2024 № 784

О реализации мер защиты информации ограниченного доступа, обрабатываемой в информационных системах администрации Баганского района Новосибирской области

В целях выполнения требований действующего законодательства Российской Федерации в области защиты информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – информация), и реализации мер защиты информации, обрабатываемой в информационных системах администрации Баганского района Новосибирской области, администрация Баганского района Новосибирской области

ПОСТАНОВЛЯЕТ:

1. Утвердить Положение по организации и проведению работ по обеспечению безопасности информации, обрабатываемой в информационных системах администрации Баганского района Новосибирской области согласно Приложению №1.

2. Утвердить Правила идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах администрации Баганского района Новосибирской области согласно Приложению № 2.

3. Утвердить Правила управления доступом субъектов доступа к объектам доступа в информационных системах администрации Баганского района Новосибирской области согласно Приложению № 3.

4. Утвердить Правила по ограничению программной среды в информационных системах администрации Баганского района Новосибирской области согласно Приложению № 4.

5. Утвердить Правила обращения с машинными носителями информации в информационных системах администрации Баганского района Новосибирской области согласно Приложению № 5.

6. Утвердить Правила регистрации событий безопасности в информационных системах администрации Баганского района Новосибирской области согласно Приложению № 6.

7. Утвердить Правила антивирусной защиты информационных систем администрации Баганского района Новосибирской области согласно Приложению № 7.

8. Утвердить Правила контроля (анализа) защищенности информации в информационных системах администрации Баганского района Новосибирской области согласно Приложению № 8.

9. Утвердить Правила обеспечения целостности и доступности информационных систем и информации в администрации Баганского района Новосибирской области согласно Приложению № 9.

10. Утвердить Регламент выявления инцидентов безопасности и реагированию на них в администрации Баганского района Новосибирской области согласно Приложению № 10.

11. Утвердить Положение по управлению конфигурацией информационных систем администрации Баганского района Новосибирской области согласно Приложению № 11.

12. Утвердить Положение по защите информации в администрации Баганского района Новосибирской области при выводе из эксплуатации информационных систем или после принятия решения об окончании обработки информации ограниченного доступа согласно Приложению № 12.

13. Колобовой Е.В., начальнику отдела строительства и дорожного комплекса администрации Баганского района ознакомить уполномоченных работников администрации с настоящим приказом.

14. Опубликовать настоящее постановление на официальном сайте органов местного самоуправления Баганского района Новосибирской области и в периодическом печатном издании органов местного самоуправления «Бюллетень органов местного самоуправления Баганского района».

15. Данное постановление вступает в силу после его публикации в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области».

16. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации Баганского района Бреус А.О.

Глава Баганского района
Новосибирской области А.А. Воличенко

ПРИЛОЖЕНИЕ №1
УТВЕРЖДЕНО
к постановлению администрации
Баганского района
Новосибирской области
от 29.08.2024 № 784

ПОЛОЖЕНИЕ
по организации и проведению работ по обеспечению безопасности информации, обрабатываемой в информационных системах администрации Баганского района Новосибирской области

1. Общие положени

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности информации, обрабатываемой в информационных системах администрации Баганского района Новосибирской области (далее – Положение), разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

1.2. Целью разработки настоящего Положения является определение порядка организации и проведения работ по обеспечению безопасности информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – информация), обрабатываемой в информационных системах (далее – ИС) администрации Баганского района Новосибирской области (далее – администрация) на всех стадиях (этапах) создания ИС, в ходе ее эксплуатации и вывода из эксплуатации.

2. Термины и определени

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

– информационная система – совокупность содержащейся 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;

– оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

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

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

– технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации, аппаратные средства защиты информации;

– пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования;

– 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;

– 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 информации, обрабатываемой в ИС администрации 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 – система ЗИ).

3.2. Система ЗИ включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности информации, уровня защищенности информации (в том числе персональных данных), который необходимо обеспечить, класса информационной системы и информационных технологий, используемых в ИС.

3.3. Защита информации, содержащейся в ИС, обеспечивается путем выполнения требований к организации и мерам защиты информации, содержащейся в ИС.

3.4. Для обеспечения защиты информации, содержащейся в ИС, администрация назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации (далее – Ответственный), содержащейся в ИС.

3.5. Для обеспечения выполнения мер, предусмотренных законодательством Российской Федерации в области персональных данных, администрацией назначается ответственный за организацию обработки персональных данных.

3.6. Для обеспечения соблюдения условий использования средств криптографической защиты информации (при их использовании) администрацией назначается ответственный за эксплуатацию средств криптографической защиты информации в администрацию.

3.7. Для проведения работ по защите информации в ходе создания и эксплуатации ИС обладателем информации (заказчиком) и оператором 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 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».

3.8. Для обеспечения защиты информации, содержащейся в ИС, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании».

3.9. Для обеспечения защиты информации, содержащейся в ИС, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании».

3.10. Защита информации, содержащейся в ИС, является составной частью работ по созданию и эксплуатации ИС 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 ИС, в рамках системы (подсистемы) защиты ИС.

3.11. Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации ИС, в зависимости от информации, содержащейся в ИС, целей создания ИС и задач, решаемых этой ИС, 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).

3.12. Для обеспечения защиты информации, содержащейся в ИС, проводятся следующие мероприятия:

– формирование требований к защите информации, содержащейся в ИС;

– разработка системы защиты информации ИС;

– внедрение системы защиты информации ИС;

– оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации (форма оценки эффективности и документов, разрабатываемых по результатам оценки эффективности, принимается администрация самостоятельно и (или) по соглашению с лицом, привлекаемым для проведения оценки эффективности реализованных мер по обеспечению безопасности информации) и ввод ее в действие;

– обеспечение защиты информации в ходе эксплуатации ИС;

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

4. Формирование требований к защите информации, содержащейся в информационных системах

4.1. Формирование требований к защите информации, содержащейся в ИС, осуществляется администрацией

4.2. Формирование требований к защите информации, содержащейся в ИС, включает:

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

– определение уровня защищенности персональных данных при их обработке в ИС и (или) классификацию ИС по требованиям защиты информации;

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

– определение требований к системе ЗИ ИС.

4.3. При принятии решения о необходимости защиты информации, содержащейся в ИС, осуществляется:

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

– определение информации, подлежащей обработке в ИС;

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

– принятие решения о необходимости создания системы ЗИ ИС, а также определение целей и задач защиты информации в ИС, основных этапов создания системы ЗИ ИС и функций по обеспечению защиты информации, содержащейся в ИС, оператора и уполномоченных лиц.

4.4. Результаты определения уровня защищенности персональных данных при их обработке в ИС оформляются актом. Результаты классификации ИС оформляются актом классификации.

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

4.6. Требования к системе ЗИ ИС определяются в зависимости от класса защищенности ИС и угроз безопасности информации, включенных в модель угроз безопасности информации.

5. Разработка системы защиты информации информационной систем

5.1. Разработка системы ЗИ ИС организуется администрацией

5.2. Разработка системы ЗИ ИС осуществляется в соответствии с техническим заданием на создание системы ЗИ ИС и включает:

– проектирование системы защиты информации ИС;

– разработку эксплуатационной документации на систему ЗИ ИС;

– макетирование и тестирование системы ЗИ ИС (при необходимости).

5.3. Система ЗИ ИС не должна препятствовать достижению целей создания ИС и ее функционированию.

5.4. При разработке системы ЗИ ИС учитывается ее информационное взаимодействие с иными ИС и информационно-телекоммуникационными сетями.

5.5. При проектировании системы ЗИ информационной системы:

–определяются типы субъектов доступа и объектов доступа, являющихся объектами защиты;

–определяются методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа, подлежащие реализации в ИС;

–выбираются меры защиты информации, подлежащие реализации в системе ЗИ ИС;

–определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

–определяется структура системы ЗИ ИС, включая состав (количество) и места размещения ее элементов;

–осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности ИС;

–определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей ИС, приводящих к возникновению угроз безопасности информации;

–определяются меры защиты информации при информационном взаимодействии с иными ИС и информационно-телекоммуникационными сетями.

5.6. Результаты проектирования системы ЗИ ИС отражаются в проектной документации на систему ЗИ ИС.

5.7. Разработка эксплуатационной документации на систему ЗИ ИС осуществляется в соответствии с техническим заданием на создание системы ЗИ ИС.

5.8. При макетировании и тестировании системы ЗИ ИС в том числе осуществляются:

– проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

– проверка выполнения выбранными средствами защиты информации требований к системе защиты информации ИС;

– корректировка проектных решений, разработанных при создании ИС и (или) системы защиты информации ИС.

6. Внедрение системы защиты информации информационной системы

6.1. Внедрение системы ЗИ ИС организуется администрацией.

6.2. Внедрение системы ЗИ ИС осуществляется в соответствии с проектной и эксплуатационной документацией на систему ЗИ ИС и в том числе включает:

– установку и настройку средств защиты информации в ИС;
– разработку документов, определяющих правила и процедуры, реализуемые администрацией для обеспечения защиты информации в ИС в ходе ее эксплуатации;
– внедрение организационных мер защиты информации;
– предварительные испытания системы ЗИ ИС;
– опытную эксплуатацию системы ЗИ ИС;
– анализ уязвимостей ИС и принятие мер защиты информации по их устранению;
– приемочные испытания системы ЗИ ИС.

6.3. Установка и настройка средств защиты информации в ИС должна проводиться в соответствии с эксплуатационной документацией на систему ЗИ ИС и документацией на средства защиты информации.

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

– управления (администрирования) системой ЗИ ИС;

– выявления инцидентов, которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности информации, и реагирования на них;

– управления конфигурацией ИС и системы ЗИ ИС;

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

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

6.5. 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 ответственных лиц по реализации организационных мер защиты информации;

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

6.6. Предварительные испытания системы ЗИ ИС включают проверку работоспособности системы ЗИ ИС, а также принятие решения о возможности опытной эксплуатации системы защиты информации ИС.

6.7. Опытная эксплуатация системы ЗИ ИС включает проверку функционирования системы ЗИ ИС, в том числе реализованных мер ЗИ, а также готовность пользователей и ответственных лиц к эксплуатации системы ЗИ ИС.

6.8. Анализ уязвимостей ИС проводится в целях оценки возможности преодоления нарушителем системы ЗИ ИС и предотвращения реализации угроз безопасности информации.

Анализ уязвимостей ИС включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения ИС.

6.9. Приемочные испытания системы ЗИ ИС включают проверку выполнения требований к системе ЗИ ИС в соответствии с техническим заданием на создание системы ЗИ ИС.

7. Оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации

7.1. Оценка эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации организуется администрацией и включает проведение комплекса организационных и технических мероприятий, в результате которых подтверждается соответствие системы ЗИ ИС требованиям по безопасности информации.

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

7.3. По решению администрации оценка эффективности реализованных мер может быть проведена в рамках работ по аттестации информационной системы в соответствии с приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

7.4. В качестве исходных данных, необходимых для аттестации ИС, используются модель угроз безопасности информации, акт классификации ИС, техническое задание на создание системы ЗИ ИС, проектная и эксплуатационная документация на систему ЗИ ИС, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей ИС, материалы предварительных и приемочных испытаний системы ЗИ ИС. Аттестат соответствия выдается на весь срок эксплуатации ИС.

7.5. В ходе эксплуатации ИС администрацией должен обеспечивать поддержку соответствия системы защиты информации аттестату соответствия в рамках реализации мероприятий по защите информации, предусмотренных п. 8 настоящего Положения.

8. Обеспечение защиты информации в ходе эксплуатации информационной системы

8.1. Обеспечение защиты информации в ходе эксплуатации ИС осуществляется администрацией в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает следующие мероприятия:

- планирование мероприятий по защите информации;
- управление (администрирование) системой ЗИ ИС;
- выявление инцидентов и реагирование на них;
- управление конфигурацией ИС и ее системы ЗИ;
- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИС.

8.2. В ходе управления (администрирования) системой ЗИ ИС осуществляются:

- заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИС;
- управление средствами защиты информации в ИС, 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 системой защиты информации ИС (при необходимости);

– регистрация и анализ событий в ИС, связанных с защитой информации;

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

– сопровождение функционирования системы ЗИ ИС в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

8.3. 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 ИС 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 ИС 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.

8.4. В ходе управления конфигурацией ИС и ее системы защиты информации осуществляются:

– поддержание конфигурации ИС и ее системы защиты информации в соответствии с эксплуатационной документацией на систему защиты информации;

– определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ИС и ее системы защиты информации;

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

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

– 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 ИС и ее системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации ИС и ее системы защиты информации в эксплуатационную документацию на систему защиты информации ИС.

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

– контроль за событиями безопасности и действиями пользователей в ИС;

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

– анализ и оценка функционирования системы ЗИ ИС, включая выявление, анализ и устранение недостатков в функционировании системы ЗИ ИС;

– периодический анализ изменения угроз безопасности информации в ИС, 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 ИС;

– принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИС.

9. Обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации

9.1. Мероприятия по выводу ИС из эксплуатации включают:

– подготовку документов, связанных с выводом ИС из эксплуатации;

– работы по выводу ИС из эксплуатации, в том числе работы по деинсталляции программного обеспечения ИС, по реализации прав на программное обеспечение ИС, демонтажу и списанию технических средств ИС (при необходимости), обеспечению хранения и дальнейшего использования информационных ресурсов ИС;

– обеспечение защиты информации, в том числе архивирование информации, содержащейся в ИС, уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

9.2. Архивирование информации, содержащейся в ИС, должно осуществляться при необходимости дальнейшего использования информации в деятельности администрации.

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

9.4. Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации осуществляется в соответствии с эксплуатационной документацией на систему ЗИ ИС и организационно-распорядительными документами по защите информации.

9.5. В ходе проведения контроля выполнения мероприятий по защите Информации при выводе из эксплуатации ИС администрации или после принятия решения об окончании обработки информации, проверяется документальное оформление процедур, предусмотренных организационно-распорядительными документами по защите информации, регламентирующими вышеназванные мероприятия, а также соблюдение требований законодательства об архивном деле в Российской Федерации.

ПРИЛОЖЕНИЕ № 1
к Положению по организации и проведению работ по обеспечению безопасности информации, обрабатываемой в информационных системах администрации Баганского района Новосибирской области

ПЛАН
мероприятий по защите информации в информационных системах администрации Баганского района Новосибирской области

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
1.	Анализ угроз безопасности информации в ИС в ходе их эксплуатации		
1.1.	Выявление, анализ и устранение уязвимостей ИС	Не реже одного раза в год	Уполномоченные сотрудники администрации, ответственный за защиту информации, содержащейся в ИС администрации (далее – ответственный за защиту информации)
1.2.	Анализ изменения угроз безопасности информации в ИС	Не реже одного раза в год	
1.3.	Оценка возможных последствий реализации угроз безопасности информации в ИС	В случае выявления новых угроз безопасности	
2.	Управление (администрирование) системой ЗИ ИС		
2.1.	Управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в ИС	При необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники администрации
2.2.	Управление средствами защиты информации ИС	При необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники администрации
2.3.	Управление обновлениями программных и программно-аппаратных средств, в том числе средств ЗИ	По мере выхода обновлений, с учетом особенностей функционирования ИС	Уполномоченные сотрудники администрации
2.4.	Централизованное управление системой ЗИ ИС (при необходимости)	При необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники администрации
2.5.	Мониторинг и анализ зарегистрированных событий в ИС, связанных с обеспечением безопасности информации	Постоянно в ходе эксплуатации ИС	Уполномоченный сотрудник администрации
2.6.	Обеспечение функционирования систем ЗИ ИС в ходе их эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации	Постоянно в ходе эксплуатации ИС	Ответственный за защиту информации

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
3.	Управления конфигурацией ИС и их системами ЗИ		
3.1.	Определение компонентов ИС и их систем ЗИ, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю	При создании системы ЗИ ИС, далее при необходимости в случае изменения состава объектов управления конфигурацией	администрация
3.2.	Управление изменениями ИС и их системами ЗИ: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в ИС и их систему защиты информации	При создании системы ЗИ ИС и далее при необходимости в ходе эксплуатации ИС	Ответственный за защиту информации
3.3.	Контроль и документирование действий по внесению изменений в ИС и их системы защиты информации	Не реже одного раза в 2 года	Ответственный за защиту информации
4.	Реагирование на инциденты		
4.1.	Обнаружение 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)	Постоянно в ходе эксплуатации ИС	Сотрудники администрации (пользователи ИС и уполномоченные ответственные лица)
4.2.	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС	Постоянно в ходе эксплуатации ИС	Сотрудники администрации (пользователи ИС и

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
			уполномоченные ответственные лица)
4.3.	Идентификация и анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	При возникновении инцидентов безопасности	Уполномоченные сотрудники администрации, ответственный за защиту информации (в пределах своих полномочий в зависимости от характера инцидента)
4.4.	Планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИС и их 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	При возникновении инцидентов безопасности	Уполномоченные ответственные лица администрации (в пределах своих полномочий в зависимости от характера инцидента)
4.5.	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	При возникновении инцидентов безопасности	
5.	Информирование и обучение персонала ИС по вопросам защиты информации		
5.1.	Информирование персонала ИС о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС	Не реже одного раза в 2 года	Ответственный за защиту информации
5.2.	Доведение до персонала ИС требований по защите информации, а также положений организационно-распорядительных документов по защите информации	Не реже одного раза в 2 года. В случае изменения нормативной правовой базы, локальных актов администрации в области защиты информации обучение сотрудников должно быть проведено не позднее одного месяца с момента изменений	Ответственный за организацию обработки персональных данных и ответственный за защиту информации (в пределах своих полномочий)

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
5.3.	Обучение персонала ИС правилам эксплуатации средств защиты информации от несанкционированного доступа и средств антивирусной защиты	При создании системы защиты информации ИС и далее при необходимости в ходе эксплуатации ИС	Уполномоченные сотрудники администрации
5.4.	Проведение практических занятий и тренировок с персоналом ИС по блокированию угроз безопасности информации и реагированию на инциденты	Не реже одного раза в 2 года	Ответственный за защиту информации, уполномоченные сотрудники администрации
5.5.	Контроль осведомленности персонала ИС об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации	Не реже одного раза в 2 года	Ответственный за защиту информации
6.	Мероприятия по защите информации, проводимые в целях обеспечения и поддержания уровня защищенности информации, содержащейся в ИС		
6.1.	Установка обновлений программного обеспечения (ПО) (общесистемного, прикладного, программных СЗИ), в том числе проверка обновлений баз средств защиты информации (для средств антивирусной защиты и средств анализа защищенности)	В автоматическом режиме при выпуске производителем новой версии ПО либо вручную (при наличии обновлений) не реже одного раза в 3 месяца	Уполномоченные сотрудники администрации (в пределах своих полномочий)
6.2.	Обеспечение работоспособности, правильности функционирования и параметров настройки программного обеспечения и средств защиты информации	Постоянно в ходе эксплуатации ИС	Уполномоченные сотрудники администрации (в пределах своих полномочий)
6.3.	Контроль состава технических средств, программного обеспечения и средств защиты информации	Не реже одного раза в год	Ответственный за защиту информации
6.4.	Соблюдение установленных правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей	В процессе эксплуатации и после вывода из эксплуатации ИС	Уполномоченные сотрудники администрации (в пределах своих полномочий)
6.5.	Учет и сохранность технической и эксплуатационной документации на технические и программные средства, применяемые в ИС	В процессе эксплуатации и после вывода из эксплуатации ИС	Ответственный за защиту информации

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
6.6.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки защищаемой информации	При необходимости в процессе эксплуатации и после вывода из эксплуатации ИС	Ответственный за организацию обработки персональных данных и ответственный за защиту информации
6.7.	Учет средств защиты информации, эксплуатационной и технической документации к ним (при необходимости)	В процессе эксплуатации и после вывода из эксплуатации ИС	Уполномоченные сотрудники администрации, ответственный за защиту информации, ответственный за эксплуатацию средств криптографической защиты СКЗИ (в пределах своих полномочий)
6.8.	Учёт машинных носителей информации	При необходимости в процессе эксплуатации и после вывода из эксплуатации ИС	Ответственный за защиту информации
6.9.	Обеспечение безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	Непрерывно в процессе эксплуатации ИС и при необходимости в случае возникновения нарушений в функционировании технических средств	Уполномоченные сотрудники администрации (в пределах своих полномочий)
6.10.	Поддержание работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий	Непрерывно в процессе эксплуатации ИС	Ответственный за защиту информации
6.11.	Проведение периодических проверок компонентов ИС на наличие вредоносных компьютерных программ (вирусов)	В автоматическом режиме в соответствии с установленным расписанием и вручную по требованию	Пользователи ИС, уполномоченные сотрудники администрации (в пределах своих полномочий)
6.12.	Проверка расположения средств отображения информации	Не реже одного раза в год	Ответственный за защиту информации
6.13.	Документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в ИС	По результатам проведения контроля за обеспечением уровня защищенности	Ответственный за защиту информации

№ п/п	Наименование мероприятия по защите информации	Условия и периодичность проведения мероприятий по защите информации	Ответственные исполнители
6.14.	Принятие решения о необходимости доработки (модернизации) системы защиты информации	информации, содержащейся в ИС	администрации
7.	Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации		
7.1.	Архивирование информации, содержащейся в ИС	При необходимости дальнейшего использования информации в деятельности ГБУ НСО «ЦЗИ НСО»	Ответственный за защиту информации, уполномоченные сотрудники администрации (в пределах своих полномочий)
7.2.	Уничтожение (стирание) данных и остаточной информации с машинных носителей информации	При необходимости передачи машинного носителя информации другому пользователю ИС или в сторонние организации	Ответственный за защиту информации
7.3.	Физическое уничтожение машинных носителей остаточной информации	При выводе из эксплуатации машинных носителей информации	Ответственный за защиту информации

Приложение № 2
к приказу от _____ № _____

ПРАВИЛА
идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящие Правила разработаны в целях реализации мер защиты информации по идентификации и аутентификации субъектов доступа к объектам доступа в информационных системах (далее – ИС) администрации Баганского района Новосибирской области (далее – администрация, оператор).

1.2 Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

2. Идентификация и аутентификация пользователей, являющихся внутренними пользователями

2.1 При доступе в ИС администрации должна осуществляться идентификация и аутентификация пользователей и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

2.2 К внутренним пользователям относятся сотрудники администрации, выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИС администрации в соответствии с должностными регламентами (инструкциями), утвержденными в администрации, и которым в ИС присвоены учетные записи.

2.3 В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, уполномоченного лица и (или) оператора иной ИС, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИС (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с заключенными соглашениями и организационно-распорядительными документами администрации.

2.4 Для каждого внутреннего пользователя в ИС администрации должны быть заведены учетные записи.

2.5 Пользователи ИС администрации должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации.

2.6 Аутентификация пользователей в ИС администрации должна осуществляться с использованием паролей. Также могут применяться аппаратные средства в случае многофакторной аутентификации.

2.7 В ИС администрации должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

3.1В ИС администрации должны быть реализованы следующие функции управления идентификаторами пользователей и устройств:

– формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

– присвоение идентификатора пользователю и (или) устройству;

– предотвращение повторного использования идентификатора пользователя и (или) устройства в течение одного года;

– блокирование идентификатора пользователя через установленный период времени неиспользования.

3.2Создание, присвоение и уничтожение идентификаторов пользователей и устройств осуществляют уполномоченные сотрудники администрации.

4. Управление средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

4.1 В ИС администрации должны быть реализованы следующие функции управления средствами аутентификации (аутентификационной

информацией) пользователей и устройств:

– изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации ИС;

– выдача средств аутентификации пользователям;

– генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации) с последующей сменой пользователями начальной аутентификационной информации;

– установление характеристик пароля: длина пароля не менее восьми символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, смена паролей не более чем через 120 дней;

– блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

– обновление аутентификационной информации (замена средств аутентификации) с установленной периодичностью не более, чем через 120 дней;

– защита аутентификационной информации от неправомерного доступа к ней и модифицирования.

4.2 В случае утраты и (или) компрометации личного пароля пользователя ИС администрации должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:

– внеплановая смена (сброс) личного пароля или удаление учетной записи пользователя ИС в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться уполномоченными сотрудниками администрации после окончания последнего сеанса работы данного пользователя с системой;

– внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) лиц, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС администрации.

4.3 Управление средствами аутентификации (аутентификационной информацией) пользователей ИС и принятие мер в случае утраты и (или) компрометации средств аутентификации (аутентификационной информации) осуществляют уполномоченные сотрудники администрации.

4.4 Руководители структурных подразделений администрации» должны обеспечить своевременное

доведение информации о прекращении полномочий пользователей ИС до уполномоченных сотрудников администрации

5. Защита обратной связи при вводе аутентификационной информации

5.1 В ИС администрации должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

5.2 Защита обратной связи «система – субъект доступа» в процессе аутентификации должна обеспечиваться исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками.

6. Ответственность при организации идентификации и аутентификации

6.1 Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

6.2 Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

6.3

6.4

Приложение № 3
к приказу от _____ № _____

ПРАВИЛА
управления доступом субъектов доступа к объектам доступа в информационных системах администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящие Правила разработаны в целях реализации мер защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация) по управлению доступом субъектов доступа к объектам доступа в информационных системах (далее – ИС) администрации Баганского района Новосибирской области (далее – администрации, оператор).

1.2 Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа,

разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в ИС правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

2. Управление учетными записями пользователей

2.1 В ИС администрации должны быть реализованы следующие функции управления учетными записями пользователей:

- определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная);
- объединение учетных записей в группы (при необходимости);
- верификация пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
- заведение, активация, блокирование и уничтожение учетных записей пользователей;
- пересмотр и, при необходимости, корректировка учетных записей пользователей с установленной периодичностью (не реже 1 раза в год);
- регламентирование порядка заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;
- оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей пользователей, предоставленных для однократного выполнения задач в ИС;
- предоставление пользователям прав доступа к объектам доступа ИС, основываясь на задачах, решаемых пользователями в ИС и взаимодействующими с ней ИС.

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

2.3 По истечении установленного срока использования временных учетных записей должно осуществляться автоматическое блокирование временных учетных записей пользователей.

2.4 Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей ИС администрации осуществляют уполномоченные сотрудники администрации.

3. Правила разграничения доступа

3.1 В зависимости от особенностей функционирования ИС, с учетом угроз безопасности информации в ИС администрации реализуется один или комбинация следующих методов управления доступом:

- дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа -

списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;

– ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности).

3.2 Правила разграничения доступа реализуются на основе матрицы доступа и обеспечивают управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

3.3 Оператором должно обеспечиваться разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС, в соответствии с их должностными обязанностями (функциями), и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей). Соответствие ролей и функций, выполняемых персоналом, представлено в таблице 1.

Таблица 1 – Роли и функции персонала, обслуживающего и эксплуатирующего ИС

№ п/п	Роль	Уровень доступа	Основные функции
	Ответственный за организацию обработки персональных данных	Доступ на правах пользователя к информации, техническим средствам, программному обеспечению, средствам защиты информации. Без доступа на изменение параметров средств защиты информации, программного обеспечения, технических средств	– осуществление внутреннего контроля за соблюдением оператором и его работниками законодательства РФ о персональных данных, в том числе требований к защите персональных данных; – доведение до сведения работников оператора положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных; – организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов
	Ответственный за защиту информации (обеспечение безопасности	Доступ на правах администратора к средствам защиты информации, на правах пользователя к информации,	– организация и обеспечение выполнения требований по защите информации в процессе ее обработки в ИС;

№ п/п	Роль	Уровень доступа	Основные функции
	персональных данных)	техническим средствам, программному обеспечению. Без доступа на изменение параметров программного обеспечения, технических средств	– планирование и организация контроля мероприятий по защите информации в ИС; – обеспечение анализа угроз безопасности информации в ИС; – информирование и обучение пользователей ИС об актуальных угрозах безопасности информации, по вопросам обеспечения защиты информации и правилам безопасной эксплуатации ИС; – контроль осведомленности пользователей ИС об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации; – обнаружение и реагирование на инциденты, которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности информации, и реагирование на них; – ведение, пересмотр и доработка документации в области защиты информации, предусмотренной локальными актами администрации; – контроль соблюдения правил разграничения доступа; – управление (администрирование) системой защиты информации ИС; – контроль работоспособности (контроль неотключения) и правильности функционирования СЗИ; – обеспечение установки обновлений программного обеспечения СЗИ, обеспечение выполнения и контроль результатов выполнения задач обновления баз данных СЗИ; – проведение инструктажа персонала по правилам работы с отдельными СЗИ; – контроль аппаратной конфигурации защищаемых технических средств (АРМ, серверов) и предотвращение попытки ее несанкционированного изменения

№ п/п	Роль	Уровень доступа	Основные функции
	Администратор ИС	Доступ на правах администратора к техническим средствам, программному обеспечению. Без доступа на изменение параметров средств защиты информации	– установка, модернизация, настройка и мониторинг работоспособности системного, базового и прикладного программного обеспечения; – конфигурирование и управление программным обеспечением и оборудованием ИС; – модернизация, настройка и мониторинг работоспособности комплекса технических средств (серверов, рабочих станций)
	Ответственный за выявление инцидентов и реагирование на них	Доступ на правах администратора к средствам защиты информации. Без доступа на изменение к информации, техническим средствам, программному обеспечению	– выявление (поиск) уязвимостей ИС администрации с использованием средств анализа (контроля) защищенности (сканеров безопасности); – обнаружение и идентификация инцидентов; – анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий; – планирование и принятие мер по устранению инцидентов; – планирование и принятие мер по предотвращению повторного возникновения инцидентов
	Ответственный за эксплуатацию средств криптографической защиты информации (СКЗИ)	Доступ на правах пользователя к информации, техническим средствам, прикладному программному обеспечению, средствам защиты информации. Без доступа на изменение параметров средств защиты информации, программного обеспечения, технических средств	поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним; контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и локальными актами администрации; учет пользователей криптосредств; надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей дистрибутивов криптосредств; проведение расследований и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации;

№ п/п	Роль	Уровень доступа	Основные функции
			разработка и принятие мер по предотвращению возможных негативных последствий нарушений
	Пользователь информационной системы	Доступ на правах пользователя к информации, техническим средствам, программному обеспечению, средствам защиты информации. Без доступа на изменение параметров настройки средств защиты информации, программного обеспечения, технических средств	– доступ к техническим средствам ИС, программному обеспечению, защищаемой информации (персональным данным); – обработка защищаемой информации (персональных данных)

3.4 В ИС администрации администрации] должно осуществляться ограничение количества неуспешных попыток входа в ИС (доступа к ИС), а также обеспечиваться блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в ИС (доступа к ИС) на установленный период времени.

3.5 В ИС администрации должно обеспечиваться блокирование сеанса доступа пользователя после установленного времени его бездействия (неактивности) в ИС или по запросу пользователя ИС.

3.6 Блокирование сеанса доступа пользователя в ИС обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к ИС (без выхода из ИС).

3.7 Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

3.8 Блокирование сеанса доступа пользователя в ИС должно сохраняться до прохождения им повторной идентификации.

3.9 Пользователям ИС запрещены любые действия до прохождения ими процедур идентификации и аутентификации (кроме необходимых для прохождения процедур идентификации и аутентификации).

4. Управление информационными потоками

4.1 В ИС администрации должно осуществляться управление информационными потоками, обеспечивающее разрешенный (установленный) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках ИС, а также между ИС или при взаимодействии с сетью «Интернет» (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления

информационными потоками, включающих контроль конфигурации ИС, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

4.2 Управление информационными потоками должно блокировать передачу защищаемой информации через сеть «Интернет» (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из ИС и (или) входящие в ИС.

5. Правила удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

5.1 В ИС администрации должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа ИС через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

5.2 Защита удаленного доступа должна обеспечиваться для всех видов доступа и включает:

– ограничение на использование удаленного доступа в соответствии с задачами (функциями) ИС, для решения которых такой доступ необходим;

– предоставление удаленного доступа только тем лицам, которым он необходим для осуществления технической поддержки на основании договора;

– мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС;

– контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИС до начала информационного взаимодействия с ИС (передачи защищаемой информации);

– использование ограниченного (минимально необходимого) количества точек подключения к ИС при организации удаленного доступа к объектам доступа ИС;

– исключение удаленного доступа от имени привилегированных учетных записей (администраторов) для администрирования ИС и ее системы защиты информации.

6. Управление взаимодействием с информационными системами сторонних организаций (внешними ИС)

6.1 Управление взаимодействием ИС администрации с внешними ИС должно включать в себя определение порядка обработки, хранения и передачи информации с использованием внешних ИС.

6.2 Оператор разрешает обработку, хранение и передачу информации с использованием внешней ИС при выполнении следующих условий:

– при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

– при наличии подтверждения выполнения во внешней ИС предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

7. Ответственность

7.1 Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

7.2 Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

7.3 ПРИЛОЖЕНИЕ
к Правилам управления доступом субъектов
доступа к объектам доступа
в информационных системах администрации
Баганского района Новосибирской области

Матрица доступа
субъектов доступа по отношению к защищаемым информационным ресурсам информационных систем администрации Баганского района Новосибирской области

Настоящий документ разработан в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17, и устанавливает полномочия субъектов доступа по доступу к защищаемым информационным ресурсам информационных систем (далее – ИС) администрации Баганского района Новосибирской области администрация). Предоставление пользователям прав доступа к объектам доступа информационных систем осуществляется на основании задач, решаемых пользователями в ИС администрации и взаимодействующими с ними информационными системами.

В ИС администрации для управления доступом используются дискреционный и ролевой методы управления доступом.

В ИС администрации обеспечено разделение полномочий (ролей) субъектов доступа ИС, и определены роли пользователей в соответствии с минимально необходимыми правами и привилегиями:

1) Пользователь – имеет непривилегированный доступ к ресурсам АРМ ИС и средствам защиты информации, разрешены действия (операции) по обработке информации в ИС с использованием технологии локального доступа, без права управления (администрирования) ИС и системы защиты ИС;

2) Администратор ИБ – имеет привилегированный доступ к ресурсам АРМ ИС (разрешены действия (операции) по управлению (администрированию) системой защиты ИС);

3) Администратор ИС – имеет привилегированный доступ к ресурсам АРМ ИС (разрешены действия (операции) по управлению (администрированию) ИС, без права управления (администрирования) средствами защиты информации).

Перечень категорий лиц, имеющих доступ к информационным ресурсам администрации, с указанием их роли приведен в таблице 1.

Таблица 1 – Перечень категорий лиц

№ п/п	Категория лиц	Роль
	Сотрудники администрации (пользователи ИС)	Пользователь
	Уполномоченный сотрудник администрации	Администратор ИБ
	Уполномоченные сотрудники администрации	Администратор ИС

Для субъектов доступа ИС администрации установлены разрешения согласно таблице 2.

Таблица 2 – Разрешения, установленные для субъектов доступа

Разрешения	Разрешить	Запретить
Администратор ИБ/Администратор ИС		
Обзор папок/Выполнение файлов	+	
Содержание папки/Чтение данных	+	
Чтение атрибутов	+	
Чтение дополнительных атрибутов	+	
Создание файлов/Запись данных	+	
Создание папок/Запись данных	+	
Запись атрибутов	+	
Запись дополнительных атрибутов	+	
Удаление подпапок и файлов	+	
Чтение разрешений	+	
Смена разрешений	+	
Смена владельца	+	
Печать	+	
Управление принтерами	+	
Управление документами	+	
Пользователь		
Обзор папок/Выполнение файлов	+	
Содержание папки/Чтение данных	+	
Чтение атрибутов	+	
Чтение дополнительных атрибутов	+	
Создание файлов/Запись данных	+	
Создание папок/Запись данных	+	
Запись атрибутов	+	
Запись дополнительных атрибутов	+	
Удаление подпапок и файлов	+	
Чтение разрешений	+	
Смена разрешений		+
Смена владельца		+
Печать	+	
Управление принтерами		+
Управление документами	+	

Наличие доступа к объектам ИС администрации в зависимости от полномочий (роли) отражено в таблице 3.

Таблица 3 – Наличие доступа к объектам ИС администрации

Объект доступа	Роль		
	Администратор ИС	Администратор ИБ	Пользователь
Устройства			
Автоматизированное рабочее место (АРМ)	+	+	+
Сетевое и коммутационное оборудование	+	+	–
Съемные машинные носители (CD/DVD, флеш-накопители и т.д.)	+ (без доступа к защищаемой информации)	+ (без доступа к защищаемой информации)	+
Объекты файловой системы			
Жесткий диск, личный каталог	+	+	+
Жесткий диск, служебные (в том числе системные) каталоги	+	+	–
Запускаемые и исполняемые модули			
Запускаемые и исполняемые модули прикладного программного обеспечения, непосредственно участвующего в обработке персональных данных	+ (без доступа к защищаемой информации)	+ (без доступа к защищаемой информации)	+ (без права конфигурирования компонентов ИС)
Запускаемые и исполняемые модули прикладного программного обеспечения, непосредственно не участвующего в обработке персональных данных	+	+	+

Приложение № 4
к приказу от _____ № _____

Правила по ограничению программной среды в информационных системах администрация Баганского района Новосибирской области

1. Общие положения

1.1 Настоящие Правила разработаны в целях реализации мер защиты информации по ограничению программной среды в информационных системах (далее – ИС) администрация Баганского района (далее администрация, оператор).

1.2 Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в ИС программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в ИС программного обеспечения.

2. Установка (инсталляция) только разрешенного к использованию программного обеспечения и его компонентов

2.1 Установка (инсталляция) в ИС администрации программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов должна осуществляться с учетом Перечня программного обеспечения, разрешенного к установке в информационных системах администрации («белый список»).

2.2 Установка (инсталляция) в ИС программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора.

2.3 В ИС администрации] должен обеспечиваться периодический контроль установленного (инсталлированного) программного обеспечения на предмет соответствия его Перечню программного обеспечения, разрешенному к установке, а также на предмет соответствия его Перечню программного обеспечения, разрешенного к использованию в информационных системах администрации, а также на предмет отсутствия программного обеспечения, запрещенного в ИС администрации.

2.4 Пересмотр Перечня программного обеспечения, разрешенного к использованию в информационных системах администрации, может осуществляться на основании заявки пользователя, согласованной с непосредственным руководителем пользователя.

3. Ответственность

3.1 Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

3.2 Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством РФ.

ПРИЛОЖЕНИЕ
к Правилам по ограничению программной среды
в информационных системах администрации
Баганского района Новосибирской области

ТИПОВАЯ ФОРМА

Перечень программного обеспечения и (или) его компонентов, разрешенного к установке в информационных системах администрации Баганского района Новосибирской области

№ п/п	Наименование	Назначение
1		
2		
3		
4		
5		

Приложение № 5

к приказу от _____ № _____

ПРАВИЛА
обращения с машинными носителями информации в информационных системах администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящие Правила разработаны в целях реализации мер по защите машинных носителей информации (персональных данных), используемых в информационных системах (далее – ИС) администрации Баганского района Новосибирской области (далее – администрация, оператор).

1.2 Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

1.3 В качестве машинных носителей информации в настоящих Правилах рассматриваются:

– машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках);

– мобильные технические средства: съемные машинные носители информации (флэш-накопители, CD, внешние накопители на жестких дисках и иные устройства).

1.4 Под использованием машинных носителей информации в ИС администрации] понимается их подключение к инфраструктуре ИС администрации с

целью обработки, приема/передачи информации между ИС и носителями информации.

2. Использование машинных носителей информации

2.1 В ИС администрации для обработки защищаемой информации допускается использование только учтенных машинных носителей информации, которые являются собственностью администрации и подвергаются регулярной ревизии и контролю.

2.2 При использовании сотрудниками машинных носителей информации необходимо:

– использовать машинные носители информации исключительно для выполнения своих служебных обязанностей;

– бережно относиться к машинным носителям информации;

– обеспечивать физическую безопасность машинных носителей информации;

– извещать ответственного за защиту информации о фактах утраты (кражи) машинных носителей информации;

– перед началом работы с машинными носителями информации пользователь обязан проверять их на наличие вредоносных программ (вирусов) с помощью штатных антивирусных программ.

2.3 При использовании машинных носителей информации запрещено:

– использовать машинные носители информации в личных целях;

– передавать носители информации третьим лицам;

– оставлять машинные носители информации без присмотра или передавать на хранение другим лицам;

– выносить без предварительного согласования с руководителем соответствующего подразделения машинные носители информации из служебных помещений для работы с ними на дому и т. д.

2.4 Ответственность за подключение машинных носителей информации, не учтенных соответствующим образом, не прошедших проверку, несет пользователь, подключивший данное устройство.

3. Защита применяемых в информационных системах мобильных технических средств

3.1 Защита мобильных технических средств (съемных машинных носителей информации) включает реализацию следующих мер:

– контроль использования в ИС мобильных технических средств информации;

– реализация в зависимости от мобильного технического средства (типа мобильного технического средства) мер по идентификации и аутентификации, управлению доступом, ограничению программной среды, защите машинных носителей информации, регистрации событий безопасности, антивирусной защите, контролю (анализу) защищенности, обеспечению целостности;

– уничтожение съемных машинных носителей информации, которые не подлежат очистке;

– выборочные проверки съемных машинных носителей информации (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации);

– запрет возможности автоматического запуска (без команды пользователя) в ИС программного обеспечения на съемных машинных носителях информации.

3.2 Контроль использования мобильных технических средств в ИС администрации включает:

– использование в составе ИС для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с настоящими Правилами;

– ограничение на использование мобильных технических средств в соответствии с задачами (функциями) ИС, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств;

– мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа ИС.

4. Учет и хранение машинных носителей информации

4.1 В администрации учету подлежат следующие машинные носители информации, используемые в ИС для обработки и хранения защищаемой информации (персональных данных):

– съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

– портативные вычислительные устройства, имеющие встроенные носители информации;

– машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

4.2 На каждый машинный носитель должна наноситься маркировка, позволяющая его идентифицировать (регистрационный номер носителя).

4.3 В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

4.4 Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства ИС нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

4.5 Учет машинных носителей информации (персональных данных), используемых в информационных системах администрации, ведется в соответствующем журнале учета машинных носителей информации (далее – Журнал учета) по форме, приведенной в Приложении № 1 к настоящим Правилам.

4.6 Регистрационные или иные номера подлежат занесению в Журнал учета или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

4.7 При поступлении нового машинного носителя информации, который будет использоваться в ИС администрации, носитель регистрируется в Журнале учета. Перед использованием новый машинный носитель информации в обязательном порядке должен пройти антивирусную проверку (при наличии технической возможности).

4.8 В случае увольнения или перевода сотрудника в другое структурное подразделение предоставленные машинные носители информации изымаются.

4.9 Хранить машинные носители информации нужно вдали от источников электромагнитного излучения и тепла.

4.10 Необходимо осуществлять хранение отчуждаемых машинных носителей персональных данных в сейфах (металлических шкафах, персональных хранилищах), оборудованных внутренними замками, либо иным образом обеспечить условия хранения машинных носителей информации, исключающие несанкционированный к ним доступ.

5. Управление доступом к машинным носителям информации

5.1 Управление доступом к машинным носителям информации, используемым в ИС администрации, должно осуществляться ответственным за защиту информации.

5.2 В[администрации должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в ИС:

– определен перечень лиц, имеющих физический доступ к машинным носителям информации;

– физический доступ к машинным носителям информации должен предоставляться только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

6. Контроль перемещения машинных носителей информации за пределы контролируемой зоны

6.1 В ИС администрации должен обеспечиваться контроль перемещения используемых машинных носителей информации за пределы контролируемой зоны. При контроле перемещения машинных носителей информации должны осуществляться:

– определение должностных лиц, имеющих права на перемещение машинных носителей информации за пределы контролируемой зоны;

– предоставление права на перемещение машинных носителей информации за пределы контролируемой зоны только тем лицам, которым оно необходимо для выполнения своих должностных обязанностей (функций);

– учет перемещения машинных носителей информации;

– периодическая проверка наличия машинных носителей информации.

6.2 При передаче средств вычислительной техники (далее – СВТ) ИС администрации в сторонние организации для проведения ремонтно-восстановительных или иных работ, несъемные машинные носители (накопители на жестких дисках) изымаются из состава СВТ, либо осуществляется предварительное уничтожение (стирание) информации, содержащейся на несъемном машинном носителе информации.

7. Уничтожение (стирание) информации на машинных носителях, уничтожение машинных носителей информации, а также контроль уничтожения (стирания) информации

7.1. В администрации должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

7.2. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации (при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации) и обеспечиваться с использованием специального программного обеспечения, гарантирующего уничтожение информации.

7.3. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

7.4. В ИС администрации должны использоваться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации: перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием.

7.5. В случае утраты машинных носителей информации немедленно ставится в известность руководитель соответствующего структурного подразделения и ответственный за защиту информации. На утраченные носители информации составляется Акт утраты машинных носителей информации (в соответствии с формой, представленной в Приложении № 2 к настоящим Правилам). Соответствующие отметки вносятся в Журнал учета.

7.6. Машинные носители информации, пришедшие в негодность или

отслужившие установленный срок, должны быть уничтожены без возможности восстановления (путем физического разрушения или сильной деформации носителя) с составлением Акта уничтожения машинных носителей информации (в соответствии с формой, представленной в Приложении № 3 к настоящим Правилам) и регистрацией в Журнале учета.

7.7. При необходимости дальнейшего использования информации в деятельности администрации должно осуществляться архивирование информации, хранящейся на машинном носителе, подлежащем уничтожению.

7.8. Ответственный за защиту информации обеспечивает регистрацию и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации путем составления соответствующих актов, и занесения соответствующей информации в Журнал учета

8. Ответственность

8.1. Ответственность за выполнение правил эксплуатации машинных носителей информации несут пользователи ИС администрации.

8.2.Контроль выполнения установленных правил эксплуатации, регистрации и учёта машинных носителей информации осуществляет ответственный за защиту информации.

8.3.Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

8.4.Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

Приложение № 1
к Правилам обращения с машинными носителями информации
в информационных системах администрации Баганского района Новосибирской области

ТИПОВАЯ ФОРМА

ЖУРНАЛ
учета машинных носителей информации, используемых в информационных системах администрации Баганского района Новосибирской области

Журнал начат «____» _____ 20 ___ г.
Журнал завершен «____» _____ 20 ___ г.
Журнал составлен на _____ листах

№ п/п	Тип машинного носителя информации	Регистрационный (учетный) номер машинного носителя информации	Ф.И.О., подпись получателя, дата, и место хранения машинного носителя информации	Ф.И.О., подпись сдавшего, дата	Ф.И.О., подпись принявшего, дата, и место хранения машинного носителя информации	Дата и номер акта об уничтожении/ акта утраты	Примечание
1	2	3	4	5	6	7	8
2							
3							

ПРИЛОЖЕНИЕ № 2
к Правилам обращения с машинными носителями информации
в информационных системах администрации Баганского района Новосибирской области

ТИПОВАЯ ФОРМА

Акт
утраты машинных носителей информации

Комиссия в составе:

_____
(должность, ФИО)

_____
(должность, ФИО)

_____
(должность, ФИО)

составила настоящий Акт об утрате нижеуказанных машинных носителей информации:

№ п/п	Тип машинного носителя информации	Учетный номер машинного носителя информации	Примечание

Всего машинных носителей _____
(цифрами и прописью)

Носители были утеряны при следующих обстоятельствах:

_____
_____
_____

Отметка об утере внесена в Журнал учета машинных носителей информации, используемых в информационных системах администрации Баганского района Новосибирской области

Члены комиссии:

_____ _____
(подпись) (ФИО)

_____ _____
(подпись) (ФИО)

_____ _____
(подпись) (ФИО)

«_____» _____ 20____ г.

ПРИЛОЖЕНИЕ № 3
к Правилам обращения с машинными носителями информации
в информационных системах администрации Баганского района Новосибирской области

ТИПОВАЯ ФОРМА

Акт
уничтожения машинных носителей информации

Комиссия в составе:

_____
(должность, ФИО)

_____
(должность, ФИО)

_____
(должность, ФИО)

составила настоящий Акт о том, что нижеуказанные машинные носители информации подлежат уничтожению как утратившие практическое значение и непригодные для дальнейшего использования:

№ п/п	Тип машинного носителя информации	Учетный номер машинного носителя информации	Примечание

Всего машинных носителей _____
(цифрами и прописью)

На машинных носителях уничтожена вся информация путем:

_____
_____
_____

Вышеуказанные машинные носители уничтожены путем:

_____
_____
_____

Отметка об уничтожении внесена в Журнал учета машинных носителей информации, используемых в информационных системах администрации Баганского района Новосибирской области.

Члены комиссии:

_____ _____
(подпись) (ФИО)

_____ _____
(подпись) (ФИО)

_____ _____
(подпись) (ФИО)

«___» _____ 20 ___ г.

Приложение № 6

к постановлению от _____ № _____

ПРАВИЛА
регистрации событий безопасности в информационных системах администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящие Правила разработаны в целях реализации мер по регистрации событий безопасности в информационных системах (далее – ИС) администрации Баганского района Новосибирской области (далее – администрация, оператор) и регламентируют состав и содержание информации о событиях безопасности, подлежащих регистрации, правила и процедуры сбора, записи, хранения и защиты информации о событиях безопасности в ИС администрации.

1.2 Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в ИС, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

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

2.1 События безопасности, подлежащие регистрации в ИС администрации, определяются с учетом способов реализации угроз безопасности для ИС.

2.2 К событиям безопасности, подлежащим регистрации в ИС, относятся любые проявления состояния ИС и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов ИС, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также на нарушение штатного функционирования средств защиты информации.

2.3 События безопасности, подлежащие регистрации в ИС, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИС. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в ИС.

2.4 Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется исходя из возможностей реализации угроз безопасности информации.

2.5 В ИС администрации подлежат регистрации следующие события безопасности:

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

– подключение машинных носителей информации и вывод информации на носители информации;

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

– попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;

– попытки удаленного доступа.

2.6 Сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа

инцидентов, возникших в ИС администрации, и устанавливаются исходя из значимости события безопасности.

3. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

3.1 Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

3.2 Основной состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, представлены в таблице 1.

Таблица 1 – Состав и содержание информации о событиях безопасности

№ п/п	События безопасности, подлежащие регистрации	Состав и содержание информации о событиях безопасности
1	Вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы	Дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа
2	Подключение машинных носителей информации и вывод информации на носители информации	Дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации
3	Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	Дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)
4	Попытки доступа программных средств к защищаемым объектам доступа	Дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип)
5	Попытки удаленного доступа	Дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе

4. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

4.1 Процедуры сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения должны предусматривать:

– возможность выбора событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 3 настоящих Правил;

– генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в пункте 3.2 настоящих Правил;

– хранение информации о событиях безопасности в течение установленного времени.

4.2 Объем памяти для хранения информации о событиях безопасности рассчитывается и выделяется с учетом типов событий безопасности, подлежащих регистрации, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

5. Реагирование на сбои при регистрации событий безопасности

5.1 Реагирование на сбои при регистрации событий безопасности в ИС администрации (в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти) осуществляется уполномоченными сотрудниками администрации.

5.2 Реагирование на сбои при регистрации событий безопасности предусматривает следующие меры:

– изменение параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИС;

– запись поверх устаревших хранимых записей событий безопасности.

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

6.1 Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться уполномоченными сотрудниками администрации для всех событий, подлежащих регистрации в соответствии с пунктом 3.2 настоящих Правил, и обеспечивать своевременное выявление признаков инцидентов безопасности в ИС.

6.2 В случае выявления признаков инцидентов безопасности в ИС администрации уполномоченными сотрудниками осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

7. Генерирование временных меток и (или) синхронизация системного времени в информационной системе

7.1 В ИС администрации должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени.

7.2 Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС администрации достигается посредством применения внутренних системных часов ИС или путем синхронизации системного времени.

8. Защита информации о событиях безопасности

8.1 Защита информации о событиях безопасности (записях регистрации (аудита)) в ИС администрации должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

8.2 Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только уполномоченным сотрудникам администрации.

9. Ответственность

9.1 Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

9.2 Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

9.3 Приложение № 7
к постановлению от _____ № _____

ПРАВИЛА
антивирусной защиты информационных систем администрации
Баганского района Новосибирской области

1. Общие положения

1.1 Настоящие Правила разработаны в целях реализации мер по антивирусной защите информационных систем (далее – ИС) администрации Баганского района Новосибирской области (далее – администрация, оператор) и регулируют вопросы организации антивирусной защиты и требования к порядку проведения антивирусного контроля при работе в ИС администрации.

1.2 Меры по антивирусной защите должны обеспечивать обнаружение в ИС компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

1.3 Установка и настройка средств антивирусной защиты осуществляется уполномоченными сотрудниками администрации в соответствии с эксплуатационной документацией на применяемые средства антивирусной защиты.

2. Обеспечение антивирусной защиты

2.1 Порядок организации антивирусной защиты

2.1.1 Для обеспечения антивирусной защиты ИС администрации должны применяться средства антивирусной защиты, установленные на все средства вычислительной техники (СВТ) (при наличии технической возможности), входящие в ИС администрации и подверженные внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы).

2.1.2 Права на установку, конфигурирование и управление (администрирование) средствами антивирусной защиты предоставляются уполномоченным сотрудникам администрации.

2.1.3 Для реализации антивирусной защиты в ИС администрации осуществляется предоставление доступа средствам антивирусной защиты к объектам ИС, которые должны быть подвергнуты проверке.

2.1.4 Сотрудники администрации не должны допускать использования в ИС программного обеспечения и данных, не связанных с выполнением их должностных обязанностей.

2.1.5 Уполномоченными сотрудниками администрации

организуется проведение периодических проверок компонентов ИС на наличие вредоносных компьютерных программ (вирусов).

2.1.6 Проверка выделенных наиболее критичных компонентов ИС (системной памяти, объектов автозапуска, системных папок) на наличие вредоносных компьютерных программ (вирусов) осуществляется в автоматическом режиме по расписанию (один раз в сутки) и при необходимости вручную пользователями ИС.

2.1.7 Расширенный (полный) антивирусный контроль всех компонентов ИС проводится в автоматическом режиме с периодичностью один раз в месяц и при необходимости вручную уполномоченным сотрудником администрации.

2.1.8 В ИС должна осуществляться автоматическая проверка в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, и других внешних источников) при загрузке, открытии или исполнении таких файлов.

2.1.9 В ИС должно осуществляться оповещение уполномоченных сотрудников администрации в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов).

2.1.10 Расширенный (полный) антивирусный контроль всех компонентов ИС проводится в автоматическом режиме с периодичностью один раз в месяц и при необходимости вручную.

2.1.11 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Контроль исходящей информации (в случае передачи информации на внешнем съемном носителе) необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель) (при наличии такой процедуры).

2.2 Порядок проведения антивирусного контроля.

2.2.1 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.) пользователь ИС администрации самостоятельно или вместе с уполномоченным сотрудником администрации проводит внеочередной антивирусный контроль своей рабочей станции для определения факта наличия или отсутствия компьютерного вируса.

2.2.2 В случае обнаружения в ИС объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами), пользователь ИС обязан:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за защиту информации, уполномоченных сотрудников администрации, владельца зараженных файлов, 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.

2.3 Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

2.3.1 Получение из доверенных источников и установка обновлений базы данных признаков вредоносных компьютерных программ (вирусов) обеспечивают уполномоченные сотрудники администрации.

2.3.2 В ИС администрации обеспечивается контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов) на соответствие предоставляемых производителем СЗИ контрольным суммам.

2.3.3 В ИС администрации обеспечивается централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов) уполномоченными сотрудниками администрации.

3. Ответственность

3.1 Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

3.2 Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

3.3 Приложение № 8
к приказу от _____ № _____

ПРАВИЛА
контроля (анализа) защищенности информации в информационных системах администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящие Правила разработаны в целях реализации мер по контролю (анализу) защищенности информации в информационных системах (далее – ИС) администрации Баганского района Новосибирской области (далее администрация, оператор).

1.2 Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в ИС, путем проведения мероприятий по анализу защищенности ИС и тестированию их систем защиты информации.

1.3 Мероприятия по контролю защищенности информации в ИС проводятся в пределах своих полномочий уполномоченными сотрудниками администрации ответственным за защиту информации, содержащейся в информационных системах администрации.

2. Выявление, анализ и устранение уязвимостей информационных систе

2.1 Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.

2.2 В ИС администрации при выявлении (поиске), анализе и устранении уязвимостей должны проводиться:

– выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и

настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

– разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

– анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

– устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

– информирование должностных лиц (пользователей, ответственных лиц) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

2.3 Анализ уязвимостей информационной системы включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.

2.4 В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

2.5 Выявление (поиск), анализ и устранение уязвимостей проводится на этапах создания и эксплуатации ИС. На этапе эксплуатации ИС поиск и анализ уязвимостей проводится не реже одного раза в год. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемых в ИС администрации.

2.6 В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (корректировка настроек средств защиты информации, изменение режима и порядка использования ИС), направленные на устранение возможности использования выявленных уязвимостей.

2.7 В ИС администрации должны использоваться для выявления (поиска) уязвимостей средства анализа (контроля) защищенности (сканеры безопасности), имеющие стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования ИС на наличие уязвимостей, оценки последствий уязвимостей, имеющие возможность оперативного обновления базы данных выявляемых уязвимостей.

2.8 В ИС администрации должно осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей (для системы анализа защищенности).

2.9 Доступ к функциям выявления (поиска) уязвимостей предоставляется только уполномоченным сотрудникам администрации.

2.10 В целях предупреждения инцидентов безопасности уполномоченные сотрудники администрации должны проводить анализ журналов регистрации событий

безопасности (журнал аудита) в целях определения, были ли выявленные уязвимости ранее использованы в ИС администрации для нарушения безопасности информации

2.11 В случае выявления уязвимостей ИС, 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.

3. Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации

3.1 В ИС администрации уполномоченными сотрудниками администрации в рамках своих полномочий обеспечивается получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

3.2 При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в ИС администрации и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

3.3 Контроль установки обновлений программного обеспечения проводится с периодичностью – не реже одного раза в два года.

3.4 При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты, баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

4. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

4.1 При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации должны осуществляться:

– контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;

– проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации;

– контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;

– восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

4.2 Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится уполномоченными сотрудниками администрации не реже одного раза в 2 года.

5. Контроль состава технических средств, программного обеспечения и средств защиты информации

5.1 При контроле состава технических средств, программного обеспечения и средств защиты информации (инвентаризации) должны осуществляться:

– контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИС администрации и принятие мер, направленных на устранение выявленных недостатков;

– контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;

– контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

– исключение (восстановление) из состава ИС администрации несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

5.2 Контроль состава технических средств, программного обеспечения и средств защиты информации проводится ответственным за защиту информации, уполномоченными сотрудниками администрации в рамках своих полномочий не реже одного раза в 2 года.

6. Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей, реализации правил разграничения доступом, полномочий пользователей в информационных системах

6.1 При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС администрации должны осуществляться:

– контроль правил генерации и смены паролей пользователей;

– контроль заведения и удаления учетных записей пользователей;

– контроль реализации правил разграничения доступом;

– контроль реализации полномочий пользователей;

– контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации в администрации;

– устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

6.2 Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС администрации проводится уполномоченными сотрудниками администрации не реже одного раза в 2 года.

7. Ответственность

7.1 Оператор несет ответственность за правонарушения в сфере информации, информационных технологий и защиты информации в соответствии с законодательством Российской Федерации.

7.2 Лица, виновные в нарушении требований настоящих Правил, могут быть привлечены к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации.

7.3 Приложение № 9
к постановлению от _____ № _____

ПРАВИЛА
обеспечения целостности и доступности информационных систем и информации в администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящие Правила разработаны в целях реализации мер по обеспечению целостности и доступности информационных систем (далее – ИС) и информации в администрации Баганского района Новосибирской области (далее – администрация, оператор).

1.2 Меры по обеспечению целостности ИС и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности ИС и содержащейся в ней информации, а также возможность восстановления ИС и содержащейся в ней информации.

1.3 Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в ИС, в штатном режиме функционирования ИС.

1.4 Защита резервируемой информации в ИС администрации обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации в администрации.

2. Обеспечение возможности восстановления программного обеспечения в информационной системе при возникновении нештатных ситуаций

2.1 Для обеспечения возможности восстановления программного обеспечения в ИС администрации] должны быть приняты соответствующие планы по действиям персонала (ответственных, пользователей) при возникновении нештатных ситуаций.

2.2 Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать:

– восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;

– восстановление и проверку работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;

– возврат ИС администрации] в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей ИС, позволяющих решать задачи по обработке информации.

2.3 В ИС администрации должны применяться компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.

3. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование

3.1 В ИС администрации должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

3.2 Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования ИС путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами).

3.3 При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с настоящими Правилами, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования.

4. Периодическое резервное копирование информации на резервные машинные носители информаци

4.1 В ИС администрации должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее:

– резервное копирование информации на резервные машинные носители информации с установленной периодичностью;

– разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;

– регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;

– принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность.

4.2 Резервное копирование и хранение данных должно осуществлять на периодической основе.

4.3 Хранение (размещение) резервных копий информации должно осуществляться на отдельных (размещенных вне ИС) средствах хранения резервных копий и в условиях, которые исключают воздействие внешних факторов на хранимую информацию.

4.4 Резервные копии должны храниться в течение установленного срока с целью обеспечения возможности восстановления данных.

4.5 Уполномоченными сотрудниками администрации в пределах своей компетенции определяются методы резервного копирования, порядок хранения и восстановления резервируемой информации и осуществляется периодическая проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий.

5. Восстановление информации с резервных машинных носителей информации

5.1 Восстановление информации из резервных копий осуществляется уполномоченными сотрудниками администрации.

5.2 Восстановление информации с резервных машинных носителей

информации (резервных копий) предусматривает определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования ИС администрации] и доступности информации:

– для защищаемой информации – не более 8 часов;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС администрации – не более 24 часов.

– Приложение № 10
к постановлению от _____ № _____

РЕГЛАМЕНТ
выявления инцидентов безопасности и реагирования на них в администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящий Регламент определяет правила и процедуры выявления и реагирования на инциденты информационной безопасности (далее – ИБ) в администрация Баганского района Новосибирской области (далее – администрация).

1.2 Под инцидентом информационной безопасности понимается непредвиденное или нежелательное событие (группа событий), которое привело (может привести) к сбоям или нарушению функционирования информационной системы (далее – ИС) и (или) к возникновению угроз безопасности информации (далее – инцидент).

1.3 Выявление инцидентов ИБ в администрации и реагирование на них обеспечивается ответственным за защиту информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее – информация), содержащейся в ИС администрации.

2. Этапы реагирования на инциденты безопасности

2.1 Жизненный цикл реагирования на инциденты состоит из следующих стадий:

– обнаружение и регистрация инцидента;

– устранение причин и последствий инцидента;

– расследование инцидента;

– реализация корректирующих мероприятий.

2.2 В ходе выявления инцидентов и реагирования на них осуществляются:

– 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 пользователями ИС лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе;

– 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 информационной системы 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.

3. Обнаружение инцидентов информационной безопасности

3.1 В качестве источников информации об инцидентах могут использоваться:

– журналы регистрации событий безопасности и оповещения системного и прикладного программного обеспечения ИС, средств защиты информации;

– информация, получаемая от сотрудников администрации;

– информация, полученная по результатам контроля (анализа) защищенности ИС и контроля эффективности СЗИ.

4. Информирование об инцидентах, анализ инцидентов

4.1 Уполномоченные сотрудники администрации, ответственный за защиту информации, содержащейся в ИС администрации (далее – ответственный за выявление и реагирование на инциденты) получает информацию о случившихся инцидентах и принимает меры по их устранению.

4.2 Сотрудники администрации, а также иные лица, имеющие доступ к ИС администрации, в том числе осуществляющие техническое сопровождение ИС администрации, обязаны при получении информации обо всех нетипичных событиях ИБ незамедлительно сообщить о них ответственному за защиту информации, содержащейся в ИС администрации.

4.3 Некорректное функционирование ИС администрации может являться индикатором атаки или нарушения функционирования системы безопасности. К нетипичным событиям, о которых следует уведомлять ответственных за выявление и реагирование на инциденты, относятся:

– крахи системы, произвольные перезагрузки системы;

– самопроизвольное появление новых учетных записей;

– самопроизвольное появление новых файлов;

– изменения в размерах и датах файлов, не соответствующие фактическим датам обращения и внесения изменений;

– попытки записи в системные файлы;

– самопроизвольные модификация или удаление данных;

– отказ в обслуживании (отсутствие доступа к программным и техническим средствам);

– необъяснимо низкая производительность системы (слишком долгое время отклика системы);

– аномалии поведения системы (например, появление сообщений на экране, частые и необъяснимые звуковые сигналы);

– подозрительные пробы (например, многочисленные неудачные попытки входа с другого узла сети);

– неконтролируемое внесение изменений в систему, ее настройки и параметры;

– неправильное срабатывание программного или аппаратного обеспечения;

– нарушения доступа (отказ в доступе в систему);

– другие нетипичные события.

4.4 Все сотрудники администрации, лица, выполняющие работы и оказывающие услуги на договорной основе, и имеющие доступ к администрации должны быть ознакомлены с процедурой информирования о выявленных инцидентах ИБ и иных нетипичных событиях.

4.5 Ответственные за выявление и реагирование на инциденты проводят сбор информации, связанной с событием, о котором поступило сообщение, для подтверждения и локализации инцидента ИБ.

5. Реагирование на инциденты информационной безопасности

5.1 В случае наличия признаков инцидента в полученной информации ответственные за выявление и реагирование на инциденты определяют предварительную степень важности инцидента, проводят первоочередные меры, направленные на локализацию инцидента ИБ, препятствующие его распространению (в том числе ограничение доступа к объектам, задействованным в инциденте ИБ) и минимизацию его последствий, принимает решение о необходимости проведения расследования.

5.2 Для реагирования на инциденты ответственный за выявление и реагирование на инциденты может привлекать по необходимости внешних экспертов. Необходимость привлечения тех или иных специалистов определяется в зависимости от вида инцидента.

5.3 Сотрудники администрации могут привлекаться к реагированию на инциденты ИБ по согласованию с заместителем главы администрации.

5.4 После локализации инцидента необходимо приступить к ликвидации последствий и восстановлению системы (приведению системы к штатному режиму функционирования), проводится расследование и анализ произошедшего инцидента.

5.5 В ходе анализа инцидента по возможности выявляются следующие показатели:

– факт или потенциальная возможность реализации угрозы безопасности защищаемой информации (далее – угрозы);

– опасность угрозы;

– область, перечень информационных ресурсов, затрагиваемых воздействием угрозы;

– потенциальные нарушители, цели и причины реализации угрозы;

– перечень мер по локализации и остановке распространения действия угрозы.

6. Анализ причин и оценка результата

6.1 Расследование инцидента ИБ проводится с целью раскрытия причинно-следственных связей и получения следующей информации:

– источники инцидента ИБ (нарушители);
– цели инцидента ИБ;
– способы осуществления инцидента ИБ.

6.2 По результатам проведенного расследования инцидента ответственные за выявление и реагирование на инциденты проводят:

– переоценку рисков, повлекших возникновение инцидента ИБ;
– анализ перечня защитных мер для минимизации выявленных рисков в случае повторения инцидента ИБ;
– анализ инструкций и правил обеспечения информационной безопасности, включая настоящий документ;
– инструктаж (информирование об угрозах безопасности информации, правилах эксплуатации системы защиты информации ИС и отдельных средств защиты информации) сотрудников администрации для повышения их осведомленности в части информационной безопасности.

Приложение № 11
к постановлению от _____ № _____

ПОЛОЖЕНИЕ
по управлению конфигурацией информационных систем администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящее Положение определяет порядок управления конфигурацией информационных систем (далее – ИС) администрации Баганского района Новосибирской области(далее – администрация, оператор) и их системы защиты информации.

2. Порядок управления конфигурацией информационных систем и системы защиты информации

2.1 Действия по внесению изменений в конфигурацию ИС администрации и их системы защиты информации разрешены уполномоченным сотрудникам администрации, а также представителям сторонних организаций, оказывающих услуги гарантийного и (или) технического обслуживания программных и программно-аппаратных средств, включая средства защиты информации, ИС администрации в пределах полномочий согласно

заключенным договорам, соглашениям, контрактам.

2.2 Управление конфигурацией ИС администрации осуществляется на основе согласованных решений уполномоченных лиц, указанных в п. 2.1 настоящего Положения, и включает:

– разработку параметров настройки, обеспечивающих защиту информации;

– анализ потенциального воздействия планируемых изменений на обеспечение защиты информации (возникновение дополнительных угроз безопасности информации и работоспособность ИС);

– санкционирование внесения изменений в ИС и их системы защиты информации;

– документирование действий по внесению изменений в ИС и их системы защиты информации и сохранение данных об изменениях конфигурации.

2.3 Объектами управления конфигурацией (компонентами ИС администрации и их системы защиты информации, подлежащих изменению в рамках управления конфигурацией) определены программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю.

2.4 Внесение изменений в ИС администрации и их системы защиты информации в отношении объектов управления конфигурацией может осуществляться в рамках гарантийного и (или) технического обслуживания (в том числе дистанционно (удаленно)), программных и программно-аппаратных средств, включая средства защиты информации, ИС администрации.

2.5 Документирование (внесение информации (данных)) об изменениях в конфигурации ИС администрации и их систем защиты информации (структуры системы защиты информации ИС, состава, мест установки и параметров настройки средств защиты информации,

программного обеспечения и технических средств) в эксплуатационную документацию на систему защиты информации ИС осуществляет ответственный за защиту информации.

Приложение № 12
к постановлению от _____ № _____

ПОЛОЖЕНИЕ
по защите информации в администрации Баганского района Новосибирской области при выводе из эксплуатации информационных систем или после принятия решения об окончании обработки информации ограниченного доступа

1. Общие положения

1.1 Настоящее Положение разработано в целях обеспечения защиты информации при выводе из эксплуатации информационных систем (далее – ИС) администрации Баганского района Новосибирской области (далее – администрация, оператор).

1.2 Меры по обеспечению защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации обеспечиваются путем выполнения требований к порядку вывода ИС из эксплуатации и дальнейшему хранению содержащихся в ее базах данных информации.

2. Требования к порядку вывода ИС из эксплуатации и дальнейшего хранения содержащейся в ее базах данных информации

2.1 Основанием для вывода ИС из эксплуатации являются:

– завершение срока эксплуатации ИС, в случае если такой срок был установлен правовым актом о вводе ИС в эксплуатацию;

– нецелесообразность эксплуатации ИС, в том числе низкая эффективность используемых технических средств и программного обеспечения, изменение правового регулирования, принятие управленческих решений, а также наличие иных изменений, препятствующих эксплуатации ИС;

– финансово-экономическая неэффективность эксплуатации ИС.

2.2 При наличии одного или нескольких оснований для вывода системы из эксплуатации, указанных в пункте 2.1 настоящего Положения, оператор утверждает правовой акт о выводе системы из эксплуатации.

2.3 Правовой акт о выводе ИС из эксплуатации включает:

– основание для вывода ИС из эксплуатации;

– перечень и сроки реализации мероприятий по выводу ИС из эксплуатации;

– порядок, сроки, режим хранения и дальнейшего использования информационных ресурсов, включая порядок обеспечения доступа к информационным ресурсам выводимой из эксплуатации ИС и обеспечения защиты информации, содержащейся в выводимой из эксплуатации ИС;

– порядок, сроки и способы информирования пользователей о выводе ИС из эксплуатации.

2.4 Перечень мероприятий по выводу ИС из эксплуатации включает:

– подготовку правовых актов, связанных с выводом ИС из эксплуатации;

– работы по выводу ИС из эксплуатации, в том числе работы по деинсталляции программного обеспечения ИС, по реализации прав на

программное обеспечение ИС, демонтажу и списанию технических средств ИС, обеспечению хранения и дальнейшего использования информационных ресурсов ИС;

– обеспечение защиты информации в соответствии с документацией на ИС и организационно-распорядительными документами по защите информации, в том числе архивирование информации, содержащейся в ИС, уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

2.5 Если нормативными правовыми актами Российской Федерации не установлено иное, то сроки хранения информации, содержащейся в базах данных системы, определяются оператором и не могут быть меньше сроков хранения информации, которые установлены для хранения документов в бумажном виде, содержащих такую информацию.

2.6 Срок вывода ИС из эксплуатации не может быть ранее срока окончания последнего мероприятия, предусмотренного правовым актом о выводе ИС из эксплуатации.

3. Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации

3.1 Обеспечение защиты информации при выводе из эксплуатации ИС или после принятия решения об окончании обработки информации, содержащейся в ИС, осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации ИС и организационно-распорядительными документами по защите информации и в том числе включает:

– архивирование информации, содержащейся в ИС;

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

3.2 Архивирование информации, содержащейся в ИС администрации], должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора и осуществляется в соответствии с требованиями законодательства об архивном деле в Российской Федерации.

3.3 Архивирование информации, содержащейся в ИС администрации, обеспечивается уполномоченными сотрудниками администрации.

3.4 Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИС 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.

3.5 Процедуры уничтожения (стирания) информации, хранящейся на машинных носителях информации, а также физическое уничтожение машинных носителей информации производится ответственным за защиту информации, содержащейся ИС администрации.

Лист ознакомления

с постановлением от _____ № _____

«О реализации мер защиты информации ограниченного доступа, обрабатываемой в информационных системах администрации Баганского района Новосибирской области»

№ п/п	ФИО	Дата ознакомления	Подпись

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

29.08.2024 № 785

Об организации работы со средствами криптографической защиты информации в администрации Баганского района

В целях обеспечения организации учета, хранения и эксплуатации средств криптографической защиты информации (далее также – СКЗИ), применяемых в администрации Баганского района Новосибирской области (далее также – администрация), администрация Баганского района Новосибирской области

ПОСТАНАВЛЯЕТ:

8. Назначить ответственным за эксплуатацию средств криптографической защиты информации в администрации Баганского района Новосибирской области Удалова Андрея Анатольевича, инженера 1 категории МКУ «Центра бухгалтерского, информационного обеспечения муниципальных закупок Баганского района».

9. Утвердить Инструкцию ответственного за эксплуатацию средств криптографической защиты информации в администрации Баганского района Новосибирской области согласно приложению № 1.

10. Утвердить Инструкцию пользователя средств криптографической защиты информации в администрации Баганского района Новосибирской области, согласно приложению № 2.

11. Утвердить типовую форму Перечня лиц, допущенных к работе со средствами криптографической защиты информации в администрации Баганского района Новосибирской области, согласно приложению № 3.

12. Утвердить Правила эксплуатации средств криптографической защиты информации в администрации Баганского района Новосибирской области согласно приложению № 4.

13. Утвердить типовую форму Перечня лиц, имеющих доступ в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, согласно приложению № 5.

14. Утвердить Порядок доступа в помещения, в которых ведется обработка персональных данных и размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях, согласно приложению № 6.

15. Начальнику отдела строительства и дорожного комплекса, Колобовой Е.В. ознакомить работников администрации с настоящим постановлением.

9. Опубликовать настоящее постановление на официальном сайте органов местного самоуправления Баганского района Новосибирской области и в периодическом печатном издании органов местного самоуправления «Бюллетень органов местного самоуправления Баганского района».

10. Данное постановление вступает в силу после его публикации в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области».

10. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации Баганского района Бреус Анастасию Олеговну.

Глава Баганского района
Новосибирской области А.А. Воличенко

ПРИЛОЖЕНИЕ №1
к постановлению администрации
Баганского района
Новосибирской области
от 29.08.2024 № 785

ИНСТРУКЦИЯ
ответственного за эксплуатацию средств криптографической защиты информации в администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящая Инструкция определяет основные права и обязанности ответственного за эксплуатацию средств криптографической защиты информации (далее также – СКЗИ, криптосредства), применяемых в администрации Баганского района Новосибирской области (далее – администрация).

1.2 Ответственный за эксплуатацию СКЗИ назначается постановлением Главы администрации Баганского района Новосибирской области из числа работников администрации.

1.3 Ответственный за эксплуатацию СКЗИ получает указания от Главы администрации или иного уполномоченного лица и подотчетно ему.

1.4 Ответственный за эксплуатацию СКЗИ в своей деятельности руководствуется действующими нормативными правовыми актами в сфере (области) применения шифровальных (криптографических) средств, эксплуатационной и технической документации на СКЗИ, локальными актами администрации по вопросам эксплуатации СКЗИ и настоящей Инструкцией.

1.5 Ответственный за эксплуатацию СКЗИ отвечает за организацию, обеспечение функционирования и безопасности СКЗИ, применяемых в администрации Баганского района Новосибирской области.

2. Обязанности ответственного за эксплуатацию СКЗИ

2.1 Ответственный за эксплуатацию СКЗИ обязан:

2.1.1 Соблюдать требования локальных актов администрации Баганского района Новосибирской области по вопросам эксплуатации СКЗИ, а также актов администрации Баганского района Новосибирской области, устанавливающих порядок обработки и обеспечения безопасности защищаемой информации.

2.1.2 Знать и обеспечивать реализацию норм действующего законодательства Российской Федерации в сфере (области) применения шифровальных (криптографических) средств, в том числе обработки и обеспечения безопасности защищаемой информации с использованием СКЗИ.

2.1.3 Обеспечивать исполнение принятых администрации Баганского района Новосибирской области обязательств в соответствии с заключенными соглашениями, касающимися обеспечения функционирования и порядка эксплуатации СКЗИ.

2.1.4 Контролировать соблюдение условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним.

2.1.5 Обеспечивать поддержание в актуальном состоянии локальных актов администрации по вопросам эксплуатации СКЗИ, Перечень лиц, допущенных к работе с СКЗИ в администрации, и лиц, имеющих доступ в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

2.1.6 Обеспечивать надежное хранение эксплуатационной и технической документации к СКЗИ, ключевых документов.

2.1.7 Осуществлять ведение Журнала учёта хранилищ СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

2.1.8 Вести поэкземплярный учет используемых в администрации СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета СКЗИ).

2.1.9 Обеспечивать пломбирование (опечатывание) и контролировать сохранность печатей (пломб) на аппаратных средствах, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ;

2.1.10 Организовывать установку, настройку, ввод в эксплуатацию и вывод из эксплуатации СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ.

2.1.11 Контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ, или, если срок уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) и фиксировать факт уничтожения/вывода из эксплуатации в Журнале учета СКЗИ.

2.1.12 Организовывать обучение и проводить инструктаж пользователей СКЗИ по правилам работы с СКЗИ.

2.1.13 Контролировать оформление и при необходимости оформлять Заключение о допуске пользователя СКЗИ к самостоятельной работе.

2.1.14 Контролировать исполнение пользователями СКЗИ требований Инструкции пользователя СКЗИ администрации Баганского района Новосибирской области, а также требований действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности защищаемой информации в пределах своей компетенции.

2.1.15 Соблюдать требования к обеспечению безопасности информации, обрабатываемой в администрации, безопасности СКЗИ и ключевых документов к ним.

2.1.16 Не разглашать информацию, к которой он допущен, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты.

2.1.17 Инициировать проведение проверок по фактам ставших известными попыток посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним, о фактах утраты или недостачи СКЗИ, ключевых документов к ним, личных печатей, ключей от хранилищ (сейфов, металлических шкафов, ящиков индивидуального пользования), помещений, в которых размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, и о других фактах, которые свидетельствуют о возможной компрометации криптографических ключей и могут привести к нарушению конфиденциальности информации ограниченного доступа, при необходимости в случае подтверждения факта компрометации криптографических ключей обеспечивать информирование всех заинтересованных участников информационного обмена о факте компрометации ключевой информации.

2.1.18 Обеспечить выведение из действия криптоключей, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ.

2.1.19 Осуществлять координацию и контроль действий пользователей СКЗИ по восстановлению скомпрометированных криптоключей.

2.1.20 Организовывать проведение служебных расследований по фактам компрометации криптоключей, а также в целях выявления причин нарушения требований безопасности функционирования СКЗИ.

2.1.21 Обобщать результаты всех видов контроля за организацией и обеспечением порядка использования СКЗИ в [краткое_наименование_ОИОГВ.предложный], анализировать причины выявленных нарушений, разрабатывать меры по их профилактике и предотвращению возможных негативных последствий подобных нарушений, контролировать выполнение рекомендаций, содержащихся в актах проверок контролирующих организаций.

2.1.22 Сдать своему непосредственному руководителю СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы, личную печать, ключи от хранилищ и помещений, в которые допущен ответственный за эксплуатацию СКЗИ, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

3. Права ответственного за эксплуатацию СКЗИ

3.1 Ответственный за эксплуатацию СКЗИ имеет право:

3.1.1 Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения возложенных на него обязанностей.

3.1.2 Получать доступ к информации, материалам, техническим средствам, и помещениям, необходимый для надлежащего исполнения своих прав и обязанностей.

3.1.3 Проходить обучение (переподготовку) по вопросам, связанным с исполнением возложенных на него обязанностей в области обеспечения учета, хранения и эксплуатации СКЗИ и защиты информации, обрабатываемой в информационных системах администрации, с использованием СКЗИ.

3.1.4 Требовать от сотрудников администрации соблюдения требований законодательства Российской Федерации, локальных актов администрации в области применения шифровальных (криптографических) средств, в том числе обработки и обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием СКЗИ.

3.1.5 Проводить и (или) организовывать проверки соблюдения в администрации условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ.

3.1.6 Инициировать проведение и принимать участие в служебных расследованиях по фактам нарушения сотрудниками администрации установленных правил эксплуатации СКЗИ.

3.1.7 Требовать прекращения сотрудниками администрации] обработки информации с использованием СКЗИ в случае установления фактов нарушения правил эксплуатации СКЗИ или нарушения функционирования СКЗИ.

3.1.8 Привлекать в случае необходимости при проведении служебных расследований сотрудников, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы.

3.1.9 Вносить предложения по вопросам использования СКЗИ, устранению выявленных нарушений правил эксплуатации СКЗИ и предупреждению подобного рода нарушений.

4. Ответственность

4.2 Ответственный за эксплуатацию СКЗИ несет предусмотренную законодательством Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

– неисполнение либо ненадлежащее исполнение своих должностных обязанностей;

– нарушения в работе информационных систем администрации, вызванные его неправомерными действиями или неправильным использованием предоставленных прав;

– нарушение законодательства Российской Федерации, локальных актов администрации, устанавливающих порядок работы с СКЗИ;

– превышение должностных полномочий и злоупотребление ими;

– применение к администрации штрафных санкций по вине ответственного за эксплуатацию СКЗИ;

– совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.

ПРИЛОЖЕНИЕ №2
к постановлению администрации
Баганского района

Новосибирской области

ИНСТРУКЦИЯ
пользователя средств криптографической защиты информации в администрации Баганского района Новосибирской области

1. Общие положения

1.1. Настоящая Инструкция пользователя средств криптографической защиты информации администрации Баганского района Новосибирской области(далее – Инструкция) определяет права и обязанности пользователей средств криптографической защиты информации (далее – СКЗИ).

1.2. Пользователями СКЗИ являются работники (сотрудники) администрации Баганского района Новосибирской области (далее – администрации), включенные в Перечень лиц, допущенных к работе с СКЗИ в администрации, утвержденный локальным актом администрации.

1.3. Для допуска к работе с СКЗИ пользователь знакомится с нормативными правовыми актами в сфере (области) применения шифровальных (криптографических) средств, локальными актами администрации по вопросам эксплуатации СКЗИ, настоящей Инструкцией и проходит обучение правилам работы с СКЗИ.

1.4. Пользователь считается допущенным к СКЗИ после оформления Заключения о допуске пользователя СКЗИ к самостоятельной работе.

1.5. Инструктаж по правилам работы с СКЗИ и оформление Заключения о допуске пользователя СКЗИ к самостоятельной работе осуществляют уполномоченные сотрудники организаций, осуществляющих ввод в эксплуатацию СКЗИ или ответственный за эксплуатацию СКЗИ в администрации.

1.6. Пользователи СКЗИ несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту СКЗИ от несанкционированного использования, а также за сохранность полученных под расписку в соответствующем журнале СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

2. Обязанности и права пользователя СКЗИ

2.1. Пользователь СКЗИ обязан:

– соблюдать требования по обеспечению безопасности функционирования СКЗИ;

– обеспечить конфиденциальность информации ограниченного распространения, доступной ему по роду выполняемых функциональных обязанностей, в том числе сведений о криптоключах;

– обеспечить хранение ключевых документов, эксплуатационной и технической документации, дистрибутивов СКЗИ, опечатываемых тубусов (пеналов) в надежно запираемых шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение;

– сообщать ответственному за эксплуатацию СКЗИ о ставших известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, сдать ответственному за эксплуатацию СКЗИ в администрации, а при его отсутствии руководителю соответствующего структурного подразделения СКЗИ,

эксплуатационную и техническую документацию к ним, ключевые документы, ключевые носители, личные печати;

– сдать имеющиеся у него ключи от замков хранилищ ответственному за эксплуатацию СКЗИ, а при его отсутствии руководителю соответствующего структурного подразделения при увольнении, либо при назначении другого лица ответственным за хранилище;

– сдать имеющиеся у него ключи от помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения) ответственному за эксплуатацию СКЗИ, а при его отсутствии руководителю соответствующего структурного подразделения при увольнении или переводе в иное структурное подразделение;

– немедленно уведомлять своего непосредственного руководителя и ответственного за эксплуатацию СКЗИ о компрометации криптоключей, фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от Помещений, хранилищ, личных печатей, удостоверений, пропусков и о других фактах, которые могут привести к разглашению защищаемой информации, а также о причинах и условиях возможной утечки таких сведений;

– незамедлительно прекратить применение скомпрометированных криптоключей (обмен электронными документами/формирование электронной подписи и пр.) и обеспечить вывод из действия криптоключей, в отношении которых возникло подозрение в компрометации, а также действующих совместно с ними других криптоключей;

– немедленно прекратить работу с СКЗИ в случае обнаружения на рабочей станции посторонних программ (в том числе вредоносного программного обеспечения), о произошедшем известить ответственного за эксплуатацию СКЗИ и ответственного за защиту информации в администрации;

– в пределах своей компетенции предоставлять по требованию ответственного за эксплуатацию СКЗИ информацию, необходимую при проведении служебных расследований по фактам компрометации криптоключей, а также в целях выявления причин нарушения требований безопасности функционирования СКЗИ.

2.2. Пользователю СКЗИ запрещается:

– осуществлять несанкционированное и безучётное копирование ключевой информации;

– хранить ключевые носители вне хранилищ и помещений, гарантирующих их сохранность и конфиденциальность ключевой информации;

– передавать ключевые носители лицам, к ним не допущенным;

– во время работы оставлять ключевые носители без присмотра (например, на рабочем столе или в разъеме системного блока персонального компьютера);

– выводить ключевую информацию на печать, дисплей монитора или иное средство визуализации данных;

– записывать на ключевые носители постороннюю информацию;

– вносить какие-либо изменения в программное обеспечение СКЗИ;

– устанавливать и эксплуатировать стороннее программное обеспечение, которое может нарушить функционирование СКЗИ.

– использовать бывшие ранее в работе ключевые носители для записи новой ключевой информации без предварительного гарантированного уничтожения ранее хранящейся на них информации;

– использовать ключевые носители, выведенные из действия;

– передавать кому-либо ключи от хранилищ и Помещений, а также личные печати кроме как в случаях, предусмотренных настоящей Инструкцией.

2.3. Пользователь СКЗИ имеет право:

– знакомиться с локальными актами администрации, регламентирующими процессы обработки и обеспечения безопасности защищаемой информации;

– требовать от своего непосредственного руководителя обеспечения организационно-

технических условий, необходимых для исполнения возложенных на него обязанностей;

– получать доступ к информации, материалам, техническим средствам, и в помещения, необходимый для надлежащего исполнения своих прав и обязанностей;

– проходить обучение по вопросам, связанным с исполнением возложенных на него обязанностей в области эксплуатации СКЗИ;

– уничтожать использованные непосредственно им (предназначенные для него) ключевые документы с обязательным уведомлением ответственного за эксплуатацию СКЗИ, если иное не предусмотрено эксплуатационной и технической документацией на СКЗИ, договорами или соглашениями, заключенными с организациями, осуществлявшими ввод в эксплуатацию СКЗИ;

– вносить предложения Главы администрации по вопросам использования СКЗИ, по устранению выявленных нарушений правил эксплуатации СКЗИ и предупреждению подобного рода нарушений.

3. Ответственность

3.1. Пользователь СКЗИ несет предусмотренную законодательством Российской Федерации в соответствии с возложенными на него обязанностями ответственность за:

– неисполнение либо ненадлежащее исполнение возложенных на него обязанностей;

– превышение, злоупотребление или неправильное использование предоставленных полномочий, предусмотренных настоящей Инструкцией;

– нарушение законодательства Российской Федерации, локальных актов администрации, устанавливающих порядок работы с СКЗИ;

– применение к администрации штрафных санкций по вине пользователя СКЗИ;

– совершение противоправных действий (уничтожение, изменение, блокирование, копирование, предоставление, распространение, а также иных неправомерных действий) в отношении информации, к которой он допущен в рамках выполнения своих должностных (функциональных) обязанностей.

Приложение № 3

к приказу от _____ № _____

ТИПОВАЯ ФОРМА

Перечень лиц, допущенных к работе со средствами криптографической защиты информации в администрации Баганского района Новосибирской области

№ п/п	ФИО работника	Должность	Структурное подразделение
1.			
2.			
3.			

Приложение № 4
к приказу от _____ № _____

ПРАВИЛА
эксплуатации средств криптографической защиты информации в администрации Баганского района Новосибирской области

1. Общие положения

1.1 Настоящие Правила эксплуатации средств криптографической защиты информации в администрации Баганского района Новосибирской области (далее – администрации) определяют порядок учета, хранения, использования, ввода в эксплуатацию, вывода из эксплуатации и уничтожения средств криптографической защиты информации (далее также – СКЗИ, криптосредства), а также порядок действий сотрудников администрации при компрометации криптографических ключей в целях обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, с использованием СКЗИ.

1.2 В настоящих Правилах применяются следующие термины и определения:

– информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

– электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

– криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе;

– закрытый ключ – криптоключ, который хранится пользователем системы в тайне;

– ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

– исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

– ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию;

– ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации);

– компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам;

– ответственный за эксплуатацию СКЗИ – сотрудник, осуществляющий организацию учета, хранения и эксплуатации СКЗИ, в том числе обеспечения работ по техническому обслуживанию СКЗИ и управлению криптографическими ключами;

– пользователи СКЗИ – сотрудники администрации, непосредственно допущенные к работе с СКЗИ;

– контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств, границей контролируемой зоны может быть: периметр охраняемой территории, ограждающие конструкции охраняемого здания, охраняемой части здания;

– спецпомещения – помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

1.3 К криптографическим (шифровальным) средствам защиты информации, включая документацию на эти средства, относятся:

– средства шифрования – аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче;

– средства имитозащиты – аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства (за исключением средств шифрования), реализующие алгоритмы криптографического преобразования информации для ее защиты от навязывания ложной информации, в том числе защиты от модифицирования, для обеспечения ее достоверности и некорректируемости, а также обеспечения возможности выявления изменений, имитации, фальсификации или модифицирования информации;

– средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций, создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи;

– средства кодирования – средства шифрования, в которых часть криптографических преобразований информации осуществляется с использованием ручных операций или с использованием автоматизированных средств, предназначенных для выполнения таких операций;

– средства изготовления ключевых документов – аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;

– ключевые документы – электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах;

– аппаратные шифровальные (криптографические) средства – устройства и их компоненты, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации без использования программ для электронных вычислительных машин;

– программные шифровальные (криптографические) средства – программы для электронных вычислительных машин и их части, в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации в программно-аппаратных шифровальных (криптографических) средствах, информационных системах и телекоммуникационных системах, защищенных с использованием шифровальных (криптографических) средств;

– программно-аппаратные шифровальные (криптографические) средства – устройства и их компоненты (за исключением информационных систем и телекоммуникационных систем), в том числе содержащие ключевую информацию, обеспечивающие возможность преобразования информации в соответствии с алгоритмами криптографического преобразования информации с использованием программ для электронных вычислительных машин, предназначенных для осуществления этих преобразований информации или их части.

1.4 Настоящие Правила в своем составе, терминах и определениях основываются на положениях следующих нормативных правовых актов:

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

– Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

– Приказ ФСБ России от 10.07.2014 № 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» (далее – Приказ ФСБ России от 10.07.2014 № 378);

– Приказ ФАПСИ от 13.06.2001 № 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»;

– иные нормативные правовые акты и методические документы по эксплуатации шифровальных (криптографических) средств.

1.5 В администрации должны использоваться только СКЗИ, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации и имеющие сертификат ФСБ России.

1.6 Класс СКЗИ определяется в соответствии с Приказом ФСБ России от 10.07.2014 № 378, а также иными нормативными правовыми актами по эксплуатации шифровальных (криптографических) средств.

1.7 Для организации и обеспечения работ по учету, хранению и эксплуатации СКЗИ приказом назначается ответственный за эксплуатацию СКЗИ.

2. Порядок допуска пользователей к работе с СКЗИ

2.1 При установке СКЗИ ответственным за эксплуатацию СКЗИ оформляется Акт ввода СКЗИ в эксплуатацию по форме согласно Приложению № 1 к настоящим Правилам.

2.2 Для работы с СКЗИ допускаются сотрудники администрации, включенные в Перечень лиц, допущенных к работе со средствами криптографической защиты информации.

2.3 Перечень лиц, допущенных к работе со средствами криптографической защиты информации, утверждается постановлением Главы администрации

2.4 Для допуска к работе с СКЗИ пользователь знакомится с нормативными правовыми актами по эксплуатации СКЗИ, локальными актами администрации по вопросам эксплуатации СКЗИ, данными Правилами и проходит инструктаж по правилам работы с СКЗИ.

2.5 Инструктаж по правилам работы с СКЗИ и оформление Заключения о допуске пользователя СКЗИ к самостоятельной работе осуществляют ответственный за эксплуатацию СКЗИ или уполномоченные сотрудники организаций, осуществляющих поставку и ввод в эксплуатацию средств криптографической защиты.

2.6 Пользователь считается допущенным к СКЗИ после оформления Заключения о допуске пользователя СКЗИ к самостоятельной работе по форме согласно Приложению № 2 к настоящим Правилам.

3. Учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

3.1.Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в соответствующем Журнале по форме согласно Приложению № 3 к настоящим Правилам.

3.2.Поэкземплярный учет СКЗИ ведет ответственный за эксплуатацию СКЗИ в журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета СКЗИ). При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатная эксплуатация. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также

совместно с соответствующими аппаратными средствами.

3.3.Единицей поэкземплярного учета криптографических ключей считается отчуждаемый ключевой носитель многократного использования. Если один и тот же ключевой носитель многократно используют для записи криптографических ключей, то его каждый раз следует регистрировать отдельно.

3.4.Все экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов выдаются пользователям СКЗИ под расписку в Журнале учета СКЗИ.

3.5.Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ под роспись в соответствующем Журнале поэкземплярного учета СКЗИ. Такая передача между пользователями СКЗИ осуществляется с разрешения Ответственного за эксплуатацию СКЗИ. Пользователи СКЗИ несут персональную ответственность за сохранность СКЗИ.

4. Хранение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

4.1 Дистрибутивы СКЗИ, ключевые документы, эксплуатационная и техническая документация к СКЗИ хранятся у ответственного за эксплуатацию СКЗИ, если иное не предусмотрено производственной необходимостью.

4.2 Хранение выданных пользователям СКЗИ ключевых документов, эксплуатационной и технической документации, дистрибутивов СКЗИ должно осуществляться в надежно запираемых шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

4.3 Ключевые носители могут храниться в тубусах (пеналах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним.

4.4 Замочные скважины вышеуказанных хранилищ, а также тубусы (пеналы) для хранения ключевых носителей должны быть оборудованы приспособлениями для опечатывания. Печати, предназначенные для опечатывания хранилищ и тубусов (пеналов), должны находиться у ответственных за эти хранилища, тубусы (пеналы).

4.5 Учет хранилищ СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведет ответственный за эксплуатацию СКЗИ в журнале учета хранилищ СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал учета хранилищ).

4.6 Порядок учета ключей для доступа к хранилищам:

– один экземпляр ключа от хранилища должен находиться у ответственного за эксплуатацию СКЗИ, другой – у ответственного за хранилище;

– дубликаты ключей хранилищ, переданные ответственному за эксплуатацию СКЗИ, хранятся в сейфе;

– количество комплектов ключей и их номера от спецпомещений и от хранилищ указываются в соответствующем Журнале по форме согласно Приложению № 4 к настоящим Правилам;

– в Журнале учета хранилищ фиксируется факт первичной выдачи ключа от спецпомещений и хранилищ, возможна повторная выдача ключа (в случае смены замка и других обстоятельствах) и сдача ключа при увольнении сотрудника или смене должностных обязанностей (переводе в иное структурное подразделение);

– дубликаты ключей от спецпомещений хранятся у ответственных лиц в соответствии с утвержденными локальными актами администрации, регламентирующими порядок обеспечения пропускного и внутриобъектового режимов;

– при увольнении, либо при назначении иного лица ответственным за хранилище, сотрудник обязан сдать имеющиеся у него ключи от механического замка хранилища ответственному за эксплуатацию СКЗИ;

– при увольнении или переводе в иное структурное подразделение пользователь СКЗИ обязан сдать имеющиеся у него ключи от спецпомещений своему непосредственному руководителю;

– пользователям СКЗИ запрещено передавать кому-либо ключи от хранилищ и спецпомещений кроме как в случаях, предусмотренных настоящими Правилами.

– Тубусы (пеналы), предназначенные для хранения ключевых носителей, подлежат учету в Журнале учета хранилищ.

4.7 Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. Опечатывание производит ответственный за эксплуатацию СКЗИ либо лицо, проводившее ввод в эксплуатацию СКЗИ. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

4.8 Вскрытие аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ, оборудованных средствами контроля за их вскрытием, для проведения ремонта и (или) технического обслуживания должно осуществляться в присутствии ответственного за эксплуатацию СКЗИ.

4.9 При необходимости передачи аппаратных средств, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ в сторонние организации для проведения ремонтно-восстановительных или иных работ, осуществляется предусмотренная эксплуатационной и технической документацией к СКЗИ процедура изъятия (удаления программного обеспечения) СКЗИ из аппаратных средств, с которыми они функционировали, и уничтожение криптоключей (исходной ключевой информации), хранящейся в аппаратных СКЗИ.

5. Мероприятия при компрометации криптоключей

5.1 К обстоятельствам, указывающим на возможную компрометацию криптографических ключей, относятся следующие:

– утрата (хищение) ключевых носителей с криптографическими ключами, в том числе с последующим их обнаружением;

– возникновение подозрений относительно утечки информации или ее искажения (подмены, подделки);

– нарушение целостности печатей на хранилищах СКЗИ и ключевых документов (при использовании процедуры опечатывания хранилищ);

– утрата ключей от хранилищ СКЗИ и ключевых документов (при нахождении в них ключевых носителей);

– нарушение правил хранения криптографических ключей;

– ошибки при нарушении криптографических операций (например, отрицательный результат по результатам проверки электронной подписи);

– несанкционированное и безучетное копирование ключевой информации;

– передача секретных ключей по линиям связи в открытом виде;

– временный доступ посторонних лиц к ключевым носителям, а также другие события, при которых достоверно не известно, что произошло с ключевыми носителями.

5.2 О нарушениях, которые могут привести к компрометации криптоключей или передававшейся (хранящейся) с их использованием информации, пользователи СКЗИ обязаны сообщать ответственному за эксплуатацию СКЗИ. В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

5.3 В случае возникновения обстоятельств, указанных в п. 6.1 настоящих Правил, пользователь СКЗИ обязан незамедлительно прекратить применение скомпрометированных криптоключей (обмен электронными документами/формирование электронной подписи и пр.) и информировать о факте возможной компрометации используемых криптоключей ответственного за эксплуатацию СКЗИ.

5.4 Решение о компрометации криптографических ключей принимает ответственный за эксплуатацию СКЗИ.

5.5 Криптоключи, которые были скомпрометированы или в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи подлежат выводу из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. Проведение мероприятий по выводу из действия криптоключей/отзыву сертификата ключа электронной подписи пользователя СКЗИ обеспечивается ответственным за эксплуатацию СКЗИ.

5.6 Сертификат скомпрометированного ключа электронной подписи, подлежит хранению ответственным за эксплуатацию СКЗИ в течение срока хранения электронных документов для проведения (в случае необходимости) расследований, связанных с применением электронной подписи.

6. Порядок вывода из действия и уничтожения СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, криптоключей (исходной ключевой информации) и ключевых носителей

6.1 Неиспользуемые или выведенные из действия криптоключи и ключевые документы подлежат уничтожению.

6.2 Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

6.3 Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (компакт-дисков, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

6.4 Ключевые носители многократного использования после стирания (разрушения) хранимых на них криптоключей (исходной ключевой информации) подлежат возврату в орган криптографической защиты (иную организацию, предоставившую СКЗИ во временное пользование на основании заключенного договора, контракта или соглашения и (или) осуществлявшую ввод в эксплуатацию СКЗИ) либо по их указанию могут быть уничтожены на месте.

6.5 Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

6.6 Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

6.7 Ключевые документы должны быть уничтожены в порядке и в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения отражается в Журнале учета СКЗИ.

6.8 Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ, и они полностью отсоединены от аппаратных средств.

6.9 Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

6.10 Вывод из эксплуатации СКЗИ осуществляется ответственным за эксплуатацию СКЗИ. По результатам уничтожения СКЗИ оформляется Акт вывода из эксплуатации СКЗИ по форме согласно Приложению № 5 к настоящим Правилам и (или) Акт уничтожения криптографических ключей, содержащихся на ключевых носителях, и ключевых документов оформляется Акт об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов по форме согласно Приложению № 6 к настоящим Правилам.

6.11 Вывод из эксплуатации иных СКЗИ осуществляется в порядке согласно заключенным договорам, контрактам или соглашениям, а также в соответствии с указаниями организаций, осуществлявших ввод в эксплуатацию средств криптографической защиты информации.

6.12 После уничтожения СКЗИ, ключевых документов и/или ключевых носителей, а также вывода из эксплуатации СКЗИ ответственный за эксплуатацию СКЗИ вносит необходимые отметки в Журнал учета СКЗИ.

7. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним

7.1 Размещение, специальное оборудование, охрана и организация режима в спецпомещениях, должны обеспечивать сохранность СКЗИ и носителей ключевой, аутентифицирующей и парольной информации СКЗИ, а также исключать возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц и просмотра ведущихся там работ.

7.2 Обеспечение безопасности используемых СКЗИ, хранящихся СКЗИ и (или) носителей ключевой, аутентифицирующей и парольной информации СКЗИ от уничтожения, изменения, копирования, а также от иных неправомерных действий достигается в том числе установлением правил доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ.

7.3 При оборудовании спецпомещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

7.4 Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

7.5 Техническое обслуживание оборудования, функционирующего с СКЗИ, и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае пользователи СКЗИ по согласованию с ответственным за эксплуатацию СКЗИ обязаны предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

7.6 Для предотвращения просмотра защищаемой информации извне спецпомещений окна должны быть защищены шторами, либо жалюзи или с использованием иных средств/методов.

7.7 В спецпомещениях для хранения ключевых документов, эксплуатационной и технической документации, носителей дистрибутивов СКЗИ необходимо иметь достаточное число надежно запираемых хранилищ (в том числе индивидуального пользования), оборудованных приспособлениями для опечатывания. Ключи от этих хранилищ подлежат учету и хранению в порядке согласно настоящим Правилам.

7.8 В обычных условиях опечатанные хранилища могут быть вскрыты только самими ответственными за хранилища, указанным в Журнале учета хранилищ.

7.9 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в хранилища или спецпомещения посторонних лиц, или в случае утраты ключа от хранилища и спецпомещения о случившемся должно быть немедленно сообщено Главе Баганского района или иному уполномоченному лицу и ответственному за эксплуатацию СКЗИ. При необходимости вызываются работники правоохранительных органов и принимаются меры по охране места происшествия до их прибытия (спецпомещения не вскрываются, сотрудники администрации и посетители в спецпомещения не допускаются). По результатам анализа случившегося, необходимо дать оценку возможности компрометации хранящихся ключевых и других документов, составить Акт об обнаружении признаков, указывающих на возможное проникновение посторонних лиц в спецпомещения администрации по форме согласно Приложению № 7 к настоящим Правилам, и принять, при необходимости, меры к локализации последствий компрометации информации и к замене скомпрометированных криптоключей.

7.10 При утрате ключа от хранилища или от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок размещения СКЗИ, хранения ключевых и других документов в хранилище или спецпомещении, от которого утрачен ключ, до замены замка или изменения секрета замка устанавливает руководитель соответствующего структурного подразделения администрации по согласованию с ответственным за эксплуатацию СКЗИ, при этом должны быть обеспечены условия, исключающие бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

7.11 Установленный режим охраны спецпомещений должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящих Правил. Правила допуска сотрудников и посетителей в спецпомещения в рабочее и нерабочее время должны учитывать специфику и условия работы конкретных пользователей СКЗИ.

7.12 Двери спецпомещений должны быть постоянно закрыты и могут открываться только для санкционированного прохода пользователей СКЗИ и посетителей в сопровождении ответственных лиц.

7.13 Ключи от входных дверей спецпомещений учитывают и выдают пользователям СКЗИ под расписку в Журнале учета хранилищ.

7.14 В случае возникновения нештатной ситуации (в том числе событий чрезвычайного характера) необходимо в обязательном порядке известить о случившемся ответственного за

эксплуатацию СКЗИ и Главу Баганского района или уполномоченное лицо.

8. Контроль за соблюдением порядка использования СКЗИ

8.1 Текущий контроль за организацией и обеспечением порядка использования СКЗИ возлагается на ответственного за эксплуатацию СКЗИ в пределах его полномочий, предусмотренных Инструкцией ответственного за эксплуатацию средств криптографической защиты информации в администрации.

8.2 Ответственный за эксплуатацию СКЗИ должен обобщать результаты всех видов контроля за организацией и обеспечением порядка использования СКЗИ в администрации, анализировать причины выявленных недостатков, разрабатывать меры по их профилактике, контролировать выполнение рекомендаций, содержащихся в актах проверок контролирующих организаций.

ПРИЛОЖЕНИЕ № 1
к Правилам эксплуатации средств криптографической
защиты информации в администрации Баганского района Новосибирской области
ТИПОВАЯ ФОРМА

АКТ
ввода в эксплуатацию средств криптографической защиты информации

Настоящий акт составлен о том, что произведена установка и настройка изделия:
Наименование средства криптографической защиты информации

Адрес: _____
Помещение:

Характеристики помещения	Да	Нет
Помещение находится в пределах контролируемой зоны		
Помещение оборудовано прочной входной дверью с замками		
Помещение оснащено охранной сигнализацией		
Помещение оснащено пожарной сигнализацией		
Окна помещения защищены от просмотра извне		
Исключена возможность неконтролируемого проникновения или пребывания в помещении посторонних лиц		

Изделие: наименование средства криптографической защиты информации:

- серийный номер дистрибутива: _____;
- регистрационный (учетный) номер СКЗИ: _____;

размещено на аппаратном средстве (№ системного блока): _____
и в соответствии с эксплуатационной и технической документацией на СКЗИ <Наименование СКЗИ> введено в эксплуатацию.

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы), место опечатывания (опломбирования) возможно контролировать визуально, номер(а) печати(ей) (пломбира(ов)): _____.

Дистрибутив СКЗИ <Наименование СКЗИ> учтен в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов администрации Баганского района Новосибирской области.

Первичный инструктаж по использованию СКЗИ проведен со специалистом:
_____
(Должность, ФИО)
_____

Ответственный за эксплуатацию
СКЗИ: _____ _____
(подпись) (ФИО)

«___» _____ 20 ___ г.

ПРИЛОЖЕНИЕ № 2
к Правилам эксплуатации средств криптографической
защиты информации в администрации Баганского района Новосибирской области
ТИПОВАЯ ФОРМА

ЗАКЛЮЧЕНИЕ
о допуске пользователя СКЗИ к самостоятельной работе

«___» _____ 20___ г.

Пользователь СКЗИ: _____
(должность, ФИО, наименование организации)
_____

(далее – пользователь СКЗИ) в соответствии с Инструкцией 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, утвержденной приказом ФАПСИ от 13.06.2001 № 152, прошел обучение правилам эксплуатации и обеспечения безопасности

_____
(наименование средства криптографической защиты информации)

Пользователь СКЗИ обязуется:

– не разглашать сведения конфиденциального характера, к которым допущен, рубежи их защиты, в том числе, сведения о криптоключах;

– соблюдать требования к обеспечению безопасности сведений конфиденциального характера с использованием СКЗИ;

– сообщать ответственному за эксплуатацию СКЗИ о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

– сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от обязанностей, связанных с использованием СКЗИ;

– немедленно уведомлять ответственного за эксплуатацию СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ (сейфов), личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Заключение: пользователь к самостоятельной работе с СКЗИ допущен.

С заключением ознакомлен(а): _____ _____
(подпись) (ФИО)

Ответственный за эксплуатацию
СКЗИ: _____ _____
(подпись) (ФИО)

ПРИЛОЖЕНИЕ № 3
к Правилам эксплуатации средств криптографической
защиты информации в администрации Баганского района Новосибирской области

ФОРМА

ЖУРНАЛ
поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Журнал начат «____» _____ 20 ___ г.
Журнал завершен «____» _____ 20 ___ г.
Журнал составлен на _____ листах

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

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. лиц, произведших	Дата подключения (установки) и подписи лиц,	Номера аппаратных средств, в которые установлены или к	Дата изъятия (уничтожения)	Ф.И.О. лиц, производивших изъятие (уничтожение)	Номер акта или расписка	

подключение (установку)	произведших подключение (установку)	которым подключены СКЗИ			об уничтожении	
9	10	11	12	13	14	15

ПРИЛОЖЕНИЕ № 4
к Правилам эксплуатации средств криптографической
защиты информации в администрации Баганского района Новосибирской области

ФОРМА

ЖУРНАЛ
учета хранилищ средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

Журнал начат «____» _____ 20 ___ г.
Журнал завершен «____» _____ 20 ___ г.
Журнал составлен на _____ листах

№ п/п	Наименование хранилища (помещение, сейф, металлический шкаф)	Инвентарный номер хранилища	Местонахождение (подразделение, номер кабинета)	Что хранится (документы, изделия)	Ф.И.О. ответственного за хранилище
1	2	3	4	5	6

Количество комплектов ключей от помещения, хранилища и их номера3	Расписка о получении ключа (ФИО, номер комплекта ключей, подпись получившего ключ, дата получения ключа), тубуса(пенала) (ФИО, номер печати, подпись получившего тубус (пенал), дата получения тубуса (пенала))	Расписка о возврате ключа (ФИО, номер комплекта ключей, подпись принявшего ключ, дата возврата ключа), тубуса (пенала) (ФИО, номер печати, подпись принявшего тубус (пенал), дата возврата тубуса (пенала))	Примечание
6	7	8	9

[3] Для тубусов (пеналов) в графе ставится прочерк

ПРИЛОЖЕНИЕ № 5
к Правилам эксплуатации средств криптографической
защиты информации в администрации Баганского района Новосибирской области
ТИПОВАЯ ФОРМА

АКТ
вывода из эксплуатации средств криптографической защиты информации

Настоящий акт составлен о том, что перечисленные в нем средства криптографической защиты информации (СКЗИ) уничтожены с предварительным стиранием программного обеспечения СКЗИ, и произведено стирание информации, оставшейся в устройствах памяти оборудования.

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним	Регистрационный номер СКЗИ, эксплуатационной и технической документации к ним	Номер аппаратного средства

Регистрационные данные на СКЗИ сверены с записями в настоящем Акте, уничтожение СКЗИ выполнено в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.

Узлы и детали аппаратных средств передать для дальнейшей эксплуатации.

В журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов администрации Баганского района Новосибирской области внесены соответствующие записи.

Ответственный за эксплуатацию СКЗИ: _____ _____
(подпись) (ФИО)

«___» _____ 20 ___ г.

ПРИЛОЖЕНИЕ № 6
к Правилам эксплуатации средств криптографической
защиты информации в администрации Баганского района
Новосибирской области

ТИПОВАЯ ФОРМА

АКТ № _____
об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов

Настоящий акт составлен о том, что произведено уничтожение нижеуказанных криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

№ п/п	Наименование носителя криптографических ключей, ключевых документов	Номер (идентификатор) криптографического ключа, наименование документа	ФИО владельца ключа (документа)	Примечание

Всего уничтожено _____

криптографических ключей на _____ ключевых носителях.

Уничтожение криптографических ключей выполнено путем их стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Ответственный за эксплуатацию СКЗИ: _____ _____
(подпись) (ФИО)

«___» _____ 20 ___ г.

ПРИЛОЖЕНИЕ № 7
к Правилам эксплуатации средств криптографической
защиты информации в администрации
Баганского района Новосибирской области

ТИПОВАЯ ФОРМА

АКТ
об обнаружении признаков, указывающих на возможное проникновение посторонних лиц в помещениях администрации Баганского района Новосибирской области

«___» _____ 20___г.

_____
(должность, фамилия, имя, отчество должностного лица)

в связи с обнаружением _____
_____

в присутствии:
_____
_____
(должность, фамилии, имена, отчества иных лиц, присутствовавших при осмотре)

произвел осмотр помещения (в котором ведется обработка информации ограниченного доступа (в том числе персональных данных) и размещены используемые средства криптографической информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ[4]), расположенного по адресу:
_____

В ходе осмотра обнаружено:
_____
_____
_____

Подписи лиц, принимавших участие (присутствовавших) при проведении осмотра:

_____	_____	_____
(должность)	(подпись)	(ФИО)
_____	_____	_____
(должность)	(подпись)	(ФИО)
_____	_____	_____
(должность)	(подпись)	(ФИО)

[4] Уточнить, оставить нужное

Приложение № 5

к постановлению от _____ № _____

ТИПОВАЯ ФОРМА

Перечень лиц, имеющих доступ в помещения, где размещены используемые средства криптографической защиты информации, хранятся средства криптографической защиты информации и (или) носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации

№ п/п	ФИО работника	Должность	Структурное подразделение	Адрес расположения и номера помещений (кабинетов), в которые разрешен доступ

Приложение № 6

к постановлению от _____ № _____

Порядок доступа в помещения, в которых ведется обработка персональных данных и размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях

1. Общие положения

1.1 Настоящий Порядок регламентирует условия и порядок осуществления доступа в помещения администрации Баганского района Новосибирской области (далее – администрация), в которых ведется обработка информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее – информация), и размещены используемые средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях (далее – Помещения) в целях организации режима обеспечения безопасности информации, препятствующего возможности неконтролируемого проникновения или пребывания в вышеуказанных помещениях лиц, не имеющих прав доступа в эти помещения.

1.2 Для обеспечения доступа сотрудников администрации в вышеуказанные помещения предусматривается комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности администрации.

1.3 Реализация комплекса мер, направленных на поддержание и обеспечение настоящего Порядка, возлагается на сотрудников администрации.

1.4 В случае нарушения настоящего Порядка сотрудники могут быть привлечены к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации.

2. Порядок доступа в помещения

2.1 Обеспечение безопасности информации от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении информации достигается, в том числе установлением правил доступа в Помещения.

2.2 Размещение информационных систем, в которых обрабатывается информация, СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, хранилищ материальных носителей персональных данных, должно осуществляться в пределах контролируемой зоны, границы которой устанавливаются постановлением администрации Баганского района Новосибирской области.

2.3 Для Помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации и средств защиты информации, криптосредств и ключевых документов к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих Помещениях посторонних лиц и просмотра ведущихся там работ.

2.4 Для предотвращения просмотра извне защищаемой информации окна Помещений должны быть защищены шторами или жалюзи.

2.5 Должны обеспечиваться контроль и управление физическим доступом в Помещения:

- в Помещения допускаются только сотрудники администрации в соответствии с Перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, и Перечнем лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими служебных (трудовых) обязанностей (далее – Перечни лиц);
- в нерабочее время пребывание в Помещениях вышеуказанных сотрудников администрации разрешается только на основании служебных записок (или иных разрешающих документов/указаний руководителя);
- в рамках внутреннего контроля должен проводиться контроль санкционирования и учета физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, СКЗИ, а также в помещения и сооружения, в которых они установлены (контроль актуальности Перечней лиц);
- нахождение в Помещениях лиц, не включенных в Перечни лиц, возможно только в присутствии уполномоченных сотрудников администрации. Время нахождения в Помещениях ограничивается временем решения вопросов, в рамках которого возникла необходимость пребывания в Помещении.

2.6 Помещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей Помещений на замок и их открытие только для санкционированного прохода.

2.7 Ключи от входных дверей Помещений учитывают и выдают только работникам (сотрудникам) администрации, включенным в Перечень лиц,

2.8 Сотрудники администрации, указанные в Перечнях лиц, не должны покидать Помещение, не убедившись, что доступ посторонних лиц к защищаемой информации невозможен. Запрещается оставлять материальные носители с защищаемой информацией без присмотра в незапертом Помещении.

2.9 При обнаружении повреждений замков или других признаков, указывающих на возможное проникновение посторонних лиц в Помещения, немедленно ставятся в известность

ответственный за организацию обработки персональных данных, ответственный за защиту информации, ответственный за эксплуатацию СКЗИ, непосредственный руководитель соответствующего структурного подразделения. При необходимости вызываются работники правоохранительных органов и принимаются меры по охране места происшествия до их прибытия (Помещения не вскрываются, сотрудники администрации и посетители в Помещения не допускается). Дальнейшие действия определяются характером произошедшего инцидента.

2.10 По результатам анализа случившегося, необходимо дать оценку возможности компрометации хранящихся ключевых и других документов, составить акт об обнаружении признаков, указывающих на возможное проникновение посторонних лиц в Помещения администрации и принять при необходимости меры к локализации последствий компрометации информации и к замене скомпроментированных криптоключей.

2.11 При утрате ключа от входной двери в Помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей, соответствующие сведения вносятся в Журнал учета хранилищ. Порядок размещения СКЗИ, хранения ключевых и других документов в Помещении, от которого утрачен ключ, до замены замка или изменения секрета замка устанавливает руководитель соответствующего структурного подразделения администрации] по согласованию с ответственным за эксплуатацию СКЗИ, при этом должны быть обеспечены условия, исключающие бесконтрольный доступ, а также непреднамеренное уничтожение СКЗИ, ключевых и иных документов.

2.12 В случае возникновения нештатной ситуации, событий чрезвычайного характера необходимо в обязательном порядке известить о случившемся Главе Баганского района.

2.13 Сотрудники органов министерства по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и аварийных служб, врачи «скорой помощи» и сотрудники правоохранительных органов допускаются в Помещения в сопровождении сотрудников администрации, включенных в Перечни лиц, имеющих доступ в помещения, или сотрудников службы охраны.

Лист ознакомления
с постановлением от _____ № _____
«Об организации работы со средствами криптографической защиты информации в администрации Баганского района Новосибирской области»

№ п/п	ФИО	Дата ознакомления	Подпись
124.			
125.			
126.			
127.			
128.			
129.			
130.			
131.			
132.			
133.			
134.			
135.			
136.			
137.			
138.			
139.			
140.			
141.			
142.			
143.			
144.			
145.			
146.			
147.			
148.			
149.			
150.			
151.			
152.			
153.			
154.			
155.			
156.			
157.			
158.			
159.			
160.			
161.			
162.			
163.			
164.			

165.			
166.			
167.			

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

29.08.2024 № 786

Об организации контролируемой зоны в администрации Баганского района Новосибирской области

В целях обеспечения защиты информации ограниченного доступа (в том числе персональных данных), не содержащей сведения, составляющие государственную тайну (далее - информация), обрабатываемой в информационных системах администрации Баганского района Новосибирской области (далее также – администрация), администрация Баганского района

ПОСТАНОВЛЯЕТ:

16. Определить границами контролируемой зоны, в пределах которой осуществляется обработка защищаемой информации, постоянно размещаются стационарные технические средства, обрабатывающие защищаемую информацию, средства защиты информации, а также средства обеспечения функционирования информационных систем администрации, в пределах которых исключено неконтролируемое пребывание работников администрации и лиц, не имеющих постоянного допуска на объекты информационных систем (не являющихся работниками администрации), а также транспортных, технических и иных материальных средств:

– ограждающие конструкции охраняемого здания, расположенного по адресу: Новосибирская область, Баганский район, с. Баган ул. М. Горького,21;

– ограждающие конструкции помещений № 15 охраняемого здания, расположенного по адресу: Новосибирская область, Баганский район, с. Баган ул. М. Горького,21.

17. Сотрудникам администрации исключить в пределах контролируемых зон неконтролируемое пребывание лиц, не имеющих постоянного допуска на объекты информационных систем администрации.

3. Опубликовать настоящее постановление на официальном сайте органов местного самоуправления Баганского района Новосибирской области и в периодическом печатном издании органов местного самоуправления «Бюллетень органов местного самоуправления Баганского района».

4. Данное постановление вступает в силу после его публикации в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района Новосибирской области».

5. Контроль за исполнением настоящего постановления возложить на заместителя главы администрации Баганского района А.О. Бреус.

Глава Баганского района
Новосибирской области А.А. Воличенко

Лист ознакомления
с постановлением от _____ № _____
«Об организации контролируемой зоны в администрации Баганского района Новосибирской области»

№ п/п	ФИО	Дата ознакомления	Подпись
168.			
169.			
170.			
171.			
172.			
173.			
174.			
175.			
176.			
177.			
178.			
179.			
180.			
181.			
182.			
183.			
184.			
185.			
186.			
187.			
188.			
189.			
190.			
191.			
192.			
193.			
194.			
195.			
196.			
197.			
198.			
199.			
200.			
201.			
202.			
203.			
204.			
205.			
206.			
207.			
208.			

209.			
210.			
211.			

АДМИНИСТРАЦИЯ
БАГАНСКОГО РАЙОНА
НОВОСИБИРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

30.08.2024 № 796

О внесении изменений в постановление администрации Баганского района Новосибирской области от 03.06.2024 № 470 «О приостановлении деятельности структурного подразделения Муниципального бюджетного общеобразовательного учреждения Вознесенской средней общеобразовательной школы имени Леонида Чекмарёва дошкольного образовательного учреждения
Вознесенского детского сада»

В связи с продолжением ремонтных работ в структурном подразделении Муниципального бюджетного общеобразовательного учреждения Вознесенской средней общеобразовательной школы имени Леонида Чекмарёва дошкольном образовательном учреждении Вознесенском детском саду, администрация Баганского района Новосибирской области,

ПОСТАНОВЛЯЕТ:

1.Внести изменения в постановление администрации Баганского района Новосибирской области от 03.06.2024 № 470 «О приостановлении деятельности структурного подразделения Муниципального бюджетного общеобразовательного учреждения Вознесенской средней общеобразовательной школы имени Леонида Чекмарёва дошкольного образовательного учреждения Вознесенского детского сада»:

1.1. в пункте 1 цифры «30.08.2024» заменить цифрами «22.09.2024».

2.Директору Муниципального бюджетного общеобразовательного учреждения Вознесенской средней общеобразовательной школы имени Леонида Чекмарёва (А.Ж. Черкасовой) вручить извещения родителям (законным представителям) воспитанников структурного подразделения Муниципального бюджетного общеобразовательного учреждения Вознесенской средней общеобразовательной школы имени Леонида Чекмарёва дошкольного образовательного учреждения Вознесенского детского сада.

3.Разместить настоящее постановление на официальном сайте органов местного самоуправления Баганского района Новосибирской области, опубликовать в периодическом печатном издании органов местного самоуправления Баганского района Новосибирской области «Бюллетень органов местного самоуправления Баганского района».

4. Контроль за исполнением настоящего постановления оставляю за собой.

Глава Баганского района
Новосибирской области А.А. Воличенко

Четвертый раздел.

ПРОТОКОЛ № U21000029020000000013-1
о признании претендентов участниками аукциона на право
заключения договора аренды земельного участка

19.08.2024

Открытый аукцион на право заключения договора аренды земельного участка в электронной форме проводится в соответствии с распоряжением администрации Баганского района Новосибирской области от 15.07.2024 № 186-р «Об организации и проведении аукциона по продаже права на заключение договоров аренды земельных участков, находящихся в неразграниченной государственной собственности».

(наименование нормативного документа)

1. Предмет аукциона на право заключения договора аренды земельного участка в электронной форме: Электронный аукцион на право заключения договоров аренды земельных участков, государственная собственность на которые не разграничена.
2. Продавец (арендодатель): АДМИНИСТРАЦИЯ БАГАНСКОГО РАЙОНА НОВОСИБИРСКОЙ ОБЛАСТИ.
3. Организатор: АДМИНИСТРАЦИЯ БАГАНСКОГО РАЙОНА НОВОСИБИРСКОЙ ОБЛАСТИ, *Юридический адрес: 632770, Россия, Новосибирская область, Баганский район, с. Баган, М.Горького, 28, Почтовый адрес: 632770, Россия, Новосибирская область, Баганский район, с. Баган, М.Горького, 28.*
4. Начальная (минимальная) цена договора: 14 000,00 руб.
5. Извещение о проведении аукциона на право заключения договора аренды земельного участка в электронной форме и документация по проведению аукциона на право заключения договора аренды земельного участка в электронной форме размещены на электронной торговой площадке i.rts-tender.ru процедура № 21000029020000000013.
6. Состав комиссии:

1.	Слепынина Ольга Владимировна	Председатель комиссии	Заместитель Главы администрации Баганского района Новосибирской области.
2.	Колосов Сергей Валерьевич	Зам. председателя комиссии	Начальник управления сельского хозяйства, имущества и земельных отношений администрации Баганского района Новосибирской области.
3.	Павловская Алёна Петровна	Секретарь	Заместитель начальника управления сельского хозяйства, имущества и земельных отношений администрации Баганского района Новосибирской области
4.	Кусь Татьяна Александровна	Член комиссии	Начальник отдела правовой и кадровой работы администрации Баганского района Новосибирской области

5.	Чмурина Оксана Александровна	Член комиссии	Начальник управления экономики и финансов администрации Баганского района Новосибирской области
6.	Колобова Елена Владимировна	Член комиссии	Начальник отдела строительства и дорожного комплекса администрации Баганского района Новосибирской области
7.	Никонов Владимир Анатольевич	Член комиссии	Главный эксперт управления сельского хозяйства, имущества и земельных отношений администрации Баганского района Новосибирской области.

6.1. На заседании комиссии присутствуют:

1.	Слепынина Ольга Владимировна	Председатель комиссии	Заместитель Главы администрации Баганского района Новосибирской области.
2.	Колосов Сергей Валерьевич	Зам. председателя комиссии	Начальник управления сельского хозяйства, имущества и земельных отношений администрации Баганского района Новосибирской области.
3.	Кусь Татьяна Александровна	Член комиссии	Начальник отдела правовой и кадровой работы администрации Баганского района Новосибирской области
4.	Чмурина Оксана Александровна	Член комиссии	Начальник управления экономики и финансов администрации Баганского района Новосибирской области
5.	Колобова Елена Владимировна	Член комиссии	Начальник отдела строительства и дорожного комплекса администрации Баганского района Новосибирской области
6.	Никонов Владимир Анатольевич	Член комиссии	Главный эксперт управления сельского хозяйства, имущества и земельных отношений администрации Баганского района Новосибирской области.

7. Начало проведения аукционного торга: 22.08.2024 в 09 часов 00 минут (по местному времени).

8. Аукционный торг проводится через систему электронной торговой площадки по адресу i.rts-tender.ru

9. На момент окончания срока подачи заявок на участие в 1 этапе аукциона на право заключения договора аренды земельного участка в электронной форме 19.08.2024 06:00:00:
подана 1 заявка.

Номер лота / Наименование лота	Наименование участника	ИНН/КПП	Почтовый адрес
№ 1 - Земельный участок	Мищенко Ольга Александровна	541750709462	Российская Федерация

10. Отозванные заявки: нет.
11. В связи с тем, что была подана одна заявка на участие в аукционе на право заключения договора аренды земельного участка в электронной форме, аукцион признается несостоявшимся, договор будет заключён с единственным участником по начальной (минимальной) цене договора: 14 000,00 руб.

Подписи членов комиссии:

Председатель комиссии /_____/ Слепынина О.В.
(подпись)
Зам. председателя комиссии /_____/ Колосов С.В.
(подпись)
Член комиссии /_____/ Кусь Т.А.
(подпись)
Член комиссии /_____/ Чмурина О.А.
(подпись)
Член комиссии /_____/ Колобова Е.В.
(подпись)
Член комиссии /_____/ Никонов В.А.
(подпись)

Извещение
о проведении аукциона в электронной форме

Администрация Баганского района Новосибирской области проводит открытый аукцион на право заключения договора аренды земельного участка, находящегося в муниципальной собственности Баганского района Новосибирской области в соответствии с Федеральным законом от 26 июля 2006 года № 135-ФЗ «О защите конкуренции» (далее – Федеральный закон), статьей 39.11 Земельного кодекса Российской Федерации, на основании распоряжение администрации Баганского района Новосибирской области от 28.08.2024 № 221-р «Об организации и проведении аукциона по продаже права на заключение договора аренды земельного участка, находящегося в муниципальной собственности Баганского района Новосибирской области».

Участники аукциона имеют право участвовать в открытом аукционе, как непосредственно, так и через своих представителей. Полномочия представителей участников подтверждаются доверенностью, выданной и оформленной в соответствии с гражданским законодательством, или ее нотариально заверенной копией.

1	Форма торгов
	Торги проводятся в виде аукциона в электронной форме, открытого по составу участников и по форме подачи заявок.
2	Срок принятия решения об отказе в проведении торгов
	Организатор аукциона вправе отказаться от проведения аукциона. Извещение об отказе в проведении аукциона размещается на сайте www.torgi.gov.ru

	организатором аукциона в течение трех дней со дня принятия данного решения. Организатор аукциона в течение трех дней со дня принятия решения об отказе в проведении аукциона обязан известить участников аукциона об отказе в проведении аукциона и возвратить его участникам внесенные задатки.
3	Предмет договора
	Лот № 1 - земельный участок, находящийся в муниципальной собственности Баганского района Новосибирской области, категория земель: земли сельскохозяйственного назначения с кадастровым номером 54:01:024301:2003 площадью 1644619 кв.м, вид разрешенного использования: Сельскохозяйственное использование. Местоположение: Новосибирская область, Баганский район, МО Лозовского сельсовета.
4	Срок договора
	Лот №1 – 49 лет.
5	Дата, время и порядок осмотра земельного участка на местности
	С момента опубликования извещения по указанному местоположению земельного участка в любое время самостоятельно.
6	Обременения земельного участка
	Лот №1 ограничения (обременения): Учетный номер части: 54:01:024301:2003/1. Площадь, 38340 кв.м. Вид ограничения (обременения): ограничения прав на земельный участок, предусмотренные статьей 56 Земельного кодекса Российской Федерации; Срок действия: не установлен; реквизиты документа-основания: карта(план) от 09.09.2013 № б/н; Содержание ограничения (обременения): Ограничения использования земель установлены в соответствии с Постановлением Совета Министров СССР от 26.03.1984 N 255 "Об утверждении правил охраны электрических сетей напряжением свыше 1000 Вольт"; Реестровый номер границы: 54.01.2.8. Учетный номер части: 54:01:024301:2003/2. Площадь, 1866 кв.м. вид ограничения (обременения): ограничения прав на земельный участок, предусмотренные статьей 56 Земельного кодекса Российской Федерации; Срок действия: не установлен; реквизиты документа-основания: акт приемки законченного строительством объекта от 02.11.2017 № 2 выдан: ПАО "Ростелеком"; Содержание ограничения (обременения): Ограничения в использовании земельных участков в охранной зоне кабеля связи установлены п.4, п.18, п.48, п.49 "Правил охраны линий и сооружений связи Российской Федерации", утвержденных Постановлением Правительства РФ от 9 июня 1995 г. №578; Реестровый номер границы: 54.01.2.61.
7	Начальная (минимальная) цена договора (рублей без НДС).
	Лот №1 – 30000,00
8	«Шаг аукциона» (3%), рублей.
	Лот №1 – 900,00
9	Размер задатка (20%), рублей.
	Лот №1 – 6000,00.
10	Реквизиты счета для перечисления задатка.
	Задаток перечисляется на реквизиты, указанные в условиях извещения на электронно-торговой площадке ООО «РТС –ТЕНДЕР».

	Задаток должен быть внесен и поступить на указанный счет не позднее времени, даты рассмотрения заявок на участие в аукционе. Возврат задатка в течение 3 (трех) рабочих дней со дня поступления уведомления об отзыве заявки. Возврат задатка лицам, не допущенным к участию в аукционе в течение 3 (трех) рабочих дней со дня оформления протокола приема заявок на участие в аукционе. Возврат задатка в течение 3 (трех) рабочих дней со дня подписания протокола о результатах аукциона лицам, участвовавшим в аукционе, но не победившим в нем.
11	Перечень документов, представляемых претендентами для участия в аукционе.
	1) заявка на участие в аукционе по установленной в извещении о проведении аукциона форме с указанием банковских реквизитов счета для возврата задатка; 2) копии документов, удостоверяющих личность заявителя (для граждан); 3) надлежащим образом заверенный перевод на русский язык документов о государственной регистрации юридического лица в соответствии с законодательством иностранного государства в случае, если заявителем является иностранное юридическое лицо; 4) документы, подтверждающие внесение задатка.
12	Порядок, место, дата начала и дата и время окончания срока подачи заявок на участие в открытом аукционе.
	Для участия в аукционе в электронной форме участник, получивший аккредитацию и зарегистрированный на электронной площадке, подает заявку на участие в аукционе в электронной форме. Участник вправе подать заявку на участие в аукционе в электронной форме в пределах срока подачи заявок, указанного в извещении о проведении такого аукциона. Заявка на участие в аукционе в электронной форме направляется участником оператору электронной площадки. Подача участником заявки на участие в аукционе в электронной форме является согласием такого участника на списание денежных средств, находящихся на его счете, открытом для проведения операций по обеспечению участия в электронных торгах, в качестве платы за участие в аукционе в электронной форме в случае, если плата за участие в таком аукционе предусмотрена регламентом электронной площадки, в порядке и по основаниям, установленным таким регламентом и иными документами электронной площадки. Электронная торговая площадка отображает время всех процедур согласно часовому поясу г. Москвы. Дата и время начала приема заявок: 02.09.2024 с 9:00 по местному времени. Дата и время окончания приема заявок: 03.10.2024 до 10:00 по местному времени.
13	Порядок предоставления документации об аукционе.
	При проведении аукциона размещение документации осуществляется на официальном сайте «torgi.gov.ru» не менее чем за тридцать дней до дня проведения аукциона, одновременно с размещением извещения о проведении аукциона.
14	Основания для недопуска к участию в аукционе.
	Заявитель не допускается к участию в аукционе по следующим основаниям:

	1. Непредоставления необходимых для участия в аукционе в электронной форме документов в электронной форме или представление недостоверных сведений; 2. Непоступления задатка на дату рассмотрения заявок на участие в аукционе в электронной форме; 3. Подачи заявки на участие в аукционе в электронной форме лицом, которое в соответствии с Земельным кодексом РФ и другими Федеральными законами не имеет права быть участником конкретного аукциона в электронной форме, покупателем земельного участка или приобрести земельный участок в аренду; 4. Наличия сведений о заявителе, об учредителях (участниках), о членах коллегиальных исполнительных органов заявителя, лицах, исполняющих функции единоличного исполнительного органа заявителя, являющегося юридическим лицом, в реестре недобросовестных участников аукциона.
15	Место, дата, время и порядок определения участников торгов.
	Организатор аукциона ведет протокол рассмотрения заявок на участие в аукционе, который должен содержать сведения о заявителях, допущенных к участию в аукционе и признанных участниками аукциона, датах подачи заявок, внесенных задатках, а также сведения о заявителях, не допущенных к участию в аукционе, с указанием причин отказа в допуске к участию в нем. Заявитель, признанный участником аукциона, становится участником аукциона с даты подписания организатором аукциона протокола рассмотрения заявок. Электронная торговая площадка отображает время всех процедур согласно часовому поясу г. Москвы. Дата и время признания участников аукциона: 03.10.2024 в 14 часов 00 минут (по местному времени).
16	Место и срок подведения итогов торгов, порядок определения победителей торгов.
	Открытый аукцион в электронной форме проводится оператором электронной площадки по адресу www.rts-tender.ru в Разделе «Имущество». Дата и время аукциона 07.10.2024 в 09 часов 00 минут (по местному времени). Электронная торговая площадка отображает время всех процедур согласно часовому поясу г. Москвы.
17	Порядок заключения договора аренды земельного участка.
	Уполномоченный орган направляет победителю аукциона или единственному принявшему участие в аукционе его участнику два экземпляра подписанного проекта договора аренды земельного участка в десятидневный срок со дня составления протокола о результатах аукциона. Не допускается заключение указанных договоров ранее чем через десять дней со дня размещения информации о результатах аукциона на официальном сайте.

Приложение №1
к извещению о проведении
аукциона в электронной
форме

ЗАЯВКА
юридического лица на участие в аукционе на право заключения договора аренды земельного участка

1. Полное наименование юридического лица:
_____
_____
_____
2. Фамилия, имя, отчество руководителя или представителя:
_____
_____
_____ ,
действующий на основании
_____
_____
_____
3. Идентификационный номер налогоплательщика:
_____
4. Адрес фактического нахождения юридического лица :
Индекс: _____ Населенный
пункт:_____
Улица: _____ Дом: _____
Корпус:_____
Телефон: _____
5. Изучив информационное сообщение, заявляем о своем согласии принять участие в аукционе по передаче в аренду земельного участка, находящегося в государственной собственности, из земель сельскохозяйственного назначения с кадастровым номером _____, площадью_____ кв. м., для использования в целях _____
_____(вид разрешенного использования земельного участка),
местоположение:_____
_____
_____(далее – земельный участок).
6. В случае победы на аукционе принимаем на себя следующие обязательства:
а) подписать с организатором аукциона протокол о результатах аукциона в день проведения торгов и заключить договор аренды земельного участка по истечении десяти дней со дня подписания данного протокола;
б) до подписания договора аренды земельного участка настоящая заявка вместе с протоколом о результатах проведения аукциона будет считаться имеющей силу предварительного договора между заявителем и организатором аукциона.

7. Гарантируем достоверность сведений, отраженных в настоящей заявке и представленных документах.
8. Реквизиты счета для возврата задатка:_____
_____
_____
9. С условиями торгов ознакомлен(а), согласен(на).

Заявитель: _____ _____
(ФИО) (подпись)
"____" _____ г.
М. П.

Заявка принята организатором аукциона: "____" _____ 202__года.
в_____ час. _____мин., зарегистрирована в журнале за номером _____

_____ _____
(ФИО уполномоченного лица организатора торгов (подпись)

ЗАЯВКА
физического лица на участие в аукционе на право заключения договора аренды земельного участка

1. Фамилия, имя, отчество заявителя_____
_____
_____
2. Фамилия, имя, отчество представителя физического лица:
_____
_____
_____
действующий на основании
_____
_____
_____
3. Дата рождения заявителя:
_____
4. Паспортные данные заявителя: серия _____, №
_____
когда выдан _____ , кем выдан
_____

5. Свидетельство о государственной регистрации в качестве индивидуального предпринимателя (в случае когда заявитель является индивидуальным предпринимателем) серия _____, № _____ ,
от _____, кем выдан
_____
6. Адрес регистрации по месту жительства (пребывания):
Индекс: _____ Населенный пункт:_____
Улица: _____ Дом: _____
Корпус:_____
Квартира: _____ Телефон: _____
7. Изучив информационное сообщение, заявляю о своем согласии принять участие в аукционе по аренде земельного участка, находящегося в государственной собственности, из земель сельскохозяйственного назначения с кадастровым номером _____, площадью_____ кв. м., для использования в целях _____
_____(вид разрешенного использования земельного участка),
местоположение которого установлено:_____
_____(далее – земельный участок).
9. В случае победы на аукционе принимаю на себя следующие обязательства:
а) подписать с организатором аукциона протокол о результатах торгов в день проведения аукциона и заключить договор аренды земельного участка по истечении десяти дней со дня подписания данного протокола;
б) до подписания договора аренды земельного участка настоящая заявка вместе с протоколом о результатах проведения аукциона будет считаться имеющей силу предварительного договора между заявителем и организатором торгов.
10. Гарантирую достоверность сведений, отраженных в настоящей заявке и представленных документах.
11. Реквизиты счета для возврата задатка:_____
_____
_____
12. С условиями торгов ознакомлен (а), согласен (на).
13. Даю согласие на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) следующих персональных данных:

фамилия, имя, отчество (последнее – при наличии);
адрес регистрации и фактического проживания;
документ, удостоверяющий личность (серия, номер, кем и когда выдан).

Заявитель: _____ _____
(ФИО) (подпись)

"____" _____202__ год.

Заявка принята организатором торгов: "____" _____ г.
в_____ час. _____мин., зарегистрирована в журнале за номером _____

_____ _____
(ФИО уполномоченного лица организатора торгов) (подпись)

Приложение №2
к извещению о проведении
аукциона в электронной
форме

Договор аренды
земельного участка на территории Баганского района
Новосибирской области

№___ « __» _____ 20___ г.

Администрация Баганского района Новосибирской области, именуемая в дальнейшем «Арендодатель» в лице
_____,
действующего на основании Устава Баганского района Новосибирской области, с одной стороны и _____, в лице _____, действующ___ на основании _____, именуемое в дальнейшем «Арендатор» с другой стороны, на основании результатов открытого аукциона от _____ заключили настоящий договор о нижеследующем:

1. Предмет договора

«Арендодатель» передает, а «Арендатор» принимает в аренду земельный участок общей площадью _____ кв. м., с кадастровым номером _____, расположенный по адресу:
_____
_____, для, в границах, указанных в кадастровом плане земельного участка, приложенном к настоящему Договору и являющимся неотъемлемой его частью (приложение №1). Категория земель – _____
На участке строений не имеется.
Обременения в отношении земельного участка _____

2. Срок договора

2.1 Срок настоящего договора ____ лет.
2.2 Настоящий договор вступает в силу с момента его регистрации в Управлении Федеральной регистрационной службы по Новосибирской области.

3. Арендная плата

3.1 Размер арендной платы составляет_____ (_____) ежегодно.
3.2 Арендная плата вносится «Арендатором» 2 раза в год равными частями не позднее 15 сентября и 15 декабря текущего года.

Получатель: ИНН 5417104650, КПП 541701001
Управление Федерального казначейства по Новосибирской области (Администрация Баганского района Новосибирской области л/с 04513008440).

КС 03100643000000015100 в СИБИРСКОЕ ГУ БАНКА РОССИИ//УФК по Новосибирской области г. Новосибирск.
ЕКС 40102810445370000043.
БИК Банка получателя: 015004950.
Код бюджетной классификации: 010 111 05013 05 0000 120
Код ОКТМО: _____

В случае неоплаты арендной платы в установленный срок Арендатор уплачивает пеню за каждый день просрочки в размере 0,1% от суммы неоплаты.

3.3 Размер арендной платы ежегодно, но не ранее чем через год после заключения настоящего Договора, изменяется в одностороннем порядке Арендодателем на размер уровня инфляции, установленного в федеральном законе о федеральном бюджете на очередной финансовый год и плановый период, который применяется ежегодно по состоянию на начало очередного финансового года, начиная с года, следующего за годом, в котором заключен настоящий Договор.

Кроме того, Арендодателем в одностороннем порядке может быть изменен порядок перечисления арендной платы.

В указанных в настоящем пункте случаях Арендодатель направляет письменное уведомление Арендатору. Арендатор обязан принять уведомление к исполнению в указанный в нем срок без подписания дополнительного соглашения.

3.4 Арендная плата и начисленная пеня уплачиваются Арендатором отдельными платежными документами по каждому договору аренды и типу платежа. Внесение арендной платы и пени по нескольким договорам аренды земельных участков одним платежным документом не допускается.

3.5 Неиспользование Арендатором земельного участка не является основанием для невнесения арендной платы.

4. Права и обязанности сторон:

4.1 Арендодатель имеет право:

4.1.1 досрочно расторгнуть настоящий договор в порядке и случаях, предусмотренных действующим законодательством РФ.

4.1.2 на беспрепятственный доступ на территорию земельного участка в целях его осмотра на предмет соблюдения условий настоящего договора.

4.1.3 на возмещение убытков, причиненных ухудшением качества земельного участка и экологической обстановки в результате хозяйственной деятельности Арендатора, также по иным основаниям, предусмотренным законодательством РФ.

4.2. Арендодатель обязан:

4.2.1 не вмешиваться в хозяйственную деятельность «Арендатора», если она не противоречит условиям настоящего договора.

4.2.2 своевременно в письменном виде извещать Арендатора об изменениях в порядке установления и взимания арендной платы, а также о смене финансовых реквизитов получателя арендной платы.

4.2.3 выполнять в полном объеме все условия настоящего договора.

4.2.4 не использовать и не предоставлять прав третьим лицам на использование природных объектов, находящихся на земельном участке без согласования с Арендатором.

4.2.5 в случаях, связанных с необходимостью изъятия земельного участка для государственных или муниципальных нужд, гарантировать Арендатору возмещение всех затрат в соответствии с действующим законодательством.

4.2.6 нести другие обязанности, предусмотренные законодательством РФ.

4.3 Арендатор имеет право:

4.3.1 использовать земельный участок на условиях, установленных настоящим договором.

4.3.2 передать земельный участок в субаренду в пределах срока действия настоящего договора письменно уведомив Арендодателя. Срок действия договора субаренды не может превышать срока действия настоящего договора. При досрочном расторжении настоящего договора договор субаренды земельного участка прекращает свое действие.

Арендатор обязан:

4.4.1 выполнять в полном объеме все условия настоящего договора.

4.4.2 использовать земельный участок в соответствии с разрешенным использованием, законодательством РФ и настоящим договором.

4.4.3 обеспечить Арендодателю, представителям органов государственного земельного контроля, доступ на земельный участок по их требованию.

4.4.4 не допускать ухудшения экологической обстановки на земельном участке и прилегающей территории в результате своей деятельности

4.4.5 в случае ухудшения состояния земельного участка в процессе его использования Арендатором, приводить его в состояние, пригодное для его использования, за свой счет.

4.4.6 своевременно в соответствии с договором вносить арендную плату.

4.4.7 не нарушать права других землепользователей.

4.4.8 письменно уведомлять Арендодателя об изменении своих юридических или финансовых реквизитов в срок не позднее, чем через 15 календарных дней с момента совершения последних.

4.4.9 письменно сообщать Арендодателю не позднее, чем за 3 месяца о предстоящем освобождении земельного участка, как в связи с окончанием срока действия настоящего договора, так и при досрочном его освобождении.

4.4.10 нести другие обязанности, предусмотренные законодательством РФ.

5. Ответственность сторон

5.1 За нарушение срока внесения арендной платы по настоящему договору Арендатор выплачивает пеню в размере 0,1% от суммы задолженности за каждый календарный день просрочки. Пеня перечисляется на счет, указанный в п.3.2 настоящего договора.

5.2 Ответственность сторон за нарушение обязательств по настоящему договору, вызванных действием обстоятельств непреодолимой силы, регулируется законодательством РФ.

5.3 Стороны обязуются в рамках исполнения настоящего договора соблюдать требования применимого антикоррупционного законодательства и не предпринимать никаких действий, которые могут нарушить нормы антикоррупционного законодательства или стать причиной такого нарушения, в том числе не требовать, не получать, не предлагать, не санкционировать, не обещать и не совершать незаконные платежи напрямую, через третьих лиц или в качестве посредника, включая (но не ограничиваясь) взятки в денежной или любой иной форме, каким-либо физическим или юридическим лицам, включая (но не ограничиваясь) коммерческим организациям, органам власти и самоуправления, государственным служащим, частным компаниям и их представителям.

5.4 В случае нарушения одной из сторон, изложенных выше антикоррупционных обязательств, вторая сторона вправе в одностороннем порядке приостановить исполнение своих обязательств по настоящему договору до устранения причин такого нарушения или отказаться от исполнения договора, направив об этом письменное уведомление.

6. Расторжение, изменение настоящего договора

6.1 Все изменения и дополнения к настоящему договору оформляются путем заключения сторонами дополнительного соглашения, подписанного сторонами за исключением случаев, предусмотренных законодательством Российской Федерации и пункта 3.3. настоящего Договора.

6.2 Истечение срока действия настоящего договора влечет за собой его прекращение.

6.3 За нарушение п.п. 4.4.2, 4.4.3, 4.4.4 договора Арендатор оплачивает штраф в размере 50 000 (пятьдесят тысяч) рублей.

6.4 Арендатор, после окончания установленного срока аренды, при досрочном расторжении настоящего договора должен произвести передачу Арендодателю земельного участка в 10-дневный срок с момента прекращения (расторжения) настоящего договора. Арендатор обязан вернуть земельный участок Арендодателю в надлежащем состоянии, пригодном для его дальнейшего использования.

6.5 Расторжение настоящего договора осуществляется в соответствии с действующим законодательством, в т.ч. Земельным кодексом РФ.

7. Рассмотрение споров

7.1 Земельные споры, возникающие при реализации настоящего договора, разрешаются соответствующей комиссией, по заявлению одной из сторон. При невозможности достижения согласия в комиссии, заинтересованная сторона обращается с исковым заявлением в суд.

8. Особые условия

8.1 Стоимость неотделимых улучшений земельного участка, произведенных Арендатором(ми) возмещению, не подлежит ни при каких условиях.

8.2 Настоящий договор аренды составлен и подписан в ____ экземплярах, имеющих одинаковую юридическую силу, один из которых находится у Арендодателя, второй выдается Арендатору, третий - в Управлении Федеральной регистрационной службы по Новосибирской области.

8.3 Настоящий договор является одновременно актом приема-передачи земли.

9. Приложения к договору

9.1 Приложение 1: выписка из Единого государственного реестра недвижимости об основных характеристиках и зарегистрированных правах на объект недвижимости.

10. Реквизиты сторон

Арендодатель:	Арендатор:
Администрация Баганского района Новосибирской области 632770, Новосибирская область, Баганский район с. Баган, ул. М. Горького, 28 ИНН 5417104650 ОГРН 1045480001885 КПП 541701001	

БИК 015004950 КС 03231643506030005100 ЕКС 40102810445370000043 СИБИРСКОЕ ГУ БАНКА РОССИИ//УФК по Новосибирской области г. Новосибирск _____ _____МП	