|  |  |  |
| --- | --- | --- |
| **ПОСТАНОВЛЕНИЕ**  **АДМИНИСТРАЦИИ СЕЛЬСКОГО ПОСЕЛЕНИЯ БРЕСЛАВСКИЙ СЕЛЬСОВЕТ УСМАНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ЛИПЕЦКОЙ ОБЛАСТИ**  **РОССИЙСКОЙ ФЕДЕРАЦИИ**      с.Бреславка  20.11.2020 г. № 42 | | |
|  |  |  |
|  |  |  |
|  |  |  |

Об утверждении

Положения о защите информации в

информационной системе «ИС Администрации сельского поселения Береславского

сельсовета Усманского муниципального района Липецкой области»

В соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющую государственную тайну, содержащейся в государственных информационных системах»:

Утвердить Положение о защите информации при ее обработке в информационной системе «ИС Администрации сельского поселения Бреславский сельсовет Усманского муниципального района Липецкой области».

2. Контроль исполнения настоящего постановления возложить на ответственного за обеспечение безопасности информации в информационной системе.

Глава администрации

сельского поселения Бреславский сельсовет\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В.Артёмов .

|  |  |  |
| --- | --- | --- |
|  |  | **УТВЕРЖДАЮ** |
|  |  | Глава  Администрации сельского поселения Бреславского сельсовета Усманского муниципального района Липецкой области  Артемов С.В.  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_г. |

**Положение о защите информации с информационной системе**

**«ИС Администрации сельского поселения Бреславского сельсовета Усманского муниципального района Липецкой области»**

1. **Общие положения**
   1. Положение о защите информации в информационной системе (далее – Положение) устанавливает состав и содержание организационных и технических мер по обеспечению безопасности информации при ее обработке в информационной системе на протяжении всего цикла её эксплуатации в Администрации сельского поселения Бреславского сельсовета Усманского муниципального района Липецкой области.

Меры по обеспечению безопасности информации, обрабатываемой в информационной системе (далее –ИС), принимаются для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации, обрабатываемой в ИС.

Меры по обеспечению безопасности информации, обрабатываемой в ИС, реализуются в рамках системы защиты в соответствии с требованиями к защите информации, установленными нормативно-правовыми актами, приведенными в п. 2 настоящего Положения, и направлены на нейтрализацию актуальных угроз безопасности информации, обрабатываемой в ИС.

* 1. Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля, а также в целях совершенствования технологий защиты ПДн, обрабатываемых в ИС.

1. **Нормативные ссылки**

Положение разработано с учетом требований, следующих нормативных правовых актов:

* Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной Обработке персональных данных»;
* Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющую государственную тайну, содержащейся в государственных информационных системах».

При разработке настоящего положения также был учтен утвержденный в Администрации сельского поселения Бреславского сельсовета Усманского муниципального района Липецкой области локальный правовый акт «Акт классификации информационной системы «ИС Администрации сельского поселения Бреславского сельсовета Усманского муниципального района Липецкой области».

1. **Описание информационной системы**

ИС располагается по адресу: 399336, Липецкая обл, Усманский р-н, Бреславка с, Молодежная ул, дом № 4 А

Актом определения класса защищенности информационной системы был установлен уровень значимости информации, обрабатываемой в ИС – низкий (УЗ 3) и класс защищенности ИС – К3.

1. **Выбор мер по обеспечению безопасности персональных данных, обрабатываемых в ИС.**

В соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющую государственную тайну, содержащейся в государственных информационных системах», базовый набор мер, необходимых для обеспечения класса защищенности ИС - К3, включает в себя меры, приведенные в таблице 1 настоящего Положения.

Таблица 1.

| **Условное обозначение меры** | **Содержание мер защиты информации** |
| --- | --- |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |
| III. Ограничение программной среды (ОПС) | |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов |
| IV. Защита машинных носителей информации (ЗНИ) | |
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |
| V. Регистрация событий безопасности (РСБ) | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |
| VI. Антивирусная защита (АВЗ) | |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| VIII. Контроль (анализ) защищенности информации (АНЗ) | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе |
| IX. Обеспечение целостности информационной системы и информации (ОЦЛ) | |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |
| XI. Защита среды виртуализации (ЗСВ) | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |
| XII. Защита технических средств (ЗТС) | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |

Проведена адаптация базового набора мер с учетом структурно-функциональных характеристик ИС, информационных технологий и особенностей функционирования информационной системы. Из базового набора мер исключены следующие меры, приведенные в таблице 2.

Таблица 2.

| **Условное обозначение меры** | **Содержание мер защиты информации** | **Причина исключения из базового набора мер** |
| --- | --- | --- |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) | В ИС нет внешних пользователей |
| УПД.13 | Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети | Удаленный доступ не реализован |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа | Беспроводной доступ не используется |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств | Мобильные технические средства не используются |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) | Взаимодействие со сторонними ИС не осуществляется |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации | В ИС не используется среда виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе | Беспроводной доступ не используется |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе | Мобильные технические средства не используются |

Для нейтрализации всех актуальных угроз безопасности ИС проведено уточнение полученного набора мер путем его дополнения с учетом не выбранных ранее мер.

С целью снижения риска неработоспособности технических средств и программных средств обработки информации использованы меры ЗНИ.3.

Более подробное описание выбранных мер по защите информации, обрабатываемой в ИС, а также способ их реализации приведены в таблице 4.

Знаком «+» обозначены меры по обеспечению безопасности информации, которые включены в базовый набор мер для 3-го уровня защищенности.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком «+», были добавлены при уточнении адаптированного базового набора мер.

Таблица 3.

| **Условное обозначение меры** | **Содержание мер защиты информации** | **Класс информационной системы 3** | **Способ реализации мер защиты информации** |
| --- | --- | --- | --- |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | | | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора | + | СЗИ от НСД |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов | + | СЗИ от НСД |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации | + | Применение организационно-технических мер |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации | + | СЗИ от НСД |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | | | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей | + | СЗИ от НСД |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа | + | СЗИ от НСД |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами | + | СКЗИ |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы | + | СКЗИ |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы | + | СЗИ от НСД |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) | + | СЗИ от НСД |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу | + | СЗИ от НСД |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации | + | СЗИ от НСД |
| III. Ограничение программной среды (ОПС) | | | |
| ОПС.3 | Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов | + |  |
| IV. Защита машинных носителей информации (ЗНИ) | | | |
| ЗНИ.1 | Учет машинных носителей информации | + | Применение организационных мер |
| ЗНИ.2 | Управление доступом к машинным носителям информации | + | Применение организационных мер |
| ЗНИ.3 | Контроль перемещения машинных носителей информации за пределы контролируемой зоны |  | Применение организационных мер |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) | + | Применение организационных мер |
| V. Регистрация событий безопасности (РСБ) | | | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения | + | Журналирование в СЗИ и применение организационных мер |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации | + | Журналирование в СЗИ и применение организационных мер |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения | + | Журналирование в СЗИ и применение организационных мер |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти | + | Журналирование в СЗИ и применение организационных мер |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них | + | Журналирование в СЗИ и применение организационных мер |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе | + | Журналирование в СЗИ и применение организационных мер |
| РСБ.7 | Защита информации о событиях безопасности | + | Журналирование в СЗИ и применение организационных мер |
| VI. Антивирусная защита (АВЗ) | | | |
| АВЗ.1 | Реализация антивирусной защиты | + | САВЗ |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) | + | САВЗ |
| VIII. Контроль (анализ) защищенности информации (АНЗ) | | | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей | + | Применение организационных мер |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации | + | Применение организационных мер |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации | + | Применение организационных мер |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации | + | Применение организационных мер |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе | + | Применение организационных мер |
| IX. Обеспечение целостности информационной системы и информации (ОЦЛ) | | | |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций | + | Применение организационно-технических мер |
| XII. Защита технических средств (ЗТС) | | | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования | + | Применение организационно-технических мер |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены | + | Применение организационных мер |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр | + | Применение организационно-технических мер |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | | | |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи | + | СКЗИ |
| ЗИС.5 | Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств | + | СКЗИ, |

1. **Реализация мер по обеспечению безопасности персональных данных в ИС.**
   1. Для реализации технических мер по обеспечению безопасности информации в ИС необходимо осуществить выбор, установку и настройку средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, в соответствии с установленным уровнем значимости информации и учетом типа актуальных угроз.
   2. Организационные меры по обеспечению безопасности информации в ИС необходимо реализовать путем утверждения инструкций, регламентирующих функции, задачи и обязанности ответственных лиц и иных пользователей, инструкций, определяющих правила и процедуры управления системой защиты информации информационной системы, выявления инцидентов безопасности обработки информации, осуществления резервного копирования информации, а также определения правил разграничения доступа субъектов доступа к объектам доступа.
   3. Для контроля за соблюдением мер по обеспечению безопасности информации, обрабатываемой в ИС, необходимо разработать документы, определяющие правила и процедуры проведения внутреннего контроля (анализа) защищенности информации.