****

**АДМИНИСТРАЦИЯ**

**БАРСУКОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**МОНАСТЫРЩИНСКОГО РАЙОНА СМОЛЕНСКОЙ ОБЛАСТИ**

**РАСПОРЯЖЕНИЕ**

от 09 октября 2019 года № 27

Об утверждении Положения о порядке использования средств защиты информации в информационных системах Администрации Барсуковского сельского поселения Монастырщинского района Смоленской области

В соответствии с Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом», «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», Постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Администрации Смоленской области от 20.07.2015 г. № 424 «О порядке использования распределительной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления муниципальных образований Смоленской области:

1.Утвердить Положение о порядке использования средств защиты информации в информационных системах Администрации Барсуковского сельского поселения Монастырщинского района Смоленской области согласно Приложению.

2.Контроль за выполнением настоящего распоряжения оставляю за собой. 3.Настоящее распоряжение вступает в силу с момента его подписания.

Глава муниципального образования

Барсуковского сельского поселения

Монастырщинского района

Смоленской области  **Т.В. Попкова**

Приложение

к распоряжению Администрации Барсуковского сельского поселения Монастырщинского района Смоленской области

от 09 октября 2019 года № 27

**Положение**

**о порядке использования средств защиты информации в информационных системах Администрации Барсуковского сельского поселения Монастырщинского района Смоленской области**

**1. Общие положения**

1.1. Настоящее Положение устанавливает организацию и порядок эксплуатации средств защиты информации в информационных системах Администрации Барсуковского сельского поселения Монастырщинского района Смоленской области.

1.2. Положение разработано на основе действующих в Российской Федерации правовых и нормативных документов по защите информации и в соответствии с «Положением о защите информации, обработке и защите персональных данных работников Администрации Барсуковского сельского поселения Монастырщинского района Смоленской области.

1.3. Средства защиты информации (далее – СЗИ) представляет собой комплекс организационных мер и программно-аппаратных средств защиты информации и средств контроля эффективности защиты информации. СЗИ реализуется в процессе создания ИС.

1.4. СЗИ эксплуатируется в рамках эксплуатации ИС. При этом выполняется следующий комплекс эксплуатационных мероприятий:

- осуществление руководства работами по обеспечению защиты информации;

- обеспечение кадровой политики организации в отношении СЗИ;

- выполнение работ по физической защите технических средств;

- техническое обслуживание и ремонт оборудования;

- сопровождение программного обеспечения;

- устранение неисправностей программных и технических средств;

- контроль выполнения установленных нормативными документами требований к эксплуатации СЗИ.

Эксплуатационные мероприятия должны обеспечивать установленный на этапе создания ИС уровень информационной безопасности ИС.

**2. Организация эксплуатации**

2.1. Функции эксплуатирующей организации может выполнять:

- орган местного самоуправления (Администрация Барсуковского сельского поселения Монастырщинского района Смоленской области), являющийся пользователем информационной системы (ИС);

- другая организация, не являющаяся пользователем ИС (привлекаемая, как правило, на конкурсной основе).

2.2. Эксплуатирующая организация осуществляет эксплуатацию ИС и СЗИ в соответствии с нормативной, технической, эксплуатационной документацией и требованиями настоящего Положения.

2.3. Ответственность за обеспечение защиты информации в процессе эксплуатации ИС возлагается на руководителя эксплуатирующей организации, ответственного за организацию работ по защите информации и специалиста по защите информации.

2.4. Ответственность за соблюдение установленных требований по защите информации при ее обработке в ИС возлагается на непосредственных исполнителей (пользователей, операторов, администраторов и обслуживающий персонал).

2.5. За нарушение установленных требований по защите информации руководитель подразделения, отвечающий за эксплуатацию ИС, и/или непосредственный исполнитель привлекаются к административной или уголовной ответственности в соответствии с действующим законодательством.

2.6. Все виды работ, связанные с автоматизированной обработкой информации, проводятся в регламентном режиме или по разовым запросам, непосредственно пользователями или операторами. В организации должны быть установлены порядок и должностные лица, имеющие право подписывать разовые запросы на обработку информации.

2.7. Порядок финансирования эксплуатации ИС определяет ее собственник.

**3. Общие требования по защите информации при эксплуатации средств защиты информации**

3.1. Эксплуатация ИС и средств защиты информации в ее составе должна осуществляться в полном соответствии с утвержденной проектной, организационно-распорядительной и эксплуатационной документацией.

3.2. С целью предотвращения либо существенного затруднения проникновения в здания, помещения посторонних лиц, хищения технических средств, документов и носителей информации должна быть организована физическая защита помещений и собственно технических средств обработки информации с использованием технических средств охраны.

3.3. Должно быть организовано ограничение доступа персонала в помещения, где размещено коммутационное и серверное оборудование.

3.4. На период обработки защищаемой информации в помещениях, где размещаются средства обработки информации, могут находиться только лица, допущенные к обрабатываемой информации в установленном порядке.

Допуск в эти помещения других лиц для проведения необходимых профилактических или ремонтных работ может осуществляться только с санкции руководителя организации или ответственного за организацию работ по защите информации, эксплуатирующего ИС, по согласованию с комиссией по защите информации Администрации Барсуковского сельского поселения Монастырщинского района Смоленской области. При этом должны быть соблюдены меры, исключающие ознакомление этих лиц с конфиденциальной информацией.

Рекомендуется обеспечивать защиту таких помещений соответствующими средствами контроля доступа.

3.5. С целью исключения предоставления избыточных прав доступа к информации в процессе эксплуатации ИС должен осуществляться периодический пересмотр прав доступа пользователей к информации.

3.6. В случае размещения в одном помещении различных технических средств одной или нескольких ИС должен быть исключен несанкционированный просмотр конфиденциальной информации.

3.7. Учет, хранение и обращение с накопителями и носителями информации на бумажной, магнитной, оптической и иной основе должны осуществляться в соответствии с требованиями Руководящих документов ФСТЭК России и в соответствии с выбранным классом защищенности АС.

Обращение с ключевыми документами средств криптографической защиты информации (СКЗИ), в случае их использования, должно осуществляться в соответствии с Положением об использовании средств криптографической защиты информации.

3.8.При увольнении или изменении должностных обязанностей пользователей, операторов, администраторов ИС по согласованию со службой информационной безопасности организации в установленном в организации порядке должны быть приняты меры по оперативному изменению соответствующих паролей и прав доступа.

3.9. Эксплуатация антивирусных средств защиты должна осуществляться в соответствии с разрабатываемой в организации политикой антивирусной защиты, содержащей порядок установки, обновления, использования антивирусных средств защиты, а также меры по восстановлению работоспособности ИС в случае поражения вирусом.

3.10. Резервное копирование (архивирование) баз данных должно осуществляться в соответствии с планом проведения резервного копирования (архивирования), который включает перечень баз данных, подлежащих резервному копированию (архивированию), и график его проведения. Восстановление функционирования ИС и обеспечение доступности информации на требуемом уровне и в требуемые сроки после сбоя или отказа оборудования и/или программного обеспечения должны осуществляться в соответствии с порядком, указанным в эксплуатационной документации. Неисправности должны регистрироваться, анализироваться, и в их отношении должны приниматься соответствующие действия.

3.11. Все пользователи и эксплуатационный персонал ИС должны сообщать специалисту по информационной безопасности о любых наблюдаемых или предполагаемых событиях, связанных с возможными нарушениями и недостатками защиты информации.

3.12. В случае нарушений безопасности при эксплуатации ИС к нарушителям должны применяться соответствующие меры.

3.13. Контроль состояния и эффективности защиты информации осуществляется специалистом по информационной безопасности организации (Администрации Барсуковского сельского поселения Монастырщинского района Смоленской области), государственными и ведомственными органами контроля и заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер, в проверке выполнения норм эффективности защиты информации ограниченного доступа.

**4.Организационное обеспечение эксплуатации**

**системы защиты информации**

4.1. Руководство организации должно поддерживать обеспечение защиты информации в организации с помощью эффективного управления СЗИ, четкого назначения и распределения обязанностей персонала по обеспечению защиты информации. При этом руководство должно проводить регулярную проверку подхода организации к управлению СЗИ и ее реализации (т.е. целей управления, правил, процессов и процедур по обеспечению защиты информации).

4.2. Руководство организации должно рассматривать и утверждать планы по устранению недостатков, выявленных в процессе проведения контроля защищенности ИС.

4.3. Руководство организации должно не реже чем раз в полгода и при возникновении чрезвычайных событий проводить совещания, на которых рассматривать текущее состояние обеспечения защиты информации, причины возникновения нарушений безопасности информации, принимать меры по повышению эффективности СЗИ. Решения совещаний (утвержденные руководством решения, заключения, протоколы) должны доводиться до сведения всего персонала организации и в необходимых случаях до соответствующих исполнителей.

4.4. В договоре найма на работу и/или в должностной инструкции сотрудника организации должны быть определены обязанности по обеспечению безопасности информации при обработке данных организации, а также меры, принимаемые в отношении сотрудника, если он нарушает требования безопасности. При заключении трудового договора сотрудник должен принять обязательства о выполнении оговоренных требований в течение определенного времени после увольнения.

4.5. Сотрудники организации должны быть ознакомлены с требованиями и правилами по обеспечению защиты информации в части, их касающейся.

4.6. Права доступа сотрудников к информации должны изменяться при изменении их должности. После увольнения сотрудника все его права на доступ, к какой - либо информации ИС должны быть аннулированы, все ранее предоставленные сотруднику технические средства и материалы должны быть возвращены.

4.7. В организации должен быть установлен порядок подготовки и переподготовки кадров в области защиты информации.

**5. Обслуживание и ремонт технических средств**

5.1. Обслуживание технических средств ИС, СЗИ (техническое обслуживание) организуется в целях предотвращения неисправностей, обеспечения долговечности компонентов системы.

5.2. При проведении технического обслуживания (ТО) и ремонта необходимо руководствоваться следующими правилами:

- технические средства необходимо обслуживать в соответствии с рекомендуемыми поставщиком периодичностью и инструкциями;

- ТО и ремонт должны проводиться только уполномоченным персоналом;

- необходимо регистрировать информацию обо всех видах ТО, ремонта и всех выявляемых в ходе работ неисправностях, а также об ошибочных сообщениях о неисправностях (когда на самом деле технические средства исправны); регистрационные журналы хранить в установленном порядке;

- на период выполнения ТО должны задействоваться соответствующие меры защиты с учётом выполнения работ персоналом эксплуатирующей или иной организации; где необходимо, конфиденциальная информация должна быть удалена;

- должны соблюдаться все требования, устанавливаемые гарантийными обязательствами поставщика технических средств.

5.3. Для технических средств должно быть предусмотрено проведение следующих видов ТО:

- ежедневное обслуживание;

- ежемесячное обслуживание;

- ежегодное обслуживание.

5.4. Процедура ежедневного ТО включает в себя:

- визуальный осмотр элементов устройств, входящих в состав технических средств (системного блока, монитора, клавиатуры, периферийного оборудования и т.д.);

- очистка поверхности элементов устройств от пыли и грязи;

- проверку состояния соединительных кабелей и разъемов (кабели должны быть уложены аккуратно и без сильных перегибов, а их разъемы надежно соединены с разъемами устройств).

Ежедневное обслуживание технических средств, размещенных на автоматизированных рабочих местах ИС, выполняют пользователи, а других средств – администраторы и обслуживающий персонал ИС.

5.5. Объемы ежемесячного и ежегодного ТО определяются в эксплуатационной документации.

5.6. Ответственность за своевременное и качественное проведение еженедельного и годового ТО, ремонта возлагается на администраторов и обслуживающий персонал.

**6. Сопровождение программного обеспечения**

6.1. Сопровождение программного обеспечения СЗИ (ПО) включает мероприятия по анализу качества, устранению выявленных ошибок, внесению изменений в ПО и документацию, извещение пользователей об изменениях, ведение эталонной версии ПО.

6.2. При сопровождении ПО необходимо руководствоваться следующими правилами:

- проводить работы по сопровождению ПО только силами уполномоченного персонала;

- выполнять требования лицензионных соглашений на использование ПО в соответствии с законодательством в области прав на результаты интеллектуальной деятельности;

- руководствоваться документацией поставщиков при сопровождении общесистемного программного обеспечения, такого, как операционные системы и системы управления базами данных;

- при использовании сертифицированного по требованиям безопасности информации ПО, его настройку осуществлять и поддерживать в соответствии с техническими условиями или формуляром;

- проводить проверки целостности ПО периодически или после устранения неисправностей в порядке, установленном эксплуатационной документацией;

- регистрировать информацию обо всех случаях неисправностей и всех видах профилактических и восстановительных работ, а также об ошибочных сообщениях о неисправностях (когда в действительности ПО функционирует корректно);

- хранить регистрационные журналы в установленном порядке;

- принимать дополнительные меры по исключению несанкционированного доступа к конфиденциальной информации, хранящейся в системе, при участии в сопровождении организаций – соисполнителей работ;

- устанавливать режим изолированной программной среды, исключающей возможность изменения пользователем состава ПО, если это не противоречит эксплуатационной документации;

- пересматривать объем и содержание работ по сопровождению ПОпри изменении состава и настроек программного обеспечения и технических средств СЗИ, а также при изменении требований безопасности информации.

**7. Устранение неисправностей технических средств и программного обеспечения**

7.1. Эксплуатирующая организация обеспечивает анализ, устранение и учет неисправностей технических средств и программного обеспечения СЗИ, принимает соответствующие действия по их предупреждению.

7.2. После выявления неисправности, отказа СЗИ обслуживающим персоналом или специалистами предприятий – поставщиков технических средств (при гарантийном обслуживании) должны выполнятся необходимые работы по восстановлению работоспособности: ремонт (настройка, юстировка, пайка и т.п.), замена составных частей, автономные и комплексные проверки.

**8. Контроль состояния и эффективности средств защиты информации**

8.1. Контроль состояния и эффективности защиты информации ИС в процессе ее эксплуатации осуществляется специалистом по информационной безопасности организации (Администрации Барсуковского сельского поселения Монастырщинского района Смоленской области), государственными и ведомственными органами контроля и заключается в оценке выполнения требований нормативных документов, обоснованности принятых мер, проверке выполнения норм эффективности защиты информации.