АДМИНИСТРАЦИЯ БЕЛЯНИЦКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ

СОНКОВСКОГО РАЙОНА ТВЕРСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

01.12.2020 с.Беляницы №15-ра

О введении в действие организационно-распорядительных

документов по обработке и защите персональных данных

в администрации Беляницкого сельского поселения

Сонковского района Тверской области

В целях обеспечения безопасности персональных данных при их обработке и защите, руководствуясь Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»:

1. Утвердить:
2. Политику информационной безопасности информационных систем персональных данных в АдминистрацииБеляницкого сельского поселенияСонковского района Тверской области (Приложение 1)
3. Места хранения материальных носителей персональных данных в Администрации Беляницкого сельского поселения Сонковского района Тверской области (Приложение 2).
4. Инструкцию по организации антивирусной защиты в АдминистрацииБеляницкого сельского поселения Сонковского района Тверской области (Приложение 3)
5. Инструкцию по организации парольной защиты в Администрации Беляницкого сельского поселенияСонковского района Тверской области (Приложение 4)
6. План внутренних проверок условий обработки персональных данных в АдминистрацииБеляницкого сельского поселенияСонковского района Тверской области (Приложение 5)
7. Список помещений АдминистрацииБеляницкого сельского поселенияСонковского района, в которых обрабатываются персональные данные (Приложение 6)
8. Информационные системы персональных данных в Администрации Беляницкого сельского поселения Сонковского района (Приложение 7)

2. Настоящее распоряжение вступает в силу со дня его подписания и подлежит размещению на сайте АдминистрацииБеляницкого сельского поселенияСонковского района в информационно-телекоммуникационной сети Интернет

Глава администрации

Беляницкого сельского поселения

Сонковского района Тверской областиН.Н.Боченкова

Приложение 1

к распоряжению

Администрации

Беляницкого сельского поселения

Сонковского района Тверской области

от 01.12.2020 № 15-ра

**Политика**

**информационной безопасностиинформационных систем персональных данных**

**в АдминистрацииБеляницкого сельского поселенияСонковскогорайона**

**ОПРЕДЕЛЕНИЯ**

В настоящем документе используются следующие термины и их определения.

**Автоматизированная система** - система, состоящая из персонала и комплексасредств автоматизации его деятельности, реализующая информационную технологиювыполнения установленных функций.

**Аутентификация отправителя данных** - подтверждение того, что отправительполученных данных соответствует заявленному.

**Безопасность персональных данных** - состояние защищенности персональныхданных, характеризуемое способностью пользователей, технических средств иинформационных технологий обеспечить конфиденциальность, целостность идоступность персональных данных при их обработке в информационных системахперсональных данных.

**Биометрические персональные данные** - сведения, которые характеризуютфизиологические особенности человека и на основе которых можно установить еголичность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенностистроения тела и другую подобную информацию.

**Блокирование персональных данных** - временное прекращение сбора,систематизации, накопления, использования, распространения, персональных данных, втом числе их передачи.

**Вирус (компьютерный, программный)** - исполняемый программный код илиинтерпретируемый набор инструкций, обладающий свойствами несанкционированногораспространения и самовоспроизведения. Созданные дубликаты компьютерного вирусане всегда совпадают с оригиналом, но сохраняют способность к дальнейшемураспространению и самовоспроизведению.

**Вредоносная программа** - программа, предназначенная для осуществлениянесанкционированного доступа и (или) воздействия на персональные данные илиресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** - технические средства исистемы, не предназначенные для передачи, обработки и храненияперсональных данных, устанавливаемые совместно с техническими средствами исистемами, предназначенными для обработки персональных данных или в помещениях,в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системыперсональных данных)** - получение возможности запуска на выполнение штатныхкоманд, функций, процедур операционной системы (уничтожения, копирования,перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** - возможность получения информации и ее использования.**Закладочное устройство** - элемент средства съема информации, скрытновнедряемый (закладываемый или вносимый) в места возможного съема информации (втом числе в ограждение, конструкцию, оборудование, предметы интерьера,транспортные средства, а также в технические средства и системы обработкиинформации).

**Защищаемая информация** - информация, являющаяся предметом собственностии подлежащая защите в соответствии с требованиями правовых документовили требованиями, устанавливаемыми собственником информации.

**Идентификация** - присвоение субъектам и объектам доступа идентификатора и(или) сравнение предъявляемого идентификатора с перечнем присвоенныхидентификаторов.

**Информативный сигнал** - электрические сигналы, акустические, электромагнитныеи другие физические поля, по параметрам которых может быть раскрытаконфиденциальная информация (персональные данные) обрабатываемая винформационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** – информационнаясистема, представляющая собой совокупность персональных данных,содержащихся в базе данных, а также информационных технологий и техническихсредств, позволяющих осуществлять обработку таких персональных данных сиспользованием средств автоматизации или без использования таких средств.

**Информационные технологии** - процессы, методы поиска, сбора, хранения,обработки, предоставления, распространения информации и способы осуществлениятаких процессов и методов.

**Использование персональных данных** - действия (операции) с персональнымиданными, совершаемые оператором в целях принятия решений или совершения иныхдействий, порождающих юридические последствия в отношении субъекта персональныхданных или других лиц либо иным образом затрагивающих права и свободы субъектаперсональных данных или других лиц.

**Источник угрозы безопасности информации** - субъект доступа, материальныйобъект или физическое явление, являющиеся причиной возникновения угрозыбезопасности информации.

**Контролируемая зона** - пространство (территория, здание, часть здания,помещение), в котором исключено неконтролируемое пребывание посторонних лиц, атакже транспортных, технических и иных материальных средств.

**Конфиденциальность персональных данных-** обязательное для соблюденияоператором или иным получившим доступ к персональным данным лицом требованиене допускать их распространение без согласия субъекта персональных данных илиналичия иного законного основания.

**Межсетевой экран** - локальное (однокомпонентное) или функционально- нераспределенноепрограммное (программно-аппаратное) средство (комплекс),реализующее контроль за информацией, поступающей в информационную системуперсональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** - физическое лицо,случайно или преднамеренно совершающее действия, следствием которых являетсянарушение безопасности персональных данных при их обработке техническимисредствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** – обработкаперсональных данных, содержащихся в информационной системе персональных данныхлибо извлеченных из такой системы, считается осуществленной без использованиясредств автоматизации (неавтоматизированной), если такие действия с персональнымиданными, как использование, уточнение, распространение, уничтожение персональныхданных в отношении каждого из субъектов персональных данных, осуществляются принепосредственном участии человека.

**Недекларированные возможности** - функциональные возможности средстввычислительной техники, не описанные или не соответствующие описанным вдокументации, при использовании которых возможно нарушение конфиденциальности,доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)-**доступ к информации или действия с информацией, нарушающие правила разграничениядоступа с использованием штатных средств, предоставляемых информационнымисистемами персональных данных.

**Носитель информации** - физическое лицо или материальный объект, в том числефизическое поле, в котором информация находит свое отражение в виде символов,образов, сигналов, технических решений и процессов, количественных характеристикфизических величин.

**Обезличивание персональных данных** - действия, в результате которыхневозможно определить принадлежность персональных данных конкретному субъектуперсональных данных.

**Обработка персональных данных** - действия (операции) с персональнымиданными, включая сбор, систематизацию, накопление, хранение, уточнение(обновление, изменение), использование, распространение (в том числе передачу),обезличивание, блокирование, уничтожение персональных данных.

**Общедоступные персональные данные** - персональные данные, доступнеограниченного круга лиц к которым предоставлен с согласия субъекта персональныхданных или на которые в соответствии с федеральными законами не распространяетсятребование соблюдения конфиденциальности.

**Оператор (персональных данных)** - государственный орган, муниципальныйорган, юридическое или физическое лицо, организующее и (или) осуществляющееобработку персональных данных, а также определяющие цели и содержание обработкиперсональных данных.

**Технические средства информационной системы персональных данных-**

средства вычислительной техники, информационно-вычислительные комплексы и сети,средства и системы передачи, приема и обработки ПДн (средства и системызвукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионныеустройства, средства изготовления, тиражирования документов и другие техническиесредства обработки речевой, графической, видео- и буквенно-цифровой информации),программные средства (операционные системы, системы управления базами данных ит.п.), средства защиты информации, применяемые в информационных системах.

**Перехват (информации)** - неправомерное получение информации с использованиемтехнического средства, осуществляющего обнаружение, прием иобработку информативных сигналов.

**Персональные данные** - любая информация, относящаяся к определенному илиопределяемому на основании такой информации физическому лицу (субъектуперсональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место

рождения, адрес, семейное, социальное, имущественное положение, образование,профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** – электромагнитныеизлучения технических средств обработки защищаемой информации, возникающие какпобочное явление и вызванные электрическими сигналами, действующими в ихэлектрических и магнитных цепях, а также электромагнитные наводки этих сигналов натокопроводящие линии, конструкции и цепи питания.

**Политика «чистого стола»** - комплекс организационных мероприятий,контролирующих отсутствие записывания на бумажные носители ключей и атрибутовдоступа (паролей) и хранения их вблизи объектов доступа.

**Пользователь информационной системы персональных данных** - лицо,участвующее в функционировании информационной системы персональных данных или

использующее результаты ее функционирования.

**Правила разграничения доступа** - совокупность правил, регламентирующихправа доступа субъектов доступа к объектам доступа.

**Программная закладка** - код программы, преднамеренно внесенный впрограмму с целью осуществить утечку, изменить, блокировать, уничтожитьинформацию или уничтожить и модифицировать программное обеспечениеинформационной системы персональных данных и (или) блокировать аппаратныесредства.

**Программное (программно-математическое) воздействие** – несанкционированноевоздействие на ресурсы автоматизированной информационной системы,осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** - умышленное или случайное нарушениеконфиденциальности персональных данных.

**Распространение персональных данных** - действия, направленные на передачуперсональных данных определенному кругу лиц (передача персональных данных) илина ознакомление с персональными данными неограниченного круга лиц, в том числеобнародование персональных данных в средствах массовой информации, размещение в

информационно-телекоммуникационных сетях или предоставление доступа кперсональным данным каким-либо иным способом.

**Ресурс информационной системы** — именованный элемент системного,прикладного или аппаратного обеспечения функционирования информационнойсистемы.

**Специальные категории персональных данных** - персональные данные,касающиеся расовой, национальной принадлежности, политических взглядов,религиозных или философских убеждений, состояния здоровья и интимной жизнисубъекта персональных данных.

**Средства вычислительной техники** - совокупность программных итехнических элементов систем обработки данных, способных функционироватьсамостоятельно или в составе других систем.

**Субъект доступа (субъект)** - лицо или процесс, действия которого регламентируютсяправилами разграничения доступа.

**Технический канал утечки информации** - совокупность носителя информации(средства обработки), физической среды распространения информативного сигнала исредств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных-** передача персональныхданных оператором через Государственную границу Российской Федерации органувласти иностранного государства, физическому или юридическому лицу иностранногогосударства.

**Угрозы безопасности персональных данных** - совокупность условий ифакторов, создающих опасность несанкционированного, в том числе случайного,доступа к персональным данным, результатом которого может стать уничтожение,изменение, блокирование, копирование, распространение персональных данных, а такжеиных несанкционированных действий при их обработке в информационной системеперсональных данных.

**Уничтожение персональных данных** - действия, в результате которыхневозможно восстановить содержание персональных данных в информационной системеперсональных данных или в результате которых уничтожаются материальные носителиперсональных данных.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемоераспространение информации от носителя защищаемой информации черезфизическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость** - слабость в средствах защиты, которую можно использовать длянарушения системы или содержащейся в ней информации.

**Целостность информации** - способность средства вычислительной техники илиавтоматизированной системы обеспечивать неизменность информации в условияхслучайного п/пли преднамеренного искажения (разрушения).

**ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

ABC — антивирусные средства

АРМ - автоматизированное рабочее место

ВТСС - вспомогательные технические средства и системы

ИСПДн - информационная система персональных данных

КЗ - контролируемая зона

ЛВС — локальная вычислительная сеть

МЭ - межсетевой экран

НСД - несанкционированный доступ

ОС - операционная система

ПДн - персональные данные

ПМВ - программно-математическое воздействие

ПО — программное обеспечение

ПЭМИН - побочные электромагнитные излучения и наводки САЗ — система

анализа защищенности СЗИ — средства защиты информации

СЗПДн — система (подсистема) защиты персональных данных СОВ — система

обнаружения вторжений ТКУИ - технические каналы утечки информации УБПДн -

угрозы безопасности персональных данных

**ВВЕДЕНИЕ**

Настоящая Политика информационной безопасности ИСПДнАдминистрацииБеляницкого сельского поселенияСонковского района (Далее - Администрации) являетсяофициальным документом, в котором определена система взглядов на обеспечениеинформационной безопасности Администрации.

Настоящая Политика определяет основные цели и задачи, а также стратегиюпостроения системы защиты персональных данных (СЗПДн) Администрации. Политикаопределяет основные требования и подходы к их реализации, для достижениятребуемого уровня безопасности информации.

Политика разработана в соответствии с системным подходом к обеспечениюинформационной безопасности. Системный подход предполагает проведение комплекса

мероприятий, включающих исследование угроз информационной безопасности иразработку системы защиты ПДн, с позиции комплексного применения технических иорганизационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенностьперсональных данных и обрабатывающей их инфраструктуре от любых случайных илизлонамеренных воздействий, результатом которых может явиться нанесение ущербасамой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачиинформационной безопасности сводятся к минимизации ущерба от возможнойреализации угроз безопасности ПДн, а также к прогнозированию и предотвращениютаких воздействий.

Политика является методологической основой для:

- принятия управленческих решений и разработки практических мер повоплощению политики безопасности ПДн и выработки комплекса согласованных мернормативно-правового, технологического и организационно-технического характера,направленных на выявление, отражение и ликвидацию последствий реализацииразличных видов угроз ПДн;

- координации деятельности структурных подразделений Администрации припроведении работ по развитию и эксплуатации ИСПДн с соблюдением требованийобеспечения безопасности ПДн;

- разработки предложений по совершенствованию правового, нормативного,методического, технического и организационного обеспечения безопасности ПДн вИСПДн Администрации.

Правовой базой для разработки настоящей Политики служат требованиядействующих в России законодательных и нормативных документов по обеспечениюбезопасности персональных данных (ПДн).

**1. Общие положения**

СЗПДн представляет собой совокупность организационных и техническихмероприятий для защиты ПДн от неправомерного или случайного доступа к ним,уничтожения, изменения, блокирования, копирования, распространения ПДн, а такжеиных неправомерных действий с ними.

Безопасность персональных данных достигается путем исключения несанкционированного,в том числе случайного, доступа к персональным данным,результатом которого может стать уничтожение, изменение, блокирование, копирование,

распространение персональных данных, а также иных несанкционированныхдействий.

Структура, состав и основные функции СЗПДн определяются исходя из классаИСПДн. СЗПДн может включает организационные меры и технические средства защиты

информации (в том числе шифровальные (криптографические) средства, средствапредотвращения несанкционированного доступа, утечки информации по техническимканалам, программно-технических воздействий на технические средства обработкиПДн), а также используемые в информационной системе информационные технологии.

Эти меры призваны обеспечить:

- **конфиденциальность** информации (защита от несанкционированногоознакомления);

- **целостность** информации (актуальность и непротиворечивость информации,ее защищенность от разрушения и несанкционированного изменения);

- **доступность** информации (возможность за приемлемое время получитьтребуемую информационную услугу).

Стадии создания СЗПДн включают:

- предпроектная стадия, включающая предпроектное обследование ИСПДн,определение требований к СЗПДн;

- стадия проектирования, определяющая встраивание СЗПДн в составе ИСПДн;

- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию иприемо-сдаточные испытания средств защиты информации, а также оценку соответствияИСПДн требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базыбезопасности ПДн и разработку (введение в действие) следующих организационно-распорядительныхдокументов:

- План мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;

- План мероприятий по контролю обеспечения защиты ПДн;

- Порядок резервирования и восстановления работоспособности ТС и ПО, базданных и СЗИ;

- Должностная инструкция сотрудников в части обеспечения безопасностиПДн при их обработке в ИСПДн;

- Инструкция на случай возникновения внештатной ситуации;

- Регламента доступа в помещения ИСПДн;

Технические меры защиты реализуются при помощи соответствующихпрограммно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатампредпроектного обследования ИСПДн Администрации.

**2. Цели СЗПДн**

Целями СЗПДн являются минимизация вероятности реализации угрозбезопасности ПДн и минимизация ущерба в случае реализации угрозы безопасностиПДн.

Для достижения своих целей система безопасности СЗПДн должна обеспечиватьадекватное решение следующих задач:

- защиты от вмешательства в процесс функционирования ИСПДн постороннихлиц (возможность использования АС и доступ к ее ресурсам должны иметь толькозарегистрированные установленным порядком пользователи);

- разграничения доступа зарегистрированных пользователей к аппаратным,программным и информационным ресурсам ИСПДн, то есть защиту отнесанкционированного доступа:

а) к информации, циркулирующей в ИСПДн;

б) средствам вычислительной техники ИСПДн;

в) аппаратным, программным и криптографическим средствам защиты,

используемым в ИСПДн;

- регистрации действий пользователей при использовании защищаемыхресурсов ИСПДн;

- контроля целостности (обеспечение неизменности) ИСПДн и ее восстановлениев случае нарушения;

- защиты от программно-математического воздействия;

- защиты ПДн от утечки по техническим каналам при ее обработке, хранении ипередаче по каналам связи;

- защиты ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, отнесанкционированного разглашения или искажения;

- своевременного выявления источников угроз безопасности ПДн, причин иусловий, способствующих нанесению ущерба субъектам ПДн, создание механизмаоперативного реагирования на угрозы безопасности ПДн и негативные тенденции;

- своевременного обнаружения попыток нарушения безопасности ПДн;

- создания условий для минимизации и локализации наносимого ущерба

неправомерными действиями физических и юридических лиц, ослабление негативного

влияния и ликвидация последствий нарушения безопасности ПДн.

**3. Объекты защиты**

Объектами защиты являются - информация, обрабатываемая в ИСПДн, итехнические средства ее обработки и защиты.

Объекты защиты включают:

1) Обрабатываемая информация.

2) Технологическая информация.

3) Программно-технические средства обработки.

4) Средства защиты ПДн.

5) Каналы информационного обмена и телекоммуникации.

6) Объекты и помещения, в которых размещены компоненты ИСПДн.

Конкретный перечень объектов защиты определяется при проведении предпроектного

обследования ИСПДн и при проведении периодических проверок.

**4. Классификация пользователей ИСПДн**

Пользователем ИСПДн является лицо, участвующее в функционированииинформационной системы персональных данных или использующее результаты еефункционирования. Пользователем ИСПДн является любой сотрудник Администрации(либо сотрудник сторонней организации), имеющий доступ к ИСПДн и ее ресурсам всоответствии с установленным порядком, в соответствии с его функциональнымиобязанностями.

Пользователи ИСПДн делятся следующие категории:

**1) Администратор ИСПДн.** Сотрудники Администрации, которые занимаютсянастройкой, внедрением и сопровождением ИСПДн, в т.ч. телекоммуникационнойподсистемы. Обеспечивает функционирование подсистемы управления доступомИСПДн и уполномочен осуществлять предоставление и разграничение доступаконечного пользователя (Оператора АРМ) к элементам, хранящим персональныеданные.Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном

обеспечении ИСПДн;

- обладает полной информацией о технических средствах и конфигурацииИСПДн;

- имеет доступ ко всем техническим средствам обработки информации иданным ИСПДн;

- обладает правами конфигурирования и административной настройкитехнических средств ИСПДн.

**2) Администратор безопасности.** Сотрудник Администрации, ответственныйза функционирование СЗПДн, включая обслуживание и настройку административной,серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;

- обладает полной информацией об ИСПДн;

- имеет доступ к средствам защиты информации и протоколирования и к частиключевых элементов ИСПДн.

Администратор безопасности уполномочен:

- реализовывать политики безопасности в соответствии с которыми пользователь(Оператор АРМ) получает возможность работать с элементами ИСПДн;

- осуществлять аудит средств защиты;

- устанавливать доверительные отношения своей защищенной сети с сетямидругих Организаций.

**3) Оператор ИСПДн (Оператор АРМ).** Сотрудник Администрации,осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотраПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов поинформации, полученной из ИСПД. Оператор не имеет полномочий для управленияподсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающимидоступ к некоторому подмножеству ПДн;

- располагает конфиденциальными данными, к которым имеет доступ.

**4) Технический специалист по обслуживанию периферийного оборудования.**

Сотрудник Администрации (или сторонней организации), осуществляетобслуживание и настройку периферийного оборудования ИСПДн. Техническийспециалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий дляуправления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнемдоступа и знаний:

- обладает частью информации о системном и прикладном программномобеспечении ИСПДн;

- обладает частью информации о технических средствах и конфигурацииИСПДн;

- не имеет атрибутов доступа к ИСПДн.

**5) Программист-разработчик (поставщик).** Сотрудник Администрации (илисторонней организации), осуществляет разработку и/или поставку прикладногопрограммного обеспечения, обеспечивает его сопровождение на защищаемом объекте. Кданной группе могут относиться как сотрудники Администрации, так и сотрудникисторонних организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информациина ИСПДн;

- обладает возможностями внесения ошибок, недекларированных возможностей,программных закладок, вредоносных программ в программное обеспечениеИСПДн на стадии ее разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн итехнических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн;

- не имеет атрибутов доступа к ИСПДн.

Категории пользователей должны быть определены для каждой ИСПДн, послечего определяются права доступа к элементам ИСПДн для всех групп пользователей иотражаются в матрице доступа в "Положении о разграничении прав доступа кобрабатываемым персональным данным".

**5. Физические меры защиты**

Физические меры защиты основаны на применении разного рода механических,электро- или электронно-механических устройств и сооружений, специальнопредназначенных для создания физических препятствий на возможных путяхпроникновения и доступа потенциальных нарушителей к компонентам системы изащищаемой информации, а также технических средств визуального наблюдения, связии охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизациидолжна осуществляться путем установления соответствующих постов охраны, спомощью технических средств охраны или любыми другими способами,предотвращающими или существенно затрудняющими проникновение в здание,помещения посторонних лиц, хищение информационных носителей, самих средствинформатизации, исключающими нахождение внутри контролируемой (охраняемой)зоны технических средств разведки.

**5.1 Физическая защита аппаратных средств ИСПДн**

Успешное применение технических средств защиты предполагает, чтовыполнение перечисленных ниже требований обеспечено организационными(административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;

- в ИСПДн Администрации разработка и отладка программ осуществляется запределами ИСПДн, на испытательных стендах;

- все изменения конфигурации технических и программных средств ИСПДнпроизводятся строго установленным порядком (регистрируются и контролируются)только на основании распоряжений руководства Администрации;

- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.)располагается в местах, недоступных для посторонних.

**6 Контроль эффективности системы защиты ИСПДн Администрации**

Контроль эффективности СЗПДн должен осуществляется на периодическойоснове. Целью контроля эффективности является своевременное выявлениененадлежащих режимов работы СЗПДн (отключение средств защиты, нарушениережимов защиты, несанкционированное изменение режима защиты и т.п.), а такпрогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться как администраторами безопасности ИСПДн(оперативный контроль в процессе информационного взаимодействия в ИСПДн) так ипривлекаемыми для этой цели компетентными организациями, имеющими лицензию наэтот вид деятельности, а также ФСТЭК России и ФСБ России в пределах ихкомпетенции.

Контроль может осуществляться администратором безопасности как с помощьюштатных средств системы защиты ПДн, так и с помощью специальных программныхсредств контроля.

Оценка эффективности мер защиты ПДн проводится с использованиемтехнических и программных средств контроля на предмет соответствия установленнымтребованиям.

**7. Сферы ответственности за безопасность ПДн**

Ответственным за разработку мер и контроль над обеспечением безопасностиперсональных данных является руководитель Администрации. Руководитель можетделегировать часть полномочий по обеспечению безопасности персональных данных.Сфера ответственности руководителя включает следующие направленияобеспечения безопасности ПДн:

1. Планирование и реализация мер по обеспечению безопасности ПДн;

2. Анализ угроз безопасности ПДн;

3. Разработку, внедрение, контроль исполнения и поддержание в актуальномсостоянии политик, руководств, концепций, процедур, регламентов, инструкций идругих организационных документов по обеспечению безопасности;

4. Контроль защищенности ИТ инфраструктуры Администрации от угроз ИБ;

5. Обучение и информирование пользователей ИСПДн, о порядке работы с ПДни средствами защиты;

6. Предотвращение, выявление, реагирование и расследование нарушенийбезопасности ПДн.

При взаимодействии со сторонними организациями в случаях, когда сотрудникамэтих организаций предоставляется доступ к объектам защиты, с этими организациямидолжно быть заключено «Соглашение о конфиденциальности», либо «Соглашение особлюдении режима безопасности ПДн при выполнении работ в ИСПДн». Подготовкатиповых вариантов этих соглашений осуществляется совместно с Юридическимотделом.

**8. Модель нарушителя безопасности**

Под нарушителем в Администрации понимается лицо, которое в результатеумышленных или неумышленных действий может нанести ущерб объектам защиты.Нарушители подразделяются по признаку принадлежности к ИСПДн. Всенарушители делятся на две группы:

• внешние нарушители - физические лица, не имеющие права пребывания натерритории контролируемой зоны, в пределах которой размещается оборудованиеИСПДн;

• внутренние нарушители - физические лица, имеющие право пребывания натерритории контролируемой зоны, в пределах которой размещается оборудованиеИСПДн.Классификация нарушителей представлена в Модели угроз безопасностиперсональных данных каждой ИСПДн.

**9. Модель угроз безопасности**

Для ИСПДн Администрации выделяются следующие основные категории угрозбезопасности персональных данных:

1. Угрозы от утечки по техническим каналам.

2. Угрозы несанкционированного доступа к информации:

3. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителейинформации путем физического доступа к элементам ИСПДн.

4. Угрозы хищения, несанкционированной модификации или блокированияинформации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математическихвоздействий).

5. Угрозы не преднамеренных действий пользователей и нарушенийбезопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев впрограммном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-заненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров,наводнений и т.п.) характера.

6. Угрозы преднамеренных действий внутренних нарушителей.

7. Угрозы несанкционированного доступа по каналам связи. Описание угроз,вероятность их реализации, опасность и актуальность

8. Представлены в Модели угроз безопасности персональных данных каждойИСПДн.

**10. Требования к персоналу**

Все сотрудники Администрации, являющиеся пользователями ИСПДн, должнычетко знать и строго выполнять установленные правила и обязанности по доступу кзащищаемым объектам и соблюдению принятого режима безопасности ПДн.При вступлении в должность нового сотрудника глава администрации обязана организовать его ознакомление сдолжностной инструкцией и необходимыми документами, регламентирующимитребования по защите ПДн, а также обучение навыкам выполнения процедур,необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики,принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники Администрации, использующие технические средства аутентификации,должны обеспечивать сохранность идентификаторов (электронных ключей)и не допускать НСД к ним, а так же возможность их утери или использования третьимилицами. Пользователи несут персональную ответственность за сохранностьидентификаторов.

Сотрудники Администрации должны следовать установленным процедурамподдержания режима безопасности ПДн при выборе и использовании паролей.

Сотрудники Администрации должны обеспечивать надлежащую защитуоборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещениеимеют доступ посторонние лица. Все пользователи должны знать требования побезопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, атакже свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение,подключать личные мобильные устройства и носители информации, а так же записывать

на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая сталаим известна при работе с информационными системами Администрации, третьим лицам.При работе с ПДн в ИСПДн сотрудники Администрации обязаны обеспечитьотсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ с помощью блокировки ключом или эквивалентного средства контроля,например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Администрации должны быть проинформированы об угрозахнарушения режима безопасности ПДн и ответственности за его нарушение. Они должныбыть ознакомлены с утвержденной формальной процедурой наложения дисциплинарныхвзысканий на сотрудников, которые нарушили принятые политику и процедурыбезопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых илиподозрительных случаях работы ИСПДн, могущих повлечь за собой угрозыбезопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасностьПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование наугрозы безопасности ПДн.

**10.1 Ответственность персонала**

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требованийданного Федерального закона, несут гражданскую, уголовную, административную,дисциплинарную и иную предусмотренную законодательством Российской Федерацииответственность.

Действующее законодательство РФ позволяет предъявлять требования пообеспечению безопасной работы с защищаемой информацией и предусматриваетответственность за нарушение установленных правил эксплуатации ЭВМ и систем,неправомерный доступ к информации, если эти действия привели куничтожению, блокированию, модификации информации или нарушению работыЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администратор ИСПДн и администратор безопасности несут ответственность завсе действия, совершенные от имени их учетных записей или системных учетныхзаписей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Администрации - пользователей ИСПДн правил,связанных с безопасностью ПДн, они несут ответственность, установленнуюдействующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информациидолжны быть отражены в Положениях Администрации,осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудниковАдминистрации.

Необходимо внести в Положения Администрации,осуществляющих обработку ПДн в ИСПДнсведения об ответственности сотрудников за разглашение и несанкционированную модификацию(искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

**11 . Технические средства защиты ПДн**

СЗПДн включает в себя следующие подсистемы:

1. Управления доступом, регистрации и учета;

2. Обеспечения целостности и доступности;

3. Антивирусной защиты;

4. Межсетевого экранирования;

5. Анализа защищенности;

6. Обнаружения вторжений;

7. Криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от классаИСПДн, определенного в Акте классификации информационной системы персональныхданных. Необходимость использования функций подсистем СЗПДн определяется длякаждой ИСПДн исходя из её класса и модели угроз.

Все используемые в ИСПДн технические решения, реализующие функционалподсистем СЗПДн должны пройти в установленном порядке процедуру оценкисоответствия (сертификацию).

**11.1 Подсистемы управления доступом, регистрации и учета**

Подсистема управления доступом, регистрации и учета предназначена дляреализации следующих функций:

1. Идентификации и проверка подлинности субъектов доступа при входе вИСПДн; ‘

2. Идентификации терминалов, узлов сети, каналов связи, внешних устройств пологическим именам;

3. Идентификации программ, томов, каталогов, файлов, записей, полей записейпо именам;

4. Регистрации входа (выхода) субъектов доступа в систему (из системы), либорегистрация загрузки и инициализации операционной системы и ее останова.

5. Регистрации попыток доступа программных средств (программ, процессов,задач, заданий) к защищаемым файлам;

6. Регистрации попыток доступа программных средств к терминалам, каналамсвязи, программам, томам, каталогам, файлам, записям, полям записей.

Функционал подсистемы может быть реализован программными и программно-аппаратнымисредствами.

**11.2 Подсистема обеспечения целостности и доступности**

Подсистема обеспечения целостности и доступности предназначена дляобеспечения целостности и доступности ПДн, программных и аппаратных средствИСПДн Администрации, а так же средств защиты, при случайной или намеренноймодификации.

Подсистема реализуется с помощью организации резервного копирования

обрабатываемых данных, резервированием ключевых элементов ИСПДн и использованиемпрограммных либо программно-аппаратных средств контроляцелостности.

**11.3 Подсистема антивирусной защиты**

Подсистема антивирусной защиты предназначена для обеспечения антивируснойзащиты серверов и АРМ пользователей ИСПДн Администрации.

Средства антивирусной защиты предназначены для реализации следующихфункций:

1. Резидентный антивирусный мониторинг;

2. Антивирусное сканирование;

3. Скрипт-блокирование;

4. Централизованную/удаленную установку/деинсталляцию антивирусногопродукта, настройку, администрирование, просмотр отчетов и статистическойинформации по работе продукта;

5. Автоматизированное обновление антивирусных баз;

6. Ограничение прав пользователя на остановку исполняемых задач и изменениянастроек антивирусного программного обеспечения;

7. Автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусногопрограммного обеспечения на все элементы ИСПДн.

**11.4 Подсистема межсетевого экранирования**

Подсистема межсетевого экранирования предназначена для реализацииследующих функций:

1. Фильтрации открытого и зашифрованного (закрытого) ГР-трафика последующим параметрам;

2. Фиксации во внутренних журналах информации о проходящем открытом изакрытом 1Р-трафике;

3. Идентификации и аутентификацию администратора межсетевого экрана приего локальных запросах на доступ;

4. Регистрации входа (выхода) администратора межсетевого экрана в систему(из системы) либо загрузки и инициализации системы и ее программного останова;

5. Контроля целостности своей программной и информационной части;

6. Фильтрации пакетов служебных протоколов, служащих для диагностики иуправления работой сетевых устройств;

7. Фильтрации с учетом входного и выходного сетевого интерфейса каксредство проверки подлинности сетевых адресов;

8. Регистрации и учета запрашиваемых сервисов прикладного уровня;

9. Блокирования доступа неидентифицированного объекта или субъекта,подлинность которого при аутентификации не подтвердилась, методами, устойчивыми кперехвату;

10. Контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексовмежсетевого экранирования на границе ЛВС либо на каждом АРМ ИСПДн.

**11.5 Подсистема анализа защищенности**

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей,связанных с ошибками в конфигурации ПО ИСПДн, которые могут бытьиспользованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратнымисредствами.

**11.6 Подсистема обнаружения вторжений**

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевыхатак на элементы ИСПДн подключенные к сетям общего пользования и (или)международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратнымисредствами.

**11.7 Подсистема криптографической защиты**

Подсистема криптографической защиты предназначена для исключения НСД кзащищаемой информации в ИСПДн Администрации, при ее передачи по каналам связисетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрения криптографических программно-аппаратныхкомплексов.

Приложение 2

к распоряжению

Администрации

Беляницкого сельского поселения

Сонковского района Тверской области

от 01.12.2020 № 15-ра

**СПИСОК МЕСТ**

**хранения материальных носителей персональных данных**

**в Администрации Беляницкого сельского поселения**

**Сонковского района Тверской области**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Носитель персональных данных** | **Должность допущенного должностного лица** | **Место расположения** |
| **1** | **2** | **3** | **4** |
| *1* | *Личные дела сотрудников* | *Глава администрации, главный специалист, ответственный за организацию обработки персональных данных* | *Металлический шкаф в кабинете главы администрации* |
| *2* | *Трудовые книжки сотрудников* | *Глава администрации, главный специалист, ответственный за организацию обработки персональных данных* | *Сейф в кабинете главы администрации* |
| *3* | *Карточки служащих* | *Глава администрации, главный специалист, ответственный за организацию обработки персональных данных* | *Металлический шкаф в кабинете главы администрации* |
| *4* | *Личные дела кадрового резерва* | *Глава администрации, главный специалист, ответственный за организацию обработки персональных данных* | *Металлический шкаф в кабинете главы администрации* |
| *5* | *Документы по аттестации* | *Глава администрации, главный специалист, ответственный за организацию обработки персональных данных* | *Металлический шкаф в кабинете главы администрации* |
| *6* | *Документы по стажу* | *Глава администрации, главный специалист, ответственный за организацию обработки персональных данных* | *Металлический шкаф в кабинете главы администрации* |
| *7* | *МНПА* | *Глава администрации, главный специалист, ответственный за организацию обработки персональных данных* | *Металлический шкаф в кабинете главы администрации* |

Приложение 3

к распоряжению

Администрации

Беляницкого сельского поселения

Сонковского района Тверской области

от 01.12.2020 № 15-ра

**ИНСТРУКЦИЯ**

**по организации антивирусной защиты**

**в Администрации Беляницкого сельского поселения**

**Сонковского района Тверской области**

1. Общие положения
   1. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в Администрации (далее - Администрация) и предотвращения возникновения фактов заражения вредоносным программным обеспечением.
   2. Данная Инструкция распространяется на всех пользователей информационных систем персональных данных (далее – ИСПДн) в Администрации
2. Установка и обновление антивирусных средств
   1. Установка и настройка антивирусных средств осуществляется только ведущим инженером-программистом Администрации
   2. Обновление антивирусных баз осуществляется по расписанию в автоматическом режиме, либо вручную при необходимости.
3. Требования к проведению мероприятий по антивирусной защите
   1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, flash дисках, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).
   2. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие заражения вредоносным программным обеспечением.
   3. Контроль информации на съёмных носителях производится непосредственно перед её использованием.
   4. Особое внимание следует обратить на недопустимость использования съёмных носителей, принадлежащих лицам, временно допущенным к работе на ЭВМ. Работа этих лиц должна проводиться под непосредственным контролем сотрудника или ответственного за информационную безопасность.
   5. Ежедневно, в начале работы, должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех загружаемых в память файлов персонального компьютера.
   6. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю.
   7. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

* Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.
* 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.).

1. Действия сотрудников при обнаружении компьютерного вируса
   1. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи обязаны:

* приостановить работу;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов Администратора информационной системы персональных данных;
* провести лечение или уничтожение зараженных файлов.
  1. При возникновении подозрения на наличие компьютерного вируса пользователь или Администратор информационной системы персональных данных должны провести внеочередной антивирусный контроль.

1. Ответственность при организации антивирусной защиты
   1. Ответственность за организацию антивирусной защиты возлагается на ведущего инженера-программиста Администрации
   2. Ответственность за выполнение требований данной Инструкции возлагается на Пользователей и на ведущего инженера-программиста Администрации
   3. Периодический контроль за соблюдением положений данной Инструкции возлагается на ведущего инженера-программиста Администрации

**Лист ознакомления**

**с Инструкцией****по организации антивирусной защиты**

**в Администрации Беляницкого сельского поселения**

**Сонковского района Тверской области**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Фамилия, имя, отчество работника** | **Дата ознакомления**  **с Инструкцией** | **Подпись работника** |
|  |  |  |  |
|  |  |  |  |

Приложение 4

к распоряжению

Администрации

Беляницкого сельского поселения

Сонковского района Тверской области

от 01.12.2020 № 15-ра

**Инструкция по организации парольной защиты**

**в информационной системе персональных данных**

1. **Общие положения**

Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы персональных данных в АдминистрацииБеляницкого сельского поселения Сонковского района Тверской области (далее – Администрация). Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системы персональных данных, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

* **Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
* **ИСПДн –** информационная система персональных данных.
* **Компрометация**- факт доступа постороннего лица к защищаемой информации, а также подозрение на него.
* **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.
* **Пароль** – уникальный признак субъекта доступа, который является его (субъекта) секретом.
* **Правила доступа** - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
* **Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.
* **Несанкционированный доступ** - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

1. **Правила генерации паролей**
   1. Персональные пароли должны генерироваться специальными программными средствами административной службы.
   2. Длина пароля должна быть не менее 6 символов.
   3. В составе пароля рекомендуется использовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.
   4. Пароль не должен включать в себя:

* легко вычисляемые сочетания символов;
* клавиатурные последовательности символов и знаков;
* общепринятые сокращения;
* аббревиатуры;
* номера телефонов, автомобилей;
* прочие сочетания букв и знаков, ассоциируемые с пользователем;
* при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.
  1. Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

**Порядок смены паролей**

* 1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в три месяца.
  2. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной зашитой.
  3. Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.
  4. В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

1. **Обязанности пользователей при работе с парольной защитой**
   1. При работе с парольной защитой пользователям запрещается:

* разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
* предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн посторонним лицам;
* записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах к которым могут иметь свободный доступ иные лица.
  1. При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

1. **Случаи компрометации паролей**
   1. Под компрометацией следует понимать:

* физическая утеря носителя с информацией;
* передача идентификационной информации по открытым каналам связи;
* проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
* визуальный осмотр носителя идентификационной информации посторонним лицом;
* перехват пароля при распределении идентификаторов;
* сознательная передача информации постороннему лицу.
  1. Действия при компрометации пароля:
* скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
* о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

1. **Ответственность пользователей при работе с парольной защитой**
   1. Повседневный контроль за действиями сотрудников Администрации при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
   2. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
   3. Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
   4. Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

**Лист ознакомления**

**с Инструкциейпо организации парольной защиты**

**в АдминистрацииБеляницкого сельского поселения**

**Сонковского района Тверской области**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Фамилия, имя, отчество работника** | **Дата ознакомления**  **с Инструкцией** | **Подпись работника** |
|  |  |  |  |
|  |  |  |  |

Приложение 5

к распоряжению

Администрации

Беляницкого сельского поселения

Сонковского района Тверской области

от 01.12.2020 № 15-ра

ПЛАН

внутренних проверок условий обработки персональных данных

в Администрации Беляницкого сельского поселения

Сонковского района Тверской области

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Тема проверки | Нормативный документ, предъявляющий требования | Срок  проведения | Исполнитель |
| 1. | Соответствие  полномочий  пользователя  правилам обработки  персональных  данных | Правила обработки персональных данных  Политика Администрации  в отношении обработки персональных данных | ежегодно | Ответственный  за организацию обработки персональных данных |
| 2. | Соблюдение  пользователями  информационных  систем  персональных данных парольной политики | Положение по защите персональных данных Администрации, обрабатываемых в ИСПДн | еженедельно | Ответственный  за организацию обработки персональных данных |
| 3. | Соблюдение  пользователями  информационных  систем  персональных данных  антивирусной  политики | еженедельно | Ответственный  за организацию обработки персональных данных |
| 4. | Соблюдение порядка доступа в помещения, где  расположены элементы  информационных  систем персональных  данных | Правила обработки персональных данных | ежегодно | Ответственный  за организацию обработки персональных данных |
| 5. | Соблюдение  порядка  резервирования баз данных и хранения резервных копий | Положение по защите персональных данных Администрации, обрабатываемых в ИСПДн | еженедельно | Ответственный  за организацию обработки персональных данных |
| 6. | Соблюдение порядка работы со средствами защиты информации | ежегодно | Ответственный  за организацию обработки персональных данных |
| 7. | Знание  пользователей  информационных  систем  персональных | ежегодно | Ответственный  за организацию обработки персональных данных |
| 8. | Хранение бумажных носителей с персональными данными | Положение по защите персональных данных Администрации, обрабатываемых без использования средств автоматизации | ежегодно | Ответственный за организацию обработки персональных данных |
| 9. | Доступ к бумажным носителям с персональными данными | ежегодно | Ответственный за организацию обработки персональных данных |
| 10. | Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными | Положение по защите персональных данных Администрации, обрабатываемых без использования средств автоматизации | ежегодно | Ответственный за организацию обработки персональных данных |

Приложение 6

к распоряжению

администрации

Беляницкого сельского поселения

Сонковского района Тверской области

от 01.12.2020 № 15-ра

**СПИСОК ПОМЕЩЕНИЙ**

**Администрации Беляницкого сельского поселения**

**Сонковского района, в которых обрабатываются персональные данные**

1. Для хранения бумажных документов предназначены кабинеты, в здании АдминистрацииБеляницкого сельского поселения Сонковского района по адресу: Тверская область Сонковский район с.Беляницыул.Школьная д.1

- Кабинет главы администрации;

- Кабинет хранилища архива;

1.1. Для размещения автоматизированных рабочих мест (АРМ) информационных систем персональных данных (ИСПДн) предназначены:

- Кабинет главы администрации.