|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Генеральный директор  ООО «ВЛАДЕЛЕЦ ИСПДН»  \_\_\_\_\_\_\_\_\_\_\_\_  М.П. |

**ПОЛОЖЕНИЕ**

**по защите персональных данных в информационной системе персональных данных «ВЛАДЕЛЕЦ ИСПДН»**

**ООО «ВЛАДЕЛЕЦ ИСПДН»**

**2024**

1. **Общие положения**

1.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных, при их обработке в информационной системе персональных данных «ВЛАДЕЛЕЦ ИСПДН» ООО «ВЛАДЕЛЕЦ ИСПДН» (далее ИСПДн «ВЛАДЕЛЕЦ ИСПДН») (далее - Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 № 152-ФЗ "О персональных данных", Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» п приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,

1.2. Цель разработки настоящего Положения - установление порядка организации и проведения работ по обеспечению безопасности персональных данных (далее - защищаемая информация, информация), в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» на всех стадиях (этапах) создания информационной системы (ИС), в ходе ее эксплуатации и вывода из эксплуатации.

1.3. К защищаемой информации относятся персональные данные, обрабатываемые в ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

**2. Порядок организации и проведения работ по обеспечению безопасности информации**

2.1. Под организацией обеспечения безопасности защищаемой информации при ее обработке в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности защищаемой информации, реализуемых в рамках создаваемой системы защиты персональных данных (далее - СЗПДн).

2.2. СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности защищаемой информации для уровня защиты 3 (УЗ 3) и информационных технологий, используемых в ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

2.3. Безопасность защищаемой информации при ее обработке в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» обеспечивает лицо, осуществляющее обработку защищаемой информации.

2.4. Защита информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», обеспечивается путем выполнения требований к организации защиты информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», и требований к мерам защиты информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

2.5. Для обеспечения безопасности защищаемой информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», назначается должностное лицо (работник), ответственное за обеспечение безопасности конфиденциальной информации, в том числе персональных данных (далее – Ответственный).

2.6. Назначается лицо, ответственное за организацию обработки защищаемой информации.

2.7. Для проведения работ по защите информации в ходе создания, эксплуатации и вывода из эксплуатации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

2.8. Для обеспечения защиты информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

2.9. Защита информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», является составной частью работ по созданию и эксплуатации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках СЗПДн.

2.10. Организационные и технические меры защиты информации, реализуемые в рамках СЗПДн, должны быть направлены на защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2.11. Для обеспечения защиты информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в ИСПДн;

- разработка СЗПДн;

- внедрение СЗПДн:

- обеспечение защиты информации в ходе эксплуатации ИСПДн;

- обеспечение защиты информации при выводе из эксплуатации, ИСПДн или после принятия решения об окончании обработки информации.

**3.****Формирование требований к защите информации, содержащейся в информационной системе**

3.1. Формирование требований к защите информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», осуществляется в соответствии с установленным уровнем защищенности при их обработке в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и требованиями действующего законодательства в сфере обеспечения безопасности персональных данных.

3.2. Формирование требований к защите информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», включает:

- принятие решения о необходимости защиты информации, содержащейся в ИСПДн;

- определение уровня защищенности ИСПДн по требованиям защиты информации;

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

- определение требований к СЗПДн.

3.3. При принятии решения о необходимости защиты информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», осуществляется:

- анализ целей создания ИСПДн и задач, решаемых этой ИСПДн;

- определение информации, подлежащей обработке в ИСПДн;

- анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать ИСПДн;

- принятие решения о необходимости создания СЗПДн, а также определение целей и задач защиты информации в ИСПДн, основных этапов создания СЗПДн и функций по обеспечению защиты информации, содержащейся в ИСПДн.

3.4. Результаты определения уровня защищённости ИСПДн «ВЛАДЕЛЕЦ ИСПДН» оформляются актом определения уровня защищенности.

3.5. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ИСПДн «ВЛАДЕЛЕЦ ИСПДН», возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

3.6. В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России.

3.7. При определении угроз безопасности информации учитываются структурно-функциональные характеристики ИСПДн «ВЛАДЕЛЕЦ ИСПДН», включающие структуру и состав ИСПДн «ВЛАДЕЛЕЦ ИСПДН», физические, логические, функциональные и технологические взаимосвязи между сегментами ИСПДн «ВЛАДЕЛЕЦ ИСПДН», с иными ИС и информационно-телекоммуникационными сетями, режимы обработки информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и в ее отдельных сегментах, а также иные характеристики ИСПДн «ВЛАДЕЛЕЦ ИСПДН», применяемые информационные технологии и особенности ее функционирования.

3.8. По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик ИСПДн «ВЛАДЕЛЕЦ ИСПДН», направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

3.9. Модель угроз и нарушителя безопасности информации должна содержать описание ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей ИСПДн «ВЛАДЕЛЕЦ ИСПДН», способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

3.10. Требования к СЗПДн определяются в зависимости от уровня защищенности ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и угроз безопасности информации, включенных в модель угроз безопасности информации.

**4.** **Разработка системы защиты информации**

4.1. Разработка СЗПДн организуется ООО «ОРГАН ПО АТТЕСТАЦИИ» в интересах ООО «ВЛАДЕЛЕЦ ИСПДН».

4.2. Разработка СЗПДн осуществляется в соответствии с техническим заданием на создание СЗПДн, и в том числе, включает:

- проектирование СЗПДн;

- разработку эксплуатационной документации на СЗПДн;

- макетирование и тестирование СЗПДн (при необходимости).

4.3. СЗПДн не должна препятствовать достижению целей создания ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и ее функционированию.

4.4. При разработке СЗПДн учитывается ее информационное взаимодействие с иными информационными системами (ИС) и информационно-телекоммуникационными сетями.

4.5. При проектировании СЗПДн осуществляются следующие мероприятия:

- определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);

- определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в ИСПДн;

- выбираются меры защиты информации, подлежащие реализации в СЗПДн; определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

- определяется структура СЗПДн, включая состав (количество) и места размещения элементов;

- осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также уровня защиты ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей ИСПДн «ВЛАДЕЛЕЦ ИСПДН», приводящих к возникновению угроз безопасности информации:

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

4.6. Результаты проектирования СЗПДн отражаются в проектной документации на ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

4.7. При отсутствии необходимых средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, организуется разработка (доработка) средств защиты информации, и их сертификация в соответствии с законодательством Российской Федерации или производится корректировка проектных решений по ИСПДн и (или) ее СЗПДн с учетом функциональных возможностей имеющихся сертифицированных средств защиты информации.

4.8. Разработка эксплуатационной документации на СЗПДн осуществляется в соответствии с техническим заданием на создание СЗПДн.

4.9. При макетировании и тестировании СЗПДн, в том числе, осуществляются: проверка работоспособности и совместимости выбранных средств защиты

– информации с информационными технологиями и техническими средствами;

– проверка выполнения выбранными средствами защиты информации требований к

СЗПДн.

– корректировка проектных решений, разработанных при создании СЗИ.

4.10. Макетирование СЗПДн и ее тестирование может проводиться, в том числе, с использованием средств и методов моделирования ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и технологий виртуализации.

**5. Внедрение системы защиты информации**

5.1. Внедрение СЗПДн организуется ООО «ОРГАН ПО АТТЕСТАЦИИ» в интересах ООО «ВЛАДЕЛЕЦ ИСПДН».

5.2. Внедрение СЗПДн осуществляется в соответствии с проектной и эксплуатационной документацией на СЗПДн и, в том числе, включает:

- установку и настройку средств защиты информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- разработку документов, определяющих правила и процедуры, реализуемые Оператором для обеспечения защиты информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» в ходе ее эксплуатации (далее организационно-распорядительные документы по защите информации);

- внедрение организационных мер защиты информации:

- предварительные испытания СЗПДн (при необходимости);

- опытную эксплуатацию СЗПДн (при необходимости);

- анализ уязвимостей ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и принятие мер защиты информации по их устранению;

- приемочные испытания СЗПДн (при необходимости).

5.3. Установка и настройка средств защиты информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» должна проводиться в соответствии с эксплуатационной документацией на СЗПДн и документацией на средства защиты информации.

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

- управления (администрирования) СЗПДн:

- выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них:

- управления конфигурацией ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн;

- контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- защиты информации при выводе из эксплуатации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» или после принятия решения об окончании обработки информации.

5.5. При внедрении организационных мер защиты информации осуществляются:

- реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

- проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов ИСПДн «ВЛАДЕЛЕЦ ИСПДН» по реализации организационных мер защиты информации;

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

5.6. Приемочные испытания СЗПДн включают проверку выполнения требований к СЗПДн в соответствии с техническим заданием на создание СЗПДн.

**6.** **Обеспечение защиты информации в ходе эксплуатации информационной системы**

6.1. Обеспечение защиты информации в ходе эксплуатации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» осуществляется в соответствии с эксплуатационной документацией на СЗПДн и организационно-распорядительными документами по защите информации и в том числе включает:

- управление (администрирование) СЗПДн;

- выявление инцидентов и реагирование на них;

- управление конфигурацией, ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн;

- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН».

6.2. В ходе управления (администрирования) СЗПДн осуществляются:

- заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИС и поддержание правил разграничения доступа в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- управление средствами защиты информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации. управление учетными записями пользователей. восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

- установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации. выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;

- централизованное управление СЗПДн (при необходимости);

- регистрация и анализ событий в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», связанных с защитой информации (далее - события безопасности);

- информирование пользователей об угрозах безопасности информации, о правилах эксплуатации СЗПДн и отдельных средств защиты информации, а также их обучение;

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

6.3. В ходе выявления инцидентов и реагирования на них осуществляются:

- определение лиц, ответственных та выявление инцидентов и реагирование на них; обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа. неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИСПДн «ВЛАДЕЛЕЦ ИСПДН» пользователями и администраторами;

- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

6.4. В ходе управления конфигурацией, ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и ее СЗПДн осуществляются:

- поддержание конфигурации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и ее СЗПДн (структуры СЗПДн, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на СЗПДн (поддержание базовой конфигурации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и ее СЗПДн);

- определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн;

- управление изменениями базовой конфигурации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн, в том числе определение типов возможных изменений базовой конфигурации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн, санкционирование внесения изменений в базовую конфигурацию ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн, документирование действий по внесению изменений в базовую конфигурацию ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн, сохранение данных об изменениях базовой конфигурации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн, контроль действий по внесению изменений в базовую конфигурацию ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и ее СЗПДн:

- анализ потенциального воздействия планируемых изменений в базовой конфигурации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн;

- внесение информации (данных) об изменениях в базовой конфигурации ИСПДн «ВЛАДЕЛЕЦ ИСПДН» и СЗПДн в эксплуатационную документацию на СЗПДн;

6.5. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», осуществляются:

- контроль за событиями безопасности и действиями пользователей в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- контроль (анализ) защищенности информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- анализ и оценка функционирования СЗПДн, включая выявление, анализ и устранение недостатков в функционировании СЗПДн;

- периодический анализ изменения угроз безопасности информации в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации:

- документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) СЗПДн.

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

7.1. Обеспечение защиты информации при выводе из эксплуатации, ИСПДн «ВЛАДЕЛЕЦ ИСПДН» или после принятия решения об окончании обработки информации осуществляется в соответствии с эксплуатационной документацией на СЗПДн и организационно- распорядительными документами по защите информации и, в том числе, включает:

- архивирование информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН»;

- уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

8.2. Архивирование информации, содержащейся в ИСПДн «ВЛАДЕЛЕЦ ИСПДН», должно осуществляться при необходимости дальнейшего использования информации.

8.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю ИСПДн «ВЛАДЕЛЕЦ ИСПДН» или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.