Политика ИБ АО «ИК Волгоград»

Оглавление

Раздел 1. Введение

Настоящая Политика информационной безопасности ИСПДн Корпорация является локальным актом, в котором определены основные направления обеспечения информационной безопасности ИСПДн. Настоящая Политика определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) Корпорации, основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Раздел 2. Цели и задачи

Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн. Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц;

- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

1) к информации, циркулирующей в ИСПДн;

2) средствам вычислительной техники ИСПДн;

3) аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

Раздел 3. Основные принципы политики ИБ

Построение системы обеспечения безопасности ПДн ИСПДн Корпорации и ее функционирование должны осуществляться в соответствии со следующими основными принципами: законность; системность; комплексность; непрерывность; своевременность; преемственность и непрерывность совершенствования; персональная ответственность; минимизация полномочий; взаимодействие и сотрудничество; гибкость системы защиты; открытость алгоритмов и механизмов защиты; простота применения средств защиты; научная обоснованность и техническая реализуемость; специализация и профессионализм; обязательность контроля.

Раздел 4. Объекты защиты

Объектами защиты являются - информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Перечне персональных данных, подлежащих защите в ИСПД.

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

Раздел 5. Классификация пользователей

Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Пользователем ИСПДн является любой работник Корпорации, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

Пользователи ИСПДн делятся на три основные категории:

1. Администратор ИСПДн - работники Корпорации, которые занимаются настройкой, внедрением и сопровождением системы.

2. Программист-разработчик ИСПДн - работники Корпорации или сторонних организаций, которые занимаются разработкой программного обеспечения.

3. Оператор ИСПДн - работники структурных подразделений Корпорации, участвующие в процессе эксплуатации ИСПДн.

Раздел 6. Меры, методы и средства обеспечения требуемого уровня защищённости

Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн одразделяются на:

- законодательные (правовые);

- морально-этические;

- организационные (административные);

- физические;

- технические (аппаратные и программные).

Раздел 7. Контроль системы защиты и ответственность за безопасность ПДн

Контроль эффективности СЗПДн должен осуществляется на периодической основе.

Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также государственными органами в пределах их компетенции.

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является руководитель Корпорации. Руководитель может делегировать часть полномочий по обеспечению безопасности персональных данных.