|  |  |
| --- | --- |
|  | Приложение № 1 к приказу «О введении в действие Концепции и Политики информационной безопасности информационных систем персональных данных ПАО «Красноярскэнергосбыт» |

**КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАО «КРАСНОЯРСКЭНЕРГОСБЫТ»**

1. **ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

ПДн – персональные данные.

ИСПДн – информационная система персональных данных.

МЭ – межсетевой экран.

НСД – несанкционированный доступ.

ОС – операционная система.

ПО – программное обеспечение.

СЗИ – средства защиты информации.

СЗПДн – система (подсистема) защиты персональных данных.

УБПДн – угрозы безопасности персональных данных.

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
   1. Настоящая Концепция информационной безопасности ПДн (далее – Концепция) ПАО «Красноярскэнергосбыт» (далее - Общество) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Политике информационной безопасности ИСПДн Общества.
   2. Концепция разработана в соответствии с требованиями ФЗ от 27.07.2006 №152-ФЗ «О персональных данных», а также других подзаконных актов, регулирующих сферу защиты информации.
   3. В Концепции определены требования к защите ПДн Общества, степень ответственности персонала, требования к системе защиты, статус и обязанности работников Общества по защите ПДн.
   4. Концепция информационной безопасности ПДн определяет стратегию Общества в области ИБ ПДн, а также те меры и средства, которые целесообразно применять для их защиты от несанкционированного доступа.
   5. Целью настоящей Концепции является обеспечение безопасности ПДн, циркулирующих в информационных системах Общества, от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз ПДн (УБПДн).
   6. Настоящая Концепция направлена на:

* соблюдение интересов субъектов ПДн, Общества и государства в информационной сфере;
* соответствие процессов сбора, накопления, обработки и предоставления ПДн нормам законодательства РФ;
* реализацию персональной ответственности за нарушения информационной безопасности;
* предотвращение и нейтрализацию угроз информационной безопасности Общества;
* постоянный системный подход к контролю состояния информационной безопасности Общества.
  1. Настоящая Концепция информационной безопасности ПДн утверждается исполнительным директором Общества.

1. **ОБЛАСТЬ ДЕЙСТВИЯ**
   1. Концепция информационной системы безопасности затрагивает все виды деятельности Общества, касающиеся сбора, обработки, накопления, предоставления и распространения ПДн. Предметом настоящей Концепции Общества являются:

* персональные данные, представленные в виде документированной информации на различные рода носителях, информационных массивах и базах данных, подлежащих защите в соответствии с законодательством РФ и внутренними организационно-распределительными документами Общества;
* средства и системы информатизации, программные средства, автоматизированные системы управления, информационные и технологические процессы, используемые для обработки ПДн.
  1. Выполнение положений Концепции информационной безопасности является обязательным для всех работников Общества. Взаимоотношения по использованию положений настоящего документа применительно к защите информации, находящейся в совместном ведении с другими организациями, регулируются на основании специальных соглашений.

1. **СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**
   1. Система защиты персональных данных разрабатывается на основании:

* федеральных законов, Указов Президента, Постановлений Правительства РФ, приказов и положениях ФСТЭК России, ФСБ России, Минкомсвязи России и других нормативно-правовых актов, регулирующих область защиты информации;
* модели угроз безопасности Общества;
* перечня персональных данных, подлежащих защите;
* классификации угроз информационной системы персональных данных.
  1. Организация системы защиты ПДн и основывается на:
* использовании ПДн только в соответствии с целями их обработки в Обществе;
* регламентации порядка доступа к информационным ресурсам;
* определении прав доступа к информационным ресурсам их владельцами;
* применении антивирусных и иных средств защиты информации.
  1. СЗПДн Общества должна обеспечивать:
* защиту серверов за счет использования механизмов управления доступом к серверам баз данных, файловым, информационным и почтовым серверам, серверам регистрации и учета событий, связанных с осуществлением доступа к ресурсам серверов;
* комплексную антивирусную защиту систем, входящих в состав ИСПДн, за счет распределения антивирусных средств (антивирусных сканеров, резидентных антивирусных мониторов и файловых ревизоров) по всем узлам системы.
  1. Для обеспечения безопасности СЗПДн необходимо использовать следующие технические средства:
* антивирусные средства для рабочих станций пользователей и серверов;
* средства идентификации пользователей;
* средства физического разграничения доступа в защищаемые помещения;
* другие средства, направленные на обеспечение информационной безопасности.

1. **МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**
   1. Комплекс мер по защите в Обществе включает в себя следующие мероприятия:

* назначение и распределение ответственности;
* разработка, реализация, внедрение и контроль исполнения планов мероприятий и других документов по обеспечению информационной безопасности;
* аудит информационной безопасности Общества.
  1. Концепция защиты ИСПДн Общества реализуется путем сочетания организационных и технических мер, направленных на защиту ИСПДн. К организационным мерам защиты ИСПДн относятся:
* управление персоналом;
* физическая защита объекта;
* поддержание работоспособности;
* инвентаризация информационных ресурсов Общества;
* реагирование на нарушение режима безопасности;
* планирование восстановительных работ.
  1. Реагирование на нарушение режима безопасности должно предусматривать набор оперативных мероприятий, положений, должностных инструкций, направленных на обнаружение и нейтрализацию угрозы. Общее руководство информационной безопасностью в Обществе осуществляет исполнительный директор.
  2. Руководство работами по обеспечению информационной безопасности ПДн осуществляет ответственный за организацию обработки ПДн.

1. **ОБЯЗАННОСТИ РАБОТНИКОВ ОБЩЕСТВА ПО ЗАЩИТЕ ПДн:**
   1. Описание обязанностей всех работников Общества по обработке и защите ПДн закреплены в [Правилах по работе с ПДн в автоматизированной системе](file:///\\heracle\e\admin\Информационная%20безопасность\Документы\Инструкции\Инструкция%20пользователя%20ИСПДн.doc).
   2. Работники Общества обязаны в незамедлительном порядке информировать о ставших им известными фактах нарушений положений настоящей Концепции и инцидентах информационной безопасности своего непосредственного руководителя, ответственного за организацию обработки ПДн, или руководство Общества.
   3. Ответственный за организацию обработки ПДн обязан инициировать и проводить служебные расследования по факту нарушений и инцидентов информационной безопасности в соответствии с установленной в Обществе процедурой и докладывать о результатах расследований руководству Общества.

1. **ОТВЕТСТВЕННОСТЬ**
   1. В соответствии с ФЗ от 27.07.2006 г.  №152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного ФЗ, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.
   2. За нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272, 273 и 274 УК РФ), несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.