ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основной целью УП «Брествторчермет» в области информационной безопасности является обеспечение целостности, доступности, сохранности, конфиденциальности информации, а также защита информации от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и/или передачи.

Руководство УП «Брествторчермет» (далее – Организация) констатирует, что защита информации является неотъемлемой составной частью успешного осуществления уставной деятельности Организации. Организация исходит из того, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности: необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических и организационных мероприятий. Меры обеспечения информационной безопасности подлежат рассмотрению с учетом финансовых, материальных и иных затрат на их реализацию, вероятности возникновения угроз и объема возможных потерь.

Данная политика относится к обеспечению информационной безопасности любой деятельности Организации и направлена на защиту информационных ресурсов, информационных систем и/или поддерживающей инфраструктуры, охватывает все автоматизированные и телекоммуникационные системы, владельцем и/или пользователем которых является Организация.

Политика информационной безопасности УП «Брествторчермет» основана на следующих принципах:

– Системности: необходимость постоянного мониторинга технического состояния оборудования и его защиты, всех уязвимых мест возможных объектов и направлений для несанкционированных попыток доступа к информации;

– Непрерывности защиты информации: целенаправленная организационная работа по обновлению программно-технических средств защиты информации, своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.;

– Комплексности: согласование работы разнородных средств защиты информации, покрытие ими всех существенных каналов реализации угроз;

– Разумной достаточности: обеспечить приемлемый уровень безопасности при оценке надежности защиты в сопоставлении с ее стоимостью, потреблением вычислительных ресурсов, удобством работы пользователей и другими характеристиками;

– Постоянного повышения квалификации персонала в области применения средств защиты информации.