Приложение № 1 к Политике информационной безопасности «ИБКОРП»

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

 **Информационная безопасность (ИБ)** – состояние защищенности информации и инфраструктуры от несанкционированного доступа, изменения, уничтожения, утечки и других угроз, направленных на нарушение ее конфиденциальности, целостности и доступности.

 **Информационные активы** – данные, программное обеспечение, аппаратное обеспечение, сети, документы и иные ресурсы, имеющие ценность для организации и подлежащие защите.

 **Критическая информация** – данные, утечка, изменение или уничтожение которых может привести к серьезным последствиям, включая финансовые потери, нарушение работы организации или угрозу национальной безопасности.

 **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному физическому лицу, включая имя, контактные данные, сведения о местоположении и т. д.

 **Коммерческая тайна** – конфиденциальная информация, имеющая ценность для организации и подлежащая защите от несанкционированного раскрытия.

 **Инцидент информационной безопасности** – событие или совокупность событий, создающих угрозу конфиденциальности, целостности или доступности информации.

 **Угроза информационной безопасности** – потенциальное или реальное действие, которое может привести к нарушению защищенности информации.

 **Риск информационной безопасности** – вероятность возникновения ущерба для организации вследствие реализации угроз ИБ.

 **Защищаемая информация** – информация, которая требует защиты в соответствии с законодательством, корпоративной политикой или иными нормативными документами.

 **Средства защиты информации** – программные, аппаратные и организационные меры, предназначенные для предотвращения угроз информационной безопасности.

 **Политика информационной безопасности (ПИБ)** – совокупность правил, норм и требований, направленных на обеспечение защиты информации в организации.

 **Система управления информационной безопасностью (СУИБ)** – комплексная структура, включающая процессы, технологии и людей, обеспечивающих защиту информации в организации.

 **Аудит информационной безопасности** – процесс проверки соответствия систем и процессов требованиям ИБ, выявление уязвимостей и предоставление рекомендаций по их устранению.

 **Информационная система (ИС)** – совокупность программного и аппаратного обеспечения, предназначенная для обработки, хранения и передачи информации.

 **Мониторинг событий безопасности** – процесс постоянного отслеживания и анализа активности в информационных системах для выявления потенциальных угроз.