Приложение № 1 к Политике информационной безопасности

АО «Банк Акционерный Кредитный Стабильный»

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

 **Автоматизированная система**: Совокупность аппаратных и программных средств, предназначенная для выполнения задач по защите информации без непосредственного участия человека.

 **Аудит информационной безопасности**: Оценка текущего состояния системы защиты информации, направленная на выявление уязвимостей, недостатков и нарушений в политике и процедурах безопасности.

 **Аутентификация**: Процесс подтверждения подлинности пользователя или системы, пытающихся получить доступ к информационным ресурсам, для предотвращения несанкционированного доступа.

 **Безопасность информации (данных)**: Комплекс мер и процессов, направленных на защиту конфиденциальности, целостности и доступности данных от угроз.

 **Безопасность информационной технологии**: Совокупность практик и технологий, обеспечивающих защиту IT-инфраструктуры от киберугроз и предотвращающих утечки данных.

 **Блокирование информации (данных)**: Меры, направленные на ограничение доступа к данным для предотвращения их утечки, несанкционированного изменения или уничтожения.

 **Вредоносная программа**: Программное обеспечение, созданное с целью нанести вред информационной системе или получить несанкционированный доступ к данным (вирусы, черви, трояны).

 **Доступ к информации (данным)**: Право или возможность пользователей системы получать, изменять или передавать данные, определяемое политикой безопасности.

 **Защищаемая информация (защищаемые данные)**: Данные, для которых установлены меры защиты, чтобы предотвратить несанкционированный доступ, модификацию или уничтожение.

 **Идентификация**: Процесс определения личности или характеристик субъекта, который запрашивает доступ к системе, для его дальнейшей аутентификации.

 **Идентификация риска**: Процесс выявления потенциальных угроз, которые могут нанести ущерб информационным активам и нарушить безопасность данных.

 **Информационная безопасность**: Совокупность мер, направленных на защиту информации и информационных систем от угроз, нарушающих конфиденциальность, целостность и доступность данных.

 **Информационная инфраструктура**: Набор средств и ресурсов, необходимых для функционирования информационной системы, включая сети, серверы, базы данных и средства безопасности.

 **Информационные ресурсы**: Данные, цифровые документы и программные средства, представляющие ценность для организации и подлежащие защите.

 **Информационная система**: Система, включающая аппаратное и программное обеспечение, предназначенная для сбора, обработки, хранения и передачи информации.

 **Информационные технологии**: Технологии, используемые для обработки, хранения и передачи информации, включающие системы безопасности для защиты данных.

 **Инцидент информационной безопасности**: Событие, которое потенциально может нарушить информационную безопасность, включая утечку данных, атаки или несанкционированный доступ.

 **Источник угрозы безопасности**: Лицо, процесс или событие, способное использовать уязвимость системы для нарушения ее безопасности.

 **Конфиденциальная информация**: Данные, доступ к которым ограничен и контролируется для предотвращения несанкционированного раскрытия.

 **Управление ИБ**: Процесс организации, контроля и улучшения мер защиты информации в компании для обеспечения ее безопасности.

 **Управление рисками ИБ**: Процесс выявления, анализа и минимизации рисков, связанных с информационной безопасностью, для защиты данных от угроз.

 **Меры обеспечения ИБ**: Технические, организационные и физические меры, применяемые для защиты информации от угроз.

 **Мониторинг ИБ**: Непрерывное наблюдение за событиями и процессами в системе для своевременного обнаружения угроз безопасности и реагирования на них.

 **Нарушитель ИБ**: Лицо или группа лиц, которые пытаются обойти меры безопасности и получить несанкционированный доступ к данным или системам.

 **Несанкционированный доступ (несанкционированные действия)**: Доступ к информации или действия в системе, выполненные без разрешения владельца данных.

 **Носитель информации (данных)**: Физическое устройство, на котором хранится информация, подлежащая защите (жесткие диски, флешки и т.д.).

 **Обеспечение ИБ**: Процесс внедрения и поддержания мер безопасности, направленных на защиту данных от угроз.

 **Обработка информации (данных)**: Действия по сбору, анализу и управлению данными, включающие меры безопасности для защиты данных.

 **Объект защиты информации**: Информационные активы, для которых необходимо обеспечить меры защиты от несанкционированного доступа и других угроз.

 **Объект информатизации**: Любой компонент системы, участвующий в процессах обработки и передачи информации, требующий защиты.

 **Оценка риска**: Процесс анализа вероятности возникновения угроз и возможного ущерба для данных и систем.

 **Политика**: Документ, регулирующий правила и процедуры, направленные на обеспечение информационной безопасности в организации.

 **Система управления информационной безопасностью (СУИБ)**: Комплекс мер и процессов, направленных на управление и улучшение информационной безопасности.

 **Система обеспечения информационной безопасности**: Совокупность технических и организационных средств, предназначенных для защиты информации от угроз.

 **Пользователь информационной системы**: Лицо, имеющее доступ к информационной системе и использующее ее ресурсы в рамках установленных полномочий.

 **Правила разграничения доступа**: Нормы и процедуры, определяющие, кто и какие действия может совершать с информацией в системе.

 **Ресурс информационной системы**: Любой элемент информационной системы, включая данные и оборудование, который может быть уязвим к угрозам.

 **Риск**: Возможность возникновения угрозы, способной нанести ущерб данным или информационной системе.

 **Средства вычислительной техники**: Аппаратные средства, используемые для обработки и защиты информации.

 **Субъект доступа**: Лицо или система, имеющее разрешение на выполнение определенных операций с данными.

 **Система защиты информации (данных)**: Комплекс технических и организационных мер, предназначенных для защиты данных от угроз.

 **Угрозы безопасности информации (данных)**: Потенциальные события, способные привести к утечке, изменению или уничтожению данных.

 **Уязвимость**: Слабое место в системе, которое может быть использовано нарушителем для компрометации безопасности.