Приложение № 1 к Политике информационной безопасности ООО АТОМОРС

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Автоматизированная система -** Комплекс взаимосвязанных устройств, программ и данных, предназначенных для выполнения определенных функций с минимальным участием человека.

**Аудит информационной безопасности -** Процесс оценки системы, приложения или сети с целью выявления и устранения уязвимостей и проверки соблюдения норм и стандартов безопасности.

**Аутентификация** - Процесс проверки подлинности пользователя или системы, обеспечивающий уверенность в том, что субъект действительно тот, за кого он себя выдает.

**Безопасность информации (данных) -** Состояние, когда информация и данные защищены от несанкционированного доступа, изменения или уничтожения.

**Безопасность информационной технологии -** Совокупность мер и практик, направленных на обеспечение безопасности информационных систем, включая аппаратное и программное обеспечение, а также данные.

**Блокирование информации (данных) -** Процесс предотвращения доступа к информации или данным, обычно для защиты от несанкционированного использования.

**Вредоносная программа** - Программное обеспечение, разработанное с целью нанесения вреда компьютерам, сетям или данным, включая вирусы, трояны и другие виды вредоносного кода.

**Доступ к информации (данным) -** Разрешение или возможность получения информации или данных.

**Защищаемая информация (защищаемые данные) -** Информация или данные, которые требуют особой защиты от утечки или несанкционированного доступа.

**Идентификация -** Процесс определения личности или сущности, часто с использованием уникальных идентификаторов, таких как логины или пароли.

**Идентификация риска -** Процесс определения потенциальных угроз и уязвимостей, которые могут привести к потере информационной безопасности, и оценка вероятности их реализации.

**Информационная безопасность –** Состояние, когда информационные ресурсы и системы защищены от угроз и рисков, которые могут подвергнуть их опасности и сохраняют конфиденциальность, целостность и доступность

**Информационная инфраструктура -** Совокупность аппаратных, программных и коммуникационных средств, используемых для обработки, хранения и передачи информации.

**Информационные ресурсы -** Данные, информация и другие активы, используемые в информационных системах и процессах.

**Информационная система** - Набор взаимосвязанных компонентов и процессов, предназначенных для сбора, хранения, обработки и передачи информации.

**Информационные технологии -** Совокупность средств и методов, используемых для обработки информации, включая аппаратное и программное обеспечение.

**Инцидент информационной безопасности -** Событие или ситуация, которая представляет угрозу информационной безопасности и требует реакции и расследования.

**Источник угрозы безопасности -** Фактор или сущность, которая может вызвать угрозу информационной безопасности, например, злоумышленник или естественное бедствие.

**Конфиденциальная информация -** Информация, доступ к которой ограничен и разрешен только определенным лицам или субъектам.

**Управление ИБ -** Процесс планирования, реализации и контроля мер и практик, направленных на обеспечение информационной безопасности.

**Управление рисками ИБ -** Процесс оценки, управления и мониторинга рисков, связанных с информационной безопасностью.

**Меры обеспечения ИБ -** Действия и средства, предпринимаемые для защиты информации и данных.

**Мониторинг ИБ -** Непрерывное отслеживание событий и активности, связанных с информационной безопасностью, для раннего выявления угроз.

**Нарушитель ИБ -** Лицо или сущность, которая пытается или совершает действия, нарушающие информационную безопасность.

**Несанкционированный доступ (несанкционированные действия) -** Действия, совершенные без разрешения или без правильной идентификации, часто с целью получения несанкционированного доступа к информации.

**Носитель информации (данных) -** Физическое устройство или средство, на котором хранятся данные, например, жесткий диск или USB-флешка.

**Обеспечение ИБ -** Меры и действия, направленные на обеспечение безопасности информации и данных.

**Обработка информации (данных) -** Процесс сбора, анализа, хранения и передачи информации или данных.

**Объект защиты информации -** Актив, который требует защиты от угроз информационной безопасности, например, база данных или сеть.

**Объект информатизации -** Часть организации или бизнес-процесс, который подвергается автоматизации и управлению информацией.

**Оценка риска** - Процесс определения вероятности и воздействия угрозы на информационную безопасность и определение мер для снижения рисков.

**Политика -** Установленные нормы, правила и стандарты, которые регулируют деятельность в области информационной безопасности.

**Система управления информационной безопасностью (СУИБ) -** Система, которая управляет и координирует меры по обеспечению информационной безопасности в организации.

**Система обеспечения информационной безопасности -** Совокупность мер и технологий, направленных на обеспечение безопасности информации и данных.

**Пользователь информационной системы -** Лицо или субъект, который использует информационную систему для выполнения задач.

**Правила разграничения доступа -** Установленные правила, которые определяют, кто имеет доступ к какой информации и с какими правами.

**Ресурс информационной системы -** Актив, который используется информационной системой для хранения, обработки или передачи данных, например, сервер или база данных.

**Риск -** Возможность потери или ущерба, связанного с угрозой информационной безопасности.

**Средства вычислительной техники -** Аппаратное и программное обеспечение, используемое для обработки информации и данных.

**Субъект доступа -** Лицо или сущность, которая пытается получить доступ к информации или данным.

**Система защиты информации (данных) -** Совокупность мер и технологий, направленных на защиту информации и данных от угроз ирисков.

**Угрозы безопасности информации (данных) -** Потенциальные опасности или события, которые могут угрожать информационной безопасности, такие как взлом, вирусы или утечка данных.

**Уязвимость -** Слабое место в системе или процессе, которое может быть использовано злоумышленниками для атаки или нарушения безопасности.