Политика ООО «Интеллектуальные Сети» в области информационной безопасности

Утверждена приказом ООО «Интеллектуальные Сети» от 18 февраля 2025 г. № 4-К

Для поддержания деловой репутации и обеспечения конкурентоспособности Общество считает важнейшей своей задачей обеспечение защиты информационных активов Общества, его клиентов и партнеров, в том числе коммерческой, служебной и других видов тайн, а также персональных данных сотрудников Общества.

Для эффективной реализации процессов обеспечения информационной безопасности в Обществе внедряется система менеджмента информационной безопасности (далее – СМИБ), соответствующая требованиям международного стандарта ISO/IEC 27001:2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»

Основные стратегические цели СМИБ:

Создание и постоянное поддержание в Обществе условий, при которых риски, связанные с обеспечением безопасности активов Общества, постоянно контролируются и находятся на приемлемом уровне

Защита конфиденциальной информации осуществляется в соответствии с требованиями российского законодательства, отраслевыми требованиями и лучшими практиками управления;

Обеспечение безопасности и непрерывности производственной и хозяйственной деятельности Общества, а также его дальнейшего развития.

Достижение целей информационной безопасности за счет

- Применения обоснованных, экономически эффективных организационных и технических мер по обеспечению информационной безопасности
- Выявление применимых требований действующего законодательства и регуляторов в области информационной безопасности, достижение соответствия этим требованиям
- Инвентаризации активов Общества и регулярного анализа рисков информационной безопасности
- Регулярной оценкой соответствия СМИБ применимым внутренним и внешним требованиям посредством проведения внутренних аудитов СМИБ, мониторинга эффективности процессов СМИБ, анализа СМИБ руководством Общества
- Внедрения корректирующих действий в случае выявления отклонений или несоответствий в работе СМИБ внутренним и внешним требованиям
- Установления ответственности сотрудников по вопросам обеспечения информационной безопасности, обучения и повышения их осведомленности в части информационной безопасности
- Подтверждения соответствия СМИБ требованиям международного стандарта ISO/IEC 27001:2021

Основные принципы информационной безопасности

Законность
При обеспечении информационной безопасности выполняются требования применимого законодательства, а также действующие нормативные требования государственных регулирующих органов.

Соответствие стандартам
Организационные и технические меры СМИБ реализуются с учётом тенденций в области информационной безопасности. Ориентация на открытые стандарты позволяет использовать накопленный опыт в области защиты информации, а также обеспечивает прозрачность процессов информационной безопасности и простоту взаимодействия в рамках задач по обеспечению информационной безопасности.

Адекватность существующим угрозам и экономическая обоснованность
Применяемые организационные и технические меры защиты выбираются исходя из потребностей бизнеса на основе результатов анализа и оценки рисков информационной безопасности, в частности, анализа актуальных угроз и затрат на внедрение и сопровождение мер управления рисками. Проводится периодическая оценка эффективности используемых мер и механизмов защиты.

Непрерывность функционирования
Обеспечиваются отказоустойчивость, надежность, доступность и корректность функционирования организационных и технических мер СМИБ.

Непрерывность совершенствования
Для успешного противодействия угрозам информационной безопасности в условиях постоянно меняющегося внешнего и внутреннего окружения реализуется непрерывный цикл развития и совершенствования СМИБ.

Минимизация влияния на бизнес-процессы
Применяемые организационные и технические меры СМИБ минимально влияют на функционирование и характеристики бизнес-процессов Общества.

Персональная ответственность
Каждый сотрудник Общества несет персональную ответственность за выполнение функций и требований, возложенных на него в рамках функционирования СМИБ.

Контроль
Осуществляется постоянный контроль выполнения сотрудниками Общества требований в области информационной безопасности.