

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «СНИИП»

Для поддержания деловой репутации и обеспечения конкурентоспособности АО «СНИИП» (далее – Общество) считает важнейшей своей задачей обеспечение конфиденциальности, целостности и доступности информационных активов Общества, его клиентов и партнеров, в том числе защиты коммерческой, служебной и других видов тайн, а также персональных данных работников Общества, работников клиентов, партнеров и других и юридических лиц, находящихся в правоотношениях с Обществом.

Для эффективной реализации процессов обеспечения информационной безопасности (далее – ИБ) в Обществе внедряется система управления информационной безопасностью (далее – СУИБ), соответствующая требованиям международного стандарта ISO/IEC 27001:2013 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

1. Основными стратегическими целями СУИБ Общества являются:

- 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 в соответствии с требованиями российского законодательства, международного законодательства, отраслевыми требованиями и лучшими практиками управления ИБ;
- обеспечение непрерывности осуществления производственной и хозяйственной деятельности, ключевого бизнес-процесса Общества, а также дальнейшего развития Общества.

2. Эти цели достигаются решением следующих задач:

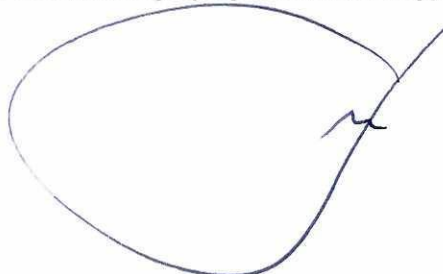
- инвентаризация активов Общества и регулярное проведение анализа рисков ИБ;
- применение обоснованных, экономически эффективных организационных и технических мер по обеспечению ИБ;
- выявление применимых требований действующего законодательства и регуляторов в области ИБ, достижение соответствия этим требованиям;
- установление ответственности работников по вопросам обеспечения ИБ. обучение и повышение их осведомленности в части ИБ;
- регулярная оценка соответствия СУИБ применимым внутренним и внешним требованиям посредством проведения внутренних аудитов СУИБ, мониторинга эффективности процессов СУИБ, анализа СУИБ руководством Общества;
- внедрение корректирующих действий в случае выявления отклонений или несоответствий в работе СУИБ внутренним и внешним требованиям;
- подтверждение соответствия СУИБ Общества требованиям международного стандарта ISO/IEC 27001:2013.

3. В области ИБ Общество руководствуется следующими принципами:

- законность. При обеспечении ИБ выполняются требования применимого законодательства, а также действующие нормативные требования государственных регулирующих органов, в том числе, международных;
- адекватность существующим угрозам и экономическая обоснованность. Применяемые организационные и технические меры защиты выбираются исходя из потребностей бизнеса на основе результатов анализа и оценки рисков ИБ, в частности, анализа актуальных угроз и затрат на внедрение и сопровождение мер управления рисками. Проводится периодическая оценка эффективности используемых мер и механизмов защиты;
- минимизация ограничивающего влияния на бизнес-процессы. Применяемые организационные и технические меры СУИБ минимально влияют на функционирование и характеристики бизнес-процессов Общества;
- перспективность и ориентация на существующие российские и международные открытые стандарты. Организационные и технические меры СУИБ реализуются с учетом мировых тенденций в области ИБ. Ориентация на открытые стандарты позволяет использовать накопленный мировой опыт в области защиты информации, а также обеспечивает прозрачность процессов ИБ и простоту взаимодействия в рамках задач по обеспечению ИБ;
- непрерывность функционирования. Обеспечиваются отказоустойчивость, надежность, доступность и корректность функционирования организационных и технических мер СУИБ;
- непрерывность совершенствования. Для успешного противодействия угрозам ИБ в условиях постоянно меняющегося внешнего и внутреннего окружения реализуется непрерывный цикл развития и совершенствования СУИБ;
- персональная ответственность. Каждый работник Общества несет персональную ответственность за выполнение функций и требований, возложенных на него в рамках функционирования СУИБ;
- контроль. Осуществляется постоянный контроль выполнения работниками Общества требований в области ИБ.

4. Деятельность по обеспечению ИБ в Обществе должна планироваться ежегодно на уровне руководства. Ресурсы на поддержку и модернизацию СУИБ должны регулярно выделяться руководством.

Генеральный директор



А.И. Карцев