



ПОЛИТИКА ООО «ИФ СНИИП АТОМ» В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для получения международного признания и укрепления имиджа компании на внутреннем и внешнем рынке, устойчивого развития Общества, повышения доверия заказчиков, партнеров и других заинтересованных сторон ООО «ИФ СНИИП АТОМ» (далее – Общество) считает важнейшей задачей обеспечение функционирования системы менеджмента информационной безопасности (далее - СМИБ) на соответствие требованиям стандарта ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001) «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

СМИБ основана на подходе оценки рисков, с целью создать, эксплуатировать, постоянно контролировать, анализировать, поддерживать в рабочем состоянии и улучшать защиту информации (информационных активов, в том числе производимых процессов, коммерческой тайны или иных чувствительных по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности ресурсов, а также персональных данных работников Общества, клиентов, партнеров и других юридических лиц, находящихся в правоотношениях с Обществом).

Основными целями СМИБ 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.
- обеспечение конфиденциальности, актуальности, целостности и доступности информационных активов Общества, выполнение требований безопасности клиентов и партнеров;
- поддержание функционирования и постоянное совершенствование СМИБ Общества в соответствии с требованиями стандарта ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001).

Для достижения заявленных целей руководство ООО «ИФ СНИИП АТОМ» обязуется:

- обеспечивать проведение инвентаризации активов Общества и соответствующую их защиту, осуществлять анализ рисков информационной безопасности (ИБ);
- обеспечивать достижение адекватности мер по защите от реальных угроз информационной безопасности;
- принимать необходимые и своевременные меры по предоставлению ресурсов для поддержания и модернизации СМИБ;
- обеспечивать соблюдение законодательных, нормативных и договорных требований, которые должны выполняться Обществом, нашими партнерами по бизнесу, подрядчиками и поставщиками;
- поддерживать безопасность информации и средств обработки информации Общества при наличии доступа к ним сторонних организаций в процессах обработки и передачи этой информации;
- обеспечивать уверенность в том, что заинтересованные стороны (работники, подрядчики и др. пользователи) осознают свою ответственность и способны выполнять предусмотренные для них функции и снижать риск мошенничества и нецелевого использования информации, а также от угроз безопасности информации;
- установить ответственность работников по вопросам обеспечения ИБ, организовывать обучение и повышение их осведомленности в части ИБ;
- поддерживать безопасность и целостность программного обеспечения и массивов информации (реализация мер по обнаружению, предотвращению проникновения и

восстановлению после проникновения вредоносного кода, обеспечение соответствующего оповещения пользователей; реализация мер от мобильного кода);

- обеспечивать поддержание осведомленности работников Общества в вопросах обеспечения информационной безопасности;
- осуществлять оценку соответствия СМИБ посредством проведения внутренних и внешних аудитов;
- проводить корректирующие действия в случае выявления отклонений или несоответствий СМИБ внутренним и внешним требованиям.

В процессе обеспечения ИБ руководство и работники Общества руководствуются принципами, приведенными ниже:

Принцип законности

При выборе и реализации мер и средств обеспечения информационной безопасности строго соблюдается законодательство Российской Федерации, требования нормативных правовых и технических документов в области обеспечения информационной безопасности государственных регулирующих органов, в том числе, международных.

Принцип адекватности и экономической обоснованности

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.

Принцип непрерывности

Обеспечиваются отказоустойчивость, надежность, доступность и корректность функционирования организационных и технических мер СМИБ. Постоянное совершенствование СМИБ для успешного противодействия угрозам ИБ в условиях постоянно меняющегося внешнего и внутреннего окружения.

Принцип персональной ответственности

Ответственность за выполнение функций и требований в рамках функционирования СМИБ возлагается на каждого работника в пределах его полномочий.

Принцип Контроля

Осуществляется постоянный контроль выполнения работниками Общества требований в области ИБ.

Развитие и совершенствование системы менеджмента информационной безопасности Общества в соответствии с требованиями стандарта ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001) помогает поддерживать качество предоставляемых нами информационных услуг, продукции, работ.

**Генеральный директор
ООО «ИФ СНИИП АТОМ»**



Ю.С. Поляшев