

АДКРЫТАЕ АКЦЫЯНЕРНАЕ
ТАВАРЫСТВА
«ИНДЭЎ САЛЮШЭНС»



ОТКРЫТОЕ АКЦИОНЕРНОЕ
ОБЩЕСТВО
«ИНДЕВ СОЛЮШЕНС»

ПОЛИТИКА информационной безопасности

Совершенство через технологии!

Информация является ценным и важным активом Общества. Общество уделяет особое внимание решению задачи обеспечения информационной безопасности. Под обеспечением информационной безопасности понимается защита информационных активов от их случайного или преднамеренного изменения, раскрытия, уничтожения.

Политика информационной безопасности (далее – Политика) устанавливает цели и принципы в области информационной безопасности, которыми руководствуются все структурные подразделения Общества и подрядные организации, и является базовым документом для Системы менеджмента информационной безопасности (далее – СМИБ). Политика является общедоступным документом, который предоставляется без ограничений всем заинтересованным сторонам.

Стратегическим направлением развития системы менеджмента информационной безопасности в Обществе является ее интеграция с процессами и общей структурой менеджмента Общества для более полного удовлетворения его потребностей.

Общество принимает на себя обязательства стремиться соответствовать применимым требованиям СМИБ, а также постоянно улучшать СМИБ и практику реализации ее требований в соответствии со следующими принципами:

вовлеченность высшего руководства Общества в процесс обеспечения информационной безопасности;

соответствие законодательным требованиям и договорным обязательствам в части информационной безопасности;

согласованность действий подразделений Общества и сторонних организаций по обеспечению информационной безопасности;

экономическая целесообразность применения средств и адекватность мер по защите информационных активов Общества;

обучение работников Общества и повышение их осведомленности об актуальности и важности соблюдения требований безопасности при выполнении своих служебных обязанностей;

предупреждение и управление инцидентами информационной безопасности;

персональная ответственность работников Общества за соблюдение требований по информационной безопасности. Обязанности по соблюдению требований информационной безопасности включаются в трудовые договоры, должностные инструкции работников Общества, а также в договоры (соглашения) с контрагентами;

своевременное и достаточное обеспечение Общества организационными, финансовыми и трудовыми ресурсами для выполнения мероприятий по информационной безопасности;

предоставление работникам Общества и контрагентам необходимых прав доступа к информационным активам и достаточных для качественного

и своевременного выполнения трудовых обязанностей и договорных обязательств.

С помощью СМИБ Общество намерено реализовать следующие цели:
обеспечение достоверности данных для принятия руководством оптимальных управленческих решений при использовании информационных технологий;

подтверждение соответствия требованиями стандарта СТБ ISO/IEC 27001;
обеспечение Общества программным обеспечением, освоение новых методик и внедрение современных технологий, позволяющих повысить уровень информационной безопасности производственных и управленческих процессов;
повышение уровня информационной безопасности производственных и управленческих процессов Общества за счёт внедрения современных методов и технологий;

повышение деловой репутации и корпоративной культуры Общества;
предотвращение и (или) минимизация ущерба от реализации угроз информационной безопасности;

обеспечение удовлетворенности потребителей и заинтересованных сторон;
обеспечение интеграции СМИБ с внедренными и успешно функционирующими в Обществе системами менеджмента;

обеспечение осведомленности и компетентности персонала в области информационной безопасности;

обеспечение контроля соответствия требованиям законодательства, государственных стандартов и договорным обязательствам в части информационной безопасности.

Активная позиция руководства Общества в вопросах информационной безопасности выражается в управлении рисками по следующим направлениям:

идентификация, классификация информационных активов, определение владельцев этих активов;

своевременное выявление уязвимостей и прогнозирование угроз информационной безопасности в отношении идентифицированных активов;

оценка вероятности реализации угроз информационной безопасности и степени их негативного воздействия на деятельность Общества;

мониторинг и своевременная обработка рисков идентифицированных активов;

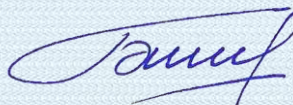
оценка эффективности применяемых методов и средств управления информационной безопасностью, в том числе с привлечением внутренних и внешних аудиторов.

В поддержку Политики внедряются нормативные и распорядительные документы Общества, которые разрабатываются в соответствии с действующим законодательством. Политика, а также поддерживающие ее внутренние нормативные и распорядительные документы обязательны для исполнения всеми работниками Общества, а также контрагентами (потребителями, поставщиками, партнерами и др.), имеющими доступ к информационным активам и информационной инфраструктуре Общества.

Все умышленные действия, направленные на подрыв безопасности информационных активов Общества или его контрагентов, являются предметом применения соответствующих дисциплинарных санкций или судебного преследования.

Политика информационной безопасности и цели информационной безопасности подлежат регулярному пересмотру.

Генеральный директор
ОАО «ИнДев Солюшенс»
18.09.2023



О.В.Беляков