



Обеспечение безопасности информационных активов при предоставлении облачных сервисов определяется руководством ЗАО «ДЖИЭНСИ-АЛЬФА» (далее - Компания) ключевым условием для осуществления деятельности Компании.

Обеспечение информационной безопасности необходимо Компании для выполнения взятых на себя договорных обязательств перед Заказчиками, поддержания конкурентоспособности Компании, обеспечения соответствия требованиям Политики информационной безопасности Компании, законодательства и нормативной базы, а также формирования деловой репутации Компании, как надежного Исполнителя и Партнера.

Данная Политика в области Системы управления информационной безопасностью при предоставлении облачных сервисов ЗАО «ДЖИЭНСИ-АЛЬФА» (далее - Политика) распространяется на Систему управления информационной безопасностью Компании при предоставлении облачных сервисов (далее - СУИБ).

Система управления информационной безопасностью

Внедренная в Обществе СУИБ, соответствующая требованиям международных стандартов ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 и PCI DSS, призвана обеспечить эффективное управление информационной безопасностью при предоставлении облачных сервисов.

Область применения СУИБ включает информационные активы Компании и функционирующие в его рамках процессы, представленные в виде документированной информации, нацеленные на защиту информационных активов как Заказчиков, так и самого Компании, при предоставлении облачных сервисов.

Процессный подход в части обеспечения и управления информационной безопасностью, внедренный в Компании для реализации положений настоящей Политики, задокументирован в формате процессной модели СУИБ. Каждому процессу соответствуют конкретные внутренние нормативные документы Общества в части информационной безопасности.

СУИБ является механизмом, обеспечивающим возможность совместного безопасного использования активов, осуществления электронных операций, а также уменьшения информационных рисков до приемлемого уровня.

В рамках реализации процессов СУИБ, следующая деятельность является фундаментальной:

- предотвращение преднамеренного или случайного несанкционированного доступа к активам Общества, включая информацию ограниченного доступа;
- обеспечение доступности активов для авторизованных пользователей тогда, когда они им необходимы, своевременное обнаружение и реагирование на угрозы, которые могут повлечь недоступность активов;
- предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных;
- разработка и управление изменениями планов обеспечения непрерывности бизнеса, процедур восстановления работоспособности информационных систем Компании после аварии, процедур резервного копирования и восстановления данных, процедур защиты от вредоносного ПО и сетевых атак, контроля доступа, управления инцидентами безопасности и оповещения об инцидентах, управления изменениями и совершенствования;
- систематический пересмотр и совершенствование СУИБ.

Общество ставит своей целью:

- создание и постоянное поддержание в Компании условий, при которых риски, связанные с обеспечением безопасности активов Компании, в том числе связанные с техническими и эксплуатационными характеристиками облачных сервисов, постоянно контролируются и находятся на приемлемом уровне за счет обеспечения основных аспектов ИБ: целостности, доступности, приватности и конфиденциальности;



- определение руководящих принципов по реализации мер обеспечения ИБ, в том числе специфичных для облачных сервисов, угроз и рисков ИБ во взаимоотношениях между потребителями и поставщиками облачных сервисов;
- защита конфиденциальной информации (в том числе при использовании облачных сервисов) в соответствии с требованиями действующего законодательства Республики Армения, международного законодательства, отраслевыми требованиями и лучшими практиками управления ИБ, в том числе специфичными для облачных сервисов угроз и рисков ИБ;
- достижение соответствия с применимым законодательством по защите персональных данных и договорными условиями, согласованными между Компанией, как поставщиком облачных сервисов, и обработчиком персональных данных, и его клиентами (потребителями облачных сервисов);
- создание единой совокупности категорий, мер обеспечения ИБ, которые могут быть реализованы компанией, как поставщиком облачных сервисов и выступающим в качестве обработчика персональных данных;
- обеспечение непрерывности при предоставлении облачных сервисов Компании;
- постоянное улучшение СУИБ Компании в соответствии с требованиями ИБ и требованиями бизнеса.

Целевые показатели информационной безопасности в Компании определяются на основе следующих стратегических задач:

- стабильное функционирование Компании, гарантирующее достижение поставленных целей;
- обеспечение защиты активов, принадлежащих Компании, его Заказчикам и Партнерам;
- обеспечение защиты персональных данных, вверенных Компании;
- обеспечение соответствия деятельности Компании требованиям законодательства Республики Армения, армянских и международных стандартов в области информационной безопасности;
- принятие и выполнение актуальных требований Заказчиков и Партнеров Компании в части обеспечения информационной безопасности;
- постоянное улучшение СУИБ Компании в соответствии с требованиями международных стандартов ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019 и PCI DSS.

Целевые показатели информационной безопасности достигаются путем:

- четкого определения требований и ожидаемых результатов в области информационной безопасности;
- выполнения комплекса мер защиты информационных активов, разработанного на основании управления рисками информационной безопасности;
- обеспечения СУИБ ресурсами, необходимыми для ее реального и эффективного функционирования;
- проведения периодической оценки эффективности, результативности в части выполнения требований настоящей Политики и Целей в области информационной безопасности;
- информирования руководства Компании о результатах оценки для последующего анализа и принятия решений;
- проведения на постоянной основе корректирующих и превентивных действий, основанных на результатах внутреннего аудита или иной соответствующей информации в целях непрерывного совершенствования;
- ежегодного подтверждения соответствия функционирующей СУИБ требованиям международных стандартов ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27018:2019 и PCI DSS результатами контрольных аудитов, проводимых силами независимого органа по сертификации.

Руководство ЗАО «ДЖИЭНСИ-АЛЬФА» берет на себя ответственность за реализацию настоящей Политики и неукоснительного выполнения изложенных в ней принципов всеми работниками Компании.



ПОЛИТИКА В ОБЛАСТИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРЕДОСТАВЛЕНИИ ОБЛАЧНЫХ СЕРВИСОВ

В целях поддержания актуальности и эффективности СУИБ и ее соответствия условиям ее функционирования, Компания осуществляет регулярный пересмотр настоящей Политики.

Со стороны Компании также может быть инициирован пересмотр настоящей Политики по результатам анализа рисков, аудитов соответствия требованиям информационной безопасности, внедрения изменений в СУИБ.