Приложение № 1
к Приказу № 69-ОД
от «29» июня 2021 года

Политика информационной безопасности

Руководство СберРешений[1] рассматривает обеспечение информационной безопасности как ключевое условие для осуществления деятельности. Обеспечение информационной безопасности необходимо для исполнения договорных обязательств, завоевания и удержания доверия контрагентов, поддержания и повышения конкурентоспособности и рентабельности бизнеса, сбережения позитивного имиджа и деловой репутации СберРешений.

СберРешения гарантируют высочайший уровень безопасности обработки данных. Достижение данного уровня возможно только при реализации полного комплекса организационных и технических мер по обеспечению целостности и конфиденциальности информации, при условии её доступности для пользователей, имеющих соответствующие права, в соответствии с требованиями действующего применимого законодательства стран присутствия СберРешений и международных стандартов обеспечения безопасности ISO/IEC 27001:2013 и SSAE18.

Реализованная в СберРешениях Система менеджмента информационной безопасности (СМИБ), соответствующая требованиям международного стандарта ISO/IEC 27001:2013, призвана обеспечить эффективное управление информационной безопасностью в рамках всех бизнес-процессов. Центральным и руководящим документом, устанавливающим общие требования к системообразующим процессам СМИБ, является «Руководство СМИБ».

СМИБ является механизмом, обеспечивающим возможность совместного безопасного использования активов, осуществления электронных операций, а также уменьшения информационных рисков до приемлемого уровня. В рамках реализации процессов СМИБ следующая деятельность является фундаментальной:

- обеспечение доступности сервисов для авторизованных пользователей;
- обеспечение непрерывности бизнеса, в том числе своевременное восстановление работоспособности информационных систем после аварий;
- обеспечение конфиденциальности информации и предотвращение преднамеренного или случайного несанкционированного доступа к активам и данным СберРешений и контрагентов;
- обеспечение контроля доступа и обеспечение контроля целостности для предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных;
- своевременное реагирование на инциденты безопасности, а также обнаружение и предотвращение угроз, которые могут повлечь недоступность активов;
- повышение уровня киберкультуры СберРешений;
- систематический пересмотр и совершенствование СМИБ.

Руководство СберРешений берет на себя ответственность за реализацию изложенной Политики информационной безопасности и обеспечение неукоснительного выполнения изложенных в ней принципов всеми работниками СберРешений и авторизованными пользователями. Каждый работник СберРешений и авторизованный пользователь несет персональную ответственность за соблюдение Политики информационной безопасности.

Руководство СберРешений возлагает на себя обязательство по выполнению периодических проверок эффективности СМИБ и персональную ответственность за её результативность, эффективность функционирования и совершенствование.

Руководство гарантирует обеспечение условий и ресурсов для реализации Политики информационной безопасности и призывает всех работников объединить усилия для достижения поставленных целей.

[1]СберРешения - Группа компаний «Интеркомп» (АО «Интеркомп», ООО «Интеркомп Аутсорсинг», ООО ЧАЗ «Интеркомп», ООО ЧАЗ МК «Персонал», ООО «ЦБУ «Интеркомп», ООО «БУиК», ООО «СберРешения», ТОО «Интеркомп Казахстан», ТОО «Интеркомп аутсорсинг-Казахстан», ООО «Интеркомп аутсорсинг Азербайджан», ООО «Интеркомп Грузия»).