
Политика безопасности

Компании MakariSoft

Кунгуров Макар 3181

Оглавление

Термины и определения	2
Сокращения и обозначения	2
Общие положения	2
Цели в области информационной безопасности	3
Задачи обеспечения информационной безопасности	3
Принципы обеспечения информационной безопасности	4
Распределение ролей и ответственности	6
Подразделения информационной безопасности:	6
Подразделения Информационных технологий:	7
Ответственность за нарушение Политики информационной безопасности	8

Термины и определения

- Аудит - систематический, независимый и документированный процесс получения свидетельств аудита и их объективного оценивания для определения степени соответствия критериям аудита. Компания - любое юридическое лицо, входящее в Группу компаний Макарсонфт или аффилированное с ними.
- Корпоративная культура Компании – это свод важных положений деятельности Компании, определяемых ее миссией и стратегией развития и находящихся выражение в совокупности социальных норм и ценностей, разделяемых всеми сотрудниками Компании.
- Работник - физическое лицо, которое состоит в трудовых отношениях с Компанией на основании заключенного Трудового договора и работающее в Компании по основному месту работы, либо по совместительству.
- Сотрудник – физическое лицо, вступившее в трудовые взаимоотношения с работодателем.

Сокращения и обозначения

ФИО – фамилия, имя, отчество. Имя и отчество указываются в виде инициалов.

Общие положения

- Под информационной безопасностью понимается состояние защищенности информации, характеризующееся способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.
- Политика информационной безопасности разработана в соответствии с положениями международного стандарта
- Политика информационной безопасности утверждается Председателем совета директоров Группы компаний MakariSoft.
- Пересмотр Политики проводится на регулярной основе не реже одного раз в год.
- Ответственность за общий контроль содержания настоящего документа и внесение в него изменений возлагается на Руководителя Департамента безопасности.

Цели в области информационной безопасности

В области информационной безопасности Группой компаний MakariSoft устанавливаются следующие стратегические цели:

- Повышение конкурентоспособности бизнеса Группы компаний MakariSoft;
- Соответствие требованиям законодательства и договорным обязательствам в части информационной безопасности;
- Повышение деловой репутации и корпоративной культуры Группы компаний MakariSoft;
- Эффективное управление информационной безопасностью и непрерывное совершенствование системы управления информационной безопасностью;
- Достижение адекватности мер по защите от угроз информационной безопасности;
- Обеспечение безопасности корпоративных активов Группы компаний MakariSoft, включая персонал, материально-технические ценности, информационные ресурсы, бизнес-процессы.

Задачи обеспечения информационной безопасности

Система обеспечения информационной безопасности Группы компаний MakariSoft должна решать следующие задачи:

- Вовлечение высшего руководства Группы компаний MakariSoft в процесс обеспечения информационной безопасности: деятельность по обеспечению информационной безопасности инициирована и контролируется высшим руководством Группы компаний MakariSoft;
- Соответствие требованиям законодательства РФ: Группа компаний MakariSoft реализует меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством и договорными обязательствами;
- Согласованность действий по обеспечению информационной, физической и экономической безопасности: действия по обеспечению информационной, физической и экономической безопасности осуществляются на основе четкого взаимодействия заинтересованных подразделений Группы компаний MakariSoft и согласованы между собой по целям, задачам, принципам, методам и средствам;
- Применение экономически целесообразных мер: Группа компаний MakariSoft стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации; Политика Информационной Безопасности

- Проверка работников: все кандидаты на вакантные должности в Группе компаний MakariSoft в обязательном порядке проходят проверку в соответствии с установленными процедурами;
- Документированность требований информационной безопасности: в Группе компаний MakariSoft все требования в области информационной безопасности фиксируются в разрабатываемых внутренних нормативных документах;
- Повышение осведомленности в вопросах обеспечения информационной безопасности: документированные требования в области информационной безопасности доводятся до сведения работников всех бизнесподразделений Группы компаний MakariSoft и контрагентов в части их касающейся;
- Реагирование на инциденты информационной безопасности: Группа компаний MakariSoft стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения информационной безопасности;
- Оценка рисков: в Группе компаний MakariSoft на постоянной основе реализуются мероприятия по оценке и управлению рисками информационной безопасности, повышению уровня защищенности информационных активов;
- Учет требований информационной безопасности в проектной деятельности: помимо операционной деятельности, Группа компаний MakariSoft стремится учитывать требования информационной безопасности в проектной деятельности. Разработка и документирование требований по обеспечению информационной безопасности осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации;
- Постоянное совершенствование системы информационной безопасностью: совершенствование системы информационной безопасности является непрерывным процессом.

Принципы обеспечения информационной безопасности

Принцип системности

В Группе компаний MakariSoft активы рассматриваются, как взаимосвязанные и взаимовлияющие компоненты единой системы. Учитывается максимально возможное количество сценариев поведения системы в случае возникновения угроз информационной безопасности. Система защиты строится с учетом не только всех известных каналов получения несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности;

Принцип полноты (комплексности)

Для обеспечения информационной безопасности используется широкий спектр мер, методов

и средств защиты информации. Комплексное их использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающие все существующие каналы угроз и не содержащие слабых мест на стыках отдельных её компонентов;

Принцип эшелонированности

Нельзя полагаться на один защитный рубеж, каким бы надежным он ни казался. Система обеспечения информационной безопасности строится таким образом, чтобы наиболее защищаемая зона безопасности находилась внутри других защищаемых зон;

Принцип равнопрочности

Эффективность защитных механизмов не должна быть сведена на нет слабым звеном, возникшим в результате недооценки реальных угроз либо применения неадекватных мер защиты;

Принцип непрерывности

В Группе компаний MakariSoft обеспечение информационной безопасности является непрерывным целенаправленным процессом, предполагающим принятие соответствующих мер на всех этапах жизненного цикла активов.

Принцип разумной достаточности

Руководство Группы компаний MakariSoft исходит из того, что создать «абсолютную» защиту активов невозможно. Поэтому выбор средств защиты активов, адекватных реально существующим угрозам (т.е. обеспечивающих допустимый уровень возможного ущерба в случае реализации угроз), осуществляется на основе проведения анализа рисков;

Принцип законности

При выборе и реализации мер и средств обеспечения информационной безопасности Группой компаний MakariSoft строго соблюдается законодательство Российской Федерации, требования нормативных правовых и технических документов в области обеспечения информационной безопасности Группы компаний MakariSoft;

Принцип управляемости

Все процессы управления и обеспечения информационной безопасностью в Группе компаний MakariSoft должны быть управляемыми, т.е. должна быть возможность мониторинга и измерения процессов и компонентов, своевременного выявления нарушений информационной безопасности и принятия соответствующих мер; - Принцип персональной ответственности

Ответственность за обеспечение безопасности активов возлагается на каждого работника в пределах его полномочий.

Распределение ролей и ответственности

Для эффективного внедрения процессов управления информационной безопасностью в Группе компаний MakariSoft внедряется система управления информационной безопасностью на основе требований Международного стандарта. Система управления информационной безопасностью регламентируется отдельными положениями и стандартами, принятыми в Группе компаний MakariSoft.

Подразделения информационной безопасности:

- Совместно с представителями бизнес-подразделений и подразделений Департамента информационных технологий, включая обособленные подразделения Компании, занимающиеся поддержкой и внедрением информационных сервисов (далее ИТ), проводят оценку рисков, связанных с защитой информации, и осуществляют управление этими рисками;
- Совместно с подразделениями ИТ разрабатывают и внедряют политики и стандарты информационной безопасности, основанные на признанных в мире стандартах информационной безопасности;
- Разрабатывают планы и технические спецификации для внедрения систем информационной безопасности;
- Определяют требования по информационной безопасности для существующих и внедряемых информационных систем;
- Обосновывают и совместно с ИТ защищают общий бюджет ИТ в части, касающейся информационной безопасности Группы компаний MakariSoft, с целью выделения достаточных средств для функционирования и развития систем информационной безопасности;
- Участвуют в разработке стандартов, инструкций и иных нормативных документов в сфере ИТ, выборе контрагентов и утверждении технических решений в части информационной безопасности;
- Проводят аудит информационных систем с целью выявления потенциальных уязвимостей в корпоративных информационных системах, используют предоставленные ИТ возможности и инструменты, организуют оповещение пользователей о попытках вторжения в информационные системы;
- Могут привлекать ресурсы сторонних фирм для проведения аудита информационных систем с точки зрения информационной безопасности;

- Организуют и проводят обучение сотрудников Компании по информационной безопасности, проверяют знания и навыки информационной безопасности сотрудников Компании;
- Принимают активное участие в процессе изменения информационных систем для обеспечения требуемого уровня информационной безопасности;
- Согласовывают и контролируют доступ пользователей к информационным ресурсам;
- Проводят постоянную работу с пользователями информационных ресурсов Компании по разъяснению им основных требований информационной безопасности.

Подразделения Информационных технологий:

- Внедряют новые информационные системы и инструменты, обеспечивающие реализацию совместно разработанных политик, стандартов информационной безопасности;
- Обеспечивают работоспособность и доступность информационных систем;
- Соблюдают все требования информационной безопасности; совместно разработанные требования
- Разрабатывают и внедряют планы развития информационных систем,
- Обеспечивают финансирование и осуществляют все виды технической деятельности в корпоративных информационных системах;
- Следуют совместно принятым корпоративным политикам, стандартам и инструкциям по информационной безопасности, равно как и своим функциональным обязанностям;
- Следуют совместно разработанным требованиям и рекомендациям подразделений информационной безопасности на всех стадиях реализации новых проектов: от предложения и планирования до осуществления;
- Управляют процессом изменения информационных систем Группы компаний MakariSoft;
- Незамедлительно информируют подразделения информационной безопасности о любых нарушениях, уязвимостях, обнаруженных в корпоративных информационных системах и попытках незаконного проникновения в них;
- Обеспечивают доступ пользователей к компьютерным системам;
- Являются держателем бюджета ИТ, включая статьи расходов на информационную безопасность, и обеспечивают финансирование утвержденных проектов информационной безопасности;
- Обеспечивают техническую эксплуатацию систем безопасности.

Ответственность за нарушение Политики информационной безопасности

В случае нарушения установленных правил работы с информационными активами работник может быть ограничен в правах доступа к таким активам, а также привлечен к ответственности в соответствии с Трудовым кодексом, Кодексом об административных правонарушениях и Уголовным кодексом РФ.