Приложение

к приказу генерального директора
ООО «Компания «МИРО»
от «19» 09 2022 г. № 64

ПОЛИТИКА
в области информационной безопасности
общества с ограниченной
ответственностью «Компания «МИРО»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящая Политика является основополагающим документом, предназначенным для выражения позиции общества с ограниченной ответственностью «Компания «МИРО» (далее – ООО «Компания «МИРО», Общества) в области информационной безопасности, определяет систему взглядов, принципов и подходов в этой области для обеспечения защищенности бизнес-процессов Общества, создания условий безопасного цифрового развития Общества и обеспечения соответствия требованиям законодательства Российской Федерации в данной области, а также применимого законодательства любого иного государства, где Общество осуществляет деятельность.

Настоящая Политика разработана в соответствии с требованиями законодательства Российской Федерации в области информационной безопасности, с учетом применимых международных стандартов, передового опыта и лучших практик.

2. Настоящая Политика обязательна для исполнения работниками ООО «Компания «МИРО».

3. Настоящая Политика является локальным нормативным документом постоянного действия.

Настоящая Политика утверждается, изменяется и признается утратившей силу в ООО «Компания «МИРО» решением единственного участника Общества и вводится в действие приказом генерального директора.

4. В рамках настоящей Политики используются следующие термины и их определения:

автоматизированная система управления - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) (АСУ), производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

компьютерная атака - действия, направленные на реализацию угроз несанкционированного доступа к ИТ-активу, воздействия на него или на ресурсы автоматизированной информационной системы с применением программных и (или) технических средств;

информационная безопасность – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах Общества;

информационная инфраструктура (ИТ-инфраструктура) - совокупность компонентов информационных технологий, в том числе аппаратное (системы обработки и хранения данных, оборудование рабочего места, периферия и т.д.), системное программное и инженерное обеспечение, сети, специализированные помещения;

информационная система (ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационная среда (ИТ-среда) – совокупность разной информации вместе с инфраструктурой, а также субъектами, которые занимаются сбором, использованием и распространением информации;

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

информация – сведения (сообщения, данные) независимо от формы их представления;

ИТ-актив - идентифицируемый предмет, вещь или объект в области информационных технологий, который имеет потенциальную или действительную ценность для Общества;

ИТ-пространство - совокупность объектов (информационные ресурсы, средства информационного взаимодействия и информационная инфраструктура), вступающих друг с другом в информационное взаимодействие, а также сами информационные технологии, обеспечивающие данное взаимодействие;

мобильное техническое средство – съемные машинные носители информации, портативные вычислительные устройства и устройства связи с возможностью обработки информации (переносные персональные компьютеры ноутбуки, нетбуки, планшетные компьютеры, а также мобильные телефоны, смартфоны, умные часы/браслеты, цифровые камеры, звукозаписывающие устройства и иные средства);

программное обеспечение - совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ;

производственная система – совокупность компонентов информационных технологий, обеспечивающих автоматизацию решения задач планирования и управления различными видами производственной деятельности и производственных процессов;

риск информационной безопасности (ИБ-риск) - сочетание вероятности реализации угрозы информационной безопасности и последствий её реализации, оказывающих негативное влияние на достижение целей Общества;

структурное подразделение - структурное подразделение Общества с самостоятельными функциями, задачами и ответственностью в рамках своих компетенций, определенных в Положении о структурном подразделении;

угроза информационной безопасности (угроза) - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации или безопасности ИТ-актива;

уязвимость ИТ-актива - недостаток (слабость) ИТ-актива в целом, который(-ая) может быть использован(а) для реализации угроз информационной безопасности;

цифровизация – применение прорывных технологий, трансформирующих операционные процессы за счет замещения или дополнения человека на базе использования качественно новой аналитики, искусственного интеллекта, мобильных и носимых устройств, роботизации, интеграционных технологических платформ.

5. В рамках настоящей Политики устанавливается следующее распределение ролей:

деловой партнер - текущие и потенциальные контрагенты ООО «Компания «МИРО»;

руководители и специалисты по информационной безопасности Общества – руководители и/или работники структурного подразделения ООО «Компания «МИРО», ответственного за координацию, планирование и организацию функционирования процессов в области информационной безопасности и за операционное управление ими;

третьи лица - хозяйственные общества, в которых ООО «Компания «МИРО» не имеет прямой либо косвенной доли в уставных капиталах, некоммерческие организации, в состав органов управления которых не входят представители Общества, а также лица, не являющиеся работниками и не занимающие должности в органах управления ООО «Компания «МИРО»;

руководство Общества – генеральный директор ООО «Компания «МИРО», заместители генерального директора, главный бухгалтер, руководители структурных подразделений.

2. ЗАЯВЛЕНИЕ О ПОЛИТИКЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Настоящая Политика выражает позицию Общества в области информационной безопасности. Принятием настоящей Политики Общество провозглашает и обязуется осуществлять все возможные меры для защиты работников, имущества, информации, деловой репутации и бизнес-процессов Общества от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности.

Руководство Общества осознает важность и необходимость продвижения и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства РФ и регулирования норм информационной безопасности, а также развития

используемых информационных технологий при автоматизации и цифровизации бизнес-процессов и технологических процессов.

Соблюдение принципов информационной безопасности дополнительно позволит упрочить конкурентные преимущества Общества, обеспечить соответствие правовым, регуляторным и договорным требованиям, снизить имиджевые риски.

Настоящая Политика разработана с целью установления принципов, определяющих общие организационные и управленческие подходы, необходимые для обеспечения и управления информационной безопасностью Общества и защиты интересов Общества от рисков и угроз информационной безопасности.

Руководство Общества придерживается взглядов, что соблюдение принципов, правил и требований информационной безопасности является, в том числе, элементом корпоративной культуры. Следование требованиям информационной безопасности является важным условием при осуществлении повседневной деятельности, включая совместную работу с Деловыми партнерами. Каждый работник Общества и его Деловой партнер несёт ответственность за безопасную работу с вверенными ему корпоративными ИТ-активами, компьютерным оборудованием, мобильными техническими средствами, носителями информации, предоставленной и обрабатываемой информацией Общества.

Руководители и специалисты по информационной безопасности Общества должны ответственно выполнять свои обязанности, осознавая, что качество их работы непосредственно влияет на состояние защищённости информации, ИТ-активов, бизнес- и технологических процессов Общества.

Работники Общества должны руководствоваться настоящей Политикой в профессиональной деятельности, при внутрикорпоративном взаимодействии, личном развитии и повышении культуры информационной безопасности.

Политика раскрывает и дополняет при необходимости правила, определенные в Кодексе деловой этики, в части принципов обеспечения информационной безопасности.

3. ЦЕЛИ И ЗАДАЧИ ОБЩЕСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Управление и обеспечение информационной безопасности Общества ориентированы на достижение следующих целей в области информационной безопасности:

- предоставление безопасной информационной среды для функционирования и развития бизнес-процессов Общества;
- снижение уровня ИБ-рисков и угроз информационной безопасности до приемлемого уровня, позволяющего осуществлять устойчивое цифровое развитие Общества.

Для достижения данных целей необходимо решение следующих задач:

- обеспечение информационной безопасности бизнес-процессов Общества в условиях возрастающего уровня угроз, включая обеспечение оперативного мониторинга и оценку состояния защищенности в Общества;
- повышение эффективности защиты от спланированных целенаправленных компьютерных атак злоумышленниками;
- применение новых современных методов для защищенной цифровизации Общества, включая организацию проработки вопросов информационной безопасности при реализации цифровых решений; организацию апробации и применения новых методов защиты информации от современных угроз, в том числе за счет взаимодействия и партнерства с лидерами отрасли информационной безопасности; обеспечение применения безопасных цифровых технологий при внедрении отечественных разработок и развитии собственного конкурентоспособного корпоративного программного обеспечения Общества;
- соответствие требованиям государства в области информационной безопасности путем обеспечения заданного уровня информационной безопасности ИТ-активов в соответствии с требованиями действующего законодательства стран присутствия Общества.

4. ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В рамках обеспечения информационной безопасности объектами защиты в Обществе являются информация, обрабатываемая в Обществе, вне зависимости от формы представления; ИТ-активы, включая, но не ограничиваясь следующим перечнем:

- автоматизированные рабочие места, средства обработки информации и мобильные технические средства;
- ИС, системы хранения данных, программное обеспечение и отдельные технические решения;
- АСУ, системы метрологии и промышленной автоматизации, в том числе измерительные системы;
- ИТ-инфраструктура, информационно-телекоммуникационные сети и системы связи;
- ИТ-сервисы;
- решения по цифровизации бизнес- и технологических процессов.

5. ПРИНЦИПЫ УПРАВЛЕНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Деятельность Общества в области информационной безопасности осуществляется с соблюдением следующих основных принципов.

Ориентация на стратегию Общества – стратегические инициативы по информационной безопасности разрабатываются и осуществляются в соответствии с общей стратегией и целями развития Общества, с учетом корпоративных стратегий в области информационных технологий и в области автоматизации, метрологии.

Централизация функций управления – принцип заключается в возможности принятия управленческих решений в области информационной безопасности на уровне Общества за счет оперативного мониторинга (ИТ-пространства Общества и внешней обстановки в информационной сфере) и оценки состояния информационной безопасности; осуществления централизованного управления стратегическими инициативами по информационной безопасности; контроля реализации мероприятий по развитию информационной безопасности; создания и развития централизованных решений в области информационной безопасности.

Проактивный подход и управление рисками – базируется на мониторинге, анализе и оценке появляющихся, актуальных и будущих ИБ-рисков и угроз информационной безопасности (включая изучение технологий, используемых злоумышленниками) с целью своевременного и осознанного принятия превентивных мер для предупреждения компьютерных атак и недопущения ущерба Обществу.

Стандартизация и унификация – подразумевает разработку и тиражирование в Обществе стандартизованных требований и подходов, типовых технических решений и элементов архитектуры обеспечения информационной безопасности для унификации средств и методов решения однотипных задач; интерфейсов управления системами информационной безопасности.

Импортозамещение – заключается в снижении рисков неблагоприятной внешней конъюнктуры за счёт ориентирования на отечественные решения, средства и сервисы при обеспечении информационной безопасности на территории Российской Федерации.

Ресурсное обеспечение – означает необходимость выделения целевого финансирования на обеспечение и развитие информационной безопасности Общества, поддержание требуемой организационной структуры.

Законность и соответствие – деятельность по обеспечению информационной безопасности Общества основывается на выполнении требований нормативных правовых актов Российской Федерации и национального законодательства стран, на территории которых осуществляет деятельность Общество.

Повышение культуры информационной безопасности – декларирует необходимость не только информировать всех работников Общества, её Деловых партнёров и третьих лиц, использующих ИТ-активы Общества, о требованиях информационной безопасности, но развивать навыки приемлемого обращения с информацией и безопасной работы с ИТ-активами Общества.

Развитие компетенций и профессионализма – принцип означает необходимость постоянного развития компетенций и практических навыков специалистов по информационной безопасности в условиях непрекращающегося изменения ИБ-рисков, ландшафта используемых информационных технологий и техник потенциальных нарушителей.

Обеспечение информационной безопасности при автоматизации технологических и производственных процессов требует компетенций и знаний в областях производственной автоматизации и метрологии.

Накопление знаний и обмен опытом – следует накапливать знания и обмениваться опытом в ходе осуществления практической деятельности по обеспечению информационной безопасности (при мониторинге и реагировании на компьютерные атаки, при внедрении и эксплуатации технических решений, при аудитах информационной безопасности и т.д.).

Информационная безопасность как неотъемлемое свойство ИТ-актива – принцип заключается в следующем:

- требования информационной безопасности учитываются на всех этапах жизненного цикла ИТ-актива, вне зависимости от уровня конфиденциальности информации, обрабатываемой в ИТ-активе;
- создание программных продуктов в интересах Общества осуществляется с применением методов безопасной разработки программного обеспечения;
- предпочтительными являются ИТ-активы с наибольшим покрытием требований информационной безопасности встроенными функциями (при прочих равных характеристиках);
- встроенные функции по информационной безопасности должны быть настроены и использоваться при эксплуатации ИТ-активов, включая программно-аппаратные средства, автоматизированные системы управления и т.д.;
- соответствие приобретаемого/внедряемого ИТ-актива требуемому уровню информационной безопасности подтверждается согласно существующими процедурами, с учетом требований применимого законодательства.

Информационная безопасность как неотъемлемое свойство ИТ-сервиса (ИТ-услуги) – означает, что предлагаемые и оказываемые Общества или в интересах Общества ИТ-услуги и ИТ-сервисы должны разрабатываться и оказываться с учетом требований информационной безопасности.

Совместимость – подразумевает подбор компонентов для обеспечения информационной безопасности способом, гарантирующим их взаимную системную совместимость на информационном, программном, электромагнитном и эксплуатационном уровнях, а также совместимость с используемыми ИТ-решениями, информационными технологиями и с решениями по автоматизации технологических и производственных процессов Общества.

Надежность – использование компонентов и средств для обеспечения информационной безопасности, соответствующих требованиям по надежности, готовности и обслуживаемости.

Адекватность и обоснованность решений – принимаемые в Общества меры и применяемые средства информационной безопасности эффективны, результативны и соразмерны с величиной ИБ-рисков и угроз информационной безопасности, влияющих на цели Общества.

Комплексность – применение любых доступных законных методов, средств и мероприятий (включая законодательные и нормативно-правовые, организационно-административные, программно-технические, инженерно-технические, физические), направленных на снижение ИБ-рисков, пресечение угроз информационной безопасности и недопущение ущерба Общества, её Деловым партнёрам и работникам.

Разделение и минимизация полномочий – означает, что выполнение критичных (итоговых) операций проводится только посредством разделения действий (например, алгоритмического разделения, временного или ресурсного - в т.ч. двумя работниками). Исключение единоличного совершения критичной операции может быть организовано на уровне организационных мер и/или программно-технических средств за счет выделения полномочий или роли пользователя.

Программно-технический способ разделений полномочий является предпочтительным относительно организационного.

Должны осуществляться контроль реализации принципов разграничения критических полномочий в ИС и в АСУ, ограничение прав доступа, в зависимости от уровня согласованных полномочий. Полномочия должны быть минимально достаточными для выполнения лицом своих должностных обязанностей, либо выполнения контрактных обязательств. При необходимости должен осуществляться контроль конфликта полномочий – организационный, а также программно-аппаратный.

Постоянство совершенствования информационной безопасности – обеспечение постоянного улучшения существующей практики и совершенствования средств и методов управления и обеспечения информационной безопасности на основе результатов аудитов информационной безопасности, мониторинга функционирования систем информационной безопасности, анализа изменений в методах и средствах компьютерных атак, анализа нормативных требований и существующего передового отечественного и зарубежного опыта в этой области.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Работники Общества должны выполнять требования и правила информационной безопасности при работе с информацией и ИТ-активами Общества и его Деловых партнёров.

Высокие корпоративные стандарты и правила обеспечения информационной безопасности обязательны для всех без исключения работников Общества и должны учитываться во взаимоотношениях с Деловыми партнерами.

Генеральный директор Общества возлагает ответственность на руководителей структурных подразделений за организацию повседневной деятельности и выделение необходимых ресурсов для обеспечения информационной безопасности как неотъемлемой составляющей бизнес- и производственных процессов; за своевременную идентификацию значимых

ИТ-активов, назначение ответственных за ИТ-активы и управление доступа к ним; за предъявление установленных требований информационной безопасности к работникам Общества и Деловым партнерам, использующим ИТ-активы Общества, и контроль за их выполнением.

При использовании сети Интернет, при общении в социальных сетях и мессенджерах, использовании электронной почты, других средств телекоммуникаций и мобильных технических средств работникам Общества рекомендуется проявлять осмотрительность и сдержанность, чтобы не допускать рисков личной безопасности, а также избегать непреднамеренной утечки рабочей информации.

Правила внешних коммуникаций устанавливаются Кодексом деловой этики ООО «Компания «МИРО».

Каждый работник Общества за несоблюдение требований информационной безопасности несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

Работники Деловых партнёров, использующие корпоративные ИТ-активы, а также предоставленную Обществом информацию, несут ответственность в соответствии с договорными отношениями, а также применимым законодательством.

7. ДОВЕДЕНИЕ И РАСПРОСТРАНЕНИЕ ПОЛИТИКИ

Настоящая Политика является публичной.

ООО «Компания «МИРО» доводит настоящую Политику до своих Деловых партнеров и взаимодействуют с ними с учетом положений настоящей Политики.