Приложение к приказу
от 03.12.2021 №ГД-01/653

Политика информационной безопасности ПАО «ММК»

1 Введение

Политика информационной безопасности (далее – Политика) ПАО «ММК» (далее – Компания) определяет систему взглядов на проблему обеспечения информационной безопасности (далее – ИБ). Представляет собой систематизированное изложение высокоуровневых целей и задач защиты, которыми необходимо руководствоваться в своей деятельности, а также основных принципов построения системы управления информационной безопасностью Компании.

Обеспечение информационной безопасности – необходимое условие для успешного осуществления уставной деятельности Компании.

Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информационных ресурсов и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Компания.

Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических и организационных мероприятий.

2 Область действия

Политика распространяется на ПАО «ММК». Следование принципам и направлениям настоящей Политики обязательно во всех структурных подразделениях (подразделениях) ПАО «ММК».

3 Цели Политики

Целью Политики является:

- Повышение конкурентоспособности бизнеса Компании.
- Соответствие требованиям законодательства РФ, международным стандартам и договорным обязательствам в части информационной безопасности.
- Повышение деловой репутации и корпоративной культуры Компании.
- Достижение адекватности мер по защите от угроз информационной безопасности.
- Предотвращение и (или) снижение ущерба от реализации угроз информационной безопасности.

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков ИБ.

Для достижения основной цели необходимо обеспечивать эффективное

решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- соответствие требованиям Федерального законодательства РФ, международных стандартов в области ИБ и договорных обязательств в части ИБ;
- обеспечение непрерывности критических бизнес-процессов;
- достижение адекватности мер по защите от угроз ИБ;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности работников;
- повышение деловой репутации и корпоративной культуры;
- предотвращение неправомерного доступа к информации;
- недопущение воздействия и восстановление функционирования информационной инфраструктуры.

4 Принципы Политики

Достижение целей Политики Компании обеспечивается соблюдением следующих принципов:

а) Вовлеченность высшего руководства Компании в процесс обеспечения информационной безопасности. Деятельность по обеспечению информационной безопасности инициирована и контролируется высшим руководством Компании. Высшее руководство Компании выполняет те же правила по обеспечению информационной безопасности, что и все работники Компании.

б) Законность обеспечения информационной безопасности. Компания реализует меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством и договорными обязательствами.

в) Экономическая целесообразность. Компания стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации.

г) Документированность требований информационной безопасности. Компания стремится, чтобы все требования в области информационной безопасности были зафиксированы в локальных нормативных актах Компании.

д) Осведомленность в вопросах обеспечения информационной безопасности. Документированные требования в области информационной безопасности доводятся до сведения работников Компании и контрагентов в части их касающейся. Компания на периодической основе осуществляет информирование, ознакомление и обучение работников по вопросам обеспечения информационной безопасности.

е) Реагирование на инциденты информационной безопасности. Компания стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения информационной безопасности.

ж) Приоритет предотвращения компьютерных атак. Компания стремится обеспечивать непрерывность и комплексность безопасности информационной инфраструктуры.

з) Персональная ответственность. Работники Компании несут персональную ответственность за соблюдение требований информационной безопасности. Обязанности по обеспечению информационной безопасности включаются в трудовые договоры и должностные инструкции работникам, а также в договоры (соглашения) с контрагентами.

и) Учет действий с информационными активами. Компания стремится вести учет всех действий работников Компании и контрагентов с информационными активами Компании.

к) Предоставление минимально необходимых прав доступа. Работникам Компании и контрагентов предоставляются минимально необходимые права доступа для качественного и своевременного выполнения трудовых обязанностей и договорных обязательств.

л) Учет требований информационной безопасности в проектной деятельности. Помимо операционной деятельности, Компания 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.

5 Основные направления деятельности при реализации Политики

Реализация Политики достигается за счет обеспечения следующей деятельности:

- управление нормативным обеспечением информационной безопасности;
- управление рисками информационной безопасности;
- управление процессом повышения осведомленности в области информационной безопасности;
- управление антивирусной защитой;
- управление политикой использования (приобретения) программного обеспечения;
- управление парольной политикой;
- определение обязанностей и ответственности пользователей информационных ресурсов;
- определение правил безопасной работы в сети Интернет;
- управление доступом пользователей к информационным ресурсам ПАО «ММК»;
- управление обеспечением физической безопасности в помещениях, в которых обрабатывается информация;
- управление инцидентами информационной безопасности;
- обеспечение непрерывности бизнеса (управление резервными копиями основных служебных данных и программного обеспечения);
- защита корпоративной сети передачи данных, в том числе беспроводных подключений;
- управление мобильными устройствами;

- управление политикой доступа к внешним носителям информации;
- управление обновлениями;
- выявление и пресечение угроз информационной безопасности;
- управление конфигурациями вычислительной техники и программного обеспечения;
- управление изменениями информационных технологий в части информационной безопасности.