Приложение № 1 к Приказу Генерального директора АО «Гланит»
№ 58 от «23» сентября 2024 г.

Акционерное общество
«Гланит»
301370, Тульская область, Алексинский район, деревня Павлово, дом 35А
ОГРН 1177154027434 | ИНН 7111022115 | КПП 711101001
тел:+7 (48753) 9-10-00 | e-mail: reception@glanit.ru | web: https://glanit.ru

Политика информационной безопасности АО «Гланит»

Утверждено Приказом Генерального директора № 58 от «23» сентября 2024 г.
Дата введения в действие «01» ноября 2024 г.

Тульская область, Алексинский район,
д. Павлово
2024 г.

Содержание

1. Назначение и область применения

1.1. Политика информационной безопасности АО «Гланит» (далее по тексту – Политика) представляет собой основополагающий документ, определяющий принятые руководством АО «Гланит» (далее по тексту – Компания) позицию, цели, задачи и принципы в области обеспечения информационной безопасности.

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

1.3. Основными целями обеспечения информационной безопасности являются:

- защита интересов Компании, работников и иных субъектов, взаимодействующих с Компанией, от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем Компании, нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;
- обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов Компании;
- соблюдение правового режима использования информации и информационных технологий.

1.4. Настоящая Политика обязательна для применения:

- всеми работниками Компании;
- работниками сторонних (в т.ч. подрядных) организаций и иными субъектами, взаимодействующими с Компанией, участвующими в информационном обмене и/или использующими информационные активы Компании.

2. Термины, определения, обозначения и сокращения

В настоящей Политике используются термины с соответствующими определениями:

Деловой партнёр – текущие и потенциальные контрагенты Компании, иные лица, взаимодействующие с Компанией, имеющие общие интересы и цели, способствующие благоприятной деятельности и устойчивому развитию Компании, а также органы государственной власти и управления.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационный актив (ИТ-актив) – идентифицируемый предмет, вещь или объект в области информационных технологий, который имеет потенциальную или действительную ценность для Компании.

Информационная безопасность (ИБ) – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в интересах Компании.

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

Информационная среда (ИТ-среда) – совокупность информации вместе с ИТ-инфраструктурой, а также субъектами, участвующими в обработке информации и использованием ИТ-инфраструктуры.

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

3. Общие положения

Принятием настоящей Политики Компания провозглашает и обязуется осуществлять все возможные меры для защиты информационных активов от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности.

Руководство Компании осознает важность и необходимость совершенствования мер и средств обеспечения информационной безопасности в контексте развития информационных технологий, автоматизации и цифровизации бизнес- и технологических процессов на производствах, а также совершенствования законодательства РФ и регулирования норм информационной безопасности.

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

Для достижения целей настоящей Политики устанавливаются принципы, определяющие общие организационные и управленческие подходы, необходимые для обеспечения и управления информационной безопасностью Компании и защиты интересов Компании от рисков и угроз информационной безопасности.

Руководство Компании придерживается взглядов, что соблюдение принципов, правил и требований информационной безопасности является важным условием при осуществлении повседневной деятельности, включая совместную работу с Деловыми партнерами.

Каждый работник Компании и/или её Деловых партнеров несёт ответственность за безопасную работу с вверенными ему ИТ-активами (компьютерным оборудованием, мобильными техническими средствами, носителями информации, предоставленной и обрабатываемой информацией Компании).

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

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

Каждый работник Компании несёт ответственность за выполнение требований информационной безопасности при работе с информационными активами.

4. Цели и задачи в области информационной безопасности

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

- предоставление безопасной информационной среды для функционирования и развития бизнеса;
- соответствие требованиям законодательства в области информационной безопасности и защиты персональных данных, а также соблюдение соответствующих договорных обязательств.

Для достижения данных целей необходимо решение следующих задач:

- проектирование, внедрение и непрерывное совершенствование системы управления информационной безопасностью (далее — СУИБ);
- вовлечение Руководства Компании в процесс функционирования СУИБ;
- повышение уровня осведомленности работников Компании и Деловых партнёров об актуальных угрозах информационной безопасности и способах минимизации рисков их реализации.

5. Принципы управления и обеспечения информационной безопасности

Деятельность Компании в области информационной безопасности осуществляется с соблюдением принципов, разработанных с учетом международных стандартов и практик в области информационной безопасности:

Ориентация на стратегию Компании – стратегические инициативы по информационной безопасности разрабатываются и осуществляются в соответствии с общей стратегией и целями развития Компании, внедрения информационных технологий и производственной автоматизации.

Централизация функций управления – управленческие решения в области информационной безопасности на уровне Компании принимаются комплексно с учетом оперативного мониторинга ИТ-пространства Компании и внешней обстановки в информационной сфере, оценки состояния информационной безопасности, особенностей ИТ-инфраструктуры.

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 Компании.

Стандартизация и унификация – подразумевает разработку и тиражирование в Компании стандартизованных требований и подходов, типовых технических решений и элементов архитектуры обеспечения 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 Компании, поддержание требуемой организационной структуры.

Законность и соответствие – деятельность по обеспечению информационной безопасности Компании основывается на выполнении требований нормативных правовых актов Российской Федерации.

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.

Неотъемлемость информационной безопасности – все элементы ИТ-среды Компании (в т.ч. сервисы, услуги) должны использоваться с учетом требований информационной безопасности, на всех этапах их жизненного цикла (проектирование, внедрение и т.д.).

Обоснованность и достаточность решений – принимаемые меры и средства информационной безопасности должны применяться с учетом экономической целесообразности: эффективности и соразмерности с величиной рисков и угроз информационной безопасности.

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

Разделение и минимизация полномочий – 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.

6. Ответственность за нарушения в области информационной безопасности

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

Руководство Компании возлагает ответственность на Директора по информационным технологиям и руководителей подразделений АСУ ТП 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.

Руководство Компании возлагает ответственность на Службу безопасности за предъявление установленных требований информационной безопасности к работникам Компании и Деловым партнерам, использующим ИТ-активы Компании, 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 Компании рекомендуется проявлять осмотрительность и сдержанность, чтобы не допускать рисков личной безопасности, а также избегать непреднамеренной утечки рабочей информации. Каждый работник Компании за несоблюдение требований информационной безопасности несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

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

РАЗРАБОТЧИК:
Руководитель группы экономического контроля

СОГЛАСОВАНО:

Директор по ИТ

Директор по безопасности

Начальник юридического отдела