УТВЕРЖДЕНА
приказом АО «Кросс технолоджис»
от 03.03.2025 № КТ/03-03-2025/2-осн

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «КРОСС ТЕХНОЛОДЖИС»

Ответственный за применение Политики	Директор по кибербезопасности
Ответственное подразделение за разработку и актуализацию документа	Служба информационной безопасности

СОДЕРЖАНИЕ

1. Общие положения

1.1. Политика информационной безопасности АО «Кросс технолоджис» (далее – Политика) является концептуальным документом, формулирующим и отображающим позицию АО «Кросс технолоджис» (далее – Компания) в сфере обеспечения информационной безопасности Компании.

1.2. Политика разработана с учётом текущих целей деятельности и стратегии развития Компании.

1.3. Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам.

1.4. Политика построена на выполнении свода лучших практик, отражённых в требованиях нормативных правовых актов, методических документов и национальных стандартов Российской Федерации в сфере информационной безопасности.

1.5. Политика является корпоративным документом в сфере информационной безопасности первого уровня, т.е. определяет высокоуровневые задачи и цель обеспечения информационной безопасности Компании. Другие частные политики, процедуры, инструкции и т.п. разрабатываются с учётом требований Политики.

1.6. Руководство Компании осознаёт важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте изменения норм регулирования деятельности по защите информации, включая персональные данные, а также в контексте ожиданий контрагентов Компании.

1.7. Руководство Компании личным примером демонстрирует своё лидерство и приверженность в отношении системы управления информационной безопасности (далее – СУИБ) и обязуется:

– обеспечивать выделение необходимых ресурсов для выполнения Политики;

– назначать ответственных лиц для достижения поставленных задач;

– создавать условия для вовлечения и активного участия всех сотрудников Компании в процессы обеспечения информационной безопасности.

2. Область применения

2.1. Требования Политики распространяются на все процессы, информационные системы, ИТ-инфраструктуру Компании и обязательны для выполнения всеми работниками Компании, а также для всех лиц, имеющих доступ к информационным системам и активам Компании.

2.2. Политика должна учитываться при взаимоотношении Компании с контрагентами, если их действия связаны с использованием, обработкой, передачей или доступом к защищаемой информации или информационным активам Компании.

2.3. Требования Политики конкретизируются в отдельных внутренних нормативных документах Компании в области информационной безопасности для каждой из областей, например:

– управление доступом;
– категорирование и обработка информации;
– физическая безопасность и защита от воздействия окружающей среды;
– области, ориентированные на конечного пользователя;
– резервное копирование;
– передача информации;
– защита от вредоносных программ (антивирусная защита);
– управление техническими уязвимостями;
– средства криптографической защиты информации (СКЗИ)
– безопасность коммуникаций (защита вычислительных сетей);
– конфиденциальность и защита персональных данных;
– взаимоотношения с контрагентами.

3. Цель и задачи обеспечения информационной безопасности

3.1. Целью обеспечения информационной безопасности является поддержание устойчивого функционирования Компании, защита процессов и информационных активов, принадлежащих Компании и её контрагентам, в том числе:

– устойчивое функционирование и развитие Компании, обеспечение непрерывности предоставления услуг;

– поддержание статуса Компании как надёжного поставщика услуг по информационной безопасности;

– повышение конкурентоспособности бизнеса Компании;

– повышение деловой репутации и корпоративной культуры Компании;

– гарантия защищённости процессов и информационных активов, принадлежащих Компании и её клиентам.

– соблюдение требований законодательства и договорных обязательств в части информационной безопасности;

– предотвращение и (или) снижение ущерба от реализации угроз безопасности информации.

3.2. Задачи, решаемые для достижения цели в области информационной безопасности:

– разработка и внедрение процессов обеспечения информационной безопасности с учетом требований нормативных правовых актов, методических документов и национальных стандартов Российской Федерации в сфере защиты информации, а также рекомендаций международных стандартов и практик;

– построение моделей угроз безопасности информации;

– управление рисками информационной безопасности;

– постоянное совершенствование и развитие СУИБ с учётом новых угроз и требований;

– интеграция экспертных знаний в области информационной безопасности на ранних этапах проектирования информационных активов и процессов Компании;

– построение процесса непрерывного мониторинга, хранения и корреляции событий информационной безопасности для своевременного выявления инцидентов, реализация которых может нанести прямой или косвенный ущерб Компании;

– применение различных организационных и технических мер защиты информации, использование передовых технологий противодействия угрозам безопасности информации;

– вовлечение работников Компании в процессы обеспечения информационной безопасности, повышение ответственности, осведомленности, проведение регулярных обучений и получение обратной связи;

– обеспечение непрерывности деятельности Компании на основе комплекса организационно-методических и технических мероприятий, направленных на минимизацию последствий утраты информационных активов и поддержание бесперебойного оказания услуг клиентам;

– регулярная оценка соответствия СУИБ внутренним и внешним требованиям через внутренние аудиты, мониторинг процессов СУИБ и анализ со стороны руководства Компании;

– внедрение корректирующих действий в случае выявления отклонений или несоответствий в работе СУИБ внутренним и внешним требованиям.

4. Принципы обеспечения информационной безопасности

4.1. В рамках деятельности, связанной с информационной безопасностью, Компания руководствуется следующими основными принципами:

– Законность. Защита информационных активов Компании должна полностью соответствовать требованиям действующих нормативных правовых актов, методических документов и национальных стандартов Российской Федерации в сфере защиты информации.

– Системность. Меры защиты информации должны принимать во внимание все взаимосвязанные, взаимодействующие и изменяющиеся во времени элементы, условия и факторы, существенно значимые для понимания и решения проблемы обеспечения информационной безопасности.

– Комплексность. Эффективное сочетание организационных и технических мер защиты информации для снижения вероятности реализации наиболее значимых угроз безопасности информации.

– Непрерывность совершенствования. Меры и средства защиты информации должны постоянно совершенствоваться по результатам анализа функционирования СУИБ с учётом появления новых способов и средств реализации угроз безопасности информации, а также опыта других организаций в сфере информационной безопасности.

– Разумная достаточность и адекватность. Программно-технические средства и организационные меры защиты информации должны быть обоснованы с точки зрения оценки рисков, обеспечивая оптимальный баланс между эффективностью защиты и минимизацией воздействия на работу Компании.

– Персональная ответственность. Ответственность за информационную безопасность распределяется между всеми работниками Компании в пределах их полномочий, включая соответствующее вовлечение в процессы повышения осведомленности и обучения.

– Контроль. Оценка эффективности СУИБ должна быть неотъемлемой частью процесса обеспечения информационной безопасности. Для своевременного выявления нарушений и их предотвращения в Компании должны быть определены процедуры регулярного контроля и анализа эффективности мер защиты информации.

4.2. Компания берёт на себя ответственность за соответствие положений Политики требованиям заинтересованных сторон, доведение и разъяснение их работникам Компании и заинтересованным сторонам, назначение ответственных за решение соответствующих задач для достижения этих целей на всех уровнях, а также за их реализацию, периодический анализ и пересмотр.

5. Порядок утверждения и пересмотра

5.1. Политика утверждается приказом Компании.

5.2. Политика подлежит пересмотру для обеспечения уверенности в сохранении её приемлемости, адекватности и результативности в следующих случаях:

– истечение 3 (трёх) лет с момента утверждения;

– изменения целей и задач Компании в области обеспечения информационной безопасности;

– существенные изменений в процессах и деятельности Компании;

– выявление новых угроз безопасности информации, технологий или уязвимостей, требующих обновления подходов;

– результаты внутреннего аудита или мониторинга эффективности СУИБ, подтверждающие необходимость корректировки.