Корпоративная политика управления данными и информационной безопасности

Версия 2.0 - 20 мая 2025 г.

1. ВВЕДЕНИЕ

1.1 Цель документа

Настоящая Корпоративная политика управления данными и информационной безопасности ("Политика") устанавливает основные принципы, требования и правила обращения с корпоративной информацией в ООО "ТехноИнновация" (далее - "Компания"). Политика разработана для обеспечения надлежащей защиты данных, соблюдения нормативных требований, минимизации рисков информационной безопасности и создания культуры ответственного отношения к информационным ресурсам.

1.2 Область применения

Действие настоящей Политики распространяется на всех сотрудников Компании, включая временных работников, консультантов, подрядчиков, деловых партнеров и третьих лиц, имеющих доступ к корпоративным информационным системам. Политика охватывает все данные, создаваемые, получаемые, хранимые и обрабатываемые Компанией, независимо от формата и местонахождения, включая облачные сервисы и мобильные устройства.

1.3 Законодательная база

Настоящая Политика разработана в соответствии со следующими нормативно-правовыми актами:

•Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (с изменениями и дополнениями)
•Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (с изменениями и дополнениями)
•Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ
•Федеральный закон "О банках и банковской деятельности" (для финансовых операций)
•Международный стандарт ISO/IEC 27001:2022 "Информационные технологии - Методы обеспечения безопасности - Системы менеджмента информационной безопасности"
•Стандарт PCI DSS (для данных, связанных с платежными картами)
•Иные применимые нормативно-правовые акты Российской Федерации

2. КЛАССИФИКАЦИЯ ИНФОРМАЦИИ

2.1 Категории данных

В рамках настоящей Политики информация, обрабатываемая Компанией, классифицируется по следующим категориям:**2.1.1 Публичная информация** Информация, которая официально одобрена руководством Компании для публичного распространения и не требует специальных мер защиты. Примеры: маркетинговые материалы, общедоступная информация о продуктах и услугах, пресс-релизы, публикации в социальных сетях, утвержденные к публикации годовые отчеты.**2.1.2 Внутренняя информация** Информация для внутреннего использования, несанкционированное раскрытие которой может нанести репутационный ущерб Компании или создать неудобства в операционной деятельности. Примеры: внутренние процедуры, регламенты, корпоративные телефонные справочники, организационные диаграммы, учебные материалы, внутренние объявления.**2.1.3 Конфиденциальная информация** Информация ограниченного доступа, несанкционированное раскрытие которой может привести к финансовым потерям или правовым последствиям. Примеры: финансовые отчеты, данные клиентов (не содержащие персональных данных), интеллектуальная собственность, коммерческие договоры, информация о ценах и скидках.**2.1.4 Строго конфиденциальная информация** Критически важная информация, требующая максимального уровня защиты, несанкционированное раскрытие которой может привести к значительному ущербу для Компании. Примеры: стратегические планы развития, патенты в разработке, исходные коды программного обеспечения, персональные данные клиентов и сотрудников, информация о безопасности.**2.1.5 Регулируемая информация** Информация, обработка которой регулируется специальными законодательными актами и нормативными требованиями. Эта категория может пересекаться с другими категориями в зависимости от контекста. Примеры: персональные данные, медицинская информация, данные платежных карт, финансовая отчетность.

2.2 Маркировка данных

Все документы и файлы, содержащие конфиденциальную и строго конфиденциальную информацию, должны быть соответствующим образом маркированы. Маркировка должна быть четкой, заметной и включать следующую информацию:

•Уровень конфиденциальности
•Владелец информации
•Дата создания/обновления
•Срок действия грифа конфиденциальности (если применимо)
•Допустимые методы распространения

Для электронных документов должны использоваться метаданные и электронные метки конфиденциальности, совместимые с системами защиты от утечек данных (DLP).

2.3 Пересмотр классификации

Владельцы информационных активов обязаны периодически (не реже одного раза в год) пересматривать классификацию подконтрольных им данных и вносить необходимые изменения

в соответствии с актуальными бизнес-требованиями и оценкой рисков. Процесс пересмотра должен документироваться для обеспечения аудиторского следа.

3. УПРАВЛЕНИЕ ДОСТУПОМ

3.1 Принципы управления доступом

Доступ к информационным системам и данным Компании основывается на следующих принципах:

•**Принцип минимальных привилегий**: сотрудники получают только тот уровень доступа, который необходим для выполнения их должностных обязанностей
•**Разделение обязанностей**: критические функции распределяются между разными сотрудниками для предотвращения конфликта интересов и мошеннических действий
•**Обоснованность доступа**: доступ предоставляется только при наличии документально оформленной служебной необходимости
•**Периодический пересмотр**: права доступа регулярно пересматриваются и обновляются
•**Принцип нулевого доверия**: постоянная верификация каждого доступа к ресурсам, независимо от местонахождения

3.2 Управление учетными записями

Все пользователи информационных систем должны иметь индивидуальные учетные записи. Запрещается совместное использование учетных данных. Процесс управления учетными записями включает:

•Создание учетных записей на основании официальных запросов, согласованных с руководителями подразделений и отделом информационной безопасности
•Временное блокирование учетных записей при длительном отсутствии сотрудника (отпуск, больничный более 14 дней)
•Немедленная деактивация учетных записей при увольнении сотрудника или изменении его должностных обязанностей, не требующих прежнего уровня доступа
•Регулярный аудит активных учетных записей и их привилегий (не реже одного раза в квартал)
•Внедрение процесса рассмотрения и утверждения привилегированных учетных записей

3.3 Парольная политика

В целях обеспечения безопасности доступа к информационным системам Компании устанавливаются следующие требования к паролям:

•Минимальная длина пароля – 14 символов
•Обязательное использование символов из различных категорий: прописные и строчные буквы, цифры, специальные символы
•Срок действия пароля – не более 90 дней для обычных учетных записей и 45 дней для привилегированных
•Запрет на повторное использование последних 15 паролей
•Блокировка учетной записи после 5 неудачных попыток ввода пароля на 30 минут

•Запрет на использование в паролях личной информации (имена, даты рождения и т.п.)
•Хранение паролей только в зашифрованном виде с использованием современных алгоритмов хеширования
•Применение проверки на распространенные и скомпрометированные пароли

3.4 Многофакторная аутентификация

Доступ к критическим системам и данным должен осуществляться с использованием многофакторной аутентификации. В качестве второго фактора могут использоваться:

•Аппаратные токены (YubiKey, смарт-карты)
•Мобильные приложения для генерации одноразовых паролей (Google Authenticator, Microsoft Authenticator)
•Биометрические данные (отпечатки пальцев, распознавание лица, сканирование сетчатки)
•Push-уведомления через авторизованные мобильные приложения

Многофакторная аутентификация является обязательной для:

•Всех административных доступов к системам
•Удаленного доступа к корпоративным ресурсам
•Доступа к системам, содержащим строго конфиденциальную информацию
•Любого доступа к облачным сервисам Компании

4. ЗАЩИТА ДАННЫХ

4.1 Защита данных при хранении

Для обеспечения безопасности хранимых данных применяются следующие меры:

•Шифрование конфиденциальных и строго конфиденциальных данных на всех носителях информации с использованием современных стандартов шифрования (AES-256, RSA 2048+)
•Сегментирование сетей хранения данных в соответствии с их классификацией
•Резервное копирование всех критических данных не реже одного раза в сутки с соблюдением правила "3-2-1" (3 копии, на 2 разных типах носителей, 1 копия офф-сайт)
•Физическая защита серверных помещений и хранилищ резервных копий, включая контроль доступа, видеонаблюдение и системы обнаружения вторжений
•Защита от вредоносного программного обеспечения с регулярным обновлением антивирусных баз и использованием технологий поведенческого анализа
•Своевременная установка обновлений безопасности для всех систем хранения данных в соответствии с процессом управления изменениями
•Внедрение системы защиты от утечек данных (DLP)

4.2 Защита данных при передаче

При передаче данных внутри и за пределы корпоративной сети должны соблюдаться следующие требования:

•Использование защищенных протоколов передачи данных (HTTPS с TLS 1.3+, SFTP, SCP и др.)

•Шифрование конфиденциальных данных перед их передачей по незащищенным каналам связи с использованием сквозного шифрования
•Использование виртуальных частных сетей (VPN) при удаленном доступе к корпоративным ресурсам с обязательной многофакторной аутентификацией
•Контроль и фильтрация сетевого трафика с помощью межсетевых экранов следующего поколения (NGFW)
•Обнаружение и предотвращение сетевых вторжений с использованием современных IDS/IPS
•Регулярный мониторинг сетевой активности и выявление аномалий с использованием систем аналитики безопасности (SIEM)
•Внедрение технологий безопасного периметра (ZTNA, SASE)

4.3 Управление мобильными устройствами

Использование мобильных устройств (ноутбуки, планшеты, смартфоны) для доступа к корпоративным данным регламентируется следующими правилами:

•Все мобильные устройства, используемые для работы с корпоративными данными, должны быть зарегистрированы в системе управления мобильными устройствами (MDM/EMM)
•Обязательное шифрование корпоративных данных на мобильных устройствах с возможностью удаленного стирания
•Настройка автоматической блокировки экрана после периода неактивности (не более 3 минут)
•Сегрегация корпоративных и личных данных с использованием контейнеризации на устройствах, работающих по модели BYOD
•Возможность удаленной очистки корпоративных данных в случае утери, кражи устройства или увольнения сотрудника
•Запрет на установку непроверенного программного обеспечения на устройства с доступом к корпоративным данным
•Регулярные обновления операционных систем и приложений
•Использование VPN для доступа к корпоративным ресурсам

4.4 Удаление и уничтожение данных

По истечении установленных сроков хранения или при отсутствии необходимости в дальнейшем использовании, данные должны быть надежно удалены или уничтожены в соответствии со следующими требованиями:

•Использование специализированного программного обеспечения для необратимого удаления данных с электронных носителей в соответствии со стандартами DoD 5220.22-M или NIST 800-88
•Физическое уничтожение носителей информации, не подлежащих повторному использованию, с использованием сертифицированных методов (размагничивание, измельчение, сжигание)
•Документирование процесса уничтожения конфиденциальных и строго конфиденциальных данных с составлением актов уничтожения
•Проверка эффективности процедур удаления данных с целью предотвращения возможности их восстановления

•Аудит процессов уничтожения данных независимыми специалистами

5. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Общие положения

Обработка персональных данных в Компании осуществляется с соблюдением принципов и правил, установленных Федеральным законом "О персональных данных" от 27.07.2006 N 152-ФЗ. Компания гарантирует конфиденциальность и безопасность обрабатываемых персональных данных.

5.2 Сбор и обработка персональных данных

При сборе и обработке персональных данных должны соблюдаться следующие принципы:

•Получение предварительного согласия субъекта персональных данных на их обработку в форме, соответствующей требованиям законодательства
•Ограничение объема собираемых данных минимально необходимым для достижения заявленных целей
•Обеспечение точности, достаточности и актуальности персональных данных
•Соблюдение целевого ограничения при обработке персональных данных
•Прозрачность процессов обработки персональных данных для субъектов персональных данных
•Обеспечение права субъектов на доступ к своим персональным данным и их корректировку
•Документирование всех операций с персональными данными для обеспечения подотчетности

5.3 Передача персональных данных

Передача персональных данных третьим лицам возможна только в следующих случаях:

•С информированного согласия субъекта персональных данных
•По требованию уполномоченных государственных органов в рамках их компетенции
•В рамках исполнения договорных обязательств, если это предусмотрено соответствующим договором
•В иных случаях, установленных законодательством РФ

При передаче персональных данных третьим лицам Компания обязуется заключать соответствующие соглашения о конфиденциальности и обеспечении безопасности передаваемых данных.

5.4 Хранение и уничтожение персональных данных

Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки, если срок хранения не установлен федеральным законом или договором. Уничтожение персональных данных производится:

•По достижении целей обработки или при утрате необходимости в их достижении
•При отзыве субъектом персональных данных согласия на их обработку (если отсутствуют иные правовые основания)

•По истечении установленных сроков хранения
•В случае выявления неправомерной обработки персональных данных
•По предписанию уполномоченного органа по защите прав субъектов персональных данных

5.5 Защита персональных данных

Для защиты персональных данных Компания принимает следующие меры:

•Назначение ответственного за организацию обработки персональных данных
•Разработка внутренних документов, определяющих политику в отношении обработки персональных данных
•Применение правовых, организационных и технических мер по обеспечению безопасности персональных данных
•Проведение оценки воздействия на защиту персональных данных (DPIA) при внедрении новых систем или процессов обработки
•Регулярный аудит соответствия обработки персональных данных требованиям законодательства
•Обучение сотрудников, имеющих доступ к персональным данным

6. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

6.1 Организация информационной безопасности

В Компании создается и поддерживается организационная структура информационной безопасности, включающая:

•Комитет по информационной безопасности под председательством Генерального директора
•Департамент информационной безопасности, возглавляемый Директором по информационной безопасности (CISO)
•Ответственных за информационную безопасность в каждом структурном подразделении
•Рабочую группу по реагированию на инциденты информационной безопасности (CSIRT)
•Центр операционной безопасности (SOC) для мониторинга и реагирования на угрозы в режиме реального времени

6.2 Управление инцидентами безопасности

В Компании разрабатывается и внедряется система управления инцидентами информационной безопасности, включающая:

•Процедуры выявления и регистрации инцидентов с использованием автоматизированных средств мониторинга
•Классификацию инцидентов по уровням критичности и приоритетам реагирования
•Порядок эскалации и информирования о инцидентах, включая обязательное уведомление регулирующих органов для определенных типов инцидентов
•Процедуры расследования причин инцидентов с использованием методологии root cause analysis
•Меры по устранению последствий инцидентов и предотвращению их повторения
•Документирование всех действий по обработке инцидентов

•Регулярные тренировки по реагированию на инциденты (tabletop exercises)

6.3 Антивирусная защита

Для защиты от вредоносного программного обеспечения в Компании применяются следующие меры:

•Установка многоуровневой защиты от вредоносного ПО на всех рабочих станциях и серверах
•Автоматическое обновление антивирусных баз данных не реже одного раза в час
•Периодическое полное сканирование информационных систем по расписанию
•Проверка входящих файлов на наличие вирусов на уровне шлюзов безопасности
•Блокировка доступа к потенциально опасным веб-сайтам с использованием систем веб-фильтрации
•Запрет на использование неавторизованного программного обеспечения
•Внедрение решений класса EDR (Endpoint Detection and Response) для выявления сложных угроз
•Анализ поведения файлов в изолированной среде (песочнице) перед их исполнением

6.4 Аудит и мониторинг

Для своевременного выявления потенциальных угроз и нарушений безопасности в Компании организован постоянный мониторинг и аудит информационных систем:

•Сбор и анализ журналов событий безопасности всех критических систем с использованием SIEM-решений
•Мониторинг сетевого трафика и выявление аномалий с применением технологий машинного обучения
•Контроль целостности системных файлов и конфигураций критической инфраструктуры
•Регулярные проверки на наличие уязвимостей в информационных системах (не реже одного раза в квартал)
•Периодические тесты на проникновение (не реже одного раза в год)
•Анализ соответствия настроек систем требованиям безопасности
•Внедрение средств обнаружения аномального поведения пользователей (UEBA)
•Мониторинг публичного периметра на предмет утечек данных и компрометации учетных записей

6.5 Управление уязвимостями

В Компании внедрен процесс управления уязвимостями, включающий:

•Регулярное сканирование информационных систем на наличие уязвимостей с использованием автоматизированных инструментов
•Оценку критичности выявленных уязвимостей на основе стандартной системы оценки CVSS
•Приоритизацию устранения уязвимостей на основе оценки рисков и потенциального воздействия на бизнес-процессы
•Своевременную установку обновлений безопасности в соответствии с установленными сроками:

•Критические уязвимости - в течение 24 часов
•Уязвимости высокого уровня - в течение 7 дней
•Уязвимости среднего уровня - в течение 30 дней
•Уязвимости низкого уровня - в течение 90 дней
•Тестирование обновлений перед внедрением в производственную среду
•Мониторинг информации о новых уязвимостях из достоверных источников (национальные CERT, бюллетени производителей)
•Регулярную отчетность о статусе управления уязвимостями для руководства

6.6 Разработка безопасного программного обеспечения

При разработке собственного программного обеспечения Компания придерживается принципов безопасной разработки:

•Внедрение методологии DevSecOps, интегрирующей аспекты безопасности в процесс разработки
•Проведение анализа защищенности кода на всех этапах разработки
•Использование безопасных библиотек и компонентов с регулярной проверкой на известные уязвимости
•Автоматизированное тестирование безопасности приложений перед выпуском новых версий
•Проведение внешнего аудита безопасности критических приложений
•Документирование всех аспектов безопасности в разрабатываемых системах
•Обучение разработчиков методам безопасного программирования

7. ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ БИЗНЕСА

7.1 План обеспечения непрерывности бизнеса

Компания разрабатывает и поддерживает в актуальном состоянии План обеспечения непрерывности бизнеса (BCP), включающий:

•Анализ влияния на бизнес (BIA) для определения критических бизнес-процессов и систем с количественной оценкой потенциальных потерь
•Оценку рисков прерывания бизнес-процессов с учетом вероятности различных сценариев
•Стратегии восстановления для различных сценариев с определением приоритетов
•Планы коммуникаций в кризисных ситуациях, включая шаблоны уведомлений для различных групп заинтересованных лиц
•Распределение ролей и ответственности при активации плана, включая формирование кризисной команды
•Процедуры возврата к нормальной работе после устранения инцидента
•Анализ эффективности реагирования на инциденты и извлеченные уроки

7.2 План аварийного восстановления

В рамках обеспечения непрерывности бизнеса разрабатывается План аварийного восстановления (DRP), определяющий:

•Приоритеты восстановления информационных систем на основе их критичности для бизнес-процессов
•Целевое время восстановления (RTO) и целевую точку восстановления (RPO) для каждой критической системы
•Технические процедуры восстановления систем и данных, включающие пошаговые инструкции
•Альтернативные площадки для размещения ИТ-инфраструктуры с возможностью быстрого переключения
•Процедуры тестирования возможности восстановления систем и данных
•Требования к резервным мощностям и ресурсам
•Автоматизированные инструменты оркестрации восстановления систем

7.3 Резервное копирование

Система резервного копирования Компании организована согласно следующим принципам:

•Определение объектов резервного копирования на основе их критичности и требований регуляторов
•Разработка графиков резервного копирования с учетом требований к сохранности данных и допустимых окон обслуживания
•Использование многоуровневой стратегии резервного копирования (полное, дифференциальное, инкрементное)
•Хранение резервных копий в географически удаленных местах с соблюдением требований к физической безопасности
•Регулярная проверка целостности и возможности восстановления из резервных копий (не реже одного раза в месяц)
•Защита резервных копий с помощью шифрования с использованием современных алгоритмов
•Автоматизация процессов создания и верификации резервных копий с минимальным участием человека
•Документирование и аудит всех операций резервного копирования

7.4 Тестирование планов

Планы обеспечения непрерывности бизнеса и аварийного восстановления подлежат регулярному тестированию:

•Настольные учения (table-top exercises) – не реже одного раза в квартал
•Функциональное тестирование отдельных компонентов – не реже одного раза в квартал
•Полное тестирование с симуляцией реальных сценариев – не реже одного раза в год
•Тестирование восстановления из резервных копий – ежемесячно
•Тестирование аварийного переключения на резервные системы – не реже двух раз в год
•Актуализация планов по результатам тестирования и при существенных изменениях в ИТ-инфраструктуре
•Привлечение внешних экспертов для независимой оценки планов и процессов тестирования

8. ОБУЧЕНИЕ И ОСВЕДОМЛЕННОСТЬ

8.1 Программа обучения по информационной безопасности

В Компании разрабатывается и реализуется комплексная программа обучения сотрудников по вопросам информационной безопасности:

•Обязательное вводное обучение для новых сотрудников в первую неделю работы
•Регулярные тренинги для всех сотрудников (не реже одного раза в полгода)
•Специализированные курсы для ИТ-персонала и сотрудников, работающих с конфиденциальной информацией
•Дополнительные тренинги при внедрении новых систем или изменении политик безопасности
•Курсы повышения квалификации для специалистов по информационной безопасности
•Программы подготовки к профессиональным сертификациям в области информационной безопасности
•Геймифицированные обучающие программы для повышения вовлеченности сотрудников

8.2 Повышение осведомленности

Для повышения осведомленности сотрудников в вопросах информационной безопасности используются следующие методы:

•Регулярные информационные рассылки о актуальных угрозах и методах защиты
•Публикация материалов по информационной безопасности на корпоративном портале
•Проведение месяца информационной безопасности с тематическими мероприятиями
•Размещение наглядных материалов (плакаты, памятки, инфографики) в офисных помещениях
•Симуляции фишинговых атак с последующим разбором результатов и дополнительным обучением
•Краткие видеоролики по вопросам информационной безопасности
•Система поощрений для сотрудников, демонстрирующих ответственное отношение к информационной безопасности

8.3 Оценка эффективности

Эффективность программ обучения и повышения осведомленности оценивается на основе:

•Результатов тестирования знаний сотрудников до и после прохождения обучения
•Статистики инцидентов безопасности, связанных с человеческим фактором
•Результатов симуляций социальной инженерии в динамике
•Обратной связи от сотрудников и руководителей подразделений
•Соответствия поведения сотрудников требованиям политик безопасности
•Процента успешного прохождения обучающих программ
•Сравнительного анализа с отраслевыми показателями

8.4 Культура информационной безопасности

Компания стремится к формированию позитивной культуры информационной безопасности, основанной на:

•Личной ответственности каждого сотрудника за информационную безопасность
•Понимании важности защиты информационных активов для успешности бизнеса
•Поощрении сотрудников за своевременное сообщение о потенциальных проблемах безопасности
•Неприменении санкций к сотрудникам, честно сообщившим о своих ошибках
•Регулярном информировании руководства о состоянии информационной безопасности
•Интеграции принципов безопасности во все бизнес-процессы Компании

9. СООТВЕТСТВИЕ ТРЕБОВАНИЯМ

9.1 Соблюдение законодательства

Компания обязуется соблюдать все применимые законодательные и нормативные требования в области информационной безопасности и защиты данных. Департамент информационной безопасности совместно с юридическим департаментом осуществляет:

•Мониторинг изменений в законодательстве и нормативных требованиях России и стран присутствия Компании
•Оценку влияния этих изменений на деятельность Компании
•Адаптацию политик и процедур для обеспечения соответствия новым требованиям
•Проведение регулярных проверок на соответствие требованиям
•Взаимодействие с регулирующими органами по вопросам информационной безопасности
•Поддержание актуальных реестров применимых нормативных требований
•Документирование свидетельств соответствия для предоставления регуляторам

9.2 Внутренний аудит

Программа внутреннего аудита информационной безопасности включает:

•Регулярные проверки соответствия практик управления информационной безопасностью требованиям настоящей Политики и других внутренних документов
•Оценку эффективности мер контроля информационной безопасности на основе объективных метрик
•Выявление областей для улучшения и систематизацию рисков информационной безопасности
•Разработку рекомендаций по устранению выявленных недостатков с определением ответственных лиц и сроков
•Контроль выполнения корректирующих мероприятий и оценку их результативности
•Регулярную отчетность перед руководством о результатах аудита
•Анализ тенденций в выявляемых нарушениях и недостатках

9.3 Внешний аудит

По решению руководства Компании могут проводиться внешние аудиты информационной безопасности с привлечением специализированных организаций для:

•Независимой оценки состояния информационной безопасности

•Подтверждения соответствия международным стандартам (ISO/IEC 27001, PCI DSS, GDPR и др.)
•Подготовки к сертификации по стандартам информационной безопасности
•Выполнения специальных требований клиентов или партнеров
•Бенчмаркинга с лучшими практиками в отрасли
•Получения рекомендаций по совершенствованию системы управления информационной безопасностью

9.4 Сертификация и стандартизация

Компания стремится к соответствию признанным международным и национальным стандартам в области информационной безопасности:

•ISO/IEC 27001 - Система менеджмента информационной безопасности
•PCI DSS - Стандарт безопасности данных индустрии платежных карт (для соответствующих систем)
•ГОСТ Р ИСО/МЭК 27001 - национальный стандарт системы менеджмента информационной безопасности
•Отраслевые стандарты и рекомендации по информационной безопасности

10. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1 Методология управления рисками

Компания применяет систематический подход к управлению рисками информационной безопасности, основанный на:

•Регулярной идентификации активов, угроз и уязвимостей
•Оценке вероятности реализации угроз и возможного ущерба
•Определении приемлемого уровня риска
•Выборе стратегии обработки рисков (снижение, передача, принятие, избегание)
•Внедрении контролей безопасности, адекватных уровню риска
•Мониторинге эффективности контролей и регулярном пересмотре рисков
•Документировании результатов оценки и обработки рисков

10.2 Оценка рисков

Оценка рисков информационной безопасности проводится:

•При внедрении новых информационных систем или существенных изменениях в существующих
•При изменении бизнес-процессов, затрагивающих обработку информации
•При выявлении новых угроз или уязвимостей, которые могут оказать существенное влияние на безопасность
•На регулярной основе, не реже одного раза в год для критических систем

10.3 Обработка рисков

Для каждого идентифицированного риска, превышающего приемлемый уровень, разрабатывается и реализуется план обработки:

•Определение конкретных мер по снижению риска
•Назначение ответственных за реализацию мер
•Установление сроков реализации
•Определение метрик для оценки эффективности принятых мер
•Регулярный мониторинг статуса выполнения планов обработки рисков

11. ОТВЕТСТВЕННОСТЬ И ДИСЦИПЛИНАРНЫЕ МЕРЫ

11.1 Ответственность сотрудников

Все сотрудники Компании несут персональную ответственность за:

•Соблюдение требований настоящей Политики и связанных с ней процедур
•Защиту конфиденциальной информации от несанкционированного доступа
•Своевременное информирование о инцидентах информационной безопасности
•Рациональное использование ресурсов информационных систем
•Соблюдение правил использования средств защиты информации
•Содействие в расследовании инцидентов информационной безопасности
•Непрерывное повышение своих знаний в области информационной безопасности

11.2 Дисциплинарные меры

За нарушение требований настоящей Политики могут применяться следующие дисциплинарные меры:

•Устное предупреждение
•Письменное замечание
•Временное ограничение доступа к информационным системам
•Лишение премий и иных поощрительных выплат
•Дисциплинарное взыскание в соответствии с трудовым законодательством
•В случае серьезных нарушений - расторжение трудового договора
•В случае причинения материального ущерба - возмещение ущерба в соответствии с законодательством

Степень дисциплинарной ответственности зависит от тяжести нарушения, умысла, последствий и других обстоятельств инцидента.

12. ОТНОШЕНИЯ С ТРЕТЬИМИ СТОРОНАМИ

12.1 Требования к поставщикам

Компания устанавливает следующие требования к поставщикам и подрядчикам, имеющим доступ к корпоративным информационным системам или данным:

•Соответствие требованиям информационной безопасности Компании
•Наличие собственной системы управления информационной безопасностью
•Прохождение процедуры оценки безопасности перед заключением контракта
•Включение положений о защите информации и ответственности за нарушения в договоры
•Подписание соглашения о конфиденциальности
•Регулярное предоставление отчетов о состоянии информационной безопасности
•Согласие на проведение аудитов безопасности со стороны Компании

12.2 Управление цепочкой поставок

Для минимизации рисков в цепочке поставок Компания:

•Проводит категоризацию поставщиков по уровню риска
•Устанавливает различные требования к безопасности в зависимости от категории риска
•Регулярно проводит переоценку рисков поставщиков
•Контролирует цепочку субподрядчиков, имеющих доступ к конфиденциальной информации
•Включает в договоры требования по защите от атак на цепочку поставок
•Проверяет целостность поставляемого программного обеспечения и оборудования

13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

13.1 Утверждение и введение в действие

Настоящая Политика утверждается Советом директоров Компании и вводится в действие приказом Генерального директора.

13.2 Пересмотр и актуализация

Политика подлежит пересмотру и актуализации не реже одного раза в год, а также в случае существенных изменений в организационной структуре Компании, ИТ-инфраструктуре, законодательстве или условиях ведения бизнеса.

13.3 Контроль исполнения

Контроль исполнения требований настоящей Политики возлагается на Директора по информационной безопасности с регулярной отчетностью перед Комитетом по информационной безопасности.

13.4 Действие Политики

Настоящая Политика действует с момента утверждения до момента ее отмены или замены новой версией. Все предыдущие версии Политики утрачивают силу с момента утверждения настоящей версии.