|  |  |  |  |
| --- | --- | --- | --- |
| п/п | **Задача** | **Действие** | **Ответственность** |
| **Месяц 1-2: Оценка и планирование:** | | | | |
|  | Оценка текущего состояния ИБ | Провести полный аудит ИБ, включая анализ политики, процедур, технических средств защиты, уязвимостей, соответствия нормативным требованиям | служба ИБ, отдел ИТ |
| Проанализировать результаты Pentest |
| Провести инвентаризацию ИТ активов | руководство, отдел ИТ |
| Провести анализ рисков. | руководство, отдел ИТ , служба ИБ |
| Оценить риски обработки персональных данных в облачной инфраструктуре |
|  | Разработка стратегии ИБ | Определить бизнес-цели и цели ИБ | руководство,  служба ИБ |
| Разработать политику ИБ с учетом законодательства. |
| Определить приоритеты и план действий. |
| Разработать план по найму специалистов по ИБ. |
|  | Формирование команды | Определить необходимые роли и функции в команде. | согласование руководства, служба ИБ |
| Начать поиск кандидатов. |
| Разработать программу обучения для новых сотрудников. |
| **Месяц 3-5: Внедрение и укрепление** | | | | |
|  | Внедрение политики и процедур ИБ | Разработать и внедрить политику по управлению доступом | служба ИБ, отдел ИТ, согласование руководства |
| Внедрить политику и процедуры реагирования на инциденты. |
| Внедрить политику по резервному копированию и восстановлению данных |
| Обновить и внедрить политики по обработке персональных данных. |
| Разработать и внедрить политику по защите информации в облачной инфраструктуре. |
|  | Закупка и внедрение технических решений | Внедрить IPS/IDS | служба ИБ, отдел ИТ, согласование руководства, финансовые ресурсы |
| Внедрить систему анализа пакетов сети. |
| Внедрить SIEM |
| Внедрить инструмент анализа уязвимостей |
| Внедрить 2FA |
| Настроить централизованный мониторинг систем ИБ |
|  | Обучение персонала | Провести тренинги по основам информационной безопасности для всех сотрудников | служба ИБ, отдел ИТ |
| Провести тренинги по политике ИБ и процедурам реагирования на инциденты. |
| Обучить сотрудников работе с новыми системами защиты |
|  | Разработка ролевой модели и сегментация сети | Разработать и внедрить ролевую модель | служба ИБ, отдел ИТ |
| Провести сегментацию сети. |
| Оптимизировать политики антивируса на сервере управления |
| **Месяц 6-7: Мониторинг и совершенствование** | | | |
|  | Мониторинг и аудит | Настроить регулярный мониторинг систем ИБ | служба ИБ, отдел ИТ |
| Проводить регулярные внутренние аудиты |
| Провести аудит соответствия требованиям законодательства. |
| Провести анализ эффективности внедренных мер |
| Оценить соответствие политики ИБ требованиям законодательства по защите информации |
|  | Управление инцидентами | Внедрить процессы управления инцидентами | служба ИБ, отдел ИТ |
| Провести учения по реагированию на инциденты |
| Провести анализ инцидентов за предыдущий период |
|  | Обновление политики и процедур ИБ | Обновить и доработать политику и процедуры ИБ на основе полученного опыта. | служба ИБ, отдел ИТ |
|  | Оценка эффективности и корректировка стратегии | Оценить эффективность внедренных мер. | служба ИБ, отдел ИТ, внешняя оценка |
| Внести необходимые корректировки в стратегию и планы ИБ. | служба ИБ, отдел ИТ |
| Подготовить отчет о достигнутых результатах. |
| Провести совещание с руководством для обсуждения дальнейших шагов. | руководство,  служба ИБ |
| **Месяц 7-9: Безопасная разработка и DevSecOps** | | | |
|  | Оценка текущего состояния процессов разработки | Разработать политику по безопасной разработке | служба ИБ, отдел ИТ разработчики |
| Определить приоритеты и план действий. |
| Разработать план по найму специалистов по AppSec, DevSecOps. |
| Определить необходимые роли и функции в команде |
| Разработать программу обучения для сотрудников по безопасной разработке |
|  | Внедрение политики и программных средств | Разработать и внедрить политику | служба ИБ, отдел ИТ разработчики |
| Учесть требования заказчиков в сфере ИБ при разработке |
| Внедрить SAST в CI/CD на начальном уровне разработки программных продуктов |
| Внедрить DAST в CI/CD на уровнях тестирования программных продуктов |
| Внедрить дополнительное тестирование в CI/CD - SCA, Vulnerability Management, Container Security |