# Основные вопросы

## Бизнес-цели и цели ИБ:

Какие главные бизнес-цели нашей организации? (например, рост прибыли, расширение рынка, вывод нового продукта, защита репутации)

Какие цели ИБ должны быть достигнуты для поддержки этих бизнес-целей? (например, защита конфиденциальности данных, целостность данных, доступность систем, предотвращение хакерских атак)

## Ресурсы:

Каков бюджет на ИБ-проекты?

Есть ли возможность нанять дополнительных специалистов по ИБ?

Есть ли доступ к специализированным инструментам и программному обеспечению?

## Текущий уровень безопасности:

Какие средства защиты у вас уже есть? (например, антивирус, фаервол, резервное копирование)

Какие уязвимости были выявлены в ходе Pentest?

Какие угрозы считаются наиболее вероятными?

## Законодательство:

Какие законы о защите информации и обработке персональных данных релевантны для вашей компании?

Есть ли специальные требования к защите информации в вашей отрасли?

## Внутренняя инфраструктура:

Какое количество физических и виртуальных серверов у вас есть?

Какая структура сети у вас используется?

Какие операционные системы и программное обеспечение используются?

Есть ли облачная инфраструктура?

Как организована сегментация сети?

Есть ли система мониторинга и логирования?

# **Дорожная карта ИБ**:

Шаги: определенные действия, которые необходимо выполнить.

Сроки: ориентировочные сроки выполнения каждого шага.

Ответственные: сотрудники, ответственные за реализацию каждого шага.

Рекомендации:

Необходимо нанять дополнительных специалистов по ИБ и ИТ - в такой ситуации, с вводом новых процессов, мониторингом событий, эффективно выполнять все задачи затруднительно.

Необходимо провести анализ законодательства по защите информации в РФ. - Особое внимание уделить обработке персональных данных в облачной инфраструктуре.

Необходимо сфокусироваться на основных целях ИБ – это позволит определить приоритеты и сфокусироваться на самых важных задачах, исходя из финансовых средств и возможностей.

**План действий:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п/п | **Задача** | **Действие** | **Сроки** | **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 | 1 месяц | служба ИБ, отдел ИТ |
| Проанализировать результаты Pentest. Изучение отчета Pentest, определение критических уязвимостей, приоритезация мер по их устранению. | 1 неделя |
| Провести инвентаризацию ИТ активов | 2 недели | руководство, отдел ИТ |
| Провести анализ рисков. Идентификация критических активов (серверы, данные, сети), определение возможных угроз (захват управления, шифрование, кража данных), расчет вероятности и последствий угроз. | 2 недели | руководство, отдел ИТ , служба ИБ |
| Оценить риски обработки персональных данных в облачной инфраструктуре | 2 недели |
|  | Разработка стратегии ИБ | Определить бизнес-цели и цели ИБ | 1 неделя | руководство,  служба ИБ |
| Разработать политику ИБ с учетом законодательства. Изучение ФЗ 153, приказов ФСТЭК 17 и 21, требований контрагентов. Определение необходимых мер для соответствия. выявление пробелов в текущей системе ИБ. | 2 недели |
| Определить приоритеты и план действий. | 1 неделя |
| **Месяц 3-5: Внедрение и укрепление** | | | | |
|  | Внедрение политики и процедур ИБ | Разработать и внедрить политику по управлению доступом | 1-2 месяца | служба ИБ, отдел ИТ, согласование руководства |
| Внедрить политику и процедуры реагирования на инциденты. Разработка и внедрение регламентов и процедур по работе с информацией, управлению уязвимостями, реагированию на инциденты. | 1-2 месяца |
| Внедрить политику по резервному копированию и восстановлению данных | 1-2 месяца |
| Обновить и внедрить политики по обработке персональных данных. | 1-2 месяца |
| Разработать и внедрить политику по защите информации в облачной инфраструктуре. | 1-2 месяца |
|  | Закупка и внедрение технических решений | Внедрить IPS/IDS. Выбор и установка IPS/IDS с учетом бюджета и характеристик сети. Настройка правил и мониторинг работы системы | 2-3 месяца | служба ИБ, отдел ИТ, согласование руководства, финансовые ресурсы |
| Внедрить систему анализа пакетов сети. Выбор и установка системы анализа пакетов сети (например, Wireshark). Настройка фильтров и анализа сетевого трафика для обнаружения подозрительной активности | 1-2 месяца |
| Внедрить SIEM. Внедрение системы управления событиями и информацией о безопасности (SIEM) для централизованного мониторинга и анализа событий безопасности. Создание инструмента для автоматизации отслеживания угроз, выявления аномалий и реагирования на инциденты. | 2-3 месяца |
| Внедрить инструмент анализа уязвимостей. Внедрение системы управления уязвимостями для автоматизации сканирования и управления уязвимостями. Создание процесса управления уязвимостями для своевременного устранения выявленных проблем. | 1 месяц |
| Внедрить 2FA | 1-2 месяца |
| Настроить централизованный мониторинг систем ИБ | 1-2 месяца |
|  | Обучение персонала | Провести тренинги по основам информационной безопасности для всех сотрудников. Регулярное проведение тренингов по информационной безопасности для сотрудников. Повышение осведомленности о рисках и правилах работы с информацией. Создание культуры безопасности в компании. | 1 месяц | служба ИБ, отдел ИТ |
| Провести тренинги по политике ИБ и процедурам реагирования на инциденты. | 2 недели |
| Обучить сотрудников работе с новыми системами защиты | 1-2 месяца |
|  | Разработка ролевой модели и сегментация сети | Разработать и внедрить ролевую модель | 2 недели | служба ИБ, отдел ИТ |
| Провести сегментацию сети. Разделение сети на сегменты для изоляции критических систем и данных. Ограничение доступа между сегментами для снижения риска распространения угроз. | 2-3 месяца |
| Создать DMZ зону. Перенести туда все общедоступные сервисы, которым необходим доступ к сети Интернет. |  |
| Оптимизировать политики антивируса на сервере управления | 1-2 месяца |
| **Месяц 6-7: Мониторинг и совершенствование** | | | | |
|  | Формирование команды | Разработать план по найму специалистов по ИБ. | 1-2 недели | согласование руководства, служба ИБ |
| Определить необходимые роли и функции в команде. | 1 неделя |
| Начать поиск кандидатов. | 1-3 месяц |
| Разработать программу обучения для новых сотрудников. | 1 недяля |
|  | Мониторинг и аудит | Настроить регулярный мониторинг систем ИБ. Внедрение системы мониторинга для слежения за работой серверов и систем ИБ. Настройка уведомлений о критических событиях. | 1 месяц | служба ИБ, отдел ИТ |
| Проводить регулярные внутренние аудиты. Определение новых уязвимостей и угроз. Внесение корректировок в планы ИБ с учетом полученных данных. | 2 недели |
| Провести аудит соответствия требованиям законодательства. | 2 недели |
| Провести анализ эффективности внедренных мер. Создание системы документирования и отчетности по ИБ. | 1 месяц |
| Оценить соответствие политики ИБ требованиям законодательства по защите информации | 2 недели |
|  | Управление инцидентами | Внедрить процессы управления инцидентами | 1-2 месяца | служба ИБ, отдел ИТ |
| Провести учения по реагированию на инциденты | 1 неделя |
| Провести анализ инцидентов за предыдущий период | 2 недели |
|  | Обновление политики и процедур ИБ | Обновить и доработать политику и процедуры ИБ на основе полученного опыта. | 1 неделя | служба ИБ, отдел ИТ |
|  | Оценка эффективности и корректировка стратегии | Оценить эффективность внедренных мер. | 2 недели | служба ИБ, отдел ИТ, внешняя оценка |
| Внести необходимые корректировки в стратегию и планы ИБ. | 2 недели | служба ИБ, отдел ИТ |
| Подготовить отчет о достигнутых результатах. | 2 недели |
| Провести совещание с руководством для обсуждения дальнейших шагов. | 1 неделя | руководство,  служба ИБ |
| **Месяц 8-10: Безопасная разработка и DevSecOps** | | | | |
|  | Оценка текущего состояния процессов разработки | Разработать политику по безопасной разработке | 2 недели | служба ИБ, отдел ИТ разработчики |
| Определить приоритеты и план действий. | 1 неделя |
| Разработать план по найму специалистов по AppSec, DevSecOps. | 2 недели |
| Определить необходимые роли и функции в команде | 2 недели |
| Разработать программу обучения для сотрудников по безопасной разработке | 1-2 месяца |
|  | Внедрение политики и программных средств | Разработать и внедрить политику | 2 недели | служба ИБ, отдел ИТ разработчики |
| Учесть требования заказчиков в сфере ИБ при разработке | 2 недели |
| Внедрить SAST в CI/CD на начальном уровне разработки программных продуктов | 2 недели |
| Внедрить DAST в CI/CD на уровнях тестирования программных продуктов | 2 недели |
| Внедрить дополнительное тестирование в CI/CD - SCA, Vulnerability Management, Container Security | 1-2 месяца |

# Дополнительные меры/рекомендации:

* Внедрить систему управления рисками. Это позволит систематически оценивать риски, приоритезировать задачи и эффективно использовать ресурсы.
* Использование автоматизированных инструментов. Автоматизация позволит нам сэкономить время и ресурсы, а также повысить эффективность работы.
* Обучение сотрудников. Сотрудники должны быть осведомлены о рисках информационной безопасности и правилах работы с информацией.
* Проведение регулярных учений по реагированию на инциденты. Это позволит проверить свои планы и действия в случае реального инцидента.
* Анализ данных. Регулярно анализируйте результаты своей работы и корректируйте свои действия в соответствии с полученными данными.

# Процессы информационной безопасности:

* управление ИТ активами – закрывает п.1
* классификация информации по степени критичности – п.1
* управление уязвимостями в используемом программном обеспечении и информационных системах – п.5
* управление учетными записями пользователей и администраторов информационных систем – п.4 и п.7
* аудит и мониторинг событий информационной безопасности – п.5 и п.8
* защита от вредоносного программного обеспечения – п.5
* обеспечение сетевой безопасности – п.5
* управление инцидентами информационной безопасности – п. 4 и п.8
* создание и поддержка документального обеспечения деятельности по защите информации – п.2 и п.10
* управление соответствием нормативным требованиям, предъявляемым к компании. – п. 2, п.10, п.11

# Итоги:

В нашей организации будет осуществлен контроль удаленного доступа. Канал передачи данных между сотрудником вне защищенного контура и защищенным сегментом сети будет зашифрован.

Внедрена ролевая модель и контроль доступа на всех уровнях нашей инфраструктуры, так же будет осуществляться контроль привилегированных пользователей. Реализована двух факторная аутентификация. Доступ к защищенным сегментам сети будет основан на ролевой модели с учетом матрицы доступа.

Все ИТ активы будут описаны и будут иметь степень критичности для нашей организации. Исходя из уровня значимости ИТ активов будут применены политики реагирования, резервного копирования, анализа уязвимости и контроля доступа.

Защита периметра и всех точек доступа будет контролироваться программно-аппаратными комплексами, включающими в себя средство предотвращения вторжений, средство детектирования атак, анализа сетевых пакетов и межсетевого экранирования (с учетом ролевой модели доступа и сегментации сети). Для общедоступных сервисов, которым необходим интернет, будет создана DMZ.

Внутри защищенного контура будут применятся средства разграничения доступа с учетом ролевой модели. Будет осуществляется мониторинг событий информационной безопасности и событий ИТ. Внедрены такие автоматизированные средства как анализ защищенности, антивирусная защита, анализ сетевых пакетов.

Инфраструктура будет распределена согласно ролевой модели:

* каждому отделу/подразделению назначена роль и уровень доступа
* каждому отделу/подразделению определена подсеть
* организован доступ к подсетям на основании ролей/функций
* серверный сегмент с доступом только для администраторов сети, администраторов серверов, администраторов СЗИ.
* сегмент сети с конфиденциальной информацией, к которому доступ будет осуществляется строго на основе ролевой модели и матрицы доступа, пользователи будут иметь минимально необходимые права для осуществления своих функций.
* сегмент сети для обработки персональных данных, к которому доступ будет осуществляется строго на основе ролевой модели и матрицы доступа, пользователи будут иметь минимально необходимые права для осуществления своих функций
* сегмент сети с общедоступными данным для всех пользователей.