Приложение № 8. Политик обеспечения непрерывности бизнес-процессов в аспекте информационной безопасности.

Заготовка

В данной главе излагаются принципы и методы, используемые организацией для профилактики, обнаружения и реагирования на киберугрозы. Основная цель — минимизация рисков и защита информационных активов организации. Для этого используются современные технологические решения, такие как системы обнаружения и предотвращения вторжений (IDS/IPS), программное обеспечение для управления инцидентами безопасности и событиями (SIEM), а также регулярное проведение пентестов и аудитов безопасности.

1. **Профилактические меры**: Включают регулярное обновление и настройку антивирусного программного обеспечения, фаерволов, а также обучение сотрудников основам кибергигиены.
2. **Мониторинг и обнаружение**: Непрерывный мониторинг сетевого трафика и логов систем для своевременного выявления подозрительных действий или аномалий.
3. **Реагирование на инциденты**: Разработка чёткого плана действий для реагирования на инциденты, включая процедуры изоляции угрозы и устранения уязвимостей.
4. **Восстановление после атак**: Планы и процедуры по восстановлению систем и данных после кибератак, чтобы минимизировать простой в работе и потерю данных.

Данные меры помогают снизить вероятность успешных кибератак и сократить потенциальный ущерб от них, обеспечивая надёжную защиту информационной инфраструктуры организации.

Мониторинг и контроль

5.1. Контроль исполнения

5.1.1. Механизмы контроля

5.1.2. Регулярные отчеты

5.1.3. Внедрение систем контроля

5.1.4. Обратная связь и корректирующие действия

5.2. Аудит и проверка

5.2.1. Регулярные проверки и аудит

5.2.2. Оценка результатов

5.3. Выявление и устранение нарушений

5.3.1. Анализ нарушений

5.3.2. Корректирующие действия

5.3.3. Мониторинг исправлений

5.4. Отчетность и улучшение

5.4.1. Отчеты о результатах аудита

5.4.2. Периодический пересмотр