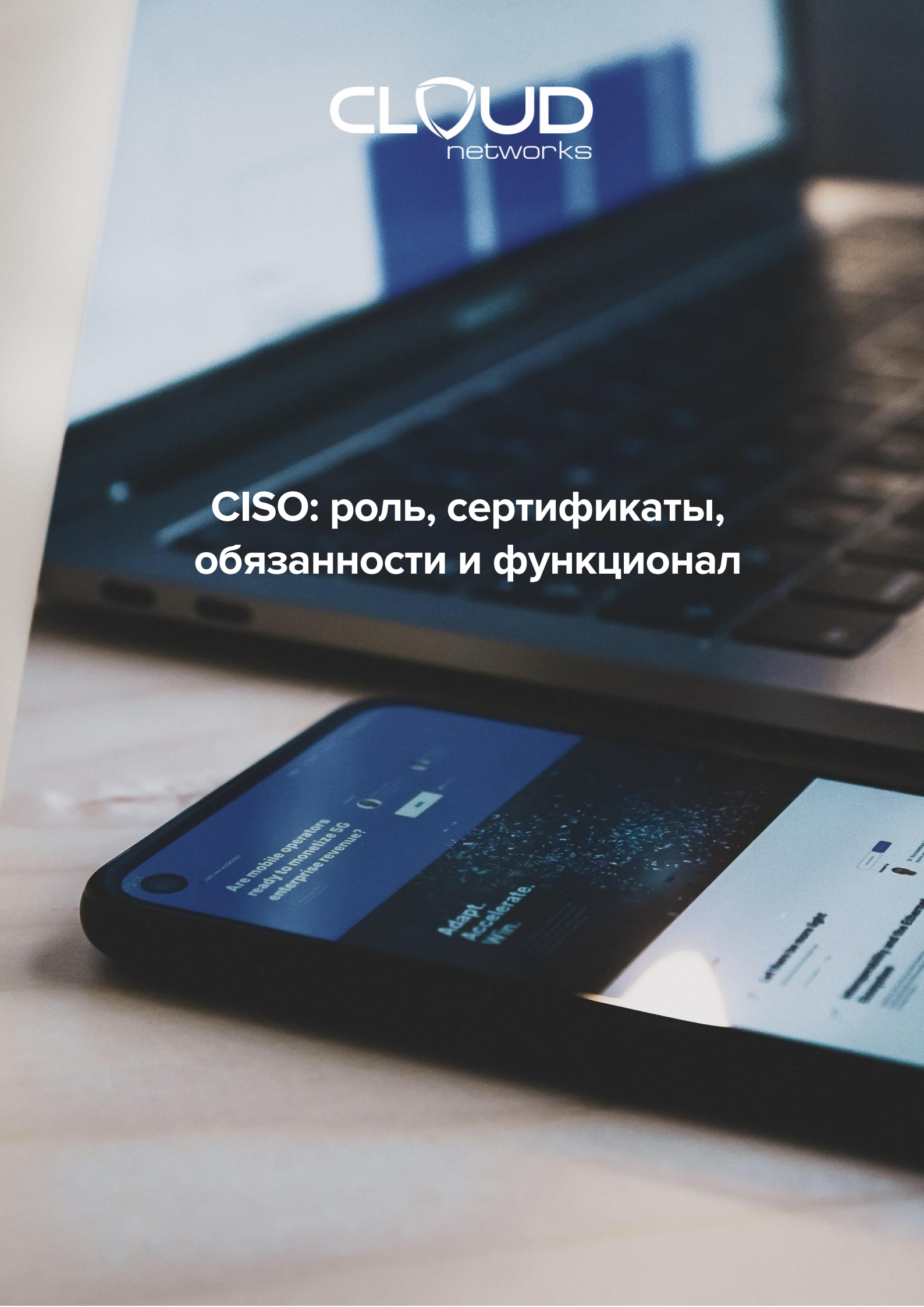


CISO: роль, сертификаты, обязанности и функционал

РОЛЬ CISO

Основная роль CISO – быть мостом между топ-менеджерами, советом директоров и техническими специалистами. А главная задача – создать стратегию развития ИБ для выполнения бизнес-целей компании. CISO стоит в первую очередь на стороне бизнеса:

Например, CISO и CIO ставится цель – обеспечить 100%-ую доступность веб-приложения и защиту данных клиентов. CIO должен создать отказоустойчивую инфраструктуру, а CISO сделать так, чтобы ее не скомпрометировали. При этом надо помнить о масштабировании бизнеса и финансовых планах компании.

CISO и CIO оценивают риски и выбирают стратегию, не противоречащую бизнес-целям либо предлагаю компромиссные решения по корректировке бизнес-задач.

СЕРТИФИКАТЫ CISO

Самые популярные сертификаты для CISO:

Certified Information Systems Security Professional (CISSP)
Сертифицированный специалист по безопасности информационных систем

Certified Information Security Manager (CISM)
Сертифицированный менеджер по информационной безопасности

Certified Information Systems Auditor (CISA)
Сертифицированный аудитор информационных систем

Certified in Risk and Information Systems Control (CRISC)
Сертифицированный специалист в области управления рисками и информационными системами

Навыки CISO

Руководитель должен:

- Решать проблемы ИБ
- Организовывать работу подразделения
- Разбираться в технической базе и ИБ-технологиях

Предпочтительно, чтобы кандидат:

- Имел высшее техническое образование
- Общий опыт работы от 7 лет, на руководящей должности от 5 лет
- Знал нормативные требования к отрасли компании

ОБЯЗАННОСТИ CISO

Управление отделом кибербезопасности и бюджетирование

- Набор, обучение и руководство командой информационной безопасности
- Эффективное использование бюджета в рамках программы ИБ и бизнес-целей

Внедрение и контроль системы обеспечения кибербезопасности

- **Соблюдение политик и законов в области информационной безопасности в компании**
- **Составление и согласование стратегии кибербезопасности и бизнес-целей**
- **Реализация проектов по ИБ**

Обеспечение кибербезопасности при реализации бизнес-целей

- Проверка программ информационной безопасности на соответствие целям компании
- Обеспечение связи между сотрудниками ИБ, руководством и другими сторонами
- Соблюдение мер безопасности при новых проектах и масштабировании бизнеса

Повышение осведомленности в информационной безопасности

- Изучение развивающихся угроз безопасности
- Продвижение культуры ИБ, а также донесение до сотрудников потенциальных проблем безопасности
- Проведение обучений по кибербезопасности

Снижение рисков ИБ при работе с поставщиками

- Оценка угроз в цепочке поставок и при работе с поставщиками услуг
- Обеспечение информационной безопасности при работе с поставщиками

Реагирование на киберинциденты

- Мониторинг действий команды ИБ по реагированию на инциденты
- Раннее обнаружение угроз безопасности
- Определение времени простоя из-за инцидентов безопасности

Обеспечение непрерывности бизнеса и аварийного восстановления

- Управление непрерывностью бизнес-процессов
- Определение причин киберинцидентов и выявление внутренних угроз
- Планирование восстановления в случае инцидента

Отчетность

- Предоставление руководству отчетности о состоянии кибербезопасности компании, рискам и рекомендациям по улучшению защиты компании
- Осведомление руководства о тенденциях в ИБ

ФУНКЦИОНАЛ CISO

Руководство

Стратегия безопасности в соответствии с бизнес-целями

Распределение обязанностей среди сотрудников ИБ

Проекты кибербезопасности

Управление ресурсами

Классификация данных

Ведение документации

Политика безопасности

Метрики и отчетность

Управление ИТ-портфелем

Отношения с клиентами и партнерами

Тимбилдинг

Наставничество

Соблюдение требований законодательства и соответствие

ФЗ-98

ФЗ-149

ФЗ-152

Форензика

Судебная практика

Требования клиента

Правовые риски

Бюджетирование

Анализ трудозатрат сторонних исполнителей

Расходы CAPEX/OPEX

Бюджет на сотрудников и их обучение

Страхование от кибер-угроз

Культура безопасности

Повышение осведомленности

Внутренние политики безопасности

Награждение за обнаружение уязвимостей

Обучение сотрудников

Управление идентификацией и доступом

Предоставление/удаление доступов сотрудникам

Единый вход (SSO)

Федеративный единый вход (FSSO)

Многофакторная аутентификация

Управление доступом на основе ролей (RBAC)

Безопасность учетных данных (LDAP, Active Directory)

Операционная информационная безопасность

Защита данных:

- Шифрование, PKI, TLS
- Предотвращение утечек информации (DLP)
- Анализ поведения пользователей (UBA)
- Безопасность электронной почты
- Брокер безопасности облачного доступа (CASB)

Сетевая безопасность:

- Брандмауэр, IDS/IPS, фильтрация прокси
- VPN, шлюз безопасности
- Защита от DDoS-атак

Безопасность приложений:

- Моделирование угроз
- Проверка безопасности
- Статический анализ
- WAF, RASP

Безопасность конечных точек:

- Антивирус
- HIDS/HIPS, FIM
- Белый список приложений

Безопасность конфигураций

Нулевое доверие

Патч менеджмент

Мобильная безопасность

Облачная безопасность

Обнаружение и реагирование

Управление журналами безопасности

Мониторинг событий информационной безопасности

Анализ сетевого трафика

Поиск угроз

Тестирование на проникновения

Red Team

Сканирование уязвимостей

Сканирование веб-приложений

Предотвращение потери данных (DLP)

Анализ поведения пользователей (UBA)

Центр управления безопасностью (SOC)

Киберразведка

Регламент реагирования на инциденты

Антикризисное управление

Обеспечение резервных каналов и способов связи

Управление рисками

Методология оценки рисков

Анализ и оценка киберрисков и их влияния на бизнес

Повышение осведомленности в области ИБ

Управление уязвимостями

Управление рисками цепочки поставок

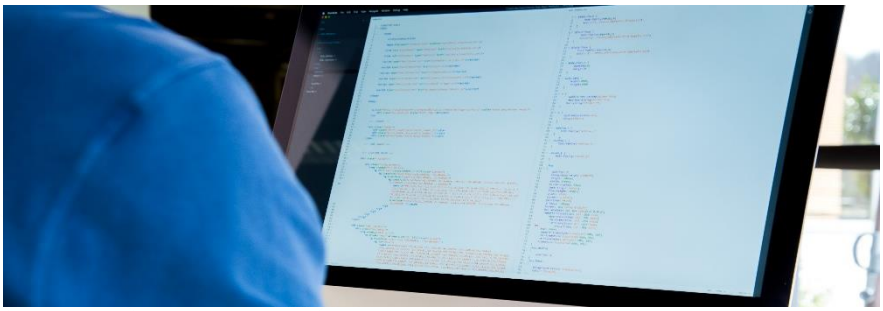
Аварийное восстановление

Обеспечение непрерывности бизнеса

Политики и процедуры

Обработка рисков:

- Мероприятия по смягчению последствий
- Управление командой
- Проверка и исправление рисков



Cloud Networks – ваш бизнес-партнер в мире информационной безопасности. Наша команда поможет определить ландшафт киберугроз и надежно защититься. Без страха занимайтесь бизнесом, остальное доверьте нам.

ПЕРЕЙТИ НА САЙТ