



ИНТЕНСИВ · 3 МОДУЛЯ · ОНЛАЙН

Практический интенсив по кибер- безопасности для CIO

Короткая образовательная онлайн-программа для ИТ-руководителей с возможностью усилить свои компетенции в вопросах кибербезопасности и поднять свою стоимость на рынке труда.

4 занятия от ИТ-директоров, уже разобравшихся в вопросах ИБ.

ПОТОК · ОНЛАЙН

21, 23, 28 и 30 октября · 10:00

по Москве · разбор кейсов участников

3

модуля: два лекционных и практикум

16

академических часов

3

документа по своей компании: карта рисков, первоочередные меры, план развития ИБ

2

эксперта: взгляд ИТ и взгляд ИБ

1

удостоверение по окончании программы

— для кого

Программа рассчитана на руководителей, у которых ИБ — часть зоны ответственности

01

ИТ-директор

Отвечает за ИТ и за безопасность одновременно, выделенной ИБ-функции в компании нет или она только формируется.

02

Руководитель ИТ-подразделения

Готовит решения и бюджет для руководства, и ему нужна методика, а также аргументы, которые примет бизнес.

03

Технический руководитель

Знает инфраструктуру глубоко, хочет достроить управленческую рамку: риски, зрелость, приоритеты, дорожная карта.

Формат. Онлайн, 4 занятия: 21, 23, 28 и 30 октября, начало в 10:00 по Москве. 3 модуля, 16 академических часов: два лекционных модуля и практикум, на котором разбираем ваши кейсы. После курса — домашнее задание: внедрение инструментов программы в своей компании.

Почему сегодня ИТ-директор отвечает и за информационную безопасность

Количество кибератак продолжает расти, и последствия одной успешной атаки — это финансовые потери, остановка бизнес-процессов, репутационный ущерб и персональная ответственность руководителя ИТ. При этом у большинства компаний нет объективной оценки собственного уровня защищённости.

01

Руководство просит подтвердить, что компания защищена

Совет директоров ждёт понятного ответа на вопрос «мы в безопасности?». Технические метрики на этот вопрос не отвечают.

02

Непонятно, какие риски действительно критичны

Список угроз бесконечен, а ресурс ограничен. Без приоритизации команда защищает всё сразу и не защищает ничего.

03

Сложно определить, во что инвестировать в первую очередь

Вендоры предлагают десятки решений. Нужен критерий выбора, который выдержит разговор с финансовым директором.

04

Нет единой стратегии развития ИБ

Решения принимаются точно — в ответ на инцидент или требование проверяющих. Связной картины на два-три года нет.

05

Нет объективной оценки зрелости ИБ

Ощущение «вроде нормально» не измеряется и не сравнивается с отраслью. Первый шаг — получить цифру, от которой можно отталкиваться.

Соберите план ИБ своей компании

4 занятия: карта рисков, первоочередные меры и план развития ИБ.

Насколько ваша компания действительно готова к современным киберугрозам?

Два лекционных модуля дают систему, третий — практический — переносит её на вашу компанию. Домашнее задание закрепляет внедрение инструментов внутри организации.

01 / 03

4 ЧАСА • ЛЕКЦИОННЫЙ

Основы современной информационной безопасности

КОНТЕКСТ И ОТВЕТСТВЕННОСТЬ

- Современные киберугрозы
- Ответственность ИТ-директора
- Модель CIA

КАК УСТРОЕНА ЗАЩИТА

- Архитектура защиты
- Пять контуров информационной безопасности
- Управление рисками

Результат: общий язык с ИБ-специалистами и рамка для оценки своей компании

02 / 03

4 ЧАСА • ЛЕКЦИОННЫЙ

Управление информационной безопасностью предприятия

ОПЕРАЦИИ: УПРАВЛЕНИЕ И ЗАЩИТА

- Защита инфраструктуры
- Управление доступами
- Реагирование на инциденты
- Аудит информационной безопасности

ЗРЕЛОСТЬ, ЗАКОН, ДЕНЬГИ

- Оценка зрелости ИБ
- Законодательные требования
- Инвестиции в информационную безопасность

Результат: критерии выбора мер и аргументация бюджета перед руководством

03 / 03

ПРАКТИКУМ • 4 ЧАСА • ПРАКТИЧЕСКИЙ

Разбор реальных кейсов участников

НА ЗАНЯТИИ

Каждый участник формирует по своей компании:

01

Карта рисков

своей компании

02

Перечень первоочередных мероприятий

что делать в первую очередь

03

План развития информационной безопасности

который можно вынести на совет директоров

Работаем с вашей ситуацией, а разбор ведут действующие практики.

ПОСЛЕ КУРСА

Домашнее задание

- ✓ Внедрение инструментов программы в своей компании
- ✓ Самостоятельная оценка зрелости ИБ по калькулятору
- ✓ Актуализация карты рисков по фактическим данным

Программа заканчивается конкретными изменениями внутри компании.

03 • ПОСЛЕ ОБУЧЕНИЯ

Каждый блок заканчивается инструментом, который вы применяете к своей компании



Оценивать уровень зрелости ИБ

Объективно, по понятной шкале — и повторно, чтобы видеть динамику.



Выявлять критичные риски

Отделять то, что способно остановить бизнес, от того, что просто беспокоит.



Понимать архитектуру современной защиты

Как складываются контуры защиты и где в вашей инфраструктуре разрывы.



Выстраивать приоритеты развития ИБ

Что делать в этом квартале, что — в следующем году, и почему именно так.



Аргументированно защищать бюджет

Говорить с руководством на языке рисков и денег, с опорой на цифры.



Сформировать дорожную карту

План развития ИБ компании, который можно вынести на совет директоров.

04 • КТО ВЕДЁТ

Программу ведут действующие практики

Люди, которые каждый день управляют реальной инфраструктурой и отвечают за её защиту — они приносят на занятия собственные решения и собственные ошибки.



ВЗГЛЯД ИТ

Роман Жарков

Директор департамента программного обеспечения, процессинга и поддержки пользователей, Абсолют Банк

Практик с многолетним опытом управления корпоративной ИТ-инфраструктурой и цифровой трансформацией.

Член СПб клуба ИТ-директоров



ВЗГЛЯД ИБ

Алексей Ахмеев

Руководитель информационной безопасности, Группа компаний «СВОЙ»

Практикующий эксперт по построению систем информационной безопасности, управлению рисками и защите корпоративной инфраструктуры.

Практика построения ИБ с нуля

Участие в интенсиве

ПОТОК ОКТЯБРЯ

Практический интенсив по кибербезопасности для CIO

35 000 ₽

онлайн · 21, 23, 28 и 30 октября, 10:00 по Москве

- ✓ **3 модуля**, 16 академических часов
- ✓ Два лекционных модуля и практикум с разбором ваших кейсов
- ✓ **Три документа** по своей компании: карта рисков, перечень первоочередных мероприятий, план развития ИБ
- ✓ Домашнее задание: внедрение инструментов программы в своей компании
- ✓ Удостоверение по окончании программы

Оплата

Частным лицам

Оплата картой на странице курса codeib.academy/cioclub.

Оплата

Компаниям

Выставляем счёт: запросите его на странице курса или напишите на academy@codeib.ru.

Запись

Идёт набор · старт 21 октября

4 занятия онлайн: 21, 23, 28 и 30 октября, начало в 10:00 по Москве.

ОРГАНИЗАТОР

Программа от проекта, который 21 год работает с российским рынком ИБ

«Код ИБ» существует с 2005 года: конференции в 36 городах, закрытый клуб действующих CISO, ежемесячные эфиры и образовательные программы с лицензией на образовательную деятельность. Программа — совместно с **Санкт-Петербургским клубом ИТ-директоров**.

1 021

мероприятие за 21 год

81 302

участника за 21 год

36

городов охвата

500+

экспертов и спикеров в пуле

№ 1 по доверию среди региональной аудитории ИБ — по исследованию «Ростелеком Солар». Конференция «Код ИБ Санкт-Петербург» ежегодно собирает около 200 профильных руководителей.

Следующий шаг — сделать ИБ управляемой

Оцените зрелость, найдите критичные риски и соберите план развития безопасности своей компании. Записаться, оплатить или запросить счёт — на странице курса.

ПОЧТА

academy@codeib.ru

TELEGRAM

[@codeib_ru](https://t.me/codeib_ru)

СТРАНИЦА КУРСА

codeib.academy/cioclubcodeib.academy/cioclub

Код ИБ Академия — образовательное направление экосистемы Код ИБ. Обучение ведёт ООО «Экспо-Линк» по образовательной лицензии ЛО35-01277-66/02876151.