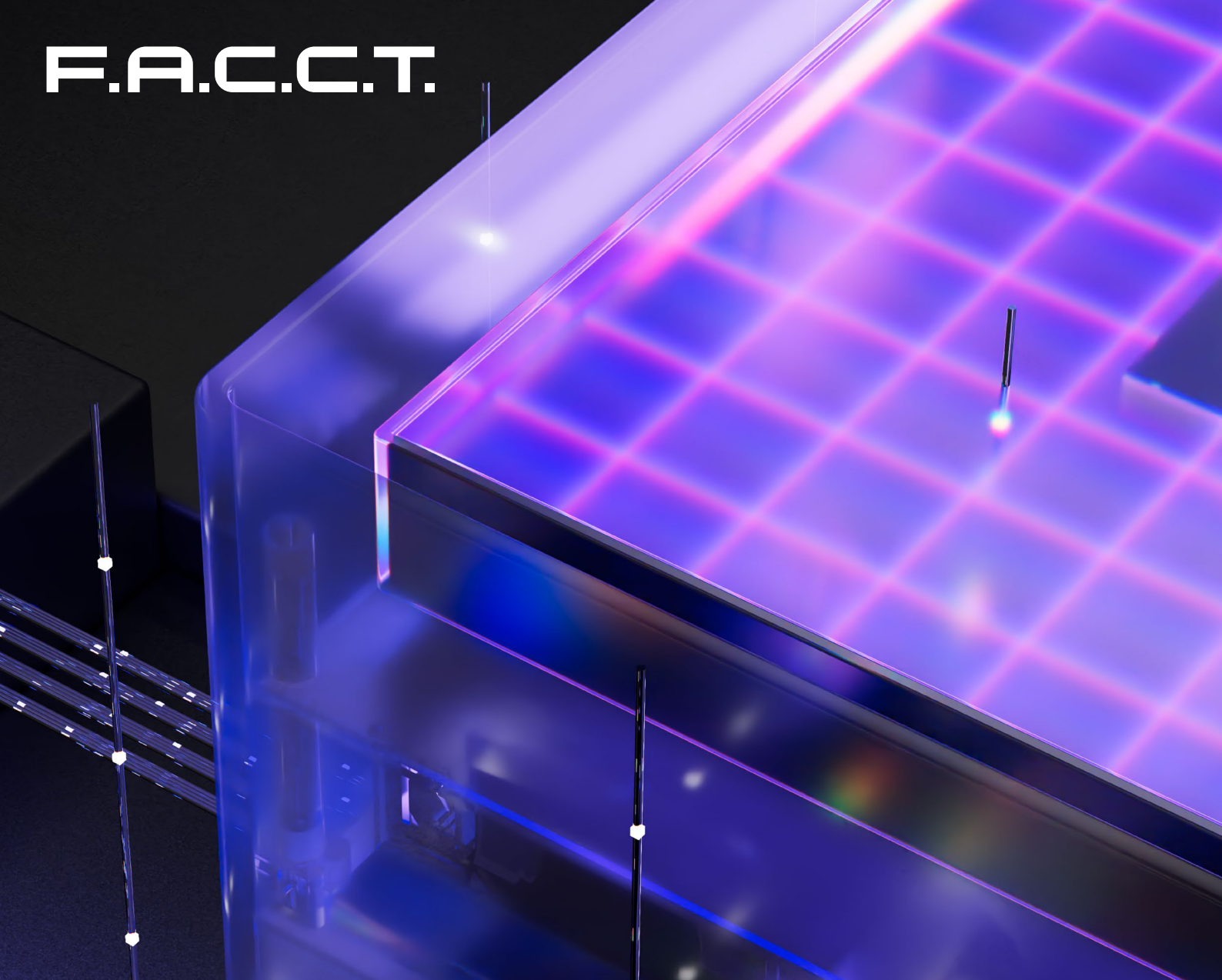


F.A.C.C.T.



ОБУЧЕНИЕ

КИБЕРПРОФЕССИИ БУДУЩЕГО

Современные образовательные
программы по информационной
безопасности

Создавайте вашу образовательную стратегию с нами

Краеугольным камнем успешного бизнеса является безопасность. Обучаясь у профессионалов по борьбе с киберпреступностью, вы инвестируете в усиление ваших команд ИБ и экспертизу собственных специалистов.

Обширный опыт в борьбе с киберугрозами

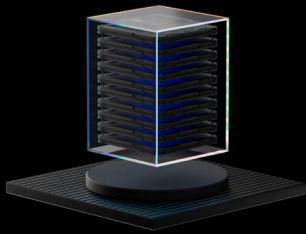
F.A.C.C.T. постоянно отслеживает более 100 000 профилей киберпреступников, составленных за 19 лет международных исследований в сфере высоких технологий. Наши эксперты и аналитики отслеживают изменения в инструментах, тактиках, техниках и процедурах, используемых злоумышленниками, а также в индикаторах компрометации новых угроз, разрабатываемых самыми опасными преступными группами, такими как Cobalt, Silence, MoneyTaker и Lazarus.

Практикующие преподаватели

Тренеры F.A.C.C.T. — это практикующие специалисты, работающие в нашей Лаборатории компьютерной криминалистики. Именно поэтому слушатели курсов получают самую свежую и актуальную информацию в сфере кибербезопасности из первых рук. Тренеры F.A.C.C.T. принимали участие в расследовании киберпреступлений, совершенных Buhtrap, Lurk, Cobalt, Fin7, APT3, MoneyTaker, DarkVishnya, Silence, BlackEnergy и другими преступными группами. Этот многолетний опыт работы с реальными кейсами позволяет регулярно пополнять программу курсов новой информацией, отражающей последние тренды.

Разнообразные форматы

Часть контента наших курсов мы перевели в видео-формат, что позволило повысить эффективность передачи информации и сконцентрироваться на живом взаимодействии с тренером при изучении наиболее важных аспектов изучаемого материала. Во время обучения на некоторых курсах F.A.C.C.T. слушатели участвуют в интерактивной игре-симуляции «Отражение атаки на организацию». Игра дает возможность слушателям потренироваться на реальном кейсе, применить полученные знания и навыки и успешно провести реагирование на киберинцидент.



11 курсов

Программы для технических специалистов



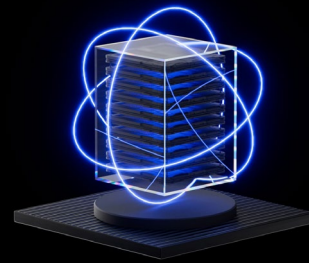
Курс для широкой аудитории

Цифровая гигиена



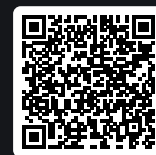
Игра

Игра-симуляция «Реагирование на инцидент»

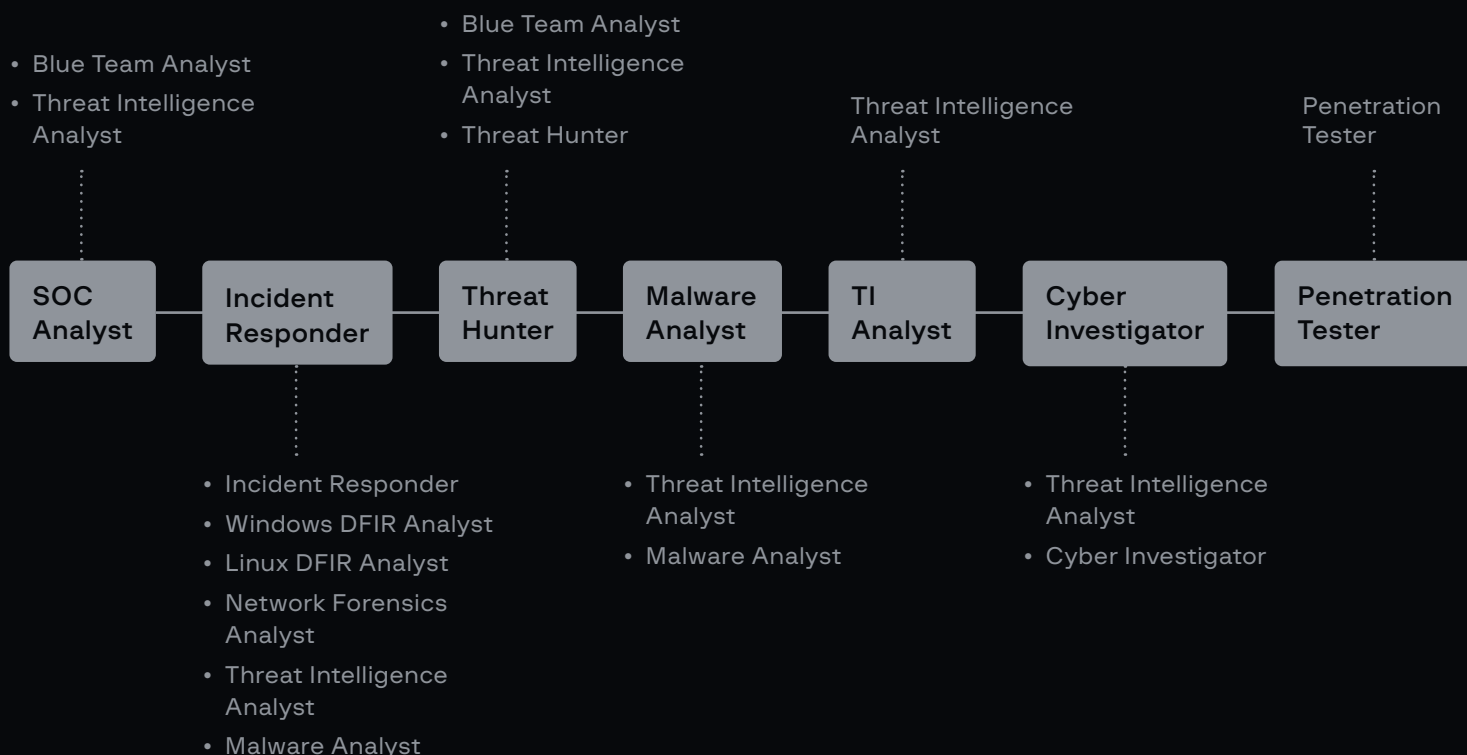


Интенсив

Защита персональных данных






Путь героя в мире кибербезопасности



Коммерческие программы для технических специалистов

Название курса	О чем курс	Длительность	Для кого	Больше информации
Реагирование на инциденты ИБ Сложность: ●●●○	Практический курс по эффективному реагированию на выявленный инцидент и ликвидации его последствий.	3 дня 6 часов / день	<ul style="list-style-type: none">• Энтузиасты в области реагирования на инциденты• Технические специалисты с опытом в ИБ• Специалисты по информационной безопасности• Сотрудники SOC/CERT	
Компьютерная криминалистика и реагирование на инциденты в ОС Windows Сложность: ●●●○	Практический онлайн-курс по проведению криминалистического анализа зараженных компьютеров на базе ОС Windows от экспертов F.A.C.C.T.	5 дней 6 часов / день	<ul style="list-style-type: none">• Специалисты по информационной безопасности• Технические специалисты с опытом работы в ИБ• Специалисты по реагированию на инциденты	
Компьютерная криминалистика и реагирование на инциденты в ОС Linux Сложность: ●●●○	Практический курс по исследованию систем на базе ОС Linux.	2 дня 6 часов / день	<ul style="list-style-type: none">• Специалисты по информационной безопасности• Технические специалисты с опытом в ИБ• Специалисты по реагированию на инциденты	
Основы защиты информационных систем Сложность: ●●○○	Узнайте, как производить мониторинг событий ИБ, детектировать угрозы, выявлять ложноположительные срабатывания и реагировать на инцидент.	3 дня 6 часов / день	<ul style="list-style-type: none">• Специалисты с опытом в ИБ• Практикующие специалисты ИБ/ИТ• Команды SOC/CERT	
Сетевая криминалистика Сложность: ●●○○	Практический курс об исследовании сетевого трафика в рамках реагирования на инциденты.	2 дня 6 часов / день	<ul style="list-style-type: none">• Специалисты ИБ• Специалисты по реагированию на инцидент• Аналитики SOC/CERT• Компьютерные криминалисты	
Исследование киберпреступлений Сложность: ●●●○	Практический курс по исследованию киберпреступлений, обнаружению инфраструктуры и отслеживанию цифровых следов злоумышленника.	2 дня 6 часов / день	<ul style="list-style-type: none">• Технические специалисты с опытом в ИБ• Специалисты по ИБ• Руководители отделов ИБ и ИТ	
Анализ вредоносного ПО. Видеокурс Сложность: ●●●○	Курс по проведению анализа вредоносных программ, обнаруженных во время реагирования на инцидент или криминалистического анализа зараженных компьютеров.	3 недели	<ul style="list-style-type: none">• Специалисты по реагированию на инциденты ИБ• Специалисты по компьютерной криминалистике• Аналитики SOC/CERT	
Проактивный поиск киберугроз Сложность: ●●●○	Практический курс по проактивному поиску скрытых недетектируемых угроз в организации.	3 дня 6 часов / день	<ul style="list-style-type: none">• Технические специалисты с опытом в ИБ• Специалисты в области информационной безопасности• Специалисты по threat hunting	

Название курса	О чем курс	Длительность	Для кого	Больше информации
Анализ данных киберразведки Сложность: ●●○○	Курс по сбору информации о киберугрозах и обогащению процессов кибербезопасности данными TI для эффективного реагирования на инциденты и мониторинга угроз.	2 дня 6 часов / день	<ul style="list-style-type: none"> • Специалисты с опытом в ИБ • Специалисты ИБ • Команды SOC/CERT 	
Тестирование на проникновение Сложность: ●●○○	Узнайте, как мыслят киберпреступники, и научитесь использовать различные техники для повышения защищенности организации.	3 дня 6 часов / день	<ul style="list-style-type: none"> • Специалисты по информационной безопасности • Системные/сетевые администраторы/инженеры • Сотрудники SOC/CERT/CSIRT • Технические специалисты с опытом работы в ИБ • Энтузиасты тестирования на проникновение 	
Основы противодействия мошенничеству Сложность: ●●○○	Вводный курс для знакомства с типами мошенничества и приемами противодействия ему, принципами работы современных систем сессионного антифрода на примере F.A.C.C.T. Fraud Protection.	2 дня 6 часов / день	<ul style="list-style-type: none"> • Специалисты по мониторингу киберугроз • Технические специалисты с базовым опытом в ИБ • Руководители служб безопасности и руководители отделов ИТ • Руководители, отвечающие за каналы ДО клиентов 	

Формат:

Онлайн

Оффлайн (по запросу)

Наборные группы

Корпоративные группы

Описание компании

F.A.C.C.T. — один из ведущих российских разработчиков решений для обнаружения и предотвращения кибератак, выявления мошенничества и защиты интеллектуальной собственности в сети.

1 300+

успешных исследований по всему миру

550+

enterprise-клиентов

120+

патентов и заявок

№1

первый поставщик услуги Incident Response в России

20 млрд +

сохраняют наши технологии в бюджете клиентов ежегодно

20 лет

практики и уникальной экспертизы на рынке РФ

Технологии и инновации

Кибербезопасность

- Threat Intelligence
- Управление поверхностью атаки
- Защита электронной почты
- Анализ сетевого трафика
- Детонация ВПО
- Защита конечных станций (EDR)
- XDR

Противодействие мошенничеству

- Противодействие мошенничеству client-side
- Адаптивная аутентификация
- Защита от ботов
- Выявление платежного мошенничества
- Поведенческий анализ

Защита бренда

- Антифишинг
- Антипиратство
- Антимошенничество
- Антиконтрафакт
- Выявление утечек данных
- Защита VIP-персон

Портфолио услуг

Аудит и консалтинг

- Анализ защищенности
- Тестирование на проникновение
- Red Teaming
- Оценка соответствия и консалтинг

- Выявление следов компрометации
- Проверка готовности к реагированию на инциденты

Обучающие программы

- Для технических специалистов
- Для широкой аудитории

- Мастер-классы для детей

Реагирование на инциденты и цифровая криминалистика

- Реагирование на инциденты
- Реагирование на инциденты по подписке

- Цифровая криминалистика
- eDiscovery

Managed Services

- Managed Detection
- Managed Threat Hunting

- Managed Response

Исследование высокотехнологичных преступлений

- Исследование киберпреступлений

Подробности об условиях участия, расписание и регистрация доступны:

через форму на сайте



или по электронной почте:
education@facct.ru