Международный центр образования НЦОТ

АНТИФРОД-ЭКСПЕРТ. СОВРЕМЕННЫЕ МЕТОДЫ БОРЬБЫ С НЕЗАКОННЫМИ ПЛАТЕЖНЫМИ ОПЕРАЦИЯМИ

Программа повышения квалификации

ЦЕЛЬ ПРОГРАММЫ

Развитие профессиональных компетенций специалистов, необходимых для противодействия мошенничеству в банковской сфере, выявления и предотвращения незаконных платежных операций, анализа фрод-рисков, расследования инцидентов, а также применения современных антифрод-систем, технологий профайлинга, поведенческого анализа и машинного обучения.

ЦЕЛЕВАЯ АУДИТОРИЯ

Программа предназначена для:

- специалистов банков и финансовых организаций, участвующие в противодействии мошенничеству и незаконным платежным операциям;
- антифрод-аналитиков и специалистов подразделений финансовой безопасности, информационной безопасности, управления рисками, внутреннего контроля, комплаенса и инцидент-менеджмента;
- специалистов по мониторингу платежных операций, анализу фрод-рисков и расследованию мошеннических инцидентов;
- ИТ-специалистов, участвующих во внедрении и сопровождении антифрод-систем, систем профайлинга и скоринговых моделей;
- сотрудников контакт-центров и клиентских подразделений, взаимодействующих с клиентами при выявлении признаков мошенничества и социальной инженерии.

ФОРМА ОБУЧЕНИЯ	СТОИМОСТЬ ОБУЧЕНИЯ	АДРЕС ОБУЧЕНИЯ	ПРОДОЛЖИТЕЛЬНОСТЬ
Очная (дневная)	1200 руб.	ул. К. Цеткин, 24	36 академических часов

По окончании обучения выдается **свидетельство о повышении квалификации**

https://ntec.by/obrazovanie/training

+375 17 344 34-63 +375 17 344 34-77

Международный центр образования НЦОТ

УЧЕБНЫЙ ПЛАН КУРСА

№	Наименования разделов, модулей, тем
I	**ОСНОВЫ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ**
1.	Правовое определение мошенничества в банковской сфере
2.	Виды мошенничества в Республике Беларусь
3.	Обзор нормативных требований Национального банка Республики Беларусь
4.	Взаимодействие с правоохранительными органами и другими финансовыми институтами. Порядок передачи информации, правовые аспекты
5.	Жизненный цикл мошеннической атаки: выявление, предотвращение, расследование
II	**СОВРЕМЕННЫЕ ТЕХНОЛОГИИ И АНТИФРОД. СРЕДСТВА ВЫЯВЛЕНИЯ И ЗАЩИТЫ**
1.	Введение в антифрод-системы. Компоненты антифрод-систем
2.	Текущие технологии и инструменты выявления мошенничества: ПО, системы мониторинга, аналитика
3.	Использование искусственного интеллекта и машинного обучения при идентификации фрод-рисков. Обзор существующих решений и перспективы развития
4.	Использование машинного обучения, поведенческого анализа и анализ больших данных для выявления аномалий. Обзор алгоритмов, примеры применения. Анализ новых угроз и выработка контрмер
5.	Задачи и роль антифрод-аналитика: анализ инцидентов, разработка механизмов предотвращения, работа с данными
6.	Лучшие практики внедрения антифрод-систем: оценка рисков, адаптация под законодательство Республики Беларусь. Формирование стратегии защиты
7.	Оценка эффективности антифрод-систем: ключевые метрики, показатели, методы тестирования и оптимизации
8.	Влияние регуляторных требований НБ РБ на построение антифрод-систем. Соответствие требованиям и лучшие практики
III	**ПРОФАЙЛИНГ КЛИЕНТОВ**
1.	Понятие и задачи профайлинга в системе антифрод
2.	Методы построения профилей клиентов: поведенческий, транзакционный, биометрический анализ
3.	Алгоритмы оценки подозрительного поведения и признаки мошенничества
4.	Различие внутренних и внешних нарушителей: профили, мотивация, механизмы выявления
5.	Применение профайлинга для борьбы с автоматизированными атаками и ботами
6.	Анализ профилей и выявление аномальной активности

№	Наименования разделов, модулей, тем
IV	**ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННЫМ ПЛАТЕЖНЫМ ОПЕРАЦИЯМ**
1.	Механизмы аутентификации и авторизации: одноразовый пароль, биометрия, поведенческий анализ. Новые технологии и тренды
2.	Риски дистанционного обслуживания (мобильный и интернет-банкинг): особенности уязвимостей, типовые атаки
3.	Роль скоринговых моделей в оценке легитимности транзакций. Построение и оптимизация скоринговых моделей
4.	Процедуры инцидент-менеджмента: выявление, блокировка, расследование. Алгоритм действий при инциденте
5.	Взаимодействие с платежными системами и регуляторами при инцидентах. Правовые аспекты
6.	Разбор и блокировка несанкционированных операций
V	**РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ**
1.	Организация расследования мошенничества: этапы и инструменты. Распределение ролей и ответственности
2.	Анализ и документирование случаев мошенничества. Формирование доказательной базы
3.	Психологические приемы для «вывода» клиента из-под воздействия мошенников. Техники убеждения и деэскалации
4.	Особенности коммуникации с клиентами, находящимися под влиянием мошенников. Сохранение спокойствия и позитивного настроя
5.	Телефонная коммуникация: распознавание жертв мошенников, техники ведения разговора и защиты информации