Московский институт электроники и математики им.А.Н.Тихонова (МИЭМ НИУ ВШЭ)

Программа повышения квалификации

Москва 2024

Цифровая гигиена. Корпоративная безопасность.

- ✓ первая в России программа-тренажер, которая меняет мышление пользователей цифровых продуктов и оборудования и направлена на профилактику репутационных и финансовых потерь от кибервторжений
- ✓ самая полная программа по охвату спектра киберугроз и отраслевых направлений
- ✓ программа дает инструментарий обучения – с целью последующего распространения внутри организации

«Очевидно, что у каждого из нас есть виртуальное «я», безопасное функционирование которого определяет успех в профессии и в жизни.

Наша программа о том, как успешно вести проекты в цифровой реальности и управлять виртуальными активами», - Елена Кабаева, руководитель программы

→ о нас пишут: https://www.hse.ru/news/edu/966071373.html

сайт программы

miem.prof@hse.ru

@MIEMPROF

Контекст:

86% опрошенных (по данным ЦБ РФ за 2023 год) осознают потенциально возможную угрозу мошенничества при получении входящей информации по разным каналам. При этом не избегают потерь.

Знают, но **финансовых потерь не избегают**

ТЕОРИЯ

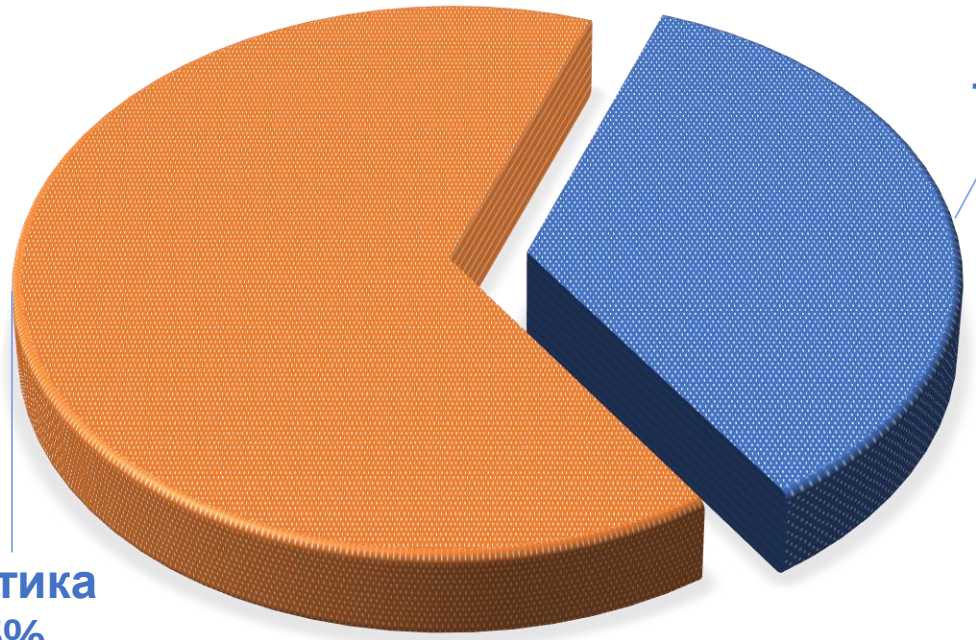
ПРАКТИКА

программа “ЦИФРОВАЯ ГИГИЕНА. КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ.” направлена на выработку именно практических навыков противостояния киберугрозам разного типа

Другие контексты. Не всегда оцениваются, но имеют место:

корпоративные потери, репутация, общественный климат, здоровье, качество жизни

Структура программы: соотношение теории и практики.



теория 35%

экспертные лекции
мастер-классы

практика 65%

кейсы-тренажеры
симуляторы

miem.prof@hse.ru
@MIEMPROF

3 тематических модуля + сквозной проект

Основы корпоративной ИБ.
Киберугрозы.
Правила корпоративной и личной ИБ.
Средства обеспечения ИБ.
Цифровой след.
Пароли, аутентификация, настройки, безопасность.
Хранение и распространение личных и корпоративных данных.
Защита от вирусов и ПО.

Цифровое гражданство.
Безопасное электронное портфолио.
Критическое мышление в интернете
Нетикет.
Кибербуллинг.
Удаленные коммуникации.
Ментальное здоровье. Информационные детокс.
Искусственный интеллект в цифровых проектах.

Информация и охраняемый контент
Цифровые активы и виртуальная собственность
Искусственный интеллект и нейронные сети: правовой аспект

Собственный безопасный цифровой проект

@MIEMPROF

Модуль 1: Цифровая безопасность.

Модуль интенсивной практики.
Отработка инструментария цифровой безопасности.
Авторские технологичные методики определения и предотвращения уязвимостей.

- ✓ Основы корпоративной информационной безопасности.
- ✓ Проектирование безопасного цифрового следа.
- ✓ Средства обеспечения информационной безопасности.
- ✓ Практики предотвращения фишинга.
- ✓ Утечки данных: случайные и преднамеренные.
- ✓ Безопасное управление данными: личными и корпоративными.
- ✓ Защита от вирусов и вредоносного ПО.

Амир Атигаев, руководитель, методист Новосибирского института современного образования (МАУ ДПО «НИСО»), обладатель медали «За верность традициям отечественного образования» Российской Академии Естествознания, 2024

Юлия Глухих, соруководитель, преподаватель информатики и программирования, куратор цифровых проектов в сегменте среднего и среднего специального образования, к.ф-м.н., разработчик ПО для сетевых Заказчиков

Денис Денисов, преподаватель, корпоративный тренер ГК InfoWatch, к.э.н.

Модуль 2: Цифровые проекты и психологическая безопасность.

Возможности разных цифровых сред.
Инструменты распознавания и предотвращения киберугроз при ведении цифровых проектов: от цифрового медиахранилища до гибких навыков.
Tilda, Wiki, Python, др.

- ✓ Цифровое гражданство
- ✓ Работа в условиях переизбытка информации и ограниченных ресурсов
- ✓ Фильтрация информации: критический анализ, списки проверенных источников, блокировка ненужного контента
- ✓ Распознавание признаков манипуляции, критическое мышление
- ✓ Особенности удаленной коммуникации. Нетикет.
- ✓ Кибербуллинг
- ✓ Ментальное здоровье и информационный детокс
- ✓ Искусственный интеллект в цифровых проектах

Наталья Фролова, руководитель, доцент НГЛУ им. Н.А.Добролюбова, доцент НИУ ВШЭ (Нижний Новгород), к.п.н., доцент, руководитель образовательных программ «Цифровая педагогика в современном лингвообразовании», «IT-лингвистика»

Модуль 3: Правовые аспекты.

Правомерность использования стороннего контента для обучения генеративных нейронных сетей.
Скрытые угрозы, связанные с виртуальным имуществом, цифровыми правами.

Руслан Будник, руководитель, профессор департамента права цифровых технологий и биоправа НИУ ВШЭ, д.ю.н., заместитель директора Международного научно-образовательного центра «Кафедра ЮНЕСКО по авторскому праву, смежным, культурным и информационным правам»

- ✓ Использование информации и охраняемого контента
- ✓ Цифровые активы и виртуальная собственность (виртуальное имущество и цифровые права, цифровая валюта, криптовалютные операции, внутриигровые ценности и другие объекты виртуальной собственности)
- ✓ Искусственный интеллект и нейронные сети, ответственность за правонарушения, совершенные ИИ).

Команда - компетенции

- Группа компаний InfoWatch
- Факультет информатики, математики и компьютерных наук НИУ ВШЭ - Нижний Новгород
- эксперты в менеджменте цифровых проектов
- МИЭМ НИУ ВШЭ
- Нижегородский государственный лингвистический университет им. Н.А.Добролюбова
- Факультет права НИУ ВШЭ
- Новосибирский институт современного образования
- эксперты сегмента среднего и среднего специального образования
- разработчики кейсов-тренажеров

Прогресс слушателя на программе

инструментарий → как противостоять → что учесть → как сделать

сквозной проект

Удостоверение о повышении квалификации

Навыки на всю жизнь

Постпрограммное сопровождение от команды

Характер активности

Симуляция, знакомство, отработка пользовательских кейсов.

Моделирование управляющих воздействий на пользователей на основе рабочей цифровой тетради.

Получение информации, корректировки по результатам

Представление безопасного цифрового профиля и цифрового проекта

Результат

- Сборник кейсов
- Библиотека методов распознавания скрытых и явных кибер-угроз
- Методика и навыки безопасного управления цифровым следом

- Безопасное электронное портфолио.
- Методика и навыки критического мышления в интернете
- Свод правил - нетикет

- Правила использования открытой информации и охраняемого контента.
- Цифровые активы и виртуальная собственность.
- Актуализированные результаты предыдущих модулей с учетом полученных знаний

- Готовый к реализации безопасный цифровой проект
- Обратная связь и рекомендации экспертов

Параметры программы

Даты программы: 21 октября - 25 декабря

Прием документов до 16 октября, зачисление слушателей до 18 октября 2024г.

Объем - 104 ак.ч., в т.ч. 72 - синхронных в прямом контакте с преподавателями и экспертами программы

Формат – онлайн, синхронное взаимодействие с экспертами и преподавателями

Стоимость – 42 000 руб.

О программе:

Расписание:

Целевые аудитории

- ответственные за информационную безопасность в корпорациях и университетах;
- организаторы корпоративного обучения - сотрудники HR-служб или корпоративных университетов;
- преподаватели дисциплин и руководителей проектов по кибербезопасности в сегментах среднего, среднего специального и высшего образования;
- руководители функциональных подразделений и команд (в т.ч. подразделений по цифровизации)
- сотрудники - пользователи цифровых систем и сервисов, не имеющие профильного образования в области информационной безопасности;
- корпоративные юристы;
- студенты и магистранты.

✓ Для корпоративных команд (от 20 чел.) программа кастомизируется

Резюме результатов программы. Слушатели:

- ❑ познакомятся со стандартами безопасной эксплуатации цифровых сервисов
- ❑ смогут организовать работу оборудования по предотвращению инцидентов и безопасному использованию информационных активов компании (университета)
- ❑ изменят поведенческие модели и реакции по отношению к информации и киберугрозам

- ✓ новые навыки и парадигмы в работе с информацией и цифровыми активами,
- ✓ распознавание и упреждение кибер-угроз,
- ✓ превентивное поведение, не допускающее возникновение угроз безопасности информации и информационной инфраструктуры,
- ✓ передача знаний и навыков в профессиональном и личном окружении

@MIEMPROF

Подать заявку на программу

онлайн-форма регистрации – быстрый способ подачи заявки

сайт программы
https://www.hse.ru/edu/dpo/958342380

Личный кабинет lk.hse.ru

miem.prof@hse.ru
@MIEMPROF

Документы для зачисления

Скан-копии или качественные цифровые фото-копии:

Для граждан РФ:

1. Паспорт гражданина России (страницы с ФИО и регистрацией).
2. Документ о высшем или среднем специальном образовании (диплом).
3. Номер СНИЛС (без скан-копии).
4. Согласие на обработку персональных данных (по форме).
5. Документ об изменении фамилии, имени, отчества (если менялись).

Для иностранных граждан:

1. Паспорт иностранного гражданина.
2. Документ о высшем образовании (диплом), перевод документа (желателен)
3. Согласие на обработку персональных данных (по форме).
4. Электронная почта слушателя.
5. Документ об изменении фамилии, имени, отчества (если менялись)

По окончании обучения

Удостоверение о повышении квалификации (электронный документ), регистрация в ФИС ФРДО.

miem.prof@hse.ru
@MIEMPROF

Образование для профессионалов в МИЭМ НИУ ВШЭ. Актуальные навыки в профессии на протяжении всей жизни.

8 флагманских инженерных направлений повышения квалификации:

- искусственный интеллект: прикладные решения
- беспроводная связь
- информационные технологии
- проектная модель
- электроника
- информационная безопасность
- геймификация, 3D-, видеотехнологии
- патентное право в инженерии

Программы реализуются в открытом и корпоративном форматах

Документ о повышении квалификации с регистрацией в ФИС ФРДО

Каталог программ ДПО МИЭМ НИУ ВШЭ
https://miem.hse.ru/dpo/

Электронный адрес «МИЭМ НИУ ВШЭ. Обучение профессионалов»: miem.prof@hse.ru

Телеграмм-канал «МИЭМ. ОБУЧЕНИЕ ПРОФЕССИОНАЛОВ»

Информация о ближайших событиях дополнительного профессионального образования МИЭМ НИУ ВШЭ