

◆ РАБОЧАЯ УЧЕБНАЯ ПРОГРАММА (СИЛЛАБУС)

Корпоративная кибергигиена и основы информационной безопасности

Ниже силлабус, для информации HR-специалистов и служб информационной безопасности (ИБ).



ТРУДОЕМКОСТЬ

36 академических часов



ФОРМАТ ПРОВЕДЕНИЯ

Дистанционный (асинхронное онлайн-обучение)



ЦЕЛЕВАЯ АУДИТОРИЯ

Государственные служащие, сотрудники корпоративного сектора, руководители подразделений.



СТРУКТУРА

15 модулей, входной и итоговый контроль

Для программ повышения квалификации госслужащих и корпоративного сектора золотым стандартом является объем в 36 академических часов (это приравнивается к 1 кредиту ECTS или стандартному краткосрочному курсу повышения квалификации).

◆ РАЗДЕЛ 1

Пояснительная записка и цели курса

Программа разработана с учетом современных требований к квалификации сотрудников в рамках обновления Трудового кодекса и стандартов информационной безопасности (ИБ).



Цель

Формирование устойчивых навыков безопасного поведения в цифровой среде, защита корпоративных и государственных информационных систем от киберугроз.



Задачи

Обучение методам распознавания социальной инженерии, правилам работы с конфиденциальной информацией, безопасному использованию цифровых активов и государственных электронных систем.

◆ РАЗДЕЛ 2

Распределение академических часов

Один академический час включает изучение мультимедийного контента (видео, тексты), разбор реальных инцидентов и самостоятельную работу в системе (ответы на проверочные вопросы).

	Контактная работа в LMS Теория, кейсы, микро-тесты	18 ч
	Самостоятельная работа слушателя (СРС)	16 ч
	Оценка и контроль Входное и итоговое тестирование	2 ч
ИТОГО		36 часов

Учебно–тематический план

№	НАЗВАНИЕ МОДУЛЯ И КРАТКОЕ СОДЕРЖАНИЕ	КОНТАКТНЫЕ ЧАСЫ (В LMS)	САМОСТ. РАБОТА (СРС)
00	Входной контроль Начальное тестирование для определения базового уровня знаний (20 вопросов).	1	0
01	Модуль 0-1: Введение и основы кибергигиены Приветствие CEO. Основные виды киберугроз. Политика информационной безопасности: роль каждого сотрудника.	1	1
02	Модуль 2: Безопасность рабочего пространства Защита ПК и смартфона. Контроль доступа в помещение. Работа с DLP-системами. Правила безопасной удаленной работы.	1,5	1,5
03	Модуль 3: Пароли Парольная политика организации. Правила создания, хранения и управления надежными паролями.	1	1
04	Модуль 4: Конфиденциальная информация Работа с бумажными и электронными документами. Риски облачных решений. Безопасное уничтожение данных.	1,5	1,5
05	Модуль 5: Обновления и ВПО (Вредоносное ПО) Важность обновлений ОС и ПО. Виды вредоносного ПО и шпионского кибероружия. Методы защиты.	1	1
06	Модуль 6: Безопасный интернет Протоколы, браузеры. Риски публичных Wi-Fi сетей. Защита корпоративной сети. Использование VPN.	1,5	1,5
07	Модуль 7: Фишинг (тотальный разбор) Социальная инженерия. Проверка сайтов и ссылок. Роль 2FA в защите от фишинга.	1,5	1,5
08	Модуль 8: Цифровые активы Что такое цифровые активы. Риски публикации личной информации (OSINT). Приватность в социальных сетях.	1	1
09	Модуль 9: Финансовая кибергигиена Безопасные онлайн-платежи и банкинг. Услуга «Стоп, Кредит» в РК. Проверка контрагентов для организаций РК.	1,5	1,5
10	Модуль 10: Безопасность и AI Риски и возможности использования искусственного интеллекта в работе (манипуляции, deepfake).	0,5	0,5
11	Модуль 11: Безопасность мобильных устройств Критическая важность защиты смартфона. Шифрование, пароли и защита от вредоносных приложений.	1	1

12	Модуль 12: Основы информационной безопасности Угрозы для государственных информационных систем. Введение в политику ИБ.	1	1
13	Модуль 13: Данные - на вес золота! Ценность данных. Специфика работы с электронными сервисами государственных органов и их защита.	1	1
14	Модуль 14: Безопасность в командировках и в отпуске Защита корпоративных данных при работе из дома и в деловых поездках. Лучшие практики.	1	1
15	Модуль 15: Инциденты безопасности (Обнаружение и реагирование) Правила первой помощи при подозрительном поведении системы и утечке информации.	1	1
16	Итоговый контроль Финальное тестирование для оценки усвоения материала (30 вопросов).	1	0
ИТОГО АКАДЕМИЧЕСКИХ ЧАСОВ			36 ч.

♦ РАЗДЕЛ 4

Методология обучения и контроля



Микрообучение (Microlearning)

Учебный материал разбит на короткие уроки (от 4 до 15 минут), что позволяет сотрудникам проходить обучение без длительного отрыва от производственного процесса.



Мультиформатность

Сочетание видеороликов, текстовых лонгридов, разбора реальных историй взломов и практических примеров из казахстанской практики (например, сервис «Стоп, Кредит»).



Текущий контроль

После каждого смыслового блока предусмотрены промежуточные проверочные вопросы для закрепления материала.



Аттестация

Для успешного завершения курса и получения сертификата (документа о повышении квалификации) слушатель должен пройти итоговое тестирование из 30 вопросов. Допуск к итоговому тесту открывается только после прохождения всех модулей.

Корпоративное обучение CitizenSec

Подробности и заявка на обучение — на странице корпоративного обучения.

citizensec.kz/lms