Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

Утверждаю
Директор ИНОТЭКУ
_____
А.Г. Мнацаканян

Тематические интерактивные занятия
«Погружение в мир безопасной экономики»

Составитель:
ассистент кафедры экономической безопасности
Дибурис Ксения Максимовна

Количество часов:

Руководитель: Дибурис Ксения Максимовна

Цель: сформировать базовые навыки защиты персональной и финансовой информации в цифровой среде.

Основные задачи:

— познакомить с типичными киберугрозами;

— обучить простым правилам цифровой гигиены;

— выработать алгоритм проверки подозрительных сообщений и ссылок;

— закрепить принципы безопасного поведения в соцсетях и на маркетплейсах.

Методы и приёмы:

— наглядность: скриншоты-примеры угроз, иконки правил;

— диалог: вопросы - ответы, мини-опрос;

— алгоритмы: готовые чек-листы («3 шага проверки ссылки»);

— практика: разбор образца фишингового сообщения (коллективно).

Материалы и ресурсы:

— презентация (5–7 слайдов) с визуальными примерами;

— раздаточный чек-лист «5 правил кибербезопасности» (формат А6);

— образцы фишинговых писем и ссылок (для разбора).

Ожидаемые результаты:

— умение перечислить 3–4 типичные киберугрозы (взлом, фишинг, утечка, мошенничество на маркетплейсах)

— формулирование основных правил создания надёжного пароля;

— понимание, зачем нужна двухфакторная аутентификация;

— применение алгоритма проверки подозрительной ссылки (3 шага);

— формулирование 2–3 принципов безопасного поведения в соцсетях и при онлайн-покупках.

Тематические интерактивные занятия
«Погружение в мир безопасной экономики»»

Дата проведения	Кол- во часов	Содержание	Вид занятий	Оборудование	Примечание
__.__.2026		Блок 1. Вводная часть: что такое киберугрозы? — краткий опрос: «С какими опасностями вы сталкивались в интернете?»; — определение понятий: взлом аккаунта, утечка данных, фишинговое письмо; — примеры (чем грозит утечка пароля от соцсети или банковского приложения).	Лекция Практические задания с элементами игры	Мультимедиа. Видеоряд, Компьютерный класс	ФГБОУ ВО «КГТУ» ИНОТЭКУ
		Блок 2. Основные киберугрозы и их признаки: — взлом аккаунта: как происходит, какие данные утекают; — утечка данных: откуда берутся базы паролей, почему важно менять пароли; — фишинговые письма и сообщения: типичные признаки (срочность, ошибки, подозрительные ссылки); — мошенничество на маркетплейсах: поддельные товары, фальшивые отзывы, «безопасная сделка» вне площадки.			
		Блок 3. Простые правила защиты — надёжные пароли: — длина от 12 символов, смесь букв/цифр/спецсимволов; — запрет на повтор паролей для разных сервисов; — двухфакторная аутентификация (2FA): зачем нужна и как включить (на примере соцсети или почты); — резервные копии: зачем сохранять важные фото и документы в облаке или на внешнем носителе.			
		Блок 4. Как проверять подозрительные ссылки и сообщения алгоритм из 3 шагов.			
		Блок 5. Безопасное поведение в соцсетях и на маркетплейсах			
1 Занятие					