

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

НИУ ВШЭ

Московский институт электроники и математики им. А.Н. Тихонова

УТВЕРЖДАЮ

Заместитель первого проректора НИУ ВШЭ

Г.В. Можаяева

УЧЕБНЫЙ ПЛАН

дополнительная профессиональная программа – программа повышения квалификации
«Цифровая гигиена»

Учебный год: 2024/2025

Трудоемкость программы: 3 зач. ед., 102 академических час. (в том числе 72 конт. час.).

Форма обучения: Очная

Формат ДОП: Онлайн синхронный

№ п/п	Названия учебных модулей, дисциплин	Трудоемкость		Объем контактной работы						Обучение с использованием ДОТ и (или) ЭО, в том числе в полном объеме (акад. ч.)	Самостоятельная работа (акад.ч.)	Форма промежуточной аттестации
		в зач. ед.	в акад. ч.	всего, конт. ч	Аудиторная работа (акад.ч.)				Обучение с использованием ДОТ и (или) ЭО, в том числе в полном объеме (акад. ч.)			
					всего, ауд. ч.	лекции	практические, семинарские, лабораторные занятия	консультации, иные виды занятий		синхр.	асинхр.	
1	2	3	4	5	6	7	8	9	10	11	12	13
1	Основы корпоративной информационной безопасности		2	2					2			
1.1	Основные понятия ИБ. Информация как объект защиты. Ответственность сотрудников за утечку данных		2	2					2			
2	Киберугрозы		2	2					2			
2.1	Преднамеренные действия сотрудников, халатность, активность в сети интернет, внешние и внутренние угрозы		2	2					2			

3	Правила корпоративной и личной информационной безопасности		2	2				2			
3.1	Политика ИБ, Политика защиты данных, защита персональных и личных данных, правила безопасного поведения в сети Интернет		2	2				2			
4	Средства обеспечения информационной безопасности		2	2				2			
4.1	Сервисы и средства обеспечения ИБ, средства обеспечения безопасной работы в сети Интернет.		2	2				2			
5	Практический модуль (деловая игра)		34	20				20		14	
5.1	Цифровой след (активный, пассивный), управление цифровым следом. Цифровой профиль (личный и корпоративный)		6	4				4		2	
5.2	Пароли, аутентификация и приватные настройки (методы аутентификации, управление паролями, защита приватности и настройки конфиденциальности)		6	4				4		2	
5.3	Безопасность в сети (фишинг и его цели, практики безопасности для предотвращения фишинга, различные типы мошенничества и их профилактика)		6	4				4		2	
5.4	Безопасное хранение и распространение личных и коммерческих данных (осознанное использование социальных сетей, каналы передачи данных, категории получ		6	4				4		2	
5.5	Защита от вирусов и вредоносного ПО (типы вредоносного ПО, методы распространения, анализ угроз и техники защиты, план действий при поражении вредонос		6	4				4		2	
5.6	Проектирование безопасного цифрового профиля		4							4	
6	Цифровые проекты и психологическая безопасность в сети		44	28				28		16	

6.1	Цифровое гражданство (понятие, фильтрация информации, стратегии безопасного поведения)		4	4				4			
6.2	Создание электронного портфолио (особенности цифрового медиохранилища, особенности работы в Tilda, Wiki, Python, в других цифровых средах)		8	4				4		4	
6.3	Критическое мышление в интернете (гибкие навыки, формула 4К, аналитика информации в сети, размещение информации в интернете и интранете)		8	4				4		4	
6.4	Нетикет (понятие, правила виртуального общения, взаимодействие с подписчиками, достоверность информации, блоггинг)		8	4				4		4	
6.5	Профилактика кибербуллинга		4	4				4			
6.6	Ментальное здоровье и информационный детокс (понятие переизбытка информации, вербальное и невербальное интернет-общение, экстралингвистические особенн		4	4				4			
6.7	Искусственный интеллект в цифровых проектах		8	4				4		4	
7	Цифровая гигиена: правовые аспекты		12	12				12			
7.1	Использование информации и охраняемого контента		4	4				4			
7.2	Цифровые активы и виртуальная собственность		4	4				4			
7.3	Искусственны интеллект и нейронные сети		4	4				4			
	ВСЕГО		98	68				68		30	
ИА	Итоговая аттестация:										
1	Зачет		4	4				4			
	ИТОГО:	3	102	72				72		30	