ХАНТЫ-МАНСИЙСКИЙ АВТОНОМНЫЙ ОКРУГ – ЮГРА

АВТОНОМНОЕ УЧРЕЖДЕНИЕ ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА – ЮГРЫ «ЮГОРСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Директор

_____ А.В.Мельников

«____» _____ 2020 г.

Примерная учебная программа курса «Основы безопасной работы в сети Интернет»

Трудоемкость программы – 12 академических часов
Форма обучения – очная
Режим занятий – 6 дней по 2 академических часа
Начальные навыки: знание основ цифровой грамотности

Примерная учебная программа курса «Основы безопасной работы в сети Интернет» предназначена для обучения граждан навыкам безопасной работы с онлайн сервисами, защиты персональных данных и предупреждения угроз кибермошенничества.

Цель обучения: увеличение числа граждан, обладающих навыками и умениями обеспечения безопасной работы в сети Интернет.

Целевая аудитория: граждане городских округов и муниципальных районов автономного округа, уже имеющие знания основ цифровой грамотности из числа работников бюджетной сферы (образование, культура, здравоохранение); работников социальных служб; студентов образовательных организаций; молодых граждан в возрасте до 35 лет; граждан предпенсионного возраста; граждан, относящихся к льготным категориям (пенсионеры, представители коренных малочисленных народов Севера, люди с ограниченными возможностями здоровья, безработные, малообеспеченные и многодетные граждане).

УЧЕБНЫЙ ПЛАН

№ п/п	Наименование модулей	Всего часов	В том числе	
			Лекции	Практи-ческие занятия
1.	**Вводное занятие.** Общая концепция развития цифровой экономики. Цифровая грамотность граждан. О проекте «Цифровой гражданин Югры».	0,2	0,2	
2.	Модуль 1. Основы информационной безопасности и персонифицированной работы с коммуникационными сервисами	0,4	0,4	
3.	Модуль 2. Компьютерная и Интернет-безопасность	2,4	1,5	0,9
4.	Модуль 3. Навыки безопасной работы в сети Интернет и социальных сетях.	2,9	1	1,9
5.	Модуль 4. Меры предосторожности при проведении Интернет-транзакций.	2,3	0,7	1,6
6.	Модуль 5. Защита персональных данных	1	0,5	0,5
7.	Модуль 6. Кибербезопасность.	1,8	0,4	1,4
8.	Итоговое тестирование	1	-	1
9.	ИТОГО	**12**	**4,7**	**7,3**

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование модулей и тем	Всего часов	В том числе	
			Лекции	Практи-ческие занятия
	Вводное занятие Общая концепция развития цифровой экономики. Цифровая грамотность граждан. О проекте «Цифровой гражданин Югры».	**0,2**	**0,2**	
1.	**Модуль 1. Основы информационной безопасности и персонифицированной работы с коммуникационными сервисами**	**0,4**	**0,4**	
1.1.	Информационная среда. Политика информационной безопасности: доступность. целостность. конфиденциальность. Личное информационное пространство.	0,4	0,4	
2.	**Модуль 2. Компьютерная безопасность и Интернет-безопасность**	**2,4**	**1,5**	**0,9**
2.1.	Компьютерная безопасность. Виды компьютерных угроз. Возможные риски и предотвращение угроз. Актуальные интернет-угрозы	0,7	0,7	
2.2.	Обзор, установка, настройка антивирусных программ.	1,2	0,3	0,9
2.3	Классификация средств защиты. Защита от вредоносных программ и спама.	0,5	0,5	
3.	**Модуль 3. Навыки безопасной работы в сети Интернет**	**2,9**	**1**	**1,9**
3.1.	Безопасная работа с личным кабинетом. Регистрация в сетевом сервисе.	1,6	0,5	1,1
3.2	Интернет безопасность в социальных сетях. Какие материалы не стоит размещать у себя на странице. Этические нормы при размещении цифрового контента. Кибербуллинг.	0,9	0,4	0,5
3.3	Дети в интернете: правила поведения, компьютерные игры. Родительский контроль. Программа Kaspersky Safe Kids.	0,4	0,1	0,3
4.	**Модуль 4. Меры предосторожности при проведении Интернет-транзакций**	**2,3**	**0,7**	**1,6**
4.1.	Онлайн-платежи: основные понятия. Оплата услуг через интернет: правила безопасности. Новые способы онлайн платежей.	1,2	0,3	0,9

4.2.	Покупаем в интернете: как могут обмануть и на что обратить внимание. Банковские карты для покупок в интернете.	1,1	0,4	0,7
5.	**Модуль 5. Защита персональных данных**	**1**	**0,5**	**0,5**
5.1.	Что такое персональные данные. Как не допустить распространение персональных данных в интернете. Как работает закон о «праве на забвение». Личные данные, законодательство в сфере защиты личной информации и ответственность граждан по предоставлению личной информации, безопасность при оплате товаров и услуг.	1	0,5	0,5
6.	**Модуль 6. Кибербезопасность**	**1,8**	**0,4**	**1,4**
6.1.	Актуальные интернет-угрозы	0,9	0,2	0,7
6.2.	Социальная инженерия	0,9	0,2	0,7
7.	**Итоговое тестирование**	**1**	**-**	**1**
8.	**ИТОГО**	**12**	**4,7**	**7,3**

СОДЕРЖАНИЕ ПРОГРАММЫ

В начале освоения учебной программы проводится вводное занятие, посвященное теме развития цифровой экономики, необходимости освоения гражданами цифровой грамотности и правил безопасного использования интернета. Слушатели информируются о проекте «Цифровой гражданин Югры».

1. Модуль 1. Основы информационной безопасности и персонифицированной работы с коммуникационными сервисами

Понятия «информационная среда» в контексте информатизации общества, политика информационной безопасности. Противодействие идеологии терроризма в сети Интернет. Личное информационное пространство. Какие материалы не стоит размещать у себя на странице (соцсети). Безопасность финансовых операций.

2. Модуль 2. Компьютерная безопасность и Интернет-безопасность

Рассматриваются вопросы обеспечения компьютерной безопасности, в том числе при работе в сети Интернет. Понятие компьютерной безопасности и сопутствующие термины. Требования по безопасности операционной системы.

2.1. Виды компьютерных угроз. Возможные риски и предотвращение угроз.

Основные понятия.

2.2. Обзор, установка, настройка антивирусных программ. Поиск и загрузка дистрибутивов антивирусных программ, пробная установка, обновление антивирусных баз, сканирование компьютера.

2.3. Классификация средств защиты. Защита от вредоносных программ и спама.

3. Модуль 3. Навыки безопасной работы в сети Интернет и социальных сетях

Рассматриваются вопросы обеспечения безопасности при использовании личных кабинетов, социальных сетей. Особое внимание уделяется детской аудитории, как наименее защищенной от Интернет-угроз и мошенников.

3.1. Безопасная работа с личным кабинетом. Как придумать и запомнить безопасный пароль. Двухфакторная аутентификация. Как защититься от взлома аккаунта.

3.2. Интернет безопасность в социальных сетях. Культура общения, личная репутация. Правила оформления профилей в соцсетях, правила поведения. Этические нормы при размещении цифрового контента.

3.2. Дети в интернете: правила поведения, компьютерные игры. Что необходимо рассказать детям для их безопасной работы в Интернете. Программа родительского контроля Kaspersky Safe Kids.

4. Модуль 4. Меры предосторожности при проведении Интернет-транзакций

Слушатели знакомятся с правилами безопасной оплаты услуг и товаров в сети Интернет.

4.1. Онлайн-платежи: основные понятия. Оплата услуг через интернет: правила безопасности. Новые способы онлайн платежей. Расчёты через Сбербанк Онлайн и Мобильный банк Сбербанка. Единая биометрическая система. Как и зачем регистрировать биометрию.

4.2. Покупаем в интернете: как могут обмануть и на что обратить внимание. Банковские карты для покупок в интернете. Безопасность при переводе денег частному лицу; возможность отзыва или прекращения банковской транзакции.

5. Модуль 5. Защита персональных данных

Слушатели знакомятся с принципами защиты персональных данных.

5.1. Что такое персональные данные? Как не допустить распространение персональных данных в интернете. Законодательство в сфере защиты личной информации и ответственность граждан по предоставлению личной информации. Ситуации, в которых можно безопасно предоставлять персональные данные. Как работает закон о «праве на забвение».

6. Модуль 6. Кибербезопасность

Рассматриваются различные способы обмана в интернете и по мобильному телефону с целью вымогательства денег. Способы защиты от мошенников.

6.1. Актуальные интернет-угрозы. Как не стать жертвой интернет-мошенников. Инструменты интернет-мошенников. Программы вымогатели. Фишинг. Как могут обмануть при поиске работы в интернете. Куда обращаться, если столкнулись с мошенничеством в интернете.

6.2. Социальная инженерия. Методы несанкционированного доступа к информации или системам хранения информации без использования технических средств; обман людей путем выманивания у них конфиденциальной информации, необходимой для работы мошеннических схем. Мобильное мошенничество. Звонок с просьбой о помощи, неожиданный выигрыш, ошибочный платеж и другие способы вымогательства денег по телефону.

КАЛЕНДАРНО-ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Наименование разделов и тем	Учебные дни
1	Основы информационной безопасности и персонифицированной работы с коммуникационными сервисами	1
2	Компьютерная безопасность и Интернет-безопасность	1-2
3	Навыки безопасной работы в сети Интернет	2-3
4	Меры предосторожности при проведении Интернет-транзакций	4-5
5	Защита персональных данных	5
6	Защита от кибермошенничества	5-6
7	Итоговое тестирование (зачет)	6