ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ФОНД «ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ «ПЕРВОЕ СЕНТЯБРЯ»

**УТВЕРЖДАЮ**
Президент Образовательного учреждения
Фонда «Педагогический университет
«Первое сентября»


Соловейчик А.С.

«1» марта 2019 г.

**Рабочая программа курса повышения квалификации**

**«Основы информационной и кибербезопасности»**

**Автор:**
Шаповалов Михаил Иванович,
к.т.н., доцент МПГУ

Москва

2019 г.

**1. Цель реализации программы**

Научить слушателей безопасной работе в сети Интернет.

**2. Совершенствуемые компетенции**

**Развитие** ОП ИКТ 2 соблюдение этических и правовых норм использования ИКТ (в том числе недопустимость неавторизованного использования и навязывания информации).

**Формирование** ОП ИКТ 8 – соблюдение принципов и правил информационной и кибербезопасности в профессиональной деятельности.

**3. Планируемые результаты обучения**

**Знать:**

- основные угрозы при работе в интернете и средства борьбы с ними.

**Уметь:**

- предотвращать попытки вредоносного воздействия на компьютер.

**4. Категория обучающихся/слушателей:** уровень образования ВО, профиль подготовки «Педагогическое образование», область профессиональной деятельности – общее образование

**5. Обучение:** с применением дистанционных технологий

**6. Трудоемкость обучения:** 36 часов

**7. Учебный (тематический) план**

| № п/п | Наименование разделов (модулей) и тем | Всего час. | Лекции | Практические занятия | Самостоятельная работа | Форма контроля |
|---|---|---|---|---|---|---|
| 1 | **Тема 1. Комплексная безопасность в сети и инструменты ее обеспечения: образы поведения, методы** | | | | | |
| 1.1 | Информационная безопасность. Определения | 5 | 1 | 2 | 2 | |
| 1.2 | Методы защиты | 4 | 1 | 1 | 2 | |
| 1.3 | Настройки доступа и восстановление информации | 4 | 1 | 1 | 2 | |
| 1.4 | Основные виды сетевого мошенничества | 4 | 1 | 1 | 2 | |
| 2 | **Тема 2. Основы безопасности финансовых транзакций, средства информационной и** | | | | | |

| № п/п | Наименование разделов (модулей) и тем | Всего час. | Лекции | Практические занятия | Самостоятельная работа | Форма контроля |
|---|---|---|---|---|---|---|
| | **кибербезопасности** | | | | | |
| 2.1 | Правила безопасности при работе в сети | 5 | 1,5 | 2 | 1,5 | |
| 2.2 | Дополнительные возможности защиты | 4 | 1,5 | 1 | 1,5 | |
| 2.3 | Кибербезопасность – дополнительная информация | 3 | 1 | 1 | 1 | |
| 2.4 | Безопасность финансовых транзакций | 3 | 1 | 1 | 1 | |
| 2.5 | Безопасность ребенка | 3 | 1 | 1 | 1 | |
| 3 | Итоговый тест | 1 | | | 1 | Онлайн-тест |
| | **Итого** | **36** | 10 | **11** | 15 | |

**8. Формы аттестации и оценочные материалы**
**8.1. Промежуточный контроль.** Задания промежуточного контроля размещены в тексте курса.
**8.2. Итоговая аттестация**
**Форма:** онлайн-тестирование с мгновенной обратной связью.
**Оценка:** зачет/незачет

**Примерные задания:**

Какое из определений не является определением информационной безопасности?
Процесс разработки и использования антивирусных программ
Состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера
Процесс обеспечения доступности, целостности и конфиденциальности информации
Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации

Crack-элементы – это:
последовательности символов, воспринимаемые защитными системами программ в качестве реальных ключей для регистрации ПО
один или несколько файлов, с помощью которых trial-копия превращается в полнофункциональную
программы для преодоления защитного экрана
программы, разрушительно действующие на структуру информации компьютера

К методам защиты организационного характера не относятся:
резервная копия, в том числе в облаке
шифрование данных
регулярная очистка «корзины»
регулярная смена паролей

**9. Организационно-педагогические условия реализации программы**
**Учебно-методическое и информационное обеспечение программы**
**Список литературы:**

В. Д. Бирюков, Э. П. Теплов. Гуманитарные аспекты информационной безопасности: логические основы, методология и методика поиска истины и выявления манипуляций – СПб.: 2014. – 168 с.
Юрий Родичев. Нормативная база и стандарты в области информационной безопасности. Учебное пособие М. 2017 256 с.
Елена Баранова, Александр Бабаш. Информационная безопасность и защита. Учебное пособие 2017, 324 с.

**Интернет-источники:**

Безопасность детей в сети интернет http://school385.ru/bezopinternet/
Безопасность в интернете – информационная безопасность в сети интернет
https://womanadvice.ru/bezopasnost-v-internete-informacionnaya-bezopasnost-v-seti-internet
Безопасность в интернете https://yandex.ru/support/common/security/

**10. Материально-технические условия реализации программы**

Компьютер или ноутбук с программным обеспечением.
Свободный доступ в интернет.
– техническое обеспечение: ПК, локальная сеть, выход в Интернет;
– программное обеспечение: операционная система Microsoft Windows 7, пакет программ Microsoft Office 2010, браузер Google Chrome или Mozilla Firefox.