

Министерство образования Пензенской области
Государственное автономное профессиональное образовательное учреждение
Пензенской области «Пензенский колледж информационных и промышленных технологий
(ИТ-колледж)»



УТВЕРЖДАЮ

Директор ГАПОУ ПО ПКПТ

Н.В. Чистякова

« 12 » 09 2024 г.

**Дополнительная профессиональная программа
повышения квалификации
«Безопасное использование сети Интернет»**

г. Пенза, 2024 год

Организация – разработчик: ГАПОУ ПО «Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»

Разработчики: А.Ю. Солодовникова, преподаватель

Дополнительная профессиональная программа повышения квалификации «Безопасное использование сети Интернет» одобрена Методическим советом ГАПОУ ПО ПКПТ (ИТ-колледж)

Протокол № 2 от 12. 09. 2024 г.

Председатель Методического совета  Е.А. Волобуева
(подпись)

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1 Пояснительная записка: Дополнительная профессиональная программа повышения квалификации направлена на развитие профессиональных практикоориентированных компетенций в области безопасного использования сети Интернет.

1.2. Квалификационная характеристика

В результате изучения дисциплины слушатель должен уметь:

- использовать технологии для защиты личной информации и данных.
- обучать учеников методам идентификации и противодействия киберугрозам.
- проводить воспитательные мероприятия по вопросам интернет-безопасности.

В результате освоения программы слушатель должен знать:

- основные понятия и термины в области интернет-безопасности.
- структуру и функционирование современных угроз в киберпространстве.
- методики и средства контроля за безопасностью в сети.
- рекомендации по безопасному использованию интернет-ресурсов в образовательном

процессе.

1.3. Форма обучения: заочная.

1.4. Режим занятий: 16 часов.

Министерство образования Пензенской области
Государственное автономное профессиональное образовательное учреждение
Пензенской области «Пензенский колледж информационных и промышленных технологий
(ИТ-колледж)»

УТВЕРЖДАЮ
Директор ГАПОУ ПО ПКИПТ
Н.В. Чистякова
« 12 » 09 2024 г.



РАБОЧИЙ УЧЕБНЫЙ ПЛАН

**Дополнительная профессиональная программа
повышения квалификации
«Безопасное использование сети Интернет»**

Категория слушателей: лица, имеющие профессию преподавателя среднего профессионального образования.

Трудоемкость обучения: 16 академических часов.

Срок обучения: 4 недели.

Форма обучения: заочная.

№ п/п	Наименование учебных дисциплин	Формы аттестации			Учебная нагрузка слушателей, час.				
		Экзам ен	Заче т	Тестир ование	Мак- си- маль- ная	Са- мо- сто- ятел ьная ра- бота	Обязательная		
							Всего	в том числе	
								теоре- тиче- ское обуче- ние	лабора- торные и практи- ческие занятия
1	Раздел 1. Введение в интер- нет-безопасность				1		1	1	
2	Раздел 2. Основные киберугрозы и их последствия				1		1	1	
3	Раздел 3. Защита личных данных				2		2	2	
4	Раздел 4. Политики конфиденциальности и правила использования онлайн-сервисов				2		2	2	
5	Раздел 5. Безопасность мобильных устройств и приложений				2		2	2	
6	Раздел 6. Правила безопасного поведения в Интернете				2		2	2	
7	Раздел 7. Обзор современных технологий безопасности				2		2	2	
8	Раздел 8. Киберпреступность и правовая основа				2		2	2	
9	Итоговое тестирование			2	2		2		
8	Итого			2	16		16	14	

Согласовано:

Заместитель директора по работе с соц. партнерами

Председатель цикловой методической комиссии

 И. А. Бочкова
 Д. А. Ручкин

2. Дисциплинарное содержание программы

2.1 Тематический план дополнительной профессиональной программы повышения квалификации «Безопасное использование сети Интернет».

№ п/п	Наименование разделов и тем	Максимальная учебная нагрузка слушателя, час.	Количество аудиторных часов			Самостоятельная работа
			Всего	Практические занятия	Лабораторные занятия	
1	Раздел 1. Введение в интернет-безопасность	1	1			
2	Тема 1.1. Введение в интернет-безопасность	1	1			
3	Раздел 2. Основные киберугрозы и их последствия	2	2			
4	Тема 2.1. Основные киберугрозы. Последствия киберугроз	1	1			
6	Раздел 3. Защита личных данных	2	2			
7	Тема 3.1 Защита личных данных	2	2			
9	Раздел 4. Политики конфиденциальности и правила использования онлайн-сервисов	2	2			
10	Тема 4.1. Политики конфиденциальности	1	1			
11	Тема 4.2 Правила использования онлайн-сервисов	1	1			
12	Раздел 5. Безопасность мобильных устройств и приложений	3	3			
13	Тема 5.1. Безопасность мобильных устройств	1	1			
14	Тема 5.2. Безопасность мобильных приложений	1	1			
15	Раздел 6. Правила безопасного поведения в Интернете	2	2			
16	Тема 6.1. Правила безопасного поведения в интернете	2	2			
17	Раздел 7. Обзор современных технологий безопасности	2	2			
18	Тема 7.1. Современные технологии безопасности					
20	Раздел 8. Киберпреступность и правовая основа	2	2			
21	Тема 8.1. Киберпреступность	1	1			
22	Тема 8.2. Правовая основа и ответственность	1	1			
23	Итоговое тестирование	2	2			
24	Итого:	16	16			

2.2. Рабочая программа повышения квалификации «Безопасное использование сети интернет»

Раздел 1. Введение в интернет-безопасность

Тема 1.1. Введение в интернет-безопасность

Определение интернет-безопасности. Значение интернет-безопасности в современном мире. Роль пользователя в обеспечении безопасности. Основные инструменты и технологии для обеспечения интернет-безопасности. Обзор современных тенденций и вызовов в области интернет-безопасности

Раздел 2. Основные киберугрозы и их последствия

Тема 2.1. Основные киберугрозы

Введение в киберугрозы. Понятие и классификация киберугроз. Основные причины и факторы возникновения угроз.

Вредоносное ПО. Определение и виды вредоносного ПО. Примеры известных вирусов и их влияние на систему. Понятие фишинга и его разновидности. Примеры фишинговых атак и их последствия. Понятие социальной инженерии и её техники. Примеры успешных нападений через социальную инженерию. Способы защиты от атак социальной инженерии.

Финансовые последствия. Ущерб репутации. Правовые последствия. Операционные последствия. Социальные и психоэмоциональные последствия.

Раздел 3. Защита личных данных

Тема 3.1 Защита личных данных

Введение в понятие личных данных. Определение личных данных и их виды. Значение защиты личных данных в современном мире. Обзор основных законов и регуляций, касающихся защиты личных данных (GDPR, Закон РФ «О персональных данных», и др.). Ответственность организаций за нарушение защиты личных данных. Угрозы личным данным.

Методы защиты личных данных. Практические рекомендации по защите личных данных. Современные технологии и тренды в области защиты личных данных.

Раздел 4. Политики конфиденциальности и правила использования онлайн-сервисов

Тема 4.1. Политики конфиденциальности

Определение и цель политики конфиденциальности. Обязательные элементы политики конфиденциальности.

Как составить политику конфиденциальности: структура и содержание. Доступность и согласие пользователей на обработку данных. Изменения в политике конфиденциальности: уведомление пользователей.

Тема 4.2 Правила использования онлайн-сервисов

Введение в правила использования: что это такое и зачем нужно. Компоненты правил использования: права и обязанности пользователей. Условия доступа и использования онлайн-сервисов. Запреты и ограничительные меры: что нельзя делать на сервисах.

Примеры правил использования популярных онлайн-сервисов. Поддержание безопасности при использовании онлайн-сервисов: личная ответственность пользователей.

Раздел 5. Безопасность мобильных устройств и приложений

Тема 5.1. Безопасность мобильных устройств

Угрозы безопасности мобильных устройств. Обновление операционной системы и приложений. Парольная защита и биометрические методы. Шифрование данных на мобильных устройствах. Рекомендации по подключению к Wi-Fi сетям. Физическая безопасность мобильных устройств.

Тема 5.2. Безопасность мобильных приложений

Определение мобильных приложений. Важность безопасности. Угрозы для приложений. Защита данных пользователя. Безопасное кодирование. Права доступа приложений. Обновление приложений. Оценка безопасности перед установкой. Роль пользователя в безопасности.

Раздел 6. Правила безопасного поведения в Интернете

Тема 6.1. Правила безопасного поведения в Интернете

Основы интернет-безопасности: важность защиты личных данных. Создание надежных паролей: советы и рекомендации. Использование двухфакторной аутентификации: как это работает.

Осторожность при открытии электронных писем и ссылок: фишинг и мошенничество. Настройки конфиденциальности в социальных сетях: защита личной информации. Безопасное пользование общественными Wi-Fi сетями: риски и меры предосторожности. Защита устройств от вирусов и вредоносного ПО: антивирусные программы и обновления.

Раздел 7. Обзор современных технологий безопасности

Тема 7.1 Обзор современных технологий безопасности

Антивирусные решения. Обзор популярных антивирусных решений. Файрволы (межсетевые экраны). Основные функции фаерволов и их работа. Управление доступом и аутентификация. Облачные технологии и безопасность. Обучение и повышение осведомленности в области безопасности.

Раздел 8. Киберпреступность и правовая основа

Тема 8.1. Киберпреступность

Определение киберпреступности. Виды киберпреступлений: мошенничество, хакерство, кража данных. Методы и техники киберпреступников. Актуальные примеры киберпреступлений. Влияние киберпреступности на бизнес и общество. Обзор киберугроз и уязвимостей.

Тема 8.2 Правовая основа и ответственность

Основные законы и нормативные акты в области кибербезопасности. Ответственность за киберпреступления: уголовная и административная. Роль правоохранительных органов в выявлении и пресечении киберпреступлений. Этические и правовые аспекты использования информационных технологий.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

3.1. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по дополнительной общеобразовательной программе: лица, имеющие профессию преподавателя среднего профессионального образования.

3.2. Требования к минимальному материально-техническому обеспечению

Реализация дополнительной профессиональной программы повышения квалификации требует наличия у слушателя следующего оборудования: персональный компьютер (ноутбук / смартфон) с выходом в сеть Интернет.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

Контроль и оценка результатов освоения программы осуществляется преподавателем в виде итогового тестирования.

Необходимо осуществить перевод полученного количества верных ответов на вопросы теста в оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Перевод ответов в оценку осуществляется в соответствии с таблицей:

Оценка	«2»	«3»	«4»	«5»
Количество верных ответов в рамках тестирования к максимально возможному, %	0 – 19,99%	20 – 39,99%	40 – 69,99%	70 – 100%