**Муниципальное бюджетное учреждение дополнительного образования «Центр детского научного и инженерно-технического творчества» города Невинномысска**

| | |
|---|---|
| СОГЛАСОВАНО | УТВЕРЖДАЮ |
| Педагогическим советом | Директор |
| Протокол № ____ | _____Т.В. Чилхачоян |
| от «__» _____ 2025 г. | «____»_____2025 г |

# Дополнительная общеобразовательная программа технической направленности

## Информационная безопасность и искусственный интеллект

7-8 класс
Срок реализации программы – 2 года

Авторы-составители:
Бенескул А.В., педагог
Гонголь А.Е., педагог
Фоменко О.Н., педагог
Завялик О.П., педагог

Невинномысск, 2025

СОДЕРЖАНИЕ

# 1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Дополнительная общеобразовательная программа технической направленности «Информационная безопасность и искусственный интеллект» (далее – программа) имеет базовый уровень и предназначается для обучающихся/воспитанников 7-8 классов образовательных центров Фонда Мельниченко.

**Актуальность программы** обусловлена требованиями современного общества к формированию системы работы с одаренными детьми в условиях дополнительного образования.

Программа разработана на основе следующих документов:

– закон Российской Федерации «Об образовании» (Федеральный закон от 29 декабря 2012 г. № 273-ФЗ);

– приказ Министерства просвещения РФ от 9 ноября 2018 г. № 196 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

– концепция развития дополнительного образования детей (Распоряжение Правительства РФ от 31 марта 2022 г. №678-р);

– постановление Главного государственного санитарного врача от 28.09.2020 г. № 28 «Об утверждении санитарных правил СП 2.4.3648–20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодёжи»;

– постановление Главного государственного санитарного врача от 28.01.2021 г. № 2 «Об утверждении санитарных правил СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания».

**Педагогическая целесообразность программы** обуславливается стимулированием интересов учащихся к дисциплинам технического направления, экспериментальным исследованиям, проектной деятельности и состоит в обеспечении адаптации школьников к жизни в обществе, профессиональной ориентации, а также в выявлении и поддержке учащихся, проявивших выдающиеся способности.

Программа может быть реализована с помощью дистанционных технологий, технологий смешанного и модульного обучения.

**Цель программы** – изучение программирования и технологий анализа данных с целью дальнейшего профессионального самоопределения учащихся.

**Задачи программы:**

– обеспечить получение навыков реализации алгоритмов в различных средах программирования;

– получить навыки реализации и применения алгоритмов по обеспечению информационной безопасности;

– сформировать и развить навыки реализации и применения алгоритмов интеллектуального анализа данных;

**Определение объема, содержания и планируемых результатов программы** осуществлялось для одаренных в области технических наук

учащихся, то есть имеющих высокий умственный потенциал, способности для достижений и деятельности и высокий уровень мотивации.

**Срок реализации программы** – 2 года.

**Общий объём** – 128 часов.

Продолжительность учебного года – 32 недели.

**Формы и режим занятий**

Занятия проводятся по 2 часа в неделю в постоянных группах учащихся 7 - 8 классов, сформированных по возрастному признаку из учащихся, прошедших конкурсный отбор (оптимальное количество участников в группе: 10 – 15 человек).

Основные формы работы – работа на компьютере, решение практических задач, индивидуальное проектирование, реализация алгоритмов в средах программирования.

Практико-ориентированная часть программы реализуется за счет проведения практических работ. Учитель самостоятельно распределяет часы на практические работы в зависимости от особенностей класса.

**Ожидаемые результаты программы**

К ожидаемым результатам реализации программы можно отнести формирование и развитие следующих необходимых навыков и умений:

- формирование навыков решения нестандартных задач;
- развитие навыков применения основных алгоритмических конструкций; навыков разработки программ в различных средах программирования; навыков использования современных информационно-коммуникационных технологий, навыков реализации и применения алгоритмов интеллектуального анализа данных.

**Результаты освоения программы** определяются с использованием 5-ти балльной (баллы от 1 до 5) системы оценивания.

**Контроль освоения программы** – текущий, промежуточный и итоговый.

Текущий контроль осуществляется на занятиях (ответы у доски, письменные работы, практические работы и устные ответы, домашние задания); после изучения блока или набора взаимосвязанных блоков (выделенных ведущим преподавателем) защита практической работы или письменный и/ или устный опрос.

Промежуточный контроль проводится в соответствии с учебно-тематическим планом после освоения темы или набора взаимосвязанных тем в форме контрольной работы, содержащей устную и практическую часть, или защиты практической работы.

Итоговый контроль – в форме экзамена после каждого года обучения, включающего в себя теоретическую и практическую части или защиту учебного творческого проекта (см. Приложение А). Программой не предусмотрено использование тестов для итогового контроля.

# 2 УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ

## УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН 7 КЛАССА

**7 класс [64 часа, 2 часа в неделю]**

| | Наименование тем и блоков | Общее количество учебных часов | Теоретические часы | Практические часы |
|---|---|---|---|---|
| **Тема 1** | **Основы информационной безопасности** | **12** | | |
| Блок 1 | Основные понятия, цели и задачи информационной безопасности | 2 | 2 | 0 |
| Блок 2 | Классификация объектов защиты | 4 | 2 | 2 |
| Блок 3 | Модель угроз и модель нарушителя | 4 | 2 | 2 |
| **Контрольная работа по теме 1** | | **2** | | |
| **Тема 2** | **Введение в методы защиты информации** | **16** | | |
| Блок 1 | Классификация компьютерных атак и методы защиты | 8 | 4 | 4 |
| Блок 2 | Социальная инженерия | 6 | 4 | 2 |
| **Контрольная работа по теме 2** | | **2** | | |
| **Тема 3** | **Введение в интеллектуальные алгоритмы** | **34** | | |
| Блок 1 | Искусственный нейрон. Многослойные нейронные сети | 16 | 4 | 12 |
| Блок 2 | Обучение нейронной сети | 16 | 4 | 12 |
| **Контрольная работа по теме 3** | | **2** | | |
| **Итоговая контрольная работа** | | **2** | | |
| **Резервные часы** | | **0** | | |
| **Всего** | | **64** | **22** | **34** |

## Содержание программы 7 класс

## ТЕМА 1. Основы информационной безопасности (ИБ)

**Блок 1. Основные понятия цели и задачи ИБ.**

Общее введение в ИБ. Понятия информации, ИБ, информационной системы, объекта информатизации и др. Основные три составляющие ИБ: целостность, доступность, конфиденциальность.

**Блок 2. Классификация объектов защиты.**

Информационная система персональных данных (ИСПДн). Государственная информационная система (ГИС). Критическая информационная инфраструктура (КИИ). Автоматизированная система управления технологическим процессом (АСУ ТП).

**Блок 3. Модель угроз и модель нарушителя.**

Возможные негативные последствия от реализации угроз, возможные объекты воздействия угроз безопасности информации, источники угроз и способы реализации. Методический документ ФСТЭК от 5 февраля 2021 г. «Методика оценки угроз безопасности информации».

**ПРАКТИЧЕСКАЯ ЧАСТЬ:**

**Практическая работа №1.** Анализ инцидента ИБ.

**Практическая работа №2.** Разработка матрицы целей и задач ИБ для организации.

**Практическая работа №3.** Реализация простого инструмента для проверки целостности файлов.

**Практическая работа №4.** Определение категории ИСПДн и требований к защите.

**Практическая работа №5.** Анализ соответствия информационной системы требованиям безопасности.

**Практическая работа №6.** Разработка скрипта для автоматической проверки соответствия парольной политики требованиям безопасности.

**Практическая работа №7.** Разработка модели угроз безопасности информации.

**Практическая работа №8.** Разработка модели нарушителя.

**Практическая работа №9.** Реализация простого инструмента для анализа лог-файлов на предмет аномальной активности.

**Контрольная работа по теме 1.**

## ТЕМА 2. Введение в методы защиты информации

**Блок 1. Классификация компьютерных атак и методы защиты.**

Классификация атак на информационную систему и сети; методы защиты.

**Блок 2. Социальная инженерия.**

Понятие и классификация; распространенные примеры; методы защиты.

**ПРАКТИЧЕСКАЯ ЧАСТЬ:**

**Практическая работа №1.** Анализ кейсов компьютерных атак.

**Практическая работа №2.** Разработка матрицы соответствия атак и методов защиты.
**Практическая работа №3.** Моделирование атаки и защиты в виртуальной среде.
**Практическая работа №4.** Разработка сценариев социальной инженерии.
**Практическая работа №5.** Ролевая игра «Атака социальной инженерии».
**Практическая работа №6.** Разработка обучающих материалов по защите от социальной инженерии.
**Контрольная работа по теме 2.**

## ТЕМА 3. Введение в интеллектуальные алгоритмы

**Блок 1. Искусственный нейрон. Многослойные нейронные сети**
Знакомство с биологическими нейронными сетями. Введение в искусственные нейронные сети. Искусственный нейрон. Однослойный персептрон Розенблатта.
**Блок 2. Обучение нейронной сети**
Обучение искусственной нейронной сети. Методы обучения нейронной сети. Обучение нейронной сети с учителем и без учителя. Понятия обучающая выборка и контрольная выборка.
**ПРАКТИЧЕСКАЯ ЧАСТЬ:**
**Практическая работа №1.** Создание искусственного нейрона.
**Практическая работа №2-4.** Создание входного, выходного, скрытого слоя нейронов.
**Практическая работа №4-6.** Реализация многослойного персептрона.
**Практическая работа №9-11.** Реализация обучения классическим методом.
**Практическая работа №10-12.** Реализация обучения стохастическим методом.
**Практическая работа №13-14.** Обучение нейронной сети. Решение задачи классификации «Ирисы Фишера»

**Контрольная работа по теме 3.**

**Итоговая контрольная работа**

## УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН 8 КЛАССА

## 8 класс [64 часа, 2 часа в неделю]

| № | Наименование тем и блоков | Общее количество учебных часов | Теоретические часы | Практические часы |
|---|---|---|---|---|
| **Тема 1** | **Криптография** | **34** | | |
| Блок 1 | Основы криптоанализа | 16 | 8 | 8 |
| Блок 2 | Функции хэширования и электронная подпись | 8 | 4 | 4 |
| Блок 3 | Стеганография | 8 | 4 | 4 |
| **Контрольная работа по теме 1** | | **2** | | |
| **Тема 2** | **Анализ данных при помощи искусственных нейронных сетей** | **26** | | |
| Блок 1 | Архитектуры нейронных сетей | 10 | 2 | 8 |
| Блок 2 | Обучение и анализ результатов работы нейронной сети | 14 | 4 | 10 |
| **Контрольная работа по теме 2** | | **2** | | |
| **Итоговая контрольная работа** | | **2** | | |
| **Резервные часы** | | **2** | | |
| **Всего** | | **64** | **22** | **34** |

## Содержание программы 8 класс

## ТЕМА 1. Криптография

**Блок 1. Основы криптоанализа.**

Основные понятия криптографии; шифры замены и шифры перестановки; основы криптоанализа, частотные характеристики текста.

**Блок 2. Абсолютные стойкие шифры, функции хэширования и ЭЦП (электронная цифровая подпись).**

Понятие абсолютно стойких шифров; алгоритмы хэширования; виды ЭЦП, принцип действия ЭЦП.

**Блок 3. Стеганография.**

Основные понятия; исторические примеры; использование стеганографии в современном мире.

**ПРАКТИЧЕСКАЯ ЧАСТЬ:**

**Практическая работа №1.** Криптоанализ шифра Цезаря.

**Практическая работа №2.** Частотный анализ текста и взлом простого шифра замены.

**Практическая работа №3.** Реализация шифров перестановки.

**Практическая работа №4.** Шифр Вернама (одноразовый блокнот).

**Практическая работа №5.** Практическое использование функций хэширования.

**Практическая работа №6.** Имитация работы ЭЦП (без использования криптографических библиотек).

**Практическая работа №7.** Сокрытие информации в изображении (LSB-метод).

**Практическая работа №8.** Анализ стеганографических инструментов.

**Практическая работа №9.** Обнаружение стеганографических сообщений.

**Контрольная работа по теме 1.**

## ТЕМА 2. Анализ данных при помощи искусственных нейронных сетей

**Блок 1. Архитектуры нейронных сетей**

Введение в нейронные сети, основные понятия (нейрон, слой, веса, смещение, функция активации). Типы нейронных сетей (полносвязные нейронные сети (Multilayer Perceptron, MLP), сверточные нейронные сети (Convolutional Neural Networks, CNN), рекуррентные нейронные сети (Recurrent Neural Networks, RNN), LSTM и GRU сети). Функции активации (Сигмоида, ReLU, Tanh, Softmax) и их свойства. Выбор архитектуры нейронной сети: Факторы, влияющие на выбор архитектуры, эвристики.

**Блок 2. Обучение и анализ результатов работы нейронной сети**

Функции потерь (Loss functions) (MSE, Cross-entropy). Методы оптимизации (градиентный спуск, стохастический градиентный спуск (SGD), Adam, RMSprop). Регуляризация (L1 и L2 регуляризация, dropout). Оценка качества модели (Метрики классификации (accuracy, precision, recall, F1-score), метрики

регрессии (MSE, MAE, R-squared)). Визуализация результатов обучения (Графики потерь, confusion matrix, ROC-кривая). Переобучение и недообучение, причины, методы диагностики и борьбы.

**ПРАКТИЧЕСКАЯ ЧАСТЬ:**

**Практическая работа №1.** Реализация полносвязной нейронной сети с использованием NumPy.

**Практическая работа №2.** Классификация изображений с использованием сверточной нейронной сети (CNN) и TensorFlow/Keras.

**Практическая работа №3.** Анализ тональности текста с использованием рекуррентной нейронной сети (RNN) и PyTorch.

**Практическая работа №4.** Сравнение различных методов оптимизации на задаче классификации.

**Практическая работа №5.** Применение регуляризации для предотвращения переобучения.

**Контрольная работа по теме 2.**

**Итоговая контрольная работа**

# 3 ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Занятия проводятся по 2 часа в неделю в постоянных группах учащихся 7-8 классов, сформированных по возрастному признаку из учащихся, прошедших конкурсный отбор (оптимальное количество участников в группе: 10–15 человек), в форме теоретических, практических и индивидуальных занятий, а также консультаций (проектная деятельность, подготовка к олимпиадам, конференциям).

Основные формы работы – работа на компьютере, решение практических задач, индивидуальное проектирование, реализация алгоритмов в средах программирования.

Практико-ориентированная часть программы реализуется за счет проведения практических работ. Учитель самостоятельно распределяет часы на практические работы в зависимости от особенностей класса.

Ожидаемые результаты программы определяются с использованием пятибалльной системы оценивания (баллы от 1 до 5).

## Методическое обеспечение программы

## Методические рекомендации по технике безопасности в компьютерном классе

К работе в компьютерном классе допускаются учащиеся, прошедшие инструктаж по технике безопасности и электробезопасности с соответствующей записью в журнале по технике безопасности и подписями.

Не разрешается заходить в компьютерный класс и находиться в нём без преподавателя.

Работа в компьютерном классе должна проходить только в строгом соответствии с расписанием занятий и графиком самостоятельной работы преподавателей и учащихся.

Учащимся запрещается открывать шкафы питания как при работающих, так и при выключенных ЭВМ.

Необходимо сидеть на рабочем месте так, чтобы линия глаз приходилась на центр экрана, чтобы, не наклоняясь, пользоваться клавиатурой и воспринимать передаваемую на экран монитора информацию.

Начинать работу можно только по указанию преподавателя.

По окончании работы о недостатках и неисправностях, обнаруженных во время работы, необходимо сделать записи в соответствующих журналах.

После окончания работы на рабочем месте не должно оставаться лишних предметов.

# 4 СПИСОК ЛИТЕРАТУРЫ

## Основная литература


1. Буэно Гарсия, Г. Обработка изображений с помощью OpenCV [Текст] / Г. Буэно Гарсия, О. Дениз Суарес, Х. Салидо Терсеро, И. Серрано Грасиа, Н. Валлез Энано [пер. с англ. Слинкин А. А]. – М.: ДМК Пресс, 2016. – 210 с.
2. Васильев, А. Н. Python на примерах. Практический курс по программированию [Текст] / А.Н. Васильев. – СПб.: Наука и техника, 2016. – 432 с.
3. Коэльо, Л. П. Построение систем машинного обучения на языке Python [Текст] / Луне Педро Коэльо, Вилли Ричарт : пер. с англ. Слинкин А. А. - М. : ДМК Пресс, 2016. – 302с.
4. Красильников, Н. Н. Цифровая обработка 2D- и 3D-изображений [Текст]: учебное пособие / Н. Н. Красильников. – СПб.: БХВ-Петербург, 2011. – 608 с.
5. МакГрат, Майк. Программирование на Python для начинающих [Текст] / Майк МакГрат; [пер. с англ. М.А. Райтмана]. – Москва: ЭКСМО, 2015. – 194 с.
6. Новиков, Б. А. Основы технологий баз данных [Текст]: учебное пособие / Б. А. Новиков, Е. А. Горшкова. – М.: ДМК Пресс, 2019. – 240 с.
7. Прохоренок, Н. А. OpenCV и Java. Обработка изображений и компьютерное зрение [Текст] / Н. А. Прохоренок. – СПб.: БХВ-Петербург, 2018. – 320 с.
8. Рашка, С. Python и машинное обучение [Текст] / С. Рашка: пер. с англ. А. В. Логунова. – М.: ДМК Пресс, 2017. – 418 с.
9. Старовойтов, В. В. Получение и обработка изображений на ЭВМ [Текст]: учебно-методическое пособие / В.В. Старовойтов, Ю.И. Голуб. – Минск.: БНТУ, 2018. – 204 с.
10. Стасышин, В. М. Базы данных, технологии доступа [Текст]: учеб. пособие для СПО / В.М. Стасышин, Т.Л. Стасышина. – 2-е изд., испр и доп. – М.: Издательство Юрайт, 2019 — 164 с.
11. Федоров, Д. Ю. Основы программирования на примере языка Python [Текст]: учебное пособие / Д.Ю. Федоров. – М.: Издательство Юрайт, 2017 — 126 с.
12. Коршунов, Н.М. Право интеллектуальной собственности / Н.М. Коршунов, Н.Д. Эриашвили, В.И. Липунов и др.; ред. Н.Д. Эриашвили; под ред. Н.М. Коршунова. – М. Юнити-Дана, 2015. – 327 с.
13. Кузнецов, И.Н. Основы научных исследований / И.Н. Кузнецов. – М.: Издательско-торговая корпорация «Дашков и К°», 2017. – 283 с.
14. Ларионов, И.К. Защита интеллектуальной собственности / И.К. Ларионов, М.А. Гуреева, В.В. Овчинников и др.; под ред. И.К. Ларионова, М.А. Гуреевой, В.В. Овчинникова. – М.: Издательско-торговая корпорация «Дашков и К°», 2018. – 256 с.
15. Нишант, Ш. Машинное обучение и TensorFlow [Текст] / Шакла Нишант. - Спб.: Питер, 2019. – 336 с.

## Дополнительная литература


1. Авшарян, Г. Слепая печать и горячие клавиши [Текст] / Г. Авшарян. – М.: НТ Пресс, 2008. – 128 с.
2. Ахмедханлы, Д. М. Основы алгоритмизации и программирования [Текст]: учеб.-метод. пособие / Д.М. Ахмедханлы, Н.В. Ушмаева. – Тольятти.: Изд-во ТГУ, 2016. – 123 с.
3. Кормен, Т. Алгоритмы: построение и анализ [Текст] / Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штейн; пер. с англ.; 3-е изд. – Москва: ООО "И.Д. "Вильямс", 2013. – 1328 с.
4. Кувшинов, Д. Р. Основы программирования [Текст]: учебное пособие для СПО / Д.Р. Кувшинов. – Екатеринбург.: Изд-во Урал. Ун-та, 2019. – 105 с.
5. Никулин, Е. А. Компьютерная геометрия и алгоритмы машинной графики [Текст] / Е.А. Никулин. – Спб. : БХВ-Петербург, 2003. – 60 с.
6. Окулов. С. М. Алгоритмы обработки строк: учебное пособие [Текст] / С. М. Окулов. – М.: БИНОМ. Лаборатория знаний, 2009. – 255 с.
7. Окулов, С. М. Динамическое программирование [Текст] / С.М. Окулов, О.А. Пестов. – М.: БИНОМ. Лаборатория знаний, 2012. –296 с.
8. Окулов, С. М. Алгоритмы компьютерной арифметики [Текст] / С.М. Окулов, А.В. Лялин, О.А. Пестов, Е.В. Разова. – М.: БИНОМ. Лаборатория знаний, 2014. – 285 с.
9. Поляков, К. Ю. Информатика. 7 класс: в 2 ч. Ч. 1 [Текст] / К.Ю. Поляков, Е.А. Еремин.– М.: БИНОМ. Лаборатория знаний, 2017. – 160 с.
10. Поляков, К. Ю. Информатика. 7 класс: в 2 ч. Ч. 2 [Текст] / К.Ю. Поляков, Е.А. Еремин.– М.: БИНОМ. Лаборатория знаний, 2017. – 160 с.
11. Поляков, К. Ю. Информатика. 8 класс [Текст] / К.Ю. Поляков, Е.А. Еремин. – М.: БИНОМ. Лаборатория знаний, 2017. – 256 с.
12. Поляков, К. Ю. Информатика. 9 класс [Текст] / К.Ю. Поляков, Е.А. Еремин. – М.: БИНОМ. Лаборатория знаний, 2017. – 256 с.
13. Поляков, К. Ю. Информатика. Углубленный уровень [Текст]: учебник для 10 класса: в 2-х ч. Ч. 1 / К.Ю. Поляков, Е.А. Еремин. – М.: БИНОМ. Лаборатория знаний, 2013. – 334 с.
14. Поляков, К. Ю. Информатика. Углубленный уровень [Текст]: учебник для 10 класса: в 2-х ч. Ч. 2 / К.Ю. Поляков, Е.А. Еремин. – М.: БИНОМ. Лаборатория знаний, 2013. – 304 с.
15. Поляков, К. Ю. Информатика. Углубленный уровень [Текст]: учебник для 11 класса: в 2-х ч. Ч. 1 / К.Ю. Поляков, Е.А. Еремин. – М.: БИНОМ. Лаборатория знаний, 2013. – 240с.
16. Поляков, К. Ю. Информатика. Углубленный уровень [Текст]: учебник для 11 класса: в 2-х ч. Ч. 2 / К.Ю. Поляков, Е.А. Еремин. – М.: БИНОМ. Лаборатория знаний, 2013. – 304с.
17. Поляков, К. Ю. Программирование. Python. C++. Часть 1 [Текст]: Учебное пособие / К.Ю. Поляков. – М.: БИНОМ. Лаборатория знаний, 2019. – 144 с.

18. Поляков, К. Ю. Программирование. Python. C++. Часть 2 [Текст]: Учебное пособие / К.Ю. Поляков. – М.: БИНОМ. Лаборатория знаний, 2019. – 176 с.

19. Сакулин, В. А. Информатика. Технология работы с табличными данными [Текст]: учеб.-методич. пособие / В.А.Сакулин, Ю.В. Сакулина. – М.: ЮНИТИ–ДАНА, 2019. – 335 с.

20. Столяр, С. Е. Информатика. Представление данных и алгоритмы [Текст] / С.Е. Столяр, А.А. Владыкин. – М.: БИНОМ. Лаборатория знаний, 2007. – 382 с.

21. Трофимов, В. В. Основы алгоритмизации и программирования [Текст]: учебник для СПО / В. В. Трофимов, Т. А. Павловская. – М.: Издательство Юрайт, 2019 — 137 с.

22. Цветкова, М. С. Культура клавиатурного письма [Текст]: методическое пособие. М.С. Цветкова, О.Б. Богомолова. – М.: БИНОМ. Лаборатория знаний, 2009. – 171 с.

23. Шульгин, В. П. Создание эффектных презентаций с использованием PowerPoint 2013 и других программ [Текст] / В.П. Шульгин, М.В. Финков, Р.Г. Прокди. – Спб.: Наука и техника, 2015. – 256 с.

# 5 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

## Примеры вопросов для проведения промежуточного контроля в 7 классе

### ТЕМА 1. Основы информационной безопасности

1. Что такое информация в контексте информационной безопасности? Опишите ее ключевые атрибуты (конфиденциальность, целостность, доступность).
2. Сформулируйте определения понятий: информационная безопасность, информационная система, объект информатизации. Приведите примеры.
3. В чем заключаются основные цели и задачи информационной безопасности? Проиллюстрируйте примерами.
4. Как связаны между собой понятия «информационная безопасность» и «кибербезопасность»?
5. Какие основные риски связаны с нарушением конфиденциальности, целостности и доступности информации?
6. Перечислите основные классы объектов защиты в соответствии с законодательством (например, ИСПДн, ГИС, КИИ, АСУ ТП).
7. В чем состоят основные особенности защиты информации в ИСПДн? Какие нормативные акты регулируют эту область?
8. Какие требования предъявляются к защите информации в государственных информационных системах (ГИС)?
9. Что такое критическая информационная инфраструктура (КИИ)? Какие объекты относятся к КИИ?
10. Какие особенности имеет защита автоматизированных систем управления технологическими процессами (АСУ ТП)?
11. Опишите основные элементы модели угроз безопасности информации.
12. Что такое уязвимость? Как она связана с угрозой?
13. Перечислите возможные источники угроз информационной безопасности. Приведите примеры.
14. Какие способы реализации угроз вы знаете? Проиллюстрируйте примерами.
15. Что такое модель нарушителя? Какие факторы учитываются при ее построении?
16. Как связаны модель угроз и модель нарушителя? Зачем они нужны?
17. Опишите возможные последствия реализации угроз безопасности информации для организации.

### ТЕМА 2. Введение в методы защиты информации

1. Опишите основные классы компьютерных атак: (например, вредоносное ПО, сетевые атаки, атаки на веб-приложения, атаки на отказ в обслуживании).

2. Какие методы защиты используются для противодействия вредоносному программному обеспечению?

3. Что такое межсетевой экран (firewall)? Какие типы межсетевых экранов вы знаете?

4. Опишите основные методы защиты от сетевых атак (например, DoS/DDoS, MITM).

5. Какие уязвимости веб-приложений являются наиболее распространенными? Как от них защититься (например, SQL-инъекции, XSS)?

6. Что такое криптографические методы защиты информации? В чем разница между симметричным и асимметричным шифрованием?

7. Какие методы контроля доступа используются для защиты информации?

8. Что такое социальная инженерия? Опишите основные принципы, на которых она основана.

9. Перечислите основные типы атак социальной инженерии (например, фишинг, претекстинг, кво про кво).

10. Приведите примеры атак социальной инженерии.

11. Какие методы защиты от социальной инженерии вы знаете? Как повысить осведомленность пользователей о рисках социальной инженерии?

12. Почему социальная инженерия является эффективным методом атак?

13. Какие организационные меры необходимо предпринять для защиты от социальной инженерии?

**ТЕМА 3. Введение в интеллектуальные алгоритмы**

1. Что такое искусственный нейрон? Опишите его основные элементы (входы, веса, функция активации, выход).

2. Какие типы функций активации вы знаете? (сигмоида, ReLU, tanh) В чем их особенности и недостатки?

3. Что такое многослойная нейронная сеть (MLP)? Какова ее архитектура?

4. Объясните принцип работы прямого распространения (forward propagation) в нейронной сети.

5. Какие преимущества и недостатки имеют многослойные нейронные сети?

6. Чем отличаются полносвязные нейронные сети от сверточных и рекуррентных?

7. Что такое обучение нейронной сети? Какие основные этапы включает этот процесс?

8. Что такое функция потерь (loss function)? Приведите примеры.

9. Объясните принцип работы обратного распространения (backpropagation) в нейронной сети.

10. Что такое градиентный спуск (gradient descent)? Как он используется для обучения нейронных сетей?

11. Какие методы оптимизации вы знаете? (SGD, Adam, RMSprop) В чем их особенности?

12. Что такое переобучение (overfitting) и недообучение (underfitting)? Как с ними бороться?

13. Что такое регуляризация? Какие типы регуляризации вы знаете? (L1, L2, dropout)

14. Как оценить качество работы обученной нейронной сети? Какие метрики используются для этого?

## Примеры билетов для проведения итогового контроля в 7 классе

**Билет №1**

1. Дайте определения понятий «информация», «информационная безопасность», «угроза безопасности информации", «уязвимость». Приведите примеры.

2. Опишите основные классы компьютерных атак (например, вредоносное ПО, сетевые атаки, атаки на веб-приложения). Для каждого класса приведите примеры конкретных атак и методов защиты от них.

3. Что такое социальная инженерия? Опишите основные типы атак социальной инженерии и приведите примеры. Какие методы защиты от социальной инженерии вы можете предложить?

4. Объясните разницу между симметричным и асимметричным шифрованием. Приведите примеры алгоритмов симметричного и асимметричного шифрования.

5. Опишите структуру искусственного нейрона. Какие основные элементы входят в его состав? Какова роль функции активации?

**Билет №2**

1. В чем заключаются основные цели и задачи информационной безопасности? Проиллюстрируйте примерами.

2. Какие объекты защиты выделяют в соответствии с законодательством (например, ИСПДн, ГИС, КИИ, АСУ ТП)? Опишите основные особенности защиты информации для каждого типа объектов.

3. Что такое межсетевой экран (firewall)? Какие функции он выполняет? Какие типы межсетевых экранов вы знаете?

4. Предложите реалистичный сценарий атаки социальной инженерии, направленной на получение конфиденциальной информации от сотрудника компании. Опишите шаги, которые предпримет злоумышленник, и методы, которые он будет использовать.

5. Опишите процесс обучения нейронной сети. Что такое функция потерь (loss function)? Что такое градиентный спуск?

**Билет №3**

1. Опишите основные элементы модели угроз безопасности информации. Что такое модель нарушителя? Как связаны эти две модели?

2. Что такое криптографическая хеш-функция? Какими свойствами она должна обладать? Приведите примеры алгоритмов хеширования.

3. Что такое стеганография? В чем ее отличие от криптографии? Приведите примеры методов стеганографии.

4. Какие основные методы защиты от сетевых атак (например, DoS/DDoS, MITM) вы знаете? Опишите их.

5. Опишите архитектуру многослойной нейронной сети (MLP). Как работает прямой проход (forward pass)?

**Билет №4**

1. Какие основные законодательные и нормативные акты регулируют вопросы информационной безопасности?

2. Объясните разницу между аутентификацией и авторизацией. Какие методы аутентификации вы знаете?

3. Какие основные уязвимости веб-приложений вы знаете? (например, SQL-инъекции, XSS, CSRF). Опишите методы защиты от этих уязвимостей.

4. Перечислите и кратко опишите основные типы нейронных сетей (полносвязные, сверточные, рекуррентные). В каких задачах применяется каждый из них?

5. Что такое переобучение (overfitting) нейронной сети? Как с ним бороться? Опишите методы регуляризации.

## Примеры вопросов для проведения промежуточного контроля в 8 классе

**ТЕМА 1. Криптография**

1. Определите понятия «криптография», «криптология», «криптоанализ». В чем их взаимосвязь?
2. Что такое шифр замены? Приведите примеры известных шифров замены (например, шифр Цезаря, шифр Атбаш).
3. Что такое шифр перестановки? Приведите примеры.
4. Опишите основные методы криптоанализа.
5. Что такое частотный анализ? Как он используется для взлома шифров замены?
6. Какие факторы влияют на стойкость шифра к криптоанализу?
7. В чем заключаются недостатки классических шифров замены и перестановки?
8. Что такое функция хэширования? Какими свойствами она должна обладать? (Односторонность, стойкость к коллизиям, детерминированность).
9. Приведите примеры известных алгоритмов хэширования (например, MD5, SHA-256).
10. Что такое электронная подпись (ЭП)? Какова ее роль?
11. Опишите основные типы электронных подписей.
12. Как работает процесс создания и проверки электронной подписи?
13. Что такое сертификат открытого ключа? Зачем он нужен?
14. В чем разница между электронной подписью и электронной цифровой подписью?
15. Что такое стеганография? В чем ее отличие от криптографии?
16. Опишите основные методы стеганографии (например, LSB, фазовая кодировка, echo hiding).
17. Приведите примеры исторических применений стеганографии.

18. Какие преимущества и недостатки имеет стеганография?

19. В каких случаях стеганография может быть более эффективной, чем криптография?

20. Какие существуют методы обнаружения стеганографических сообщений?

21. Каковы перспективы использования стеганографии в современном мире?

**ТЕМА 2. Анализ данных при помощи искусственных нейронных сетей**

1. Что такое искусственный нейрон? Опишите его основные компоненты (входы, веса, смещение, функция активации, выход).

2. Какие типы функций активации вы знаете? (например, сигмоида, ReLU, tanh) В чем их особенности и недостатки?

3. Что такое многослойная нейронная сеть (MLP)? Какова ее архитектура?

4. Объясните принцип работы прямого распространения (forward propagation) в нейронной сети.

5. Что такое сверточная нейронная сеть (CNN)? Опишите ее основные слои (сверточный слой, слой пулинга, полносвязный слой).

6. В каких задачах целесообразно использовать сверточные нейронные сети?

7. Что такое рекуррентная нейронная сеть (RNN)? В каких задачах она применяется?

8. Опишите принцип работы LSTM и GRU сетей. В чем их преимущества по сравнению с обычными RNN?

9. Что такое обучение нейронной сети? Какие основные этапы включает этот процесс?

10. Что такое функция потерь (loss function)? Приведите примеры функций потерь, используемых для задач классификации и регрессии.

11. Объясните принцип работы обратного распространения (backpropagation) в нейронной сети.

12. Что такое градиентный спуск (gradient descent)? Как он используется для обучения нейронных сетей?

13. Какие методы оптимизации вы знаете? (например, SGD, Adam, RMSprop) В чем их особенности и преимущества?

14. Что такое переобучение (overfitting) и недообучение (underfitting)? Как с ними бороться?

15. Что такое регуляризация? Какие типы регуляризации вы знаете? (L1, L2, dropout)

16. Как оценить качество работы обученной нейронной сети? Какие метрики используются для этого? (например, accuracy, precision, recall, F1-score, MSE, MAE, R-squared).

17. Что такое кросс-валидация? Зачем она нужна?

18. Как настроить гиперпараметры нейронной сети? Какие методы используются для этого? (например, grid search, random search).

**Примеры билетов для проведения итогового контроля в 8 классе**

**Билет №1**

1. Опишите основные методы криптоанализа. Приведите пример использования частотного анализа для взлома шифра Цезаря.
2. Что такое электронная подпись? Как она работает? Опишите процесс создания и проверки электронной подписи.
3. Что такое стеганография? В чем ее отличие от криптографии? Приведите примеры методов стеганографии.
4. Опишите архитектуру сверточной нейронной сети (CNN). Какие слои входят в ее состав? Для решения каких задач она обычно используется?
5. Что такое переобучение нейронной сети? Как его обнаружить и какие методы борьбы с ним вы знаете (регуляризация, dropout и т.д.)?

**Билет №2**

1. Сравните шифры замены и шифры перестановки. Приведите примеры каждого типа шифра и опишите их основные недостатки с точки зрения криптостойкости.
2. Что такое функция хэширования? Какими свойствами она должна обладать? Объясните, почему важна стойкость к коллизиям.
3. Опишите методы обнаружения стеганографических сообщений.
4. Какие типы функций активации вы знаете (сигмоида, ReLU, tanh)? Опишите их особенности и недостатки.
5. Какие метрики используются для оценки качества работы нейронных сетей в задачах классификации и регрессии? Опишите их.

**Билет №3**

1. Что такое частотный анализ? Как он используется для взлома шифров замены? Приведите пример.
2. Что такое сертификат открытого ключа? Зачем он нужен в контексте электронной подписи?
3. В каких реальных сценариях может применяться стеганография? Приведите примеры.
4. Опишите архитектуру рекуррентной нейронной сети (RNN). Для решения каких задач она обычно используется? В чем заключаются проблемы, связанные с обучением RNN?
5. Опишите основные методы оптимизации, используемые при обучении нейронных сетей (SGD, Adam, RMSprop). В чем их различия?

**Билет №4**

1. Объясните разницу между симметричными и асимметричными шифрами.
2. Почему стойкость к коллизиям важна для функции хеширования?
3. Где стеганография может быть полезной, а где ее использование может привести к проблемам?
4. Что такое полносвязная нейронная сеть?
5. Как работают регуляризация и dropout?

**Приложение А**

# ПОЯСНЕНИЕ ФОРМ КОНТРОЛЯ ОСВОЕНИЯ ПРОГРАММЫ

## Итоговый контроль

**Итоговую контрольную работу** принимает преподаватель или коллектив преподавателей, ведущих предмет. Аттестация проводится в устной или письменной форме по билетам. Преподавателю предоставляется право задавать дополнительные вопросы сверх содержимого билета, а также, помимо теоретических вопросов, давать задачи и примеры, связанные с курсом. Время подготовки обучающегося для последующего ответа не более одного академического часа.

**Защита учебного творческого проекта**

В рамках курса «Информатика и программирование для робототехников» выполняется учебный творческий проект, а по окончании курса проходит защита проекта в виде презентации результатов. Проект должен быть направлен на решение актуальных задач в области науки или техники. Во время выполнения проекта учащиеся должны продемонстрировать полученные знания за предыдущие годы обучения в виде комплексного решения. На защите проекта обучающийся представляет свой реализованный проект перед группой и преподавателем по следующему (примерному) плану:

0. Тема и краткое описание сути проекта.
1. Актуальность проекта.
2. Положительные эффекты от реализации проекта, которые получат как сам автор, так и другие люди.
3. Ресурсы (материальные и нематериальные), которые были привлечены для реализации проекта, а также источники этих ресурсов.
4. Ход реализации проекта.
5. Риски реализации проекта и сложности, которые обучающемуся удалось преодолеть в ходе его реализации.

## Промежуточный контроль

**Контрольная работа** может проводиться в письменной форме по билетам, содержащим тестовые и практические задания, или в форме учебного проекта.

## Текущий контроль

В результате выполнения **самостоятельной работы** обучающимся формируется набор отчетов, в которых приводится результат выполнения домашних заданий, выполненных в свободной форме.