Разбор заданий олимпиады ВСОШ по ИБ и ИИ

История.

- 2023 – 2024, 2024-2025 в предмете технология
- 2025 – 2026, 2026 - 2027 в предмете информатика
- **Дисклеймер: на данный момент, по олимпиаде нет официальных учебников (по ФГОС), как и значимо большого количества материалов в целом.**

- Полный разбор регионального и заключительного этапа по олимпиаде ВСОШ информационная безопасность
- https://vsosh.miem.hse.ru/prepare

- **siriusolymp.ru**. На странице муниципального этапа 2025 года (раздел `inf_security`) есть и текстовые, и видеоразборы заданий по ИБ.
- Выбирайте разбор по своему классу — для 7–8, 9–10 или 11 классов

Уровень сложности

- [x] Для начинающих
- [ ] Для продолжающих
- [ ] Для профи
- [ ] Для всех

Цена

От 0 ₽ – До 250000 ₽

Бесплатно | до 5 000 | до 10 000

Только со скидкой

Только с сертификатом

Язык

- [x] Любой
- [ ] Русский



Александр Пикуль

Здравствуйте! Рады приветствовать Вас для изучения курса по информационной безопасности. Курс нацелен на изучение основ ИБ, с элементами практической части. В рамках курса будут рассмотрены основные определения ИБ, безопасность мобильных устройств, приложений, ПО, веб-технологий, операционных систем и многое другое. Отдельно рассматривается работа с вредоносным ПО и способы... Ещё

456 26 ч начало 1 сентября 2026 г.



«Информационная безопасность: основы цифровой грамотности» Бесплатно

Андрей Автамонов

Курс по цифровой грамотности сотрудников: фишиговые письма, социальная инженерия, DDoS атаки и работа с корпоративными данными.

★★★★★ 4.9 (35) 1K 1 ч



Основы информационной безопасности Бесплатно

Егор Князев, Кирилл Саблин, Андрей Толстиков

Курс направлен на получение основных знаний в области информационной безопасности.

★★★★☆ 4 (60) 2.3K 1 ч

Интенсив по информационной безопасности Бесплатно

Советы

- На сириусе проходить пригласительный этап, где можно познакомиться с подобными заданиями.
- Разбирать задания прошлых лет
- Успех на олимпиаде - это решение до 1000 задач

- **Отличие от классического олимпиады по программированию:** В ИБ и ИИ побеждает не тот, кто быстрее пишет эффективный код, а тот, кто глубже понимает архитектуру систем, математику и уязвимости.

Структура заданий ИБ:

Задачи ВсОШ в этом профиле делятся на несколько категорий:

- Криптография: шифры замены, перестановки, анализ простых алгоритмов шифрования.
- Стеганография: поиск скрытой информации в изображениях, аудио или текстах.
- Анализ трафика и логов: поиск подозрительной активности в массивах данных.
- Поиск уязвимостей: анализ кода на наличие логических ошибок или небезопасных функций.

5, 6 класс

1. Шифр простой перестановки – это шифр, при котором исходный текст делится на блоки определённой длины и буквы в пределах одного блока меняются местами по определённому правилу. Например, при шифровании слова «ПОЧТАЛЬОН», используя блоки длины 3 и перестановку «312», получим следующее:

ПОЧТАЛЬОН → ПОЧ ТАЛ ЬОН → ЧПО ЛТА НЬО → ЧПОЛТАНЬО

Зашифруйте фразу АМЫВЫИГРАЛИОЛИМПИАДУ, разделив предварительно текст на блоки длины 5 и используя перестановку «53142».

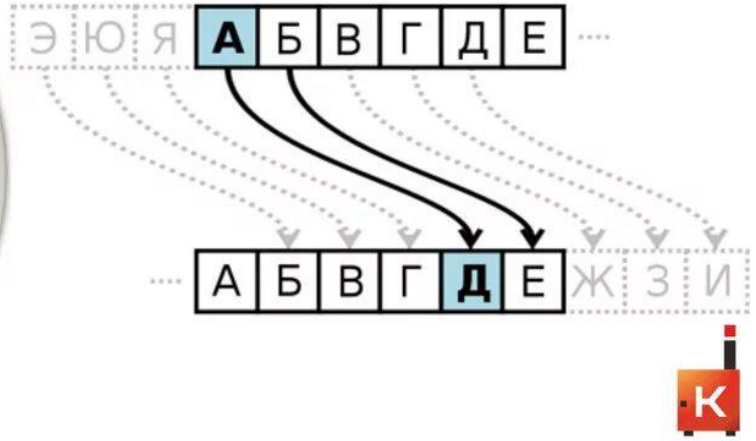
Ответ запишите без пробелов.

Криптография

Криптография

- Симметричная (один ключ для шифровки и дешивровки Шифр Вижинера)
- Ассиметричная (два ключа)
- Гибридная





	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
-	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
А	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-
Б	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А
В	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б
Г	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В
Д	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г
Е	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д
Ж	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е
З	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж
И	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З
Й	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И
К	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Щ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ъ	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Ы	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ь	Ь	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Э	Э	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
Ю	Ю	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Я	Я	-	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

2. Хакерская группировка атакует правительственные сайты. Для того, чтобы раскрыть её, необходимо решить задачу технического характера.

Есть информация о численности группировки и навыках, которыми владеет каждый хакер. При запросе в базе данных для обозначения логической операции «И» используется символ «&», а для логической операции «ИЛИ» символ «|». В таблице приведены запросы и количество найденных по ним записей.

Запрос	**Найдено**
Социальная инженерия	852
Технические навыки	524
Социальная инженерия | технические навыки	1198

Разумеется, самыми опасными являются те, кто владеют и социальной инженерией, и техническими навыками. Вычислите их количество.

Логика. Решение задач при помощи кругов Эйлера

3. Записан набор символов, в котором скрыто осмысленное слово на русском языке:

? _ _ _ **** . _

Также известно, какие символы и комбинации символов соответствуют некоторым буквам русского алфавита.

_ _	* * #	. _	_ _ _	_ !	?	.	*	# .	#	* * *	_	? _
А	Б	Д	Е	З	М	Н	О	Р	С	Т	Х	Ы

- Какое слово скрыто?
- Сколько букв в скрытом слове?

4. Придумайте пароль в соответствии со следующей маской: G_*?.0fK

В маске звёздочка (*) обозначает латинскую букву или цифру. Вопросительный знак же показывает, что на этом месте находится цифра.

Какие **два** из нижеперечисленных паролей соответствуют предложенной маске?

- G_*8.0fK
- G_m4.0fK
- G_*75fK
- G_15.0fK
- J_x?.0fK
- Gk6.0fK

Знание маски поиска

5. Реализацию угроз информационной безопасности можно разделить на этапы.

1. Разведка – нарушитель собирает информацию о потенциальной жертве.
2. Первоначальный доступ – нарушитель, у которого нет прав доступа в систему жертвы, осуществляет проникновение в неё.
3. Закрепление – нарушитель создаёт условия для повторного доступа. Например, меняет права доступа, пароль взломанной учётной записи и т. п.
4. Вывод данных – нарушитель передаёт из взломанной системы похищенные данные.
5. Сокрытие атаки – нарушитель предпринимает меры маскировки своих действий от защитных мер потенциальной жертвы.
6. Вредоносное воздействие – нарушитель реализует цель атаки: похищает, модифицирует, удаляет информацию, выводит из строя или нарушает работы информационной системы и т. п.

Для каждого события выберите соответствующий номер этапа реализации угроз.

	1	2	3	4	5	6
Случайное повреждение электриком сервера компании						
Удаление базы данных вредоносной программой						
Передача троянской программой похищенных паролей своему владельцу						
Изучение хакером страницы сотрудника компании в социальной сети						
Взлом пароля учётной записи одноклассника в социальной сети						
Создание новой учётной записи администратора во взломанной системе						

5. Реализацию угроз информационной безопасности можно разделить на этапы.

1. Разведка – нарушитель собирает информацию о потенциальной жертве.
2. Первоначальный доступ – нарушитель, у которого нет прав доступа в систему жертвы, осуществляет проникновение в неё.
3. Закрепление – нарушитель создаёт условия для повторного доступа. Например, меняет права доступа, пароль взломанной учётной записи и т. п.
4. Вывод данных – нарушитель передаёт из взломанной системы похищенные данные.
5. Сокрытие атаки – нарушитель предпринимает меры маскировки своих действий от защитных мер потенциальной жертвы.
6. Вредоносное воздействие – нарушитель реализует цель атаки: похищает, модифицирует, удаляет информацию, выводит из строя или нарушает работы информационной системы и т. п.

Для каждого события выберите соответствующий номер этапа реализации угроз.

	1	2	3	4	5	6
Случайное повреждение электриком сервера компании						+
Удаление базы данных вредоносной программой						+
Передача троянской программой похищенных паролей своему владельцу				+		
Изучение хакером страницы сотрудника компании в социальной сети	+					
Взлом пароля учётной записи одноклассника в социальной сети		+				
Создание новой учётной записи администратора во взломанной системе			+			

За каждый верный ответ – 1 балл. Максимум за задание – 6 баллов.

Чек-лист тренировки для 5-6 класса (Темы для подготовки)

- **Задания на соответствие:** Соотнести термин (например, «Троян») с его описанием или картинку (замок в браузере) с его значением.
- **Текстовые задачи на логику:** «У Пети пароль из 4 цифр...», задачи на количество комбинаций.
- **Шифры:** Прорешать 10–15 примеров на шифр Цезаря (сдвиги разные: +3, -5, +10) и простую замену.
- **Табличная маршрутная перестановка:** Тренировка вписывания слов в квадраты разного размера (4x4, 5x5) и выписывания их разными маршрутами.
- **Фишинг:** Разбор 5–10 примеров писем. Найти 3 признака того, что письмо мошенническое (например: общоое обращение «Дорогой клиент», грамматические ошибки, ссылка, ведущая на go0gle-login.ru вместо google.com).
- **Безопасность устройств:** Выбрать правильный алгоритм действий при обнаружении вируса или при первом включении нового компьютера.

7, 8 класс

1. Сопоставьте расширения файлов с описанием типов файлов, соответствующих этим расширениям.

Расширения файлов: .h, .exe, .csv, zip, .sig.

Файлы с подписями, используемые для проверки целостности и аутентичности	.h
Архивы, которые могут содержать данные о безопасности или инструменты	.exe
Файлы с данными, которые могут содержать списки уязвимостей или инцидентов	.csv
Заголовочные файлы, содержащие определения функций и переменных, которые могут использоваться во вредоносных программах	.zip
Исполняемые файлы, которые могут содержать вредоносные программы	.sig

1. Сопоставьте расширения файлов с описанием типов файлов, соответствующих этим расширениям.

Расширения файлов: .h, .exe, .csv, zip, .sig.

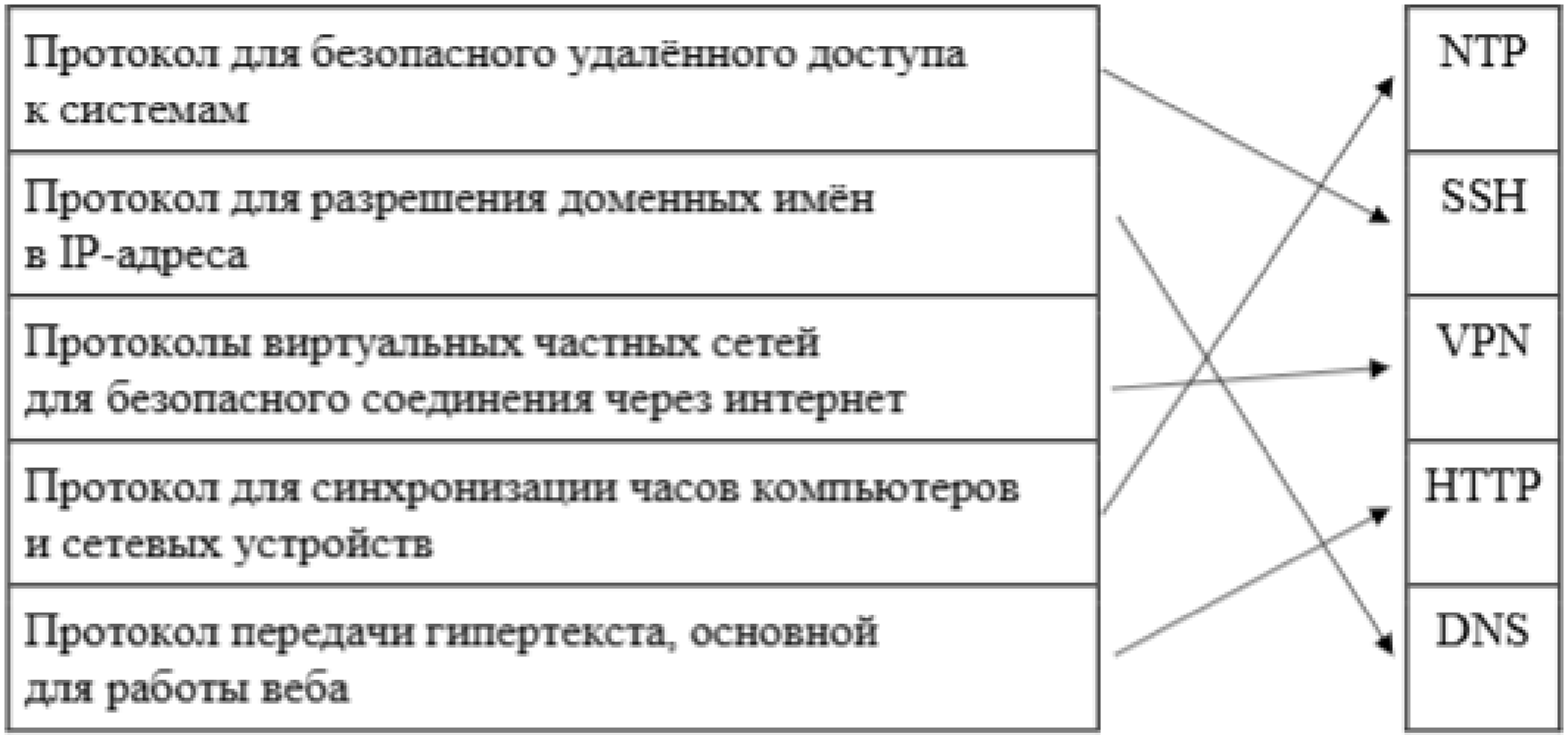


2. Сопоставьте названия протоколов передачи данных с их назначениями.

Названия протоколов: NTP, SSH, VPN, HTTP, DNS.

Протокол для безопасного удалённого доступа к системам	NTP
Протокол для разрешения доменных имён в IP-адреса	SSH
Протоколы виртуальных частных сетей для безопасного соединения через интернет	VPN
Протокол для синхронизации часов компьютеров и сетевых устройств	HTTP
Протокол передачи гипертекста, основной для работы веба	DNS

Названия протоколов: NTP, SSH, VPN, HTTP, DNS.



3. В таблицу размера 6×6 было вписано послание определённым образом: начиная с крайней левой ячейки верхней строки и вдоль всей диагонали до крайней правой ячейки последней строки, вписали первые 6 символов послания, затем, начиная с правой крайней ячейки верхней строки вдоль всей диагонали до крайней левой ячейки последней строки, вписали следующие 6 символов послания. Потом, двигаясь по столбцам сверху вниз, вносили в свободные ячейки таблицы следующие буквы послания, начиная с самого левого столбца, пока вся таблица не заполнилась. Затем в получившейся таблице поменяли местами первый и четвёртый столбцы, второй и шестой. В итоге после всех преобразований над таблицей выписали символы по строкам, начиная с верхней строки.

УПНЗКЫЖЛНАЕАРЫЩЛТХИНСЬУДЕАЫНТОААХНАА

Расшифруйте полученное после всех преобразований сообщение. Ответ запишите без пробелов.

Ответ: ЗАЩИТАПЕРСОНАЛЬНЫХДАННЫХУЖЕАКТУАЛЬНА

4. Вы получили скриншот работы утилиты ping, которая проверяет доступность веб-сайта example.com и измеряет время, необходимое для отправки и получения пакета данных. Используя информацию из скриншота, ответьте на вопросы.

```
Pinging example.com [93.184.216.34] with 32 bytes of data:
Reply from 93.184.216.34: bytes=32 time=20ms TTL=56
Reply from 93.184.216.34: bytes=32 time=22ms TTL=56
Reply from 93.184.216.34: bytes=32 time=21ms TTL=56
Reply from 93.184.216.34: bytes=32 time=19ms TTL=56

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 19ms, Maximum = 22ms, Average = 20ms
```

- Какой IP-адрес имеет веб-сайт example.com?
- Сколько пакетов было отправлено и сколько получено обратно?
- Какое среднее время отклика для пакетов? Ответ укажите в миллисекундах.

5. В одном из марсианских обучающих центров изучали тексты и различные способы передачи информации землян. Роботам попался следующий фрагмент в книге про защиту информации.

С	Ш	И	Н	Г	А	И	Ю	Е	Т	Р	О	М	Ю	С	П	М	Я	Ш	Р	А	К	Ж	Л	Р
А	К	З	Ъ	С	В	Т	З	Ж	П	Н	Э	Й	И	Б	Ч	О	Н	Т	Г	У	Ч	М	Б	Я
В	О	С	Д	М	Б	У	Д	Л	А	Г	А	Л	Н	В	Ж	А	С	К	З	В	С	Т	А	П
Г	У	П	Я	З	С	Г	Й	О	К	Е	Ч	Б	Д	К	Е	Э	Л	Щ	Б	Я	Н	О	К	З
Д	Е	В	Ю	А	Ч	А	М	П	Б	И	З	С	Я	О	Г	З	Ч	М	П	Й	Л	Г	У	Ч

```
Кошка спокойно зевает, собака бегает за букашками, чайка бьёт своими
крыльями, когда сегодняшний закат золотит чистый берег
с зелёными кустами, за которыми скачут быстрые кузнечики.
```

Один из них засомневался в том, что книга по информационной безопасности Земли будет содержать тексты про зверей на природе. Какое тайное послание здесь содержится? Ответ запишите без пробелов и дополнительных знаков препинания.

6. Эти рекламщики доберутся до тебя, где бы ты ни был... Что тут, очередное предложение купить крутой пылесос?
Кажется, тут что-то есть…
Данные для выполнения этого задания находятся в файле Задание 6.docx.

Ответ запишите в формате

СЛОВО_СЛОВО_СЛОВО_СЛОВО_СЛОВО_СЛОВО_СЛОВО_СЛОВО.

Самое интересное спрятано не в баннере, а у кнопки «Оплатить». К сожалению, наши разработчики оставили мелкий недостаток: приложение может зависнуть на моменте оплаты. Но заказ точно проходит, мы обещаем это поправить!

И наконец, обрати внимание на шрифт сносок рядом с ценой: он скромнее, но в нём вся конкретика — те пункты, из-за которых потом не придётся спорить с поддержкой. Выбирай уверенно — и забирай лучшее по-настоящему выгодно.

- <span style='font-size:1.0pt;line-height:115%;font-family:
- "Times New Roman",serif'>Дочитывая этот текст до конца, вы соглашаетесь с тем, что умеете читать мелкий шрифт и согласны на рассылку наших рекламных сообщений и покупку всех наших товаров прямо сейчас. Чтобы отменить своё решение, введите
- ответ в систему :)
-
- </body>
- </html>

Реальность.

Школьная почта «Сова» весь день автоматически ставила письмам ярлык СПАМ .

За этот день пришло 100 писем: 60 из них – действительно спам, а 40 – обычные.

Фильтр пометил «СПАМ» 55 писем. Позже администратор сверил результаты: из 60 настоящих спам-писем 48 оказались помечены «СПАМ», а из 40 обычных – 7 получили ярлык по ошибке.

Определите условную вероятность : если письмо уже помечено ярлыком «СПАМ», какова вероятность, что оно действительно спам.

Решение

Помечено как спам 48/60=0,8 (Администратор проверил)

Доля спама во всех письмах 60/100=0,6

Помечено как спам фильтром 55/100=0,55

Помечено как спам обычное письмо 7/40 = 0,175

0,6 *0,8/0,55 = 0,87

Формула Байеса:

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)},$$

где

$P(A)$ — априорная вероятность гипотезы *A* (смысл такой терминологии см. ниже);

$P(A|B)$ — вероятность гипотезы *A* при наступлении события *B* (апостериорная вероятность);

$P(B|A)$ — вероятность наступления события *B* при истинности гипотезы *A*;

$P(B)$ — полная вероятность наступления события *B*.

Чек-лист тренировки 7,8 классы (Темы для прорешивания)

- **Системы счисления:** Решить 20–30 примеров на перевод чисел. Особое внимание — сложение и вычитание в разных системах.
- **ASCII-таблица:** Написать скрипт (или натренироваться вручную), который переводит шестнадцатеричные дампы в читаемый текст.
- **Крипто-задачи:**
  - Взломать шифр Цезаря методом частотного анализа (если ключ неизвестен).
  - Решить задачу на шифр Виженери с коротким ключом.
- **Задания на соответствие:** Соотнести типы атак (XSS, SQLi, Phishing) с их описанием или способом предотвращения.
- **Сетевые задачи:** По фрагменту дампа трафика (в текстовом виде) определить, какой протокол используется и какая команда передается.
- **Логические задачи:** Задачи на количество паролей, энтропию, комбинаторику (например, «Сколько существует 4-значных ПИН-кодов, если цифры не могут повторяться?»).

9, 11 класс

1. Временная калькуляция

Инженер Дмитрий забыл пароль от системы контроля доступа в своём офисе. На табличке рядом с терминалом указаны требования к паролю:

- длина пароля составляет 6 символов;
- разрешены буквы английского алфавита (26 символов, регистр только нижний), цифры, спецсимволы;
- цифры только чётные;
- спецсимволы – только эт (@), восклицательный знак (!).

Сколько времени максимально затратит программа подбора паролей, работающая со скоростью 300 паролей в секунду?

Ответ выразите в секундах, арифметически округлите до целых.

Комбинаторика

Определите количество элементов множества (**n**), из которого выбирается **k** элементов

Порядок выбранных элементов важен

НЕТ

Среди выбранных элементов есть повторения?

НЕТ

Сочетания

$$C_n^k = \frac{n!}{k! * (n-k)!}$$

ДА

Сочетания с повторениями

$$\overline{C}_n^k = C_{n+k-1}^k = \frac{(n+k-1)!}{k! * (n-1)!}$$

ДА

Выбираем все n элементов?

НЕТ

Среди выбранных элементов есть повторения?

НЕТ

Размещения

$$A_n^k = \frac{n!}{(n-k)!}$$

ДА

Размещения с повторениями

$$\overline{A}_n^k = n^k$$

ДА

Среди выбранных элементов есть повторения?

НЕТ

Перестановки

$$P_n = n!$$

ДА

Перестановки с повторениями

$$\overline{P}_n(k_1, \dots, k_l) = \frac{n!}{k_1! * \dots *$$

2. Сопоставьте расширения файлов с описанием типов файлов, соответствующих этим расширениям.

Расширения файлов: .pcap, .md5, .pem, .apk, .sh.

файлы с хешами, используемые для проверки целостности данных	**.pcap**
скрипты оболочки, которые могут содержать команды для тестирования безопасности	**.md5**
файлы с сертификатами и ключами для шифрования	**.pem**
файлы захвата сетевого трафика	**.apk**
файлы приложений для Android, которые могут содержать уязвимости	**.sh**

2. Сопоставьте расширения файлов с описанием типов файлов, соответствующих этим расширениям.

Расширения файлов: .pcap, .md5, .pem, .apk, .sh.

файлы с хешами, используемые для проверки целостности данных	.pcap
скрипты оболочки, которые могут содержать команды для тестирования безопасности	.md5
файлы с сертификатами и ключами для шифрования	.pem
файлы захвата сетевого трафика	.apk
файлы приложений для Android, которые могут содержать уязвимости	.sh

3. В офисе компании N подверглись хакерской атаке *почтовый сервер, сервер базы данных и рабочий компьютер руководителя*. Глава службы безопасности подозревает в причастности к преступлению *бухгалтера, программиста и системного администратора*, работающих в компании N.

1) Опросив всех трёх подозреваемых на детекторе лжи, следователь-психолог пришёл к выводу, что каждый из них в тот день совершил хакерскую атаку, причём только на один из объектов.
2) В результате анализа логов сетевого трафика выяснилось, что программист в тот день не контактировал с почтовым сервером.
3) Работники, обслуживающие сервер, подтвердили, что во время инцидента системный администратор контролировал сервисное обслуживание сервера базы данных и не отвлекался на другие дела.

Выясните, кто какой объект атаковал.

системный администратор
программист
бухгалтер

почтовый сервер
сервер базы данных
компьютер руководителя

Выясните, кто какой объект атаковал.

системный администратор	почтовый сервер
программист	сервер базы данных
бухгалтер	компьютер руководителя

Решение

Из 2) пункта вытекает, что программист не атаковал почтовый сервер. Из пункта 3) следует, что системный администратор не мог атаковать ни почтовый сервер, ни компьютер руководителя. Значит, системный администратор атаковал базу данных, программист – компьютер руководителя, а бухгалтер (методом исключения) – почтовый сервер.

Логика

4. На кодовом замке в голове робота установлена последовательность из пяти символов, каждый из которых – либо ***X***, либо ***Y***, либо ***Z***.

Известна парольная политика:

- буква ***X*** должна встречаться в шифре ровно два раза,
- буквы ***Y*** и ***Z*** могут присутствовать в шифре любое количество раз, в том числе и отсутствовать.

Сколько различных вариантов шифра можно составить, соблюдая указанные условия?

Решение

Шаг 1: Выбор позиций для буквы X. Нам нужно выбрать 2 позиции из 5, на которые мы поставим символ X. Это классическая задача на сочетания:

$$C_5^2 = \frac{5!}{2! \cdot (5-2)!} = \frac{5 \cdot 4}{2 \cdot 1} = 10$$

Шаг 2: Заполнение оставшихся позиций. На каждой из трёх оставшихся позиций может стоять либо Y, либо Z (то есть у нас 2 варианта для каждой позиции). Поскольку выбор на каждой позиции независим, общее количество способов заполнить эти позиции равно:

$$2^3 = 8$$

Шаг 3: Вычисление общего числа вариантов. Чтобы получить общее количество подходящих шифров, перемножим результаты первого и второго шагов:

$$10 \cdot 8 = 80$$

```
$ curl -v https://example.com
*   Trying 93.184.216.34:443...
* Connected to example.com (93.184.216.34) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
*   CApath: /etc/ssl/certs
* SSL connection using TLS1.2 / ECDHE_RSA_AES_256_GCM_SHA384
* ALPN, server accepted to use h2
> GET / HTTP/2
> Host: example.com
> User-Agent: curl/7.68.0
> Accept: */*
>
< HTTP/2 200
< content-type: text/html; charset=UTF-8
< content-length: 1256
< date: Wed, 04 Oct 2023 12:00:00 GMT
< server: ExampleServer/1.0
< last-modified: Mon, 02 Oct 2023 10:00:00 GMT
< etag: "123456789abcdef"
< accept-ranges: bytes
<
<!doctype html>
<html>
<head>
    <title>Example Domain</title>
...
...
* Connection #0 to host example.com left intact
```

Вам представлен скриншот части вывода работы консольной утилиты, которая используется для выполнения HTTP –запросов.
Рассмотри скрин и ответьте на вопросы. Какой IP-адрес был использован для подключения к серверу?
Какой метод HTTP – запроса был отправлен на сервер?
Какова длина содержимого, возвращенного в байтах?

- Сервер вернул статус-код 200. Что он обозначает?

1. Статус-код 200 означает, что запрос клиента был успешно обработан и сервер вернул запрашиваемые данные.
2. Статус-код 200 указывает на то, что сервер временно недоступен из-за перегрузки или технического обслуживания.
3. Статус-код 200 означает, что произошла ошибка на стороне клиента и запрос не может быть выполнен.
4. Статус-код 200 сигнализирует о необходимости аутентификации для доступа к запрашиваемым данным.

Запишите номер верного варианта ответа.

Ответ: 93.184.216.34

За верный ответ – 1 балл.

- Какой метод HTTP-запроса был отправлен на сервер?

Ответ: GET

За верный ответ –1 балл.

- Какова длина содержимого, возвращённого сервером, в байтах?

Ответ: 1256

За верный ответ – 1 балл.

- Сервер вернул статус-код 200. Что он обозначает?

1. Статус-код 200 означает, что запрос клиента был успешно обработан и сервер вернул запрашиваемые данные.
2. Статус-код 200 указывает на то, что сервер временно недоступен из-за перегрузки или технического обслуживания.
3. Статус-код 200 означает, что произошла ошибка на стороне клиента и запрос не может быть выполнен.
4. Статус-код 200 сигнализирует о необходимости аутентификации для доступа к запрашиваемым данным.

Запишите номер верного варианта ответа.

Ответ: 1

6. Пассивный анализ

Рекомендуемые утилиты: Python

Файл: reverse_11_3.py

Товарищ, на конвейере генератора ключей обнаружен сбой: каждый байт ключа сдвинули по позиции, «покрутили» и замаскировали. Верните исходный порядок и укажите корректный ключ.

6. Пассивный анализ

Рекомендуемые утилиты: Python

Файл: reverse_11_3.py

Товарищ, на конвейере генератора ключей обнаружен сбой: каждый байт ключа сдвинули по позиции, «покрутили» и замаскировали. Верните исходный порядок и укажите корректный ключ.

Формат ответа: vsosh{...}

Ответ: vsosh{idx_ror1_xor5A_ok}

За верный ответ – 7 баллов.

- Сетевая безопасность:
  - Стек протоколов TCP/IP, модель OSI.
  - Работа снифферов (Wireshark): анализ дампов, поиск флагов в трафике, извлечение файлов.
  - Принципы работы VPN, TLS/SSL, PKI (инфраструктура открытых ключей)
- Криптография (современная):
  - Симметричное шифрование (AES,
  - Асимметричное шифрование (RSA
  - Хеширование (MD5, SHA-family) и
  - Электронная подпись.
- Безопасность ОС и веба:
  - Типы уязвимостей OWASP Top 10 (SQLi, XSS, RCE, LFI/RFI, SSRF).
  - Работа с бинарными уязвимостями: Buffer Overflow, Use-After-Free.
  - Механизмы защиты ОС: ASLR, DEP/NX, Stack Canaries.
- Форензика (Цифровая криминалистика):
  - Анализ дампов оперативной памяти (Volatility Framework).
  - Анализ файловых систем, восстановление удаленных данных.
  - Анализ логов (Event Logs, Apache/Nginx access logs).
- Реверс-инжиниринг (Обратная разработка):
  - Чтение ассемблерного кода (x86/x64).
  - Работа с декомпиляторами (Ghidra, IDA Free).
  - Понимание работы компилятора и структуры PE/ELF файлов.

Чек лист.
Теоретические основы

Особенности заданий для 10–11 классов

На старшей ступени (9–11 классы) олимпиада максимально приближена к формату профессиональных соревнований CTF (Capture The Flag). Задания требуют не только теоретических знаний, но и уверенных практических навыков работы в командной строке Linux.

Проектный (теоретический) тур является обязательной частью муниципального и заключительного этапов Всероссийской олимпиады школьников (ВсОШ) по профилю «Информационная безопасность». В отличие от практического тура (CTF), где нужно быстро находить флаги, проектный тур проверяет умение школьника мыслить как системного архитектора или аналитика ИБ.

Формат и направления (Red Team и Blue Team)

1. **Red Team (Нападение и исследование):**
    - **Суть:** Выявление, доказательство и демонстрация уязвимостей в информационных системах, программном обеспечении или организационных процессах.
    - **Задача проекта:** Не просто найти баг, а оценить его критичность, показать реальный сценарий эксплуатации и доказать, что угроза актуальна для конкретной системы (например, для инфраструктуры школы или вымышленного банка).
    - **Пример темы:** «Разработка методики обхода биометрической аутентификации в образовательных терминалах с использованием силиконовых накладок и анализа отражений в очках».

2. **Blue Team (Защита и разработка):**

   - **Суть:** Создание решения, которое повышает уровень безопасности, упрощает работу аналитиков SOC или автоматизирует рутинные операции.
   - **Задача проекта:** Разработать прототип инструмента, написать скрипт для автоматизации или составить регламент, который решает конкретную проблему безопасности.
   - **Пример темы:** «Разработка автоматизированной системы классификации фишинговых писем для школьной почты на базе машинного обучения».

Критерии оценивания

- **Актуальность:** наличие реального запроса на решение проблемы.
- **Техническая глубина:** понимание протоколов, алгоритмов и архитектуры систем.
- **Реализуемость:** возможность внедрения проектного продукта в жизнь.
- **Положительный эффект:** как решение снизит риски или упростит защиту.
- **Презентация:** умение четко и лаконично (ответы на вопросы часто ограничены 150 словами) донести суть. vos.olimpiada

Направление	Тема проекта	Краткое описание
Red Team	Аудит безопасности протокола MQTT в системах «Умный дом»	Поиск уязвимостей в публичных брокерах IoT-устройств, перехват управления освещением или замками.
Red Team	Атаки на системы электронного голосования	Анализ уязвимостей веб-интерфейса и базы данных гипотетической системы ДЭГ (дистанционного электронного голосования).
Blue Team	Разработка автономного honeypot-ловушки для малваре	Создание легковесного скрипта, имитирующего уязвимый сервис, который собирает образцы атак для последующего анализа в Cuckoo Sandbox.
Blue Team	Система автоматического реагирования на инциденты (SOAR) для школы	Скрипт на Python, который при обнаружении сканирования портов (по логам Suricata) автоматически блокирует IP на MikroTik роутере.
Blue Team	Методика расследования инцидентов в сетях LoRaWAN	Разбор специфики атак на энергоэффективные сети интернета вещей и создание чек-листа для криминалиста.

Структура задач ИИ

Форматы и типы задач:

Задания олимпиады носят междисциплинарный характер и интегрируют математику, программирование, анализ данных и основы машинного обучения. Типичная структура включает:

- **Теоретический блок:** Задачи на логику, математическую статистику, теорию вероятностей, линейную алгебру и понимание архитектур нейросетей.

Чек лист 5, 6 класс

1. Работа с алгоритмами и исполнителями (самый частый тип задач)

Умение выполнять команды пошагово. Пример из школьного этапа 2025/26: *«На экране у робота число 1. Команда СЛЕДУЮЩЕЕ (+1), команда УДВОЙ (2). Сколько чисел можно получить за 4 команды?».

Умение строить дерево вариантов (не пропускать цепочки команд).

Понимание того, что порядок команд важен (1+1*2 не равно (1+1)*2).

Тренировка на простых «Черепашках» и роботах из школьных учебников информатики.

2. Логика и теория множеств

Решение задач на круги Эйлера (пересечение групп).

Умение работать с таблицами и схемами (кто с кем сыграл в турнире, кто куда пошел).

Пример из школьного этапа: «В турнире 5 моделей ИИ, каждая сыграла с каждой. За победу 2 очка, за ничью 1. Распределить очки».

Понимание условий «ровно один», «хотя бы один», «каждый с каждым».

3. Текстовые логические задачи

Внимательное чтение условия (самая частая причина ошибок в 5–6 классах).

Перевод текста в математическую модель или таблицу.

Чек лист для 7, 8 класса

1. Базовая математика и логика (фундамент)

Дискретная математика: освоить теорию множеств, основы комбинаторики (перестановки, сочетания), теорию графов (поиск в ширину и глубину, кратчайшие пути).

Теория вероятностей: понимать классическое определение вероятности, уметь решать задачи на независимые и зависимые события, комбинаторные вероятности.

Математическая логика: уметь работать с логическими операциями (И, ИЛИ, НЕ), таблицами истинности, законами де Моргана.

Линейная алгебра (базово): понимать, что такое вектор и матрица, уметь складывать векторы и умножать матрицу на вектор (это основа работы нейронов).

Статистика: понимать понятия среднего арифметического, медианы, моды и стандартного отклонения.

2. Программирование (инструмент)

Выбор языка: уверенно владеть Python (наиболее предпочтителен из-за библиотек) или C++. Для 7–8 класса Python — оптимальный выбор.

Синтаксис и структуры данных: безошибочно использовать списки, словари, кортежи, множества.

Алгоритмы: уметь реализовывать сортировки, бинарный поиск, обходы графов, динамическое программирование на простых задачах.

Функции и модули: уметь писать чистый код, разбивать решение на функции, подключать стандартные библиотеки.

Практика: ежедневно решать задачи на платформах вроде Codeforces, «Школе программиста», «Кружке 239» или Stepik.

3. Основы искусственного интеллекта и анализа данных

Машинное обучение (ML): понимать разницу между обучением с учителем (классификация, регрессия) и без учителя (кластеризация). Знать, что такое обучающая и тестовая выборки.

Метрики качества: понимать, что такое точность (accuracy), полнота (recall) и F1-мера на интуитивном уровне.

Регрессия: понимать принцип линейной регрессии (поиск линии тренда).

Классификация: понимать принцип работы логистической регрессии и метода ближайших соседей (k-NN).

Нейронные сети (базово): понимать, что такое перцептрон, как работает один искусственный нейрон (взвешенная сумма + активация), что такое переобучение.

Обработка данных: уметь очищать данные (удалять пропуски), нормализовать их и выделять признаки (feature engineering).

4. Работа с данными и инструментами

Таблицы: уверенно работать в Excel или Google Таблицах (фильтрация, сортировка, формулы, сводные таблицы).

Библиотеки Python: освоить pandas для таблиц (чтение CSV, фильтрация, группировка), matplotlib или seaborn для построения простых графиков.

Форматы данных: понимать структуру CSV, JSON, XML.

Среды разработки: настроить VS Code или PyCharm, уметь запускать код в Jupyter Notebook.

Чек лист для 9-11 классов

- **1. Олимпиадное программирование (Hard Skills)**
- Язык: свободное владение Python (с обязательным знанием NumPy для векторизации вычислений) или C++. Python предпочтителен для задач на прототипирование моделей, C++ — для тяжелых вычислений.
- Сложность алгоритмов: уверенно решать задачи уровня Advanced на Codeforces (рейтинг 1600–2000).
- Ключевые темы: динамическое программирование (в том числе по подотрезкам и подмножествам), графы (потоки в сетях — алгоритм Диница, поиск сочетаемости), геометрия, сложные структуры данных (деревья отрезков, Sparse Table, DSU).
- **2. Математика для Data Science (Теоретический фундамент)**
- Линейная алгебра: векторы, матрицы, тензоры. Собственные значения и векторы, SVD (сингулярное разложение), проекции, решение систем линейных уравнений. Понимание того, как умножение матриц реализует слои нейросети.
- Математический анализ: производные функций многих переменных, градиент, частные производные. Понимание цепного правила (chain rule) для обратного распространения ошибки (backpropagation).
- Теория вероятностей и статистика: распределения (нормальное, Бернулли), условная вероятность, формула Байеса, метод максимального правдоподобия (MLE), центральная предельная теорема.
- Выпуклая оптимизация: понимание того, что такое градиентный спуск, его стохастическая версия (SGD), момент (Momentum), Adam..

Чек лист для 9-11 классов

- **3. Машинное обучение и архитектура ИИ**
- Классические алгоритмы: глубокое понимание логистической регрессии, SVM (метод опорных векторов), деревьев решений и Random Forest, кластеризации (K-Means, DBSCAN).
- Нейронные сети (Deep Learning):
- Архитектура полносвязных сетей (MLP).
- Сверточные сети (CNN) для работы с изображениями (свертки, пулинг, padding, stride).
- Рекуррентные сети (RNN) и LSTM/GRU для работы с последовательностями.
- Механизм внимания (Attention) и базовое устройство трансформеров (Transformers).
- Обучение и регуляризация: функции потерь (Cross-Entropy, MSE), переобучение, L1/L2 регуляризация, Dropout, Batch Normalization.
- Обучение без учителя: автоэнкодеры, генеративно-состязательные сети (GAN) на концептуальном уровне.
- **4. Инженерия данных и инструменты**
- Библиотеки Python: pandas (сложные операции с данными), NumPy (быстрые вычисления), Matplotlib/Seaborn (визуализация), scikit-learn (классические ML-модели), PyTorch или TensorFlow (нейросети).
- Работа с данными: умение парсить сложные форматы, обрабатывать пропуски, нормализовать признаки, писать свои даталоадеры.
- Git: использование систем контроля версий для командных задач (на командных турах или при подготовке в кружке).

Задачи логические, на шифрование для мотивации детей 5 - 7 классов на участие в олимпиадах по ИБ и ИИ.

- Сборник Н. А. Владимировой «Увлекательная информатика. 5–11 классы» — содержит систематизированные логические задачи, кроссворды и игры, соответствующие школьной программе.
- Учебно-методические пособия для олимпиад (например, Н. Д. Золотарёва, М. В. Федотов) — в них собраны задачи повышенной сложности с подробными решениями и указаниями для 5–7 классов.
- Сценарии внеклассных мероприятий — на порталах «Мультиурок», «Инфоурок» и «Социальная сеть работников образования» можно найти готовые уроки-игры «Юный криптограф» с полным набором заданий для печати.

- Математическая криптография (простейшая)
- Замена букв цифрами в математическом ребусе.
- Задача: КИС + КСИ = ИСК. Одинаковые буквы — одинаковые цифры, разные — разные. Найдите значение слова «ИСК».