ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. 2025 г.
ПРИГЛАСИТЕЛЬНЫЙ ЭТАП. 8–10 КЛАССЫ

Максимальный балл за работу – 30.

1. Выберите **все** характерные особенности для мандатной модели разграничения доступа.

- добавление нового объекта сводится к присвоению единственного атрибута
- добавление нового объекта требует заполнения столбца матрицы
- добавление субъектов с аналогичным набором прав осуществляется заполнением одной строки матрицы доступа
- определение наличия права доступа производится на основе сопоставления двух значений
- права доступа предоставляются к неразделимым группам объектов
- допускает настройку произвольных прав доступа для субъекта

2. Маша решила составить пароль, соответствующий следующей маске:

SC[a-gA-S][*|!?]OL.

Всё, что находится в этой маске вне квадратных скобок, не подлежит изменению.

[...] Пара квадратных скобок соответствует любому символу из тех, что записаны в скобках. Первый и последний символ в наборе разделяются дефисом.

Например

[123] соответствует цифре 1, 2 или 3.

[a-z] соответствует любой букве от a до z.

| Вертикальная черта указывает на чередование и соответствует оператору ИЛИ.

Например

[a-z|123] соответствует любой строчной букве латинского алфавита ИЛИ любой цифре от 1 до 3.

* Звёздочка соответствует любой непустой подстроке из букв и цифр.

Отметьте только те пароли, которые соответствуют придуманной маске.

Выберите **три** верных ответа.

- SCHOOOL
- SChoOL
- SCHOO!L
- SCHOOLOL
- SCH*!OL
- SCH?OL

3. Установите соответствия между терминами, относящимися к социальной инженерии, и их описаниями.

Термины из социальной инженерии: спуфинг, тайпсквоттинг, претекстинг, смишинг.

1. Мошенническое действие, отработанное по заранее составленному сценарию и состоящее в выдаче себя за другого человека для получения желаемых данных.

2. Отправление жертве SMS-сообщения, содержащего ссылку на сайт и мотивирующего войти на этот сайт.

3. Допущение ошибки при введении имени сайта в адресную строку и попадание на зеркало сайта, созданного специально злоумышленниками.

4. Подмена телефонного номера или адреса электронной почты.

4. В офисе компании N были реализованы 4 угрозы безопасности информации, объектами которых являлись: *почтовый сервер, сервер БД, ПК и смартфон руководителя*. Глава службы безопасности подозревает в причастности к случившемуся *бухгалтера, программиста, системного администратора и уборщицу*, работающих в компании N.

Опросив всех четырёх подозреваемых на детекторе лжи, следователь-психолог пришёл к выводу, что каждый из них в тот день был причастен только к одному инциденту и только к одному из вышеперечисленных объектов.

- В результате анализа логов сетевого трафика выяснилось, что программист в тот день не контактировал с почтовым сервером.
- Работники, обслуживающие сервер, подтвердили, что во время инцидента системный администратор контролировал сервисное обслуживание сервера базы данных и не отвлекался на другие дела.
- На записи с камер видеонаблюдения охранник компании N увидел, что уборщица случайно пролила воду на рабочий стол руководителя, и лежавший на нём телефон заискрился.

Выясните, кто был причастен к какому объекту.

сервер БД	бухгалтер
почтовый сервер	системный администратор
ПК руководителя	уборщица
смартфон руководителя	программист

5. На следующий день, когда обстоятельства и подробности минувших событий прояснились, было решено изучить, к каким негативным

последствиям привели события минувшего дня. Техническая поддержка компании заявила, что каждое происшествие привело только к одному из перечисленных негативных последствий: *модификации персональных данных клиентов, утечке коммерческой тайны, отказе в обслуживании и необходимости дополнительных затрат на ремонт.*

- Просмотрев отчёт системы контроля целостности сервера базы данных выяснилось, что попыток модификации данных не было.
- В результате нового допроса руководитель компании признался, что в течение того рабочего дня часто оставлял без присмотра незаблокированный компьютер, где находились файлы с коммерческой тайной в единственном экземпляре в компании.

Сопоставьте негативные последствия объектам, которые подверглись атаке.

модификация персональных данных клиентов	сервер БД
утечка коммерческой тайны	почтовый сервер
отказ в обслуживании	ПК руководителя
необходимость дополнительных затрат на ремонт	смартфон руководителя

6. Известно, что злоумышленник сымитировал встраивание сообщения в секретный стегоконтейнер, символами которого являлись буквы русского алфавита. Для этого он инвертировал по последнему биту в коде каждого символа контейнера, сымитировав стеганографический метод LSB. Известно, что код каждого символа контейнера представляет собой номер символа в русском алфавите, переведённый в двоичную систему счисления и дополненный незначащими нулями до длины в восемь бит. Как выглядел фрагмент стегоконтейнера до его повреждения злоумышленником?

00001101 00010101 00010001

7. Нарушитель хочет сымитировать встраивание секретного сообщения в известный стегоконтейнер «ПУСК». Для этого он собирается инвертировать по последнему биту в коде каждого символа контейнера, имитируя стеганографический метод LSB. Код каждого символа контейнера представляет собой номер символа в русском алфавите, переведённый в двоичную систему счисления и дополненный незначащими нулями до длины в восемь бит. Определите, как будет выглядеть фрагмент контейнера. В ответе укажите суммарное количество единиц в кодах получившихся символах.

8. Шифр, известный как «квадрат Полибия», устроен следующим образом. В квадратную или прямоугольную таблицу вписываются буквы алфавита (для

кодирования – в алфавитном порядке, для шифрования – в произвольном, при этом расположение букв в таблице является ключом), строки и столбцы таблицы обозначаются цифрами. При зашифровании буквы открытого текста заменяются на пары цифр, которыми отмечены, соответственно, строка и столбец, в которых стоит данная буква. Например, на иллюстрации ниже буква «О» зашифрована сочетанием цифр «34», а слово «ОКО» – «34 26 34».

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	.	,	?

Таким шифром с некоторым (неизвестным) ключом зашифрован некоторый текст (без пробелов, но с сохранением знаков препинания – точки, запятой и вопросительного знака):
11 63 22 31 21 24 42 25 63 63 22 63 32 24 66 56 32 63 22 22 63 25 13 12 63 31 65 24 62 24 66 16

- Известно, что в тексте сообщения есть слово «МЕТОД». Укажите часть шифртекста, которой зашифрованы последние 3 буквы пятого слова сообщения. Ответ запишите одним числом без разделителей.

- Установите шифробозначение (замену) буквы «Ж» в использованном ключе.

- Зашифруйте слово «ВИРУС» тем же ключом шифрования. Впишите результат как одно число без разделителей.

Максимальный балл за работу – 30.