МАТЕРИАЛЫ ЗАДАНИЙ МЕЖРЕГИОНАЛЬНОЙ ОЛИМПИАДЫ ШКОЛЬНИКОВ ИМЕНИ И.Я. ВЕРЧЕНКО ПО ПРОФИЛЮ «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ» (2024/2025 УЧЕБНЫЙ ГОД)

ОТБОРОЧНЫЙ ЭТАП
8-10 КЛАССЫ

СОДЕРЖАНИЕ

Задача 1. Контрольная сумма

Вариант 1

В ходе расследования утечки данных из крупной компании отделом информационной безопасности было перехвачено несколько сообщений и их контрольных сумм. Известно, что было передано одно подлинное сообщение и несколько поддельных, все с корректными контрольными суммами.

Известно, что слово «ДА» имеет контрольную сумму – 5 + 1 = 6,

«НЕТ» – 15 + 6 + 20 = 41.

Контрольная сумма подлинного сообщения равна **55**. Определите подлинное сообщение.

ПАРОЛЬ
ВИРУС
АТАКА
ВЗЛОМ

Ответ: ВЗЛОМ – 55 ***(выбрать)***

Вариант 2

В ходе расследования утечки данных из крупной компании отделом информационной безопасности было перехвачено несколько сообщений и их контрольных сумм. Известно, что было передано одно подлинное сообщение и несколько поддельных, все с корректными контрольными суммами.

Известно, что слово «ДА» имеет контрольную сумму – 5 + 1 = 6,

«НЕТ» – 15 + 6 + 20 = 41.

Контрольная сумма подлинного сообщения равна **55**. Определите подлинное сообщение.

СКРИПТ
ФАЙЛ
ПАРОЛЬ
ШИФР

Ответ: ШИФР – 76 ***(выбрать)***

Задача 2. Вирус

Вариант 1

На одном из серверов компании была обнаружена программа с вредоносным кодом, которая распространяется по системе. Программа работает по следующему принципу: она заражает один новый процесс на сервере ежедневно, начиная со следующего после заражения дня. Каждый зараженный процесс ежедневно запускается ровно один раз, создавая ещё одну свою копию в новом процессе, если он ещё не заражен.

Сколько процессов будет заражено через **14** дней, если изначально заражен только один процесс, и на сервере одновременно работает до **50 000** процессов?

Ответ: 16384 (вписать)

Вариант 2

На одном из серверов компании была обнаружена программа с вредоносным кодом, которая распространяется по системе. Программа работает по следующему принципу: она заражает один новый процесс на сервере ежедневно, начиная со следующего после заражения дня. Каждый зараженный процесс ежедневно запускается ровно один раз, создавая ещё одну свою копию в новом процессе, если он ещё не заражен.

Сколько процессов будет заражено через **12** дней, если изначально заражен только один процесс, и на сервере одновременно работает до **10 000** процессов?

Ответ: 4096 ***(вписать)***

Задача 3. Идентификатор

Вариант 1

Для доступа к конфиденциальному ресурсу в компании используется система генерации уникальных идентификаторов. Идентификатор состоит из **8** цифр, каждая из которых может принимать значение от 1 до 5 включительно, а сумма любых трех соседних цифр должна быть равна **10**.

Какое максимальное число пользователей могут одновременно работать с ресурсом, при условии, что у каждого должен быть свой уникальный идентификатор?

Ответ: 18 ***(вписать)***

Вариант 2

Для доступа к конфиденциальному ресурсу в компании используется система генерации уникальных идентификаторов. Идентификатор состоит из **10** цифр, каждая из которых может принимать значение от 1 до 5 включительно, а сумма любых трех соседних цифр должна быть равна **8**.

Ка кое максимальное число пользователей могут одновременно работать с ресурсом, при условии, что у каждого должен быть свой уникальный идентификатор?

Ответ: 18 ***(вписать)***

Задача 4. Защита от НСД

Вариант 1

В компании используется система с тремя уровнями доступа: низкий (**100** сотрудников), средний (**200** сотрудников) и высокий (**100** сотрудников). Каждый уровень характеризуется различной вероятностью несанкционированного доступа (НСД). Компания выбирает одно из имеющихся средств защиты, которые по-разному влияют на снижение вероятности НСД на каждом уровне.

Средство А: Установка системы многофакторной аутентификации:
Низкий уровень доступа – снижение на 50%;
Средний уровень доступа – снижение на 40%;
Высокий уровень доступа – снижение на 30%.

Средство Б: Мониторинг и анализ поведения пользователей:
Низкий уровень доступа – снижение на 30%;
Средний уровень доступа – снижение на 50%;
Высокий уровень доступа – снижение на 40%.

Средство В: Ограничение доступа по времени и геопозиции:
Низкий уровень доступа – снижение на 40%;
Средний уровень доступа – снижение на 30%;
Высокий уровень доступа – снижение на 50%.

Средство Г: Поведенческий анализ действий пользователей:
Низкий уровень доступа – снижение на 30%;
Средний уровень доступа – снижение на 40%;
Высокий уровень доступа – снижение на 40%.

Определите лучшее средство защиты, показывающее наименьшую среднюю вероятность НСД для всей системы и всех пользователей, если изначальная вероятность НСД:
для низкого уровня доступа – 4%;
для среднего уровня доступа – 6%;
для высокого уровня доступа – 8%.

Ответ: Б *(выбрать)*

Вариант 2

В компании используется система с тремя уровнями доступа: низкий (**100** сотрудников), средний (**100** сотрудников) и высокий (**200** сотрудников). Каждый уровень характеризуется различной вероятностью несанкционированного доступа (НСД). Компания выбирает одно из имеющихся средств защиты, которые по-разному влияют на снижение вероятности НСД на каждом уровне.

Средство А: Установка системы многофакторной аутентификации:
Низкий уровень доступа – снижение на 50%;
Средний уровень доступа – снижение на 40%;
Высокий уровень доступа – снижение на 30%.

Средство Б: Мониторинг и анализ поведения пользователей:
Низкий уровень доступа – снижение на 30%;
Средний уровень доступа – снижение на 50%;
Высокий уровень доступа – снижение на 40%.

Средство В: Ограничение доступа по времени и геопозиции:
Низкий уровень доступа – снижение на 40%;
Средний уровень доступа – снижение на 30%;
Высокий уровень доступа – снижение на 50%.
Средство Г: Поведенческий анализ действий пользователей:
Низкий уровень доступа – снижение на 40%;
Средний уровень доступа – снижение на 40%;
Высокий уровень доступа – снижение на 40%.

Определите лучшее средство защиты, показывающее наименьшую среднюю вероятность НСД для всей системы и всех пользователей, если изначальная вероятность НСД:
для низкого уровня доступа – 4%;
для среднего уровня доступа – 6%;
для высокого уровня доступа – 8%.

Ответ: В *(выбрать)*

Задача 5. Решетка Кардано

Вариант 1

Отдел информационной безопасности расследует инцидент, связанный с утечкой конфиденциальной информации в компании. Во время проверки было выявлено, что внутренний сотрудник, работающий в отделе IT, планирует осуществить DDoS-атаку на сервер компании. Для передачи информации о времени атаки этот сотрудник использовал решетку Кардано для шифрования сообщения.

В ходе расследования была перехвачена решетка Кардано и зашифрованное сообщение.

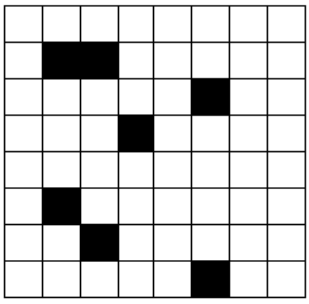
Определите время проведения сетевой атаки. В качестве ответа укажите полную строку расшифрованного сообщения.

т	т	д	ж	е	в	д	м
э	а	т	й	о	с	ч	п
л	о	д	д	б	а	э	т
з	ж	я	к	ч	ъ	п	ь
и	ь	т	ж	х	я	к	с
л	у	л	у	ж	з	к	ц
ю	и	е	в	х	д	ш	а
н	щ	о	ы	н	м	у	ь

а	д	ь	ф	й	з	и	щ
г	с	е	б	д	т	п	ф
щ	а	ж	о	ы	т	е	л
я	т	в	ь	е	я	д	о
а	з	п	с	з	ш	й	е
м	-	т	щ	э	р	е	ж
ч	ы	-	г	з	а	щ	й
х	ф	ф	ю	ъ	-	ц	к

с	й	б	ч	ц	з	ц	п
т	н	о	ш	ц	п	б	ж
й	и	ч	т	й	ч	л	-
х	ч	г	ь	р	ш	ъ	а
ш	з	г	ь	с	х	й	д
й	ю	о	я	ы	ж	-	а
з	н	-	п	н	ю	ю	ы
ы	п	б	й	о	-	т	р

й	у	я	о	ф	м	м	н
й	с	е	к	г	н	ы	ч
б	п	ю	п	с	г	д	м
о	е	н	о	и	ы	ж	щ
и	з	п	л	о	о	е	н
м	д	г	г	ъ	ф	д	з
о	а	н	с	н	е	с	й
е	р	т	й	и	я	е	я



Ответ: АТАКУЕМ СЕТЬ СЕГОДНЯ НОЧЬЮ *(вписать)*
ИЛИ
АТАКУЕМ СЕТЬ НОЧЬЮ СЕГОДНЯ

Вариант 2

Отдел информационной безопасности расследует инцидент, связанный с утечкой конфиденциальной информации в компании. Во время проверки было выявлено, что внутренний сотрудник, работающий в отделе IT, планирует осуществить DDoS-атаку на сервер компании. Для передачи информации о времени атаки этот сотрудник использовал решетку Кардано для шифрования сообщения.

В ходе расследования была перехвачена решетка Кардано и зашифрованное сообщение.

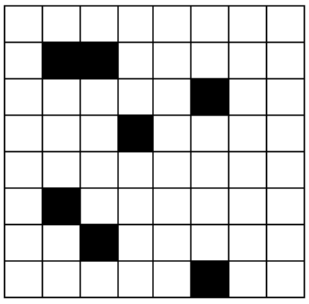
Определите время проведения сетевой атаки. В качестве ответа укажите полную строку расшифрованного сообщения.

ю	х	и	ю	ш	а	к	а
ш	а	т	п	д	с	х	ь
ю	ш	ж	ч	т	а	щ	а
я	к	ь	к	н	б	р	щ
ф	е	у	д	е	к	ъ	о
ч	у	с	ж	н	щ	п	ю
ш	й	е	ц	с	а	ы	з
г	ю	ч	л	и	м	з	ц

о	з	л	ф	р	л	н	ъ
к	с	е	ш	б	в	п	д
ж	а	ф	ц	у	т	е	н
у	у	ш	ь	е	н	л	д
п	ш	ж	а	й	м	т	ъ
м	-	ц	ш	з	р	х	щ
д	р	-	ж	з	щ	ъ	ь
й	б	ь	б	ю	-	ы	ч

л	ц	з	д	ъ	и	с	ю
к	у	т	ф	р	ю	э	п
в	и	ч	ь	й	р	о	-
а	и	у	о	о	ю	у	ъ
я	и	с	ь	я	к	з	х
п	м	щ	п	в	р	-	р
в	н	-	э	з	ю	ф	к
и	с	н	ф	д	-	е	о

ъ	к	я	к	п	н	т	ж
ж	з	а	н	ъ	н	ч	ш
к	б	з	ю	ф	в	д	д
ф	ш	з	т	ф	л	ю	а
ч	ж	а	ь	о	у	х	л
я	р	г	й	я	д	и	а
д	ь	а	ч	л	е	с	щ
д	е	м	ц	к	-	й	б



Ответ: АТАКУЕМ СЕТЬ ЗАВТРА УТРОМ *(вписать)*
ИЛИ
АТАКУЕМ СЕТЬ УТРОМ ЗАВТРА