Задания муниципального этапа по предмету «Технология»
Профиль «Информационная безопасность»
7-8 класс

Специальные задания

1. Штирлиц приехал домой и включил радио. По радо он услышал:
«Центр – Юстасу. Примите сообщение: (8, 6) (3, 3) (3, 4) (13, 2) (4, 3) (4, 4)»
После этого Штирлиц открыл книгу Шекспира на нужной странице и прочитал монолог Гамлета. Он помнил, как эти слова звучат в русском переводе:

Быть или не быть, вот в чем вопрос. Достойно ль
Смиряться под ударами судьбы,
Иль надо оказать сопротивленье
И в смертной схватке с целым морем бед
Покончить с ними? Умереть. Забыться.
И знать, что этим обрываешь цепь
Сердечных мук и тысячи лишений,
Присущих телу. Это ли не цель
Желанная? Скончаться. Сном забыться.
Уснуть… и видеть сны? Вот и ответ.
Какие сны в том смертном сне приснятся,
Когда покров земного чувства снят?
Вот в чем разгадка. Вот что удлиняет
Несчастьям нашим жизнь на столько лет.

Вспомнив эти строки, он быстро набросал сообщение из центра.

Вопросы к заданию:
1) Какое слово могла бы быть зашифрована парой чисел (12, 2)?
2) Мог ли Штирлиц получить в подобной шифровке пару чисел (12, 12)?
3) Укажите фразу, которая была передана Штирлицу.
4) Зашифруйте ответное сообщение «Достойно оказать сопротивленье».

2. Прочитайте отрывок из романа А. С. Пушкина «Евгений Онегин». Этот текст содержит скрытое сообщение.

«Мой *д*ядя самых честных пр*а*вил,
Когда не в шутку занемог,
Он у*ва*жать себя заставил
И лучше выдумать не мог.
Его пример другим наука;
Но, боже мо*й*, какая скука
С больным сиде*т*ь и д*е*нь и ночь,
Не отходя ни шагу прочь!
Какое низкое коварство
Полу*жи*вого забавл*я*т*ь*,
Ему подушки поправлять,
Печально подносить лекарство,
Вздыхать и думать про себя:

Когда же черт возьмет тебя!»

Задания:

1) Определите число букв в скрытом сообщении.
2) Определите количество вхождений буквы «В» в скрытом сообщении. Если этой буквы в сообщении нет, запишите в ответ 0.
3) Определите количество вхождений буквы «А» в скрытом сообщении. Если этой буквы в сообщении нет, запишите в ответ 0.
4) Восстановите скрытое сообщение. Впишите его без пробелов и знаков препинания.

3. Вася получил записку от Вити, который при передаче записки сказал ему: «Запомни лозунг – ПОБЕДЯ».
Текст записки: МНЁФЛДЁ Б МПНЗ

Задания:

1) Определите вид шифра.
2) Определите, какую букву открытого текста заменяет буква «З» в шифротексте
3) Определите, какой буквой в шифротексте заменяется буква «К» открытого текста
4) Определите, есть ли в открытом тексте слово «норка». Укажите номер символа (без учета пробелов и знаков препинания – считайте только буквы), с которого оно начинается. Если такого слова в открытом тексте нет, укажите в ответе 0
5) Определите, какую букву открытого текста может заменять буква «Б» в произвольном шифротексте
6) Приведите зашифрованное сообщение
7) Зашифруйте ответное сообщение «Я согласен»

Кейс-задание

Перед Вами политика информационной безопасности одной компании. Укажите ошибочные пункты и/или подпункты этой Политики.

Политика информационной безопасности Компании

1. Информационные активы, информационные системы/компоненты ИТ–инфраструктуры применяются для выполнения бизнес–процессов и достижения целей деятельности Группы. Допускается использование информационных активов, информационных систем/компонентов ИТ – инфраструктуры в личных целях.
2. Пользователям запрещается загружать, публиковать или распространять информацию, которая, содержит угрозы, оскорбления, клевету на других лиц, вводит в заблуждение, подрывает или нарушает репутацию Компании или конфиденциальность частной жизни иных лиц, а также иную информацию, запрещенную к распространению на территории Российской Федерации в соответствии с действующим законодательством.

3. Для управления рисками информационной безопасности применяются предупредительные, обнаруживающие, корректирующие и компенсирующие организационно–технические меры информационной безопасности.
4. Пользователи обязаны обеспечивать физическую защиту предоставленных им технических средств в моменты своего отсутствия (например, в помещениях Компании в нерабочее время, в публичных местах или неохраняемых помещениях при удаленной работе) путем применения разумно обоснованных и доступных пользователю мер для предотвращения повреждения, утери/кражи технических средств (включая мобильные устройства).
5. Пользователям запрещается использование специализированных устройств, позволяющих получить доступ к сети Интернет (Yota, GPRS-модемы, подключать мобильный телефон в качестве модема).
6. Пользователям разрешается использовать ресурсы и устройства, не принадлежащие Компании для обработки и хранения информации Компании, в том числе:
    - съемные носители информации;
    - технические средства (ноутбуки, мобильные телефоны);
    - персональные облачные хранилища (например, Google Drive, Dropbox, Yandex Disk, Облако Mail.ru).
7. Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий. Должны быть рассмотрены следующие этапы:

    7.2. должны быть идентифицированы привилегии доступа, связанные с каждым системным продуктом, например, с операционной системой, системой управления базой данных и каждым приложением, а также пользователи, которым они должны быть предоставлены;

    7.1. привилегии должны предоставляться пользователям на весь срок трудовой деятельности с максимально возможными правами доступа
8. Пользователи, покидая свои рабочие места, обязаны блокировать компьютеры, ноутбуки, мобильные устройства средствами операционных систем или производить выключение питания указанных устройств.
9. Пользователям запрещается раскрывать свои пароли другим лицам или использовать учетные записи других лиц для доступа к информации Компании.
10. Уничтожение бумажных носителей информации должно осуществляться способом, препятствующим возможность их восстановления (например, с использованием шредеров или корзин для уничтожения документов).
11. Все Пользователи, участвующие в обработке информации, несут ответственность за соблюдение установленных правил работы с информацией и недопущение ее несанкционированного использования и распространения.
12. Пароли – средство проверки личности пользователя для доступа к информационным системам или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

12.1. пароли должны храниться в электронном виде только в защищенной форме;
12.2. все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;
12.3. необходимо использовать только пароль, официально выданный администратором системы
12.4. необходимо избегать передачи паролей с использованием третьих лиц или не зашифрованной электронной почтой;
12.5. Для сброса паролей к учетным данным пользователя необходимо позвонить на номер телефона ответственной IT службы Компании и сообщить номер карты-пропуска, в ответ работник сообщит новый, временный пароль.