

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ
РЕГИОНАЛЬНЫЙ ЭТАП
ТЕОРЕТИЧЕСКИЙ ТУР

9 класс

Профиль «Информационная безопасность»

Уважаемый участник олимпиады!

Вам предстоит выполнить теоретические и тестовые задания.

Время выполнения заданий теоретического тура 2 академических часа (90 минут).

Выполнение тестовых заданий целесообразно организовать следующим образом:

- не спеша, внимательно прочитайте тестовое задание;
- обратите внимание, что задания, в которых варианты ответа являются продолжением текста задания, предполагают единственный ответ; задания, в которых имеется инструкция «укажите все», предполагает несколько верных ответов;
- определите, какой (или какие) из предложенных вариантов ответа наиболее верный и полный;
- напишите букву (или набор букв), соответствующую выбранному Вами ответу;
- продолжайте, таким образом, работу до завершения выполнения тестовых заданий;
- после выполнения всех предложенных заданий еще раз удостоверьтесь в правильности ваших ответов;
- если потребуется корректировка выбранного Вами варианта ответа, то неправильный вариант ответа зачеркните крестиком, и рядом напишите новый.

Выполнение теоретических (письменных, творческих) заданий целесообразно организовать следующим образом:

- не спеша, внимательно прочитайте задание и определите, наиболее верный и полный ответ;
- отвечая на теоретический вопрос, обдумайте и сформулируйте конкретный ответ только на поставленный вопрос;
- если Вы выполняете задание, связанное с заполнением таблицы или схемы, не старайтесь детализировать информацию, вписывайте только те сведения или данные, которые указаны в вопросе;
- особое внимание обратите на задания, в выполнении которых требуется выразить Ваше мнение с учетом анализа ситуации или поставленной проблемы. Внимательно и вдумчиво определите смысл вопроса и логику ответа (последовательность и точность изложения). Отвечая на вопрос, предлагайте свой вариант решения проблемы, при этом ответ должен быть кратким, но содержать необходимую информацию;
- после выполнения всех предложенных заданий еще раз удостоверьтесь в правильности выбранных Вами ответов и решений.

Предупреждаем Вас, что:

- при оценке тестовых заданий, где необходимо определить один правильный ответ, 0 баллов выставляется за неверный ответ и в случае, если участником отмечены несколько ответов (в том числе правильный), или все ответы;
- при оценке тестовых заданий, где необходимо определить все правильные ответы, 0 баллов выставляется, если участником отмечены неверные ответы, большее количество ответов, чем предусмотрено в задании (в том числе правильные ответы) или все ответы.

Задание теоретического тура считается выполненным, если Вы вовремя сдаете его членам жюри.

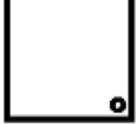
Максимальная оценка – 25 баллов (из них кейс-задание оценивается в 5 баллов).

Общая часть

1. Верны ли следующие утверждения?

Утверждения	да / нет
1. Проектировщик личной безопасности – это специалист, оценивающий и прогнозирующий жизнь человека с точки зрения всех возможных рисков (от генетической предрасположенности к определенным заболеваниям до вероятности аварий и того, что человек станет жертвой преступления) и их предотвращения.	
2. Оценщик интеллектуальной собственности определяет стоимость нематериальных активов, таких как идеи, бизнес-модели, изобретения, материальные и социальные технологии и пр.	
3. Экопроповедником называют специалиста, проводящего комплексную оценку соответствия инвестиций критериям и оценивающего кредитные риски с точки зрения экологического воздействия.	
4. Специалиста по эффективному использованию и распределению личного и общего времени называют тайм-брокером.	

2. Соотнесите условные графические обозначения на видах сверху и на планах элементов внутренних систем водоснабжения и канализации с их названиями.

				
1	2	3	4	5

- а. ванна
- б. поддон душевой
- в. раковина
- г. унитаз
- д. фонтанчик питьевой

3. Для выработки электрического тока на электростанциях необходимы энергоресурсы. Выберите из предложенного перечня пример вторичного энергоносителя.

- а. уголь
- б. энергия Солнца
- в. мазут
- г. природный газ

4. Обычная лампа накаливания потребляет электроэнергию 100 Вт·ч, а энергосберегающая лампа – 12 Вт·ч. Сколько рублей в месяц составит экономия от снижения потребления электроэнергии при замене простой лампы накаливания на энергосберегающую, если лампа будет работать 8 ч в сутки? Стоимость электроэнергии в квартире с электрической плитой при однотарифном счетчике составляет 4 рубля 30 копеек за 1 кВт·ч. Считаем, что в месяце 30 дней.

5. Как называется направление биотехнологии, включающее в себя совокупность приёмов, методов и технологий создания новых генетических структур, входящих в состав каждой клетки живого организма, выделения генов из организма, осуществления манипуляций с генами и введения их в другие организмы?

Специальная часть

6. Опасаясь подслушивания в собственном офисе, бизнесмен предложил своему поставщику обсудить детали предстоящей сделки на случайно выбранной скамейке в сквере. Неожиданно его внимание привлек находящийся на другой стороне многополосной дороги человек, который, как казалось, наблюдал за встречами. Опасения бизнесмена, что этот человек мог подслушать разговор, являются в такой ситуации

- а. обоснованными, так как нарушитель может использовать для подслушивания направленный микрофон;
- б. необоснованными, так как большое расстояние не позволит осуществить подслушивание;
- в. обоснованными, так как нарушитель может использовать для подслушивания электронный стетоскоп;
- г. необоснованными, так как в людном месте подслушать разговор было бы можно лишь предварительно разместив скрытое устройство, но из-за случайного выбора места это исключено.

7. Еще раз проанализировав возможности нарушителя, абоненты пришли к выводу, что встреча в общественном месте не обеспечивает необходимой безопасности. В качестве подходящего места встречи они решили воспользоваться специальной переговорной комнатой в офисе. Эта комната оборудована устройствами, создающими вибрации на оконных стеклах, если в ней происходят переговоры. Таким образом планируется предотвратить перехват информации при помощи:

- а. электронного стетоскопа
- б. направленного микрофона
- в. бинокля
- г. ненаправленного микрофона
- д. лазерного стетоскопа

8. Цифровые водяные знаки используют для:

- а. защиты документов и ценных бумаг от подделки;
- б. передачи конфиденциальной информации;
- в. защиты авторства цифровых произведений;
- г. контроля неизменности передаваемых данных датчиков

9. Сотрудник организации обратился к администратору безопасности, заметив некоторые признаки возможного заражения рабочего ноутбука вредоносным программным обеспечением. Стремясь оценить, чем могло произойти заражение, администратор попросил владельца зараженного устройства перечислить действия в течение рабочего дня.

В ответ сотрудник сообщил, что утром открыл браузер и посетил сайт организации, после чего загрузил через почтовый клиент свежие письма, которые не содержали вложенных файлов. При этом одно из писем гласило, что по распоряжению руководства на переносные устройства требуется установить программу, позволяющую пользователям постоянно быть подключенными к беспроводной сети организации без необходимости повторной авторизации. Сотрудник ввел в адресной строке указанный адрес и, попав в служебную область сайта организации, решил загрузить данный файл, однако вовремя заметил, что указанный адрес отличается от адреса сайта организации одной буквой, после чего он немедленно покинул сайт. Далее он обратился к своему коллеге с запросом о том, существует ли указанная в письме программа, на что получил утвердительный ответ и предложение передать ее на внешнем носителе. Устройство коллеги было подключено, программа скопирована, однако еще до ее запуска пользователь решил пойти на обед. Вернувшись, он решил первым делом проверить почту, в процессе чего и заподозрил возможное заражение.

Оценив ответ пользователя, администратор безопасности пришел к выводу, что в рамках описанных событий устройство, наиболее вероятно, было заражено

- а. троянской программой
- б. вирусом
- в. руткитом
- г. бэкдором

10. Вспомнив подробности дня, тот же сотрудник сообщил администратору безопасности, что во время обеденного перерыва он отправился в ближайшее кафе, где получил телефонный звонок от своего коллеги, просившего немедленно ответить на письмо на электронную почту. Для проверки почты рабочий ноутбук потребовалось подключить к беспроводной сети кафе, что и было успешно сделано. Просмотрев почту и ответив на указанное письмо, сотрудник вернулся в офис, где и продолжил работу.

Учтя новые подробности, администратор безопасности добавил к вероятным категориям вредоносной программы, которой произошло заражение,

- а. руткит
- б. троянскую программу
- в. спуфер
- г. сетевого червя

11. Сотруднику службы информационной безопасности банка поручено разработать должностные инструкции для работников финансового отдела. Наименее подверженным угрозам, с точки зрения информационной безопасности, будет решение составлять должностные инструкции таким образом, чтобы каждый сотрудник

- а. имел повседневные обязанности, составляющие часть больших задач, и полномочия в системе, жестко необходимые для выполнения таких обязанностей
- б. мог полностью выполнять все задачи, связанные с его деятельностью
- в. имел полномочия в системе, которые могут ему потребоваться для исполнения должностных обязанностей в любой ситуации.
- г. мог замещать сотрудников, реализующих смежные с его обязанностями операции, и имел для этого необходимые полномочия в системе.

12. Системы асимметричного шифрования позволяют абонентам:

- а. обойтись без необходимости хранить ключи в секрете;
- б. обеспечить абсолютную секретность сообщений;
- в. обойтись без необходимости передавать секретные ключи;
- г. гарантировать невозможность получения ключа путём анализа шифртекстов.

13. Вставьте пропущенный термин в следующем утверждении:

Приводя сервер с базой данных в состояние «отказ в обслуживании», нарушитель реализует угрозу нарушения _____ информации.

14. Вставьте пропущенный термин в следующем утверждении:

Заменяя в базе данных контактные данные пользователей на подложные, нарушитель реализует угрозу нарушения _____ информации.

15. При обработке информации, содержащей коммерческую тайну, сотрудниками организации существует угроза ее передачи посторонним лицам (утечка информации). Для пересылки такой информации по электронной почте недобросовестные сотрудники могут встраивать информацию в не вызывающие подозрения файлы – например, фотографии или звуковые записи. Не желая явно запрещать передачу таких файлов, но стремясь разрушить возможные стегоконтейнеры, администратор безопасности может

- а. настроить корпоративный почтовый сервер так, чтобы вложения пересылались отдельным письмом
- б. сохранять такие вложения, изменив качество изображения или звука
- в. принудительно помещать вложения в облачное хранилище, а в письмо помещать ссылку на них
- г. добавлять к вложениям блок данных, содержащих сведения о компании

16. Руководитель службы безопасности крупной организации готовится к проведению собрания, на котором должны обсуждаться сведения, составляющие коммерческую тайну. По полученной им информации, конкуренты планируют использовать для перехвата устного доклада электронный стетоскоп. Для устранения такой угрозы ему следует поручить сотрудникам

- а. закрыть окна в конференц-зале шторами,
- б. поместить на инженерные конструкции в конференц-зале источники вибрации,
- в. удостовериться в отсутствии силовых и информационных кабелей вне специальных коробов,
- г. поместить на стекла окон в конференц-зале источники вибрации.

17. Для передачи ключа симметричного шифра абоненты стремятся выбрать место, как можно менее подверженное угрозе перехвата информации. Рассмотрев ряд вариантов, они решили провести встречу в отдельном зале кафе, отгороженном занавесками, сильно ослабляющими звуки разговора. Таким образом они стремятся реализовать прием защиты от утечки речевой информации, известный как

- а. экранирование
- б. зашумление
- в. изолирование
- г. блокирование
- д. рассеивание

18. Прочтя книгу по криптографии, Антон узнал о существовании функций хэширования и решил написать свою собственную программу, которая бы преобразовывала любую поданную на вход информацию – файл или строку текста – в строку длиной 1024 байт. Когда он показал программу своей однокласснице, та попросила день на тестирование программы, после чего заявила, что функция хэширования, которую она реализует, получилась слабой и для криптографических целей применять ее нельзя. Среди аргументов, которые она привела, могло быть то, что

- а. программа работает слишком медленно,
- б. алгоритм преобразования входного значения в выходную строку не содержит секретных параметров
- в. по полученному выходному значению можно установить, текст или файл был подан на вход
- г. число раундов обработки входной информации слишком мало

19. В шифре, известном как шифр Виженера, для определения символа замены буквы открытого текста на каждом шаге зашифрования и расшифрования используется секретный ключ (пароль). Алфавиты замены построены с последовательными значениями сдвига — от 0 до 32 и выбираются на основе букв ключа. Их удобно представить в виде таблицы:

	А	Б	В	Г	Д	Е	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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
Ё	Ё	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	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	Ё
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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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	Ё	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

Буква открытого текста всегда определяет столбец на основе заголовочной строки, а строка определяется соответствующей буквой ключа на основе заголовочного столбца. Например, строка из 5 букв «А» при использовании ключа «ШЕСТЬ» будет зашифрована буквами алфавита, стоящими в первом столбце (потому что в заголовочной строке «А» стоит на первой позиции) в строках, в заголовочном столбце которых стоят буквы «Ш», «Е», «С», «Т» и «Ь» соответственно. Нетрудно удостовериться, что шифртекст будет совпадать с ключом – «ШЕСТЬ».

Таким шифром с каким-то (неизвестным) ключом длиной 7 букв зашифрован текст: «С талантом человеку не пропасть. Соедините только в каждой

роли воображение, чувство, ум и страсть, и юмора достаточную долю.». Определите, какой из шифртекстов мог быть при этом получен (пробелы и знаки препинания остались без изменений – зашифрованы только буквы).

а. т юеэтшыпш ьцющкёцш яч ьщпыегеж. ьприъауыё юуэохч г цешщт сьрь фщчвьешчшеё, гшудэкп, яс ь дэщбэчн, ы ихпье хбьыбюуиаюж еьрп.

б. т юеэтшыпш ьцющкёцш яч ьщпыегеж. ьприъауыё юуэохч г цешщт сьрь фщчвьешчшеё, гшудэкп, яс ь дэщбэчн, ы ихпье хбьыбюуиаюж еьрп.

в. т юеэтшыпш ьцющкёцш яч ьщпыегеж. ьприъауыё юуэохч г цешщт сьрь фщчвьешчшеё, гшудэкп, яс ь дэщбэчн, ы ихпье хбьыбюуиаюж еьрп.

г. т юеэтшыпш ьцющкёцш яч ьщпыегеж. ьприъауыё юуэохч г цешщт сьрь фщчвьешчшеё, гшудэкп, яс ь дэщбэчн, ы ихпье хбьыбюуиаюж еьрп.

20. Шифр, известный как шифр Плейфера, заключается в замене пар символов, стоящих один за другим, на пары символов того же алфавита. Замена происходит по следующему принципу: символы алфавита вносятся в прямоугольную таблицу в случайном порядке, например, так:

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

Далее в таблице находятся буквы шифруемой пары.

Если они стоят в одной строке, то для каждой из них берется ее сосед справа. Для буквы в крайнем правом столбце соседом справа будет считаться буква той же строки из крайнего левого столбца. Совпадающие буквы считаются

стоящими в одной строке. Например, «ОД» зашифровывается парой «ВШ» (для каждой буквы сосед берется независимо), «ЛЛ» – «ДД», «ОН» – «ВО».

Если они стоят в одном столбце, то для каждой из них берется ее сосед снизу. Для буквы из нижней строки соседом снизу считается буква того же столбца из верхней строки. Например, «УВ» – «ЙФ», «НИ» – «ЧЦ».

Если они стоят в разных строках и столбцах, то для определения букв замены требуется мысленно расположить эти буквы в противоположных углах прямоугольника, так, чтобы соединяющий их отрезок являлся его диагональю. Буквы замены должны находиться в других углах прямоугольника, а записать их нужно, двигая по другой диагонали в противоположном направлении. Например, «ЗУ» – «ГА», «ОТ» – «ШЦ».

Таким шифром с некоторым (неизвестным) заполнением таблицы был зашифрован текст:

Кто к тайнам жизни рвется мыслью каждой, в своей душе находит их родник

или без пробелов и знаков препинания:

КТОКТАЙНАМЖИЗНИРВЕТСЯМЫСЛЬЮКАЖДОЙВСВОЕЙДУШЕНАХОДИ
ТИХРОДНИК

В результате был получен следующий шифртекст:

ДЧЪТЗОУПЭЗВПЧУЯВИВЫДИТГЕЮАЖЪЪШТЦМИЕФЭЫБМЗУГИЩШТЦЯ
МНВЯЫБЧПМ

Определите заполнение таблицы, на основе которой было осуществлено зашифрование. В этой таблице пары символов «Е» и «Ё», «И» и «Й», «Ъ» и «Ь» объединены и занимают по одной ячейке. Для зашифрования берется первый символ из пары. Известно положение одной из букв – «У».

		у			

21. Полина – стажер в отделе продаж в компании «КровМетСтрой». Для доступа к рабочей среде на корпоративном компьютере она должна ввести пароль, состоящий из заглавных букв русского алфавита (33 символа) и цифр от 0 до 9. При этом 2 одинаковых символа не могут идти подряд. Так как пароль требуется менять ежемесячно, то для простоты запоминания Полина решила использовать пароли следующего вида: сначала идет имя ее собаки – «ЁЛКА», а затем – набор, содержащий от 2 до 4 цифр.

А) Определите, сколько различных паролей она может составить. Изложите кратко принцип подсчета.

Василий работает в одном офисе с Полиной, он занимает руководящую должность в отделе контроля качества продукции. Однако основная его деятельность — это сбор и передача данных компании-конкуренту. Василий имеет доступ к той же рабочей среде и знает, что пароль, состоит из заглавных букв русского алфавита (33 символа) и цифр от 0 до 9, при этом 2 одинаковых символа не могут идти подряд. Он наблюдал за Полиной в течение трех месяцев и выявил закономерности в структуре пароля. Теперь он знает, что ее пароли состоят из слова «ЁЛКА» и нескольких цифр после. Он написал программу, которая перебирает пароли: сначала содержащие только одну цифру, потом – две, затем – три и т. д. Для каждого из случаев он перебирает числа от меньшего к большему (например, перебирая пароли с пятью цифрами, он сначала рассмотрит пароль «ЁЛКА01010», потом «ЁЛКА01012», потом «ЁЛКА01013» и т. д., последним будет пароль «ЁЛКА98989»).

Полученную программу он загрузил на удаленный сервер. После этого Василий незаметно подключил к компьютеру Полины внешний носитель информации, когда та ушла на обед. После подключения устройства к компьютеру с удаленного сервера за минуту была загружена программа перебора паролей. Пароли перебираются со скоростью 1 пароль в секунду. После входа в рабочую среду другая программа с носителя устанавливается на компьютер, и в течение двух минут выгружает из рабочей системы необходимые Василию данные на удаленный сервер.

Установите следующие обстоятельства:

Б) Успеет ли Василий реализовать спланированное действие за 25 минут после подключения съемного носителя информации, если текущий пароль «ЁЛКА0510»? Приведите решение.

В) Наличие какой модели или каких моделей разграничения доступа в рабочей среде компании «КровМетСтрой» можно предположить на основе описанной ситуации?

Г) Рассмотрим ситуацию, в которой Василий вместо локального доступа к устройству Полины предпринял бы успешную попытку заражения его вредоносным программным обеспечением по сети. Какие типы вредоносных программ по реализуемым ими функциям ему бы в таком случае потребовались для скачивания программы перебора паролей и отправки интересующей его информации в некоторый момент по его запросу?