

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ
РЕГИОНАЛЬНЫЙ ЭТАП
ТЕОРЕТИЧЕСКИЙ ТУР

11 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.

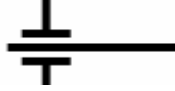
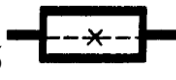
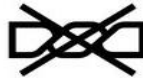






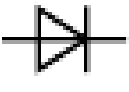
Максимальная оценка – 25 баллов (из них кейс-задание оценивается в 5 баллов).

Общая часть.

1. Установите соответствие между элементами правого и левого столбцов.

1.	Внутриличностный процесс, развитие которого проявляется в появлении новообразований в представлениях учащихся о собственном профессиональном становлении и изменении осознанности и активности в отношении процесса выбора будущих вариантов профессионального труда	а	Профессиональная ориентация
2.	Обобщенное понятие одного из компонентов общечеловеческой культуры, проявляющегося в форме заботы общества о профессиональном становлении подрастающего поколения, поддержки и развития природных дарований, а также проведения комплекса специальных мер содействия человеку в профессиональном самоопределении	б	Профессиональная консультация
3.	Оказание помощи человеку в профессиональном самоопределении с целью принятия осознанного решения о выборе профессионального пути с учетом его психологических особенностей и возможностей, а также потребностей общества	в	Профессиональное самоопределение
4.	Профессиональное испытание, моделирующее элементы конкретного вида профессиональной деятельности	г	Профессиональная проба

2. Соотнесите условные графические обозначения, используемые в современном обществе, с областью их применения.

а 	б 	в 	г 	д 
е 	ж 	з 	и 	к 

1. электротехнические схемы
2. кинематические схемы
3. уход за одеждой

3. Передача электроэнергии на большие расстояния является важнейшей технической задачей в электротехнике. Российские ученые второй половины XIX века одержали крупнейшую победу, став признанными лидерами в области электротехники. Что они изобрели?

- а. радиосвязь
- б. теория электромагнитного поля
- в. трансформатор
- г. все ответы верные

4. Два брата Виктор и Анатолий сделали вклады на год в двух разных банках. Виктор – под 9 % годовых с потерей процентов в случае досрочного закрытия вклада, а Анатолий – под 7 % годовых, но с сохранением процентов в случае досрочного закрытия. Через год при закрытии своих вкладов они получили равные суммы денег. Сколько денег положил в банк каждый из братьев, если общая сумма их вкладов была равна 250000 рублей?

5. Как называется система доставки материальных предметов, веществ и продуктов из одной точки в другую по оптимальному маршруту?

Специальная часть.

6. Моделируя возможные угрозы безопасности информации, администратор безопасности рассматривает возможность того, что сотрудники, осуществляющие уборку помещений, могут случайно повредить оборудование в серверной- например, пролить воду, уронить, нанести удар своим инвентарем. Укажите все обстоятельства, которые могут считаться уязвимостями относительно описанной угрозы.

- а. Возможное небрежное отношение сотрудников, осуществляющих уборку, к находящимся в помещении объектам
- б. Выход из строя некоторых устройств при попадании на них воды, падении, физическом воздействии
- в. Проведение уборки в серверной сотрудниками, не имеющими отношения к работе оборудования
- г. Использование жидкостей и громоздкого инвентаря в процессе уборки
- д. Стремление сотрудников, проводящих уборку, завершить работу как можно быстрее
- е. Неготовность системных администраторов включить уборку в серверной в свои обязанности

7. При моделировании угроз информационной безопасности рассматривают возможные сценарии реализации таких угроз. Сценарий традиционно делится на

возможные тактики, условно соответствующие этапам реализации атаки или решаемым нарушителем тактическим задачам. Реализовать некоторую тактику (то есть решить тактическую задачу) нарушитель может одним из ряда конкретных способов, традиционно называемых техниками. Соотнесите примеры применяемых нарушителями техник с соответствующими им тактиками.

- а. Получение первоначального доступа к компонентам систем и сетей
 - б. Закрепление (сохранение доступа) в системе или сети
 - в. Соккрытие действий и применяемых при этом средств от обнаружения
-
- 1. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей
 - 2. Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты
 - 3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы
 - 4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию
 - 5. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением
 - 6. Создание скрытых файлов, скрытых учетных записей

8. Для контроля доступа к особо важной базе данных организации принято решение организовать трехфакторную аутентификацию. Рассмотрев несколько предложений от своих сотрудников, руководитель отдела информационной безопасности решил, что поставленному заданию будет соответствовать система, в которой пользователю для прохождения аутентификации потребуется

- а. предъявить пропуск охраннику,
- б. отсканировать отпечаток пальца и оставить подпись в специальном журнале;
- в. отсканировать смарт-карту, ввести пароль и решить задание (капчу);

- г. отсканировать смарт-карту, ввести пароль и прочесть в микрофон фразу с экрана устройства
- д. ввести личный номер пользователя, пароль и пройти распознавание лица.

9. Планируя систему информационной безопасности банка, руководство принимает решение о выборе наиболее соответствующей ее структуре модели разграничения доступа. Банк включает сотрудников, которые обслуживают запросы клиентов, специалистов кредитного отдела, принимающих решения по выдаче кредитов, аналитиков, разрабатывающих условия вкладов и еще ряд аналогично организованных отделов.

Обязательным требованием руководства является то, что руководители каждого из отделов не должны иметь доступ к рабочим материалам других отделов, однако полностью контролировать возглавляемые ими подразделения, в каждом из которых от нескольких до нескольких десятков сотрудников. При этом в отделах имеются несколько уровней должностей для сотрудников, так что наиболее успешные сотрудники повышаются в должности, а наименее успешные регулярно переводятся в другие подразделения или увольняются. Для описанной организации наиболее предпочтительной является

- а. дискреционная модель;
- б. мандатная модель;
- в. ролевая модель;
- г. модель, использующая уровни секретности объектов и уровни допуска субъектов;

10. При использовании в некоторых шифрах замены соответствующего определенным требованиям ключа можно получить шифр, не поддающемуся взлому полным перебором ключей. Такой шифр известен как идеальный или абсолютно стойкий. Одной из причин, по которым такие шифры не используются повсеместно в настоящее время, является

- а. необходимость передачи абонентам ключей, длина которых в несколько раз превышает сообщение, которое требуется передать;
- б. высокая сложность программной реализации таких шифров;
- в. низкая скорость зашифрования и расшифрования сообщений такими шифрами;
- г. необходимость выработки случайных последовательностей символов, длиной не уступающих длине передаваемых сообщений ;

11. В ходе работы над проектом Анне потребовалось создать собственную реализацию функции хэширования. Написав программу, она предусмотрела несколько возможных вариантов преобразования входных данных в выходную строку. Далее она отдала программу для тестирования работающему с ней над одним проектом Борису, попросив его выбрать наилучшую реализацию. Для тестирования Борис подал на вход тестовый файл, записал полученную строку, после чего удалил последний символ файла и снова обработал его программой. Сравнивая выходные значения, он счел наиболее соответствующим требованиям к функциям хэширования вариант, для которого получились строки:

- а. 0L/RgNC40LzQt dGA и 0L/RgNC40LzQt dGA
- б. 266f263f0211048c и 529057b143e93468
- в. e3b0c44298fc1c14 и e3b0c44298fc1c1
- г. e58f1e8c55fa105b и e58f1e8c55ga105b

12. Сотрудник организации обратился к администратору безопасности, заметив некоторые признаки возможного заражения рабочего ноутбука вредоносным программным обеспечением. Запустив проверку антивирусным средством, администратор безопасности определил, что на устройстве присутствует программа, относящаяся к категории вирусов. Стремясь определить, в какой момент могло произойти заражение, администратор попросил владельца зараженного устройства перечислить действия в течение рабочего дня. Проанализировав ответ, он пришел к выводу, что заражение могло произойти в момент

- а. подключения внешнего носителя
- б. проверки писем электронной почты
- в. загрузки и запуска файла из сети Интернет
- г. отправки письма по электронной почте

13. Одним из способов обнаружения вредоносных программ является анализ поведения запускаемых в системе программ. К его недостаткам можно отнести

- а. низкая доля обнаруженных вредоносных программ
- б. большое количество ложных срабатываний
- в. зависимость от обновления вирусных баз
- г. неспособность обнаруживать новые вредоносные программы

14. Администратор безопасности произвел настройки системы предотвращения утечки информации (DLP-системы). Для этого он снабдил все соответствующие документы грифами “Коммерческая тайна”, на каждой странице таких файлов добавил соответствующие колонтитулы, а также вычислил и внес в систему контрольные суммы файлов в неизменном виде, а также с удаленными титульным листом и колонтитулами – вместе и отдельно. Для обхода такой защиты недобросовестный сотрудник, стремящийся отправить договор, с которым он работает, на свой личный адрес электронной почты с корпоративного адреса, может

- а. удалить титульный лист документа и колонтитулы со страниц
- б. удалить титульный лист документа и колонтитулы, а также постараться удалить слова “договор” и все сочетания с ним из текста документа
- в. сохранить документ в другом формате.
- г. используя слабости алгоритма выработки контрольной суммы, удалить метки секретности и колонтитулы, а затем доработать текст файла так, чтобы значение контрольной суммы совпадало со значением исходного файла.

15. Расследуя выявленный факт утечки информации, составляющей коммерческую тайну, администратор безопасности установил, что для маскировки своих действий нарушитель удалял из пересылаемых файлов титульный лист с названием документа и реквизитами организации, а также вставлял случайным образом произвольные слова на каждую страницу документа. Для предотвращения подобной утечки в дальнейшем принято решение внедрить систему предотвращения утечки информации, определяющую факт утечки информации на основе

- а. грифа “Коммерческая тайна” на титульном листе документа и контрольной суммы файла
- б. контрольной суммы файла, определенной для исходного файла и некоторых сценариев модификации файла
- в. обнаружения в тексте документа определенных слов и словосочетаний, характерных для документов, содержащих сведения, составляющие коммерческую тайну
- г. контрольных сумм содержимого отдельных страниц документа, позволяющих обнаруживать передачу даже отдельной страницы

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 лазерный стетоскоп. Для устранения такой угрозы ему следует поручить сотрудникам

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

17. Абонентам, использующим симметричный шифр, требуется согласовать общий секретный ключ. Оценив возможности потенциальных нарушителей, они рассматривают угрозу перехвата звуковой информации как актуальную, поэтому не хотели бы произносить его вслух. Вместо этого один из них предлагает продемонстрировать ключ остальным на листе бумаги в отдельной переговорной комнате в офисе, не имеющей окон, отключив основное освещение и используя лишь подсветку фонариком. По мнению другого абонента такой вариант тоже не обеспечивает безопасности, поскольку информация все равно может быть перехвачена нарушителем, даже не находящимся в том же здании, если ему удастся использовать:

- а. прибор ночного видения
- б. тепловизор
- в. систему теленаблюдения
- г. световод
- д. лазерный стетоскоп

18. Начальник службы информационной безопасности готовит помещение для проведения совещания, на котором будут обсуждаться сведения, составляющие коммерческую тайну. В процессе обследования комнаты он обнаружил в нем извещатель пожарной сигнализации, а также отметил, что присутствуют окна и батарея центрального отопления. Соотнесите выделенные им объекты с устройствами, которые потенциальный нарушитель мог бы использовать для перехвата речевой информации, распространяющейся по этим объектам.

1. Батарея отопления
2. Окна
3. Силовые кабели

- а. Лазерный стетоскоп
- б. Электронный стетоскоп
- в. Низкочастотный усилитель

19. Шифр, известный как “Два квадрата”, заключается в замене пар символов, стоящих один за другим, на пары символов того же алфавита. Замена происходит по следующему принципу: символы алфавита вносятся в две квадратные или прямоугольные таблицы 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

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

Далее в таблицах отыскиваются символы шифруемой пары: первая буква отыскивается в левой таблице, вторая – в правой. Зашифрование пары символов происходит по следующим правилам:

Если они стоят в разных строках и столбцах, то для определения символов замены требуется мысленно расположить символы открытого текста в противоположных углах прямоугольника, так, чтобы соединяющий их отрезок являлся его диагональю. Символы замены должны находиться в других углах прямоугольника, а записать их нужно, двигаясь по другой диагонали из правой таблицы в левую. Например, «ЗУ» – «ВЩ», «ОТ» – «.Е».

Если символы шифруемой пары стоят в одной строке, то для замены берется пара символов, расположенных в той же строке, но номера столбцов обмениваются местами. То есть, если первая буква стоит в столбце №2 левой таблицы, а вторая – в столбце №4 правой таблицы, то для замены нужно взять

буквы той же строки из столбца №2 правой таблицы и столбца №4 левой таблицы. Например, «СВ» зашифровывается парой «ЛБ», «ЗЛ» – «ОС», «УМ» – «ЯП».

Если координаты символов шифруемой пары в соответствующих таблицах совпадают, то для получения пары замены символы обмениваются местами. Например, «ЗО» – «ОЗ», «ЖИ» – «ИЖ».

Таким шифром с некоторым (неизвестным) заполнением таблицы был зашифрован текст: «Луна тихо смотрела на беспокойную, но покорную ей стихию». Обратите внимание, что символы пробела (или «_»), точки и запятой являются полноправными символами алфавита, учитываемыми в открытом тексте и используемыми в шифртексте. Определите, какой из шифртекстов мог быть при этом получен.

- а. ЫВЮХАЩПЁЪЧЕЯЛЧШПЁДМХШЗШЙРЫЬКФЧДЪСФМТЬЧВМЦЧ.ТТЭМФЕЧЪЬПЁЛЮ
- б. ЫВЮХАЩПЁЪЧЕЯЛЧШПЁДМХШЗШЙРЫЬКФЧДЪСФМХЪЧВМЦЧ.ТТЭМФЕЧЪЬПЁЛЮ
- в. ЫВЮХАЩПЁНРЕЯЛЧШПЁДМХШЗШЙРЫЬКФЧДЪСФМТЬЧВМЦЧ.ТТЭМФЕЧЪЬПЁЛЮ
- г. ЫВЮХАЩПЁНРЕЯЛЧШПЁДМХШЗШЙРЫЬКФЧДЪСФМХЪЧВМЦЧ.ТТЭМФЕЧЪЬПЁЛЮ

20. 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
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 некоторым (неизвестным) ключом зашифрован текст. Определите длину ключа по полученному шифртексту (здесь символ «|» отделяет десятки букв, а каждая строка содержит 50 букв):

ЩБЯЦНВНОЧУ | ЫСФРЯРЫОДК | ТСЮУЁЧЭЭТЙ | ЙОЧСЩОУКАЯ | ЦЭФЭЭРЦДЖА
ХЯСЦХЫЩЪЫМ | МОЫПБДФЭВЁ | НСФКХХЦЗПЧ | ОБИХЁЪХШПН | РРМЦНСФЯДЧ
ЩОУКАЪНМЖЪ | ЮЭЭОИЧЬОЪН | ВЁХЯААПЛГЭ | АЗПОЫЪТВРС | РЪЦРХЩЯШЪН
ЁВИВОУТЬДМ | ЯМКЯПУАОПА | ХЯСЦЖПХТЮ | ЖРХАТЛЮУЭЭ | ХАТНХБЪНФО
ЩЪЯТДОАЯЦР | РТЛЯНСМЯЛР | НЕФЮБУСИЙВ | ЭЪТНПЭОТВШ | РШЮУООЕЪЩН
ЯВЖВЪЭЦБНО | УЭСАФЪАРЯЁ | ДЩБВРМЖЪПЦ | СЕУКВТЦВПЭ | ЪСЩУГЧЮЭЧВ
УФГРЪРЩУВВ | ПОСЯЩАЪДЭЮ | БУСООЪЯШАЕ | СУБКЪНЖАЪЭ | ПООВФЯТЦВЮ
ЯЪМТПЭТЫЦР | ЁВЁЭПНВЫФЭ | ЯТХЮХЪЭУФК | ЮЭБМФРЯШЯП | КВЩЦЫЕОЭУО
МОХЁХЪЦКДЭ | ВАААПКЫВЭА | БРЪВЕАЧЦРЯ | ЦЗЖЫЮВЛГТВ | ФК

21. Полина - менеджер по продажам в компании «КровМетСтрой». Для доступа к рабочей среде на корпоративном компьютере она должна ввести пароль, состоящий из заглавных букв латинского алфавита (26 символов), знаков «-», «.», «_» 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 любимого киноперсонажа - «R2-D2», затем - набор, содержащий от 1 до 4 цифр, а затем окончание «.RU» или «.COM».

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

Василий работает с Полиной в одной компании ровно на той же должности. Однако основная его деятельность — это сбор и передача данных компании-конкуренту. Василий также имеет доступ к рабочей среде и знает, что пароль, состоит из заглавных букв латинского алфавита (26 символов), знаков «-», «.», «_» и цифр от 0 до 9. При этом 2 одинаковых символа не могут идти подряд.

Он наблюдал за Полиной в течение нескольких месяцев и выявил закономерности в структуре пароля. Теперь он знает, что ее пароли состоят из слова «R2-D2», нескольких цифр после и окончания вида «.RU» или «.COM». Он написал программу, которая сначала перебирает все пароли с окончанием «.COM». (Сначала те, где после слова «R2-D2» идет одна цифра, потом - две, затем - три и т. д. до пяти цифр. Для каждого из случаев она перебирает числа от меньшего к большему, например, перебирая пароли с двумя цифрами после «R2 - D2», он сначала рассмотрит пароль «R2 -D201», потом «R2-D202», потом «R2-D203» и т. д., последним будет пароль «R2-D298»). После чего в том же порядке перебираются пароли с окончанием «.RU».

Итоговая программа после запуска на компьютере перебирает пароли со скоростью 1 пароль в секунду и останавливается после авторизации в рабочей среде. Василий использует также и вспомогательные программы: одна из них, находясь на компьютере, подключенном к рабочей среде, выгружает необходимые ему документы из рабочей среды и отправляет их в неизменном виде на внешний сервер по запросу автора программы, а другая скрывает присутствие описанных выше программ на компьютере.

Чтобы внедрить свои вредоносные программы на компьютер Полины, Василий разместил их на удаленном сервере, а по корпоративной почте отправил Полине письмо, содержащее картинку со встроенным в нее загрузчиком. После скачивания картинки и ее открытия, загрузчик установил на компьютер вредоносное ПО с сервера.

Установите следующие обстоятельства:

Б) Сколько времени уйдет на автоматизированный подбор пароля Полины, если ее текущий пароль «R2-D2986.COM»? Приведите решение.

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

Г) Какие типы вредоносного программного обеспечения (кроме загрузчика) использовал Василий?

Д) Исходя из подробностей описанной ситуации, оцени те, используются ли в информационной системе компании «КровМетСтрой» а) системы предотвращения утечки информации (DLP-системы), б) средства антивирусной защиты. Аргументируйте свой ответ.