ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ

РЕГИОНАЛЬНЫЙ ЭТАП

ТЕОРЕТИЧЕСКИЙ ТУР

10 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.

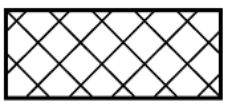
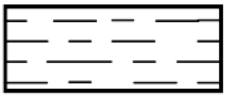
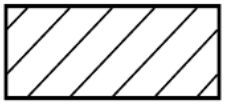
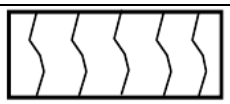
Задание теоретического тура считается выполненным, если Вы вовремя сдаете его членам жюри.

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

Общая часть

1. *О чем идет речь?* «Это универсальная технология передачи опыта, знаний, формирования навыков, компетенций, метакомпетенций и ценностей через неформальное взаимообогащающее общение, основанное на доверии и партнерстве».

2. Соотнесите условные графические обозначения материала с их названиями.

				
1	2	3	4	5

а. металлы и твёрдые сплавы
б. неметаллические материалы
в. стекло
г. жидкость
д. древесина

3. Каждому элементу электрической цепи присвоен единый международный буквенный код, который указывают рядом с элементом на электротехнических схемах, а также на самом элементе. Какой буквенный код соответствует выключателю? В ответе укажите букву.

а. FU
б. GB
в. SA
г. HL

4. Доход открытого акционерного общества (ОАО) за текущий год составил 50 млн. рублей, а издержки – 32 млн. рублей. На собрании акционеров было решено выплатить по дивидендам 40% от прибыли предприятия. Сколько денег получит гражданин А, владеющий 7 % акций ОАО?

5. Как называются растения, в которые пересажены гены других организмов?

Специальная часть

6. 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 условиях 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. ролевая модель;

б. дискреционная модель

в. модель, использующая уровни секретности объектов и уровни допуска субъектов;

г. мандатная модель;

7. 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. `e58f1e8c55fa105b` и `e58f1e8c55ga105b`

б. `0L/RgNC40LzQtdGA` и `0L/RgNC40LzQtdGA`

в. `266f263f0211048c` и `529057b143e93468`

г. `e3b0c44298fc1c14` и `e3b0c44298fc1c1`

8. 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. поместить на инженерные конструкции в конференц-зале источники вибрации,

б. поместить на стекла окон в конференц-зале генераторы источники вибрации,

в. закрыть окна в конференц-зале шторами,

г. удостовериться в отсутствии силовых и информационных кабелей вне специальных коробов.

9. Моделируя возможные угрозы безопасности информации, администратор безопасности рассматривает возможность того, что произвольный сотрудник организации подсмотрит и передаст конкурентам служебную информацию, обрабатываемую его коллегами, чьи рабочие места находятся в одном помещении с ним или в помещении, куда он может прийти в рамках своих рабочих вопросов. Укажите все обстоятельства, которые могут считаться уязвимостями относительно описанной угрозы

а. Стремление некоторых сотрудников к дополнительному заработку, даже нелегальными методами;

б. Возможность сотрудников свободно перемещаться между рабочими местами и помещениями в офисе;

в. Готовность конкурентов приобретать похищенную информацию, представляющую для них интерес;

г. Отсутствие полной лояльности работников своему нынешнему работодателю;

д. Возможность для человека, находящегося за спиной работающего сотрудника, подсмотреть информацию с его экрана;

е. Обработка сотрудниками служебной информации в одном помещении с сотрудниками, не имеющими прав доступа к ней;

10. Начальник службы информационной безопасности готовит помещение для проведения совещания, на котором будут обсуждаться сведения, составляющие коммерческую тайну. Он удостоверился, что при закрытых окнах звук за пределами помещения не слышен, то есть находящийся на улице прямо под окном человек не может разобрать, о чем говорят. Это означает, что угроза несанкционированного перехвата выступлений по акустическому каналу нарушителем, находящимся вне здания организации,

а. присутствует – нарушитель может воспользоваться электронным стетоскопом.

б. присутствует – нарушитель может воспользоваться направленным микрофоном.

в. присутствует – нарушитель может воспользуется лазерным стетоскопом.

г. отсутствует.

11. 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. Сокрытие действий и применяемых при этом средств от обнаружения

б. Получение первоначального доступа к компонентам систем и сетей

в. Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям

г. Закрепление (сохранение доступа) в системе или сети

1. Нецелевое использование ресурсов системы

2. Несанкционированное создание учетных записей или кража существующих учетных данных

3. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением
4. Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода вредоносного ПО, данных и команд управляющего трафика

12. 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 электронном устройстве в отдельной переговорной комнате. По мнению другого абонента, такой вариант тоже не обеспечивает безопасности, поскольку информация все равно может быть перехвачена, если в выбранном для встречи помещении имеются

а. устройства, чувствительные к высокочастотному излучению
б. устройства звукоусиления
в. низкочастотные усилители
г. незаземленные электрические провода

13. 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. контрольных сумм отдельных страниц файлов
б. контрольной суммы всего файла
в. проставленного в файлы на титульных страницах грифа “коммерческая тайна”
г. встраивания в защищаемые файлы и считывания из них при проверке надежных цифровых водяных знаков

14. Сотрудник организации обратился к администратору безопасности после того, как на его рабочем ноутбуке появилось сообщение с требованием уплаты выкупа за восстановление доступа к рабочим файлам. Запустив проверку средством антивирусной защиты, администратор безопасности определил, что на устройстве присутствует программа, относящаяся к категории трояноввымогателей. 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 электронной почты

в. загрузки и запуска файла из сети Интернет

г. отправки письма по электронной почте

15. Одним из основных способов обнаружения вредоносных программ является сигнатурный анализ - поиск в объектах системы известных фрагментов вредоносного кода. Его недостатком является

а. большое количество ложных срабатываний

б. пропуска подавляющего числа вредоносных программ в любых условиях работы

в. низкая скорость работы

г. неспособность обнаруживать новые или модифицированные вредоносные программы

16. Сотруднику службы информационной безопасности поручено организовать для контроля доступа к информационной системе двухфакторную аутентификацию. Для того, чтобы обеспечить соответствие поставленному заданию, он может внедрить систему, которая будет требовать от пользователей

а. ввести фамилию работника и пароль

б. ввести пароль работника и его конфиденциальный персональный номер

в. ввести пароль и решить задание (капчу)

г. отсканировать смарт-карту и приложить палец к сканеру

д. отсканировать отпечаток пальца и произнести в микрофон слово с экрана компьютера

17. Администратор безопасности произвел настройки системы предотвращения утечки информации (DLP-системы). Для этого он снабдил все соответствующие документы грифами “Коммерческая тайна”, а в систему внес перечень фраз, которые не должны встречаться в выводимых из системы (отправляемых по электронной почте, загружаемым в облачные хранилища, копируемым на съемные носители и т. п.) файлах. Среди этих фраз присутствуют как указанный гриф, так и названия документов, а также относящиеся к сфере деятельности организации словосочетания – около 30 слов и словосочетаний. Для обхода такой защиты недобросовестный сотрудник, стремящийся отправить договор, с которым он работает, на свой личный адрес электронной почты с корпоративного адреса, может

а. ограничиться удалением титульного листа документа, содержащего гриф “Коммерческая тайна”

б. удалить титульный лист документа, а также постараться удалить слова “договор” и все сочетания с ним из текста документа

в. сохранить документ в формате pdf

г. переписать основные положения договора своими словами, заменяя слова “договор”, “заказчик”, “исполнитель” и подобные синонимами или условными обозначениями.

18. 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

д. необходимость передачи абонентам ключей, длина которых в несколько раз превышает сообщение, которое требуется передать;

е. высокая сложность программной реализации таких шифров;

ж. низкая скорость зашифрования и расшифрования сообщений такими шифрами;

з. необходимость выработки последовательностей символов, длиной не уступающих длине передаваемых сообщений, удовлетворяющих условиям случайности и равновероятности;

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 соответствуюших таблицах совпадают, то для получения пары замены символы обмениваются местами. Например, «ЗО» – «ОЗ», «ЖИ» – «ИЖ».

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

«Смотреть ни в даль, ни в прошлое не надо, лишь в настоящем ».

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. ЯХЫЯЦФЛЪЁЬШЖЗШХ,ЮЖЖЙСГЦРВЦЦ.ЬЩБЯЁЬЫПФГЙ,ЖЙСЬМХЦРЁЬ,ФЙУК,ЭПВ

б. ЯХЫЯЦ.ЛЪЁЬШЖЗШХ,ЮЖЖЙСГЦРВЦЦ.ЬЩБЯЁЬЫПФГЙ,ЖЙСЬМХЦРЁЪ,ФЙУК,ЭПВ

в. ЯХЫЯЦФЛЪЁЬШЖЗШХ,ЮЖЖЙСГЦРВЦЦ.ЬЩБЯЁЬЫПФГЙ,ЖЙСЬМХЦРЁЪ,ФЙУК,ЭПВ

г. ЯХЫЯЦ.ЛЪЁЬШЖЗШХ,ЮЖЖЙСГЦРВЦЦ.ЬЩБЯЁЬЫПФГЙ,ЖЙСЬМХЦРЁЬ,ФЙУК,ЭПВ

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

```
ЬУЯТЛТЩЛРЧ|ЁУШТАПЪЁЬК|ФЯБГЛЫТЛРБ|ТЮЮГЬДЧУЯК|ЪЭАЕЫЯНЗФА
НРЛЫЪЯЦББВ|ЩУЭРФГТКРХ|ЯУЬВПЫРЦЬР|ЖГЬДЛЯЙШРЖ|ЁЛЛВАТЯЧНО
ЩУШРЯГЬЮШШ|ЩКЪЭХАМДНС|ЖХНЕЮЫТЛРБ|МНЪЕЬЛЩЙТВ|ЭСТЕЫВОЕЧЮ
БСШОПАРЁШС|РДТДФБТДЩТ|ПСРИЬЧРЁДВ|РЕАЬЬВЯТЪЮ|ЦВРЁШАЩВЫА
ВХТТЖХТСЩУ|ЯКЯГНИНАТС|ЮВЫИБЕПОРЭ|ЮАЭЙПЕЮЮЬЙ|ЫШЯТЬЬАВЪЕ
ШРРЕЫАКЁЬЛ|ЫУПЗОЯМНФВ|АСЙЧНВЩЬХС|ЯЁТСЛБНГЪД|ЬДФЛШОЯВАК
ЪЕНСШВАРФЮ|НКНУЩИЮХСА|ЧПЫАЬВСИУЕ|ААЬОГГЪДЬД|ЭЮЦХНВЮОЮХ
ЯЕШИЬЧРЁЯЯ|НЫСОББББТЗЕ|ПОМВСНРЭПС|РДПУЮЕМВЪБ|ЦЗЮВЩКЪЁЫИ
НЧТНЗХЬСЦД|ТСРБЦЯОВЯП|ЪЧЫЯНВЯКЬШ|ЯЛФЁНКТШЦО|ЩЬ
```

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 системы счисления с основанием 6. Так как пароль требуется менять ежемесячно, то для простоты запоминания Полина решила использовать пароли следующего вида: сначала идет слово «КМС» – сокращение от «КровМетСтрой», а затем – набор, содержащий от 2 до 4 цифр, причем в пароле не должно встречаться сочетание «53», то есть цифры 5 и 3 (именно в таком порядке) не могут следовать одна за другой.

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 восьмеричной системы счисления. Он наблюдал за Полиной в течение трех месяцев и выявил закономерности в структуре пароля. Теперь он знает, что ее пароли состоят из слова «КМС» и нескольких цифр после. Он написал программу, которая перебирает пароли, сначала те, где одна цифра, 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 «КМС00000», потом «КМС00001», потом «КМС00002» и т. д.).

Полученную программу он замаскировал под приложение типа «календарь событий». После чего Василий со сторонней почты якобы от имени компании отправил на корпоративную почту Полины предложение установить получившееся приложение. После установки программа перебора паролей начала работу. Пароли перебираются со скоростью 1 пароль в секунду. После входа в рабочую среду другая программа, заранее внедренная на компьютер Полины, в течение двух минут выгружает из рабочей системы необходимые Василию данные на внешний сервер по его запросу.

Установите следующие обстоятельства:

Б) Сколько времени пройдет от момента запуска программы перебора паролей до момента, когда данные окажутся на внешнем сервере, если текущий пароль «КМС0135»? Приведите решение.

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

Г) К какой (или каким) категории вредоносного программного обеспечения можно отнести использованные Василием программы?