

Предмет	Технология - Информационная безопасность
Автор	Четвергов А.Б., Дерягин А.В., Седов С.А. и др.
Класс	10-11
Описание	<i>Верхний = 1 дюйм (пт) Левый = 0,75 дюйм (пт) Нижний = 1 дюйм (пт) Правый = 0,75 дюйм (пт) Ширина = 11,69 дюйм (пт) ЛИСТА Высота = 8,27 дюйм (пт) ЛИСТА 2 колонки = 2*35,63 Интервал м/у колонками = 2,14 Межстрочный интервал = 1 ИЛИ 1,5</i>
Шрифт*	<i>Times New Roman</i>
Размер шрифта*	<i>11</i>
Формат документа*	<i>word</i>

Инструкция олимпиаде
<p>Всероссийская олимпиада школьников по технологии профиль «Информационная безопасность» Муниципальный этап 10-11 классы</p>
<p>Вам предстоит выполнить теоретические и тестовые задания. Время выполнения заданий теоретического тура 2 академических часа (90 минут).</p> <p>Выполнение тестовых заданий целесообразно организовать следующим образом: – не спеша, внимательно прочитайте тестовое задание; – определите, какой из предложенных вариантов ответа наиболее верный и полный; – напишите букву, 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.</p> <p>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.</p> <p>Предупреждаем, 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. Максимальное количество баллов – 100.</p>

Задания Общая часть

Задание 1. В трехрожковой люстре используются лампы накаливания, каждая из которых потребляет электроэнергии 60 Вт·ч. Было принято решение заменить эти лампы на светодиодные с энергопотреблением каждой = 5 Вт·ч.

Определите, сколько рублей в месяц составит экономия при замене ламп накаливания на светодиодные, если люстра будет работать 8 ч в сутки? Стоимость электроэнергии в квартире с электрической плитой по Татарстану составляет 3 рубля 58 копеек за 1 кВт·ч. Считаем, что в месяце 30 дней.

Привести решение. Ответ записать так «... руб. ... коп.» (т.е. результат при необходимости округлить до сотых).

Задание 2. Для окрашивания стен в помещении площадью 30 кв.м (площадь указана по полу) и высотой потолков 2,75 м использовали краску, вес которой в банке составил 2,5 кг. Для лучшей укрывистости стены прокрашивали дважды. При окрашивании в один слой на 1 кв.м уходит 150 гр краски.

Определите, сколько было потрачено денег на приобретение краски.

Известно, что одна банка краски стоит 1000 руб.

Проемы (окна/дверь) в ремонтируемом помещении принять равным = 5,5 м.

Длина одной из стен = 5 м.

Привести решение. Ответ записать в руб.

Задание 3. Организация приобрела у фирмы «А» товар за 450 руб. (с НДС 20%) и продала его фирме «Б» за 600 руб. (с НДС 20%).

Определите:

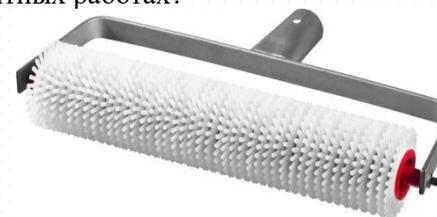
– А) Сколько денег останется у организации после уплаты (вычета) НДС?

Ответ запишите числом в рублях.

– Б) Сумму налога на прибыль к уплате организацией. Ответ запишите числом в рублях.

– В) Сумму денег, которая останется у организации после уплаты НДС и налога на прибыль. Ответ запишите числом в рублях.

Задание 4. Для чего именно такой игольчатый валик используется в строительном-ремонтных работах?



Задание 5. Дополните алгоритм создания индивидуального проекта, восстановив правильную последовательность действий в каждом этапе.

<i>Поисково-исследовательский этап</i>	<i>Конструкторско-технологический этап</i>	<i>Заключительный этап</i>
– А) Формулирование проблемы	– Д) Разработка графической документации	– И) Подготовка проекта к защите
– Б) ?	– Е) ?	– К) Презентация проекта
– В) ?	– Ж) ?	
– Г) ?	– З) ?	

В пустых ячейках напротив букв «Б», «В», «Г», «Е», «Ж» и «З» поставить только латинские буквы «Q», «W» и др. (т.е. не писать в бланке ответов полное название действий)

Q – декоративная отделка;

W – составление плана работы и паспорта проекта;

R – подготовка рабочего места, инструментов, материалов;

Y – обоснование выбора проекта, постановка цели;

S – технологический процесс изготовления изделия;

F – сбор информации, выполнение экологического и экономического обоснования.

Специальная часть

Задание 6. Шифр, известный как «квадрат Полибия», устроен следующим образом. В квадратную или прямоугольную таблицу вписываются буквы алфавита (для кодирования – в алфавитном порядке, для шифрования – в произвольном, при этом расположение букв в таблице является ключом), строки и столбцы таблицы обозначаются цифрами. При зашифровании буквы открытого текста заменяются на пары цифр, которыми отмечены, соответственно, строка и столбец, в которых стоит данная буква. Например, на иллюстрации ниже буква

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	.	,	?

«М» зашифрована сочетанием цифр «32», а слово «МАЙ» – «32 11 25».

Таким шифром зашифрован некоторый текст (без пробелов, но с сохранением знаков препинания – точки, запятой и вопросительного знака):
41 34 13 16 53 11 33 24 63 34 42 32 16 33 16 33 55 64 41 32 34 42 36 16 42 56
33 16 31 56 23 63 65 42 34 31 56 26 34 41 31 43 52 11 42 56 64

Установите, сколько гласных букв зашифровано в сообщении.

Задание 7. Напишите слово открытого текста, которое начинается с гласной буквы (смотрите зашифрованное сообщение в задании 6) без изменения его написания.

Задание 8. По приведённому квадрату Полибия зашифруйте слово «ТЕХНОСФЕРА». Ответ запишите как одно число без разделителей.

Задание 9. Определите, какое слово зашифровано шифртекстом
36 16 35 43 42 11 46 24 63.

– А) РЕПУТАЦИЯ. – Б) РЕНОВАЦИЯ. – В) РЕПЕТИЦИЯ

Задание 10. Установите шифробозначение (замену) буквы «Т» в шифртексте 33 34 13 34 41 31 56

Условие (описание ситуации) для заданий №№ 11-14:

Компании «W» требуется уделять внимание обеспечению целостности обрабатываемой информации.

Задание 11. Укажите, какую из предложенных ниже мер предпочтительно использовать самой компании для контроля целостности пользовательских данных, хранимых в облачном хранилище. Эти данные могут передаваться и храниться клиентами в зашифрованном виде.

- А) _хрупкие цифровые водяные знаки_
- Б) _электронная подпись_
- В) _надежные цифровые водяные знаки_
- Г) _функции хэширования_

Задание 12. Укажите меру из перечисленных ниже, которая наиболее предпочтительна для клиентов облачного хранилища с целью контроля целостности хранимых в нём данных.

- А) _хрупкие цифровые водяные знаки_
- Б) _электронная подпись_
- В) _надежные цифровые водяные знаки_
- Г) _функции хэширования_

Задание 13. Передавая партнёрам программные продукты, дальнейшее распространение которых не допускается лицензионным соглашением, компании следует использовать для отслеживания несанкционированного распространения

- А) _хрупкие цифровые водяные знаки_
- Б) _электронная подпись_
- В) _надежные цифровые водяные знаки_
- Г) _функции хэширования_

Задание 14. Укажите две меры, которые компания может использовать для подтверждения внесения клиентами изменений в библиотеки распространённого по лицензии программного обеспечения.

- А) _хрупкие цифровые водяные знаки_
- Б) _электронная подпись_

- В) _надежные цифровые водяные знаки_
- Г) _функции хэширования_

Условие (описание ситуации) для заданий №№ 15-18:

Разработка решений для обеспечения целостности данных – одно из направлений деятельности компании «Q».

Задание 15. Одна из наиболее распространённых задач – обеспечение контроля целостности информации, передаваемой по открытым каналам связи. Выберите меру защиты информации, которая подойдёт для решения указанной задачи.

- А) _надежные цифровые водяные знаки_
- Б) _электронная подпись_
- В) _вычисление контрольной суммы_
- Г) _система хэширования_

Задание 16. Одной из категорий продуктов, выпускаемых компанией «О», являются программные средства выработки функций хэширования. Выберите задачу, для решения которой может применяться одно из таких средств. обеспечение целостности информации, передаваемой по открытым каналам связи

- А) _контроль неизменности отправляемых сообщений_
- Б) _обеспечение целостности хранимых на сервере файлов_
- В) _обеспечение контроля достоверности поступающих сообщений_

Задание 17. Для функций хэширования коллизией называется

- А) _пара входных значений, для которых значения функции совпадают_
- Б) _ситуация, когда невозможно корректно вычислить значение функции хэширования_
- В) _входное значение, для которого не определено выходное значение функции_
- Г) _значение функции, для которого не определено ни одного входного значения_

Задание 18. В отдельных случаях для контроля целостности могут применяться цифровые водяные знаки. Для решения какой задачи они используются?

- А) _контроль неизменности продуктов, распространяемых по лицензии_
- Б) _контроль целостности записей в базе данных_
- В) _контроль неизменности данных, хранимых на сервере_

Условие (описание ситуации) для заданий №№ 19-21:

Руководство банка решило усовершенствовать системы информационной безопасности и для этого внедрит новые способы аутентификации. На основе анализа угроз было принято решение защищать как информационные ресурсы организации, так и служебные помещения от несанкционированного доступа.

Задание 19. Для обеспечения контроля пропуска сотрудников была нанята охрана и установлены пропускные турникеты, к которым сотрудники должны прикладывать смарт-карты. Какие типы аутентификации реализованы? Выберите 2 варианта.

- А) _двухфакторная аутентификация_
- Б) _однофакторная аутентификация_
- В) _аутентификация на основе фактора владения_
- Г) _аутентификация по ЭЦП_

Задание 20. Перед входом в каждый служебный кабинет стоит робот, который получает уведомление о посетителе и просит его пройти аутентификацию, чтобы войти внутрь. Для этого требуется встать на отмеченную позицию перед роботом и замереть на несколько секунд, пока робот проводит «осмотр» и сопоставляет отсканированную картинку с внутренней базой данных сотрудников. Какой тип аутентификации используется?

- А) _аутентификация по GPS_
- Б) _биометрическая аутентификация_
- В) _аутентификация на основе фактора знания_
- Г) _аутентификация по ЭЦП_

Задание 21. Для запуска компьютера на рабочем месте сотрудника руководство установило следующую систему: сначала она требует ввести PIN-код, после его успешного ввода пользователю требуется поднести электронный ключ к считывателю, а если ключ распознан как корректный, то пользователю предлагается приложить палец к сканеру. Укажите, какая система аутентификации реализована.

- А) _двухфакторная аутентификация_
- Б) _трёхфакторная аутентификация_
- В) _однофакторная аутентификация_

Условие (описание ситуации) для заданий №№ 22-25:

В компании «U» усовершенствовали системы защиты информации и теперь предоставляют полный цикл услуг по хранению и обеспечению безопасности пользовательских данных в облачном хранилище. После этого системы организации подверглись атаке, направленной на разные объекты и реализованной различными нарушителями.

Задание 22. Выберите все правильные ответы. Для сбора сведений об информационной системе компании злоумышленники похитили внешний носитель администратора безопасности с паролями нескольких пользователей, при этом больше пароли нигде зафиксированы не были. Реализация этой угрозы нарушила

- А) _конфиденциальность похищенных данных_
- Б) _целостность похищенных данных_
- В) _доступность похищенных данных_

Задание 23. Обнаружив пропажу, системный администратор немедленно заблокировал учётные записи пользователей, чьи пароли были на похищенном носителе, тем самым

- А) _предотвратил угрозу нарушения конфиденциальности информации на носителе_
- Б) _нарушил целостность информации в системе компании_
- В) _нарушил доступность информации, к которой имели доступ пользователи_

Задание 24. Выберите все правильные ответы. Не используя пароли с внешнего носителя, нарушители подобрали пароль одного из пользователей, авторизовались в системе под его учётными данными, после чего скопировали его служебные данные и сменили пароль пользователя. Реализация этой угрозы нарушила

- А) _конфиденциальность данных_
- Б) _целостность данных_
- В) _доступность данных_

Задание 25. Выберите все правильные ответы. Для нанесения финального удара нарушители одновременно провели DDoS- атаку на облачное хранилище компании, а также проникли в него и изменили права доступа одного из клиентов к его базе данных таким образом, чтобы он больше не мог запрашивать из неё сведения. Реализация этой угрозы нарушила

- А) _конфиденциальность данных_
- Б) _целостность данных_
- В) _доступность данных_

Условие (описание ситуации) для заданий №№ 26-29:

В компании «Ё» усовершенствовали систему информационной безопасности. После этого информационная система компании стала целью атаки со стороны злоумышленников.

Задание 26. Сначала нарушители решили скомпрометировать системы шифрования компании, для чего осуществили перехват ключа шифрования в момент передачи с аппаратного носителя в систему шифрования. Реализация такой угрозы нарушила

- А) _конфиденциальность похищенных данных_
- Б) _целостность похищенных данных_
- В) _доступность похищенных данных_

Задание 27. Выберите все правильные ответы. После успешной компрометации ключа шифрования нарушители перехватили несколько передаваемых по сети зашифрованных сообщений и, заблокировав их

доставку получателю, прочли их и подменили на собственные, которые затем были отправлены по назначению. Реализация такой угрозы нарушила

- А) _конфиденциальность похищенных данных_
- Б) _целостность похищенных данных_
- В) _доступность похищенных данных_

Задание 28. В другом случае нарушители просто исказили хранимую на сервере в зашифрованном виде информацию таким образом, чтобы при попытке её расшифровать пользователь получал лишь бессмысленный набор символов.. Реализация такой угрозы нарушила

- А) _конфиденциальность хранимых данных_
- Б) _целостность хранимых данных_
- В) _доступность хранимых данных_

Задание 29. Помимо системы шифрования целью атаки стала и система электронной подписи, разработанная компанией. Однако ещё до действий нарушителей отправитель (один из сотрудников компании) ошибся в выборе ключа генерации подписи, в результате чего отправленное сообщение не могло пройти проверку подлинности подписи на стороне получателя. Такие действия отправителя

- А) _нарушили доступность передаваемой информации_
- Б) _нарушили целостность передаваемой информации_
- В) _не нарушили безопасность передаваемой информации_
- Г) _нарушили достоверность передаваемой информации_

Условие (описание ситуации) для заданий №№ 30-33:

Компания «S» расширила круг предоставляемых услуг и теперь занимается комплексным обеспечением информационной безопасности. К сожалению, недавно одно из её новых решений – система контроля и протоколирования действий пользователей – подверглось атаке злоумышленников с целью демонстрации её слабостей.

Задание 30. Выберите все правильные ответы. На начальном этапе атаки нарушители внедрили в базы данных систем, в которых было развёрнуто решение от компании «S», вредоносную программу, которая могла

блокировать или искажать (каждое из этих действий было реализовано примерно в половине заражённых систем) записи о действиях пользователей.

Реализация такой угрозы нарушила

- А) _конфиденциальность похищенных данных_
- Б) _целостность похищенных данных_
- В) _доступность похищенных данных_

Задание 31. После реализации описанной выше угрозы часть клиентов отказались от использования системы и самостоятельно удалили или заблокировали собранную информацию об активности собственных сотрудников. Такое действие

- А) _нарушили конфиденциальность удаленных данных_
- Б) _нарушили целостность удаленных данных_
- В) _не нарушили информационную безопасность_
- Г) _нарушили доступность удаленных данных_

Задание 32. Выберите все правильные ответы. Другие клиенты компании «S» приняли решение передать собранные данные на хранение в облачное хранилище, уже контролирующееся нарушителями. Что могут нарушить злоумышленники, полностью контролируя такое хранилище?

- А) _конфиденциальность хранимых данных_
- Б) _целостность хранимых данных_
- В) _доступность хранимых данных_

Задание 33. Стремясь снизить последствия от воздействия на развёрнутые у клиентов продукты, компания приняла решение без ведома клиентов сохранять копии собираемой в их системах информации на своих серверах, передавая её в зашифрованном виде по сети Интернет. Такое действие, относительно информации клиентов

- А) _никак не повлияло на информационную безопасность_
- Б) _обеспечило целостность собираемой информации_
- В) _обеспечило конфиденциальность собираемой информации_
- Г) _нарушило конфиденциальность собираемой информации_
- Д) _нарушило доступность собираемой информации_

Условие (описание ситуации) для заданий №№ 34-37:

Для обеспечения возможности надёжного использования своих продуктов компания «S» принимает меры по обеспечению целостности хранимых записей.

Задание 34. Укажите меру из предложенных ниже, подходящую для контроля целостности записей на сервере, сохраняемых в виде файлов, в которые не производится запись.

- А) _цифровая подпись_
- Б) _электронная подпись_
- В) _система контроля версий_
- Г) _функции хэширования_

Задание 35. Для схем цифровой подписи открытый (публичный) ключ используется для

- А) _зашифрования отправляемых сообщений_
- Б) _проверки электронной подписи_
- В) _вычисления значения функции хэширования_
- Г) _для формирования электронной подписи_

Задание 36. Строя коллизию для известной функции хэширования, нарушитель стремится

- А) _осуществить подмену информации, от которой вычислена функция_
- Б) _подобрать входное значение функции, для которой известен результат вычисления функции_
- В) _нарушить целостность отправляемого сообщения_
- Г) _не дать возможность заметить внесённые в передаваемую информацию изменения_

Задание 37. Для качественной функции хэширования одним из требований является

- А) _простота вычисления значения функции_
- Б) _существенное изменение значения функции при внесении изменений во входное значение_

- В) _отсутствие коллизий, вычисляемых при известной размерности выходного значения_
- Г) _простота вычисления прообраза_

Условие (описание ситуации) для заданий №№ 38-40:

Руководство МФЦ стремится повысить уровень защищённости для своих сотрудников, для чего решило усилить меры аутентификации на ряде позиций объекта.

Задание 38. Для обеспечения пропускного режима в организации была нанята охрана и установлены пропускные турникеты. Сотрудник должен поднести к турникету пропуск, представляющий собой смарт-карту, при этом охранник визуально определяет, соответствует ли входящий фотографии, отображаемой на экране. Какой тип аутентификации реализован?

- Б) _двухфакторная на основе факторов знания и биометрии_
- В) _двухфакторная на основе факторов владения и биометрии_
- А) _двухфакторная на основе факторов знания и владения_

Задание 39. Каждому директору выдаётся служебный ноутбук для работы в корпоративной сети вне офиса. Ноутбук имеет сенсорную панель, клавиатуру, качественный микрофон со встроенной системой распознавания голоса и камеру. Для входа требуется ввести логин и пароль от учётной записи пользователя, с которой связано портативное электронное средство аутентификации, его требуется представить системе (подключить к ноутбуку). Какой тип аутентификации реализован?

- А) _двухфакторная биометрическая на основе факторов знания и владения_
- Б) _двухфакторная на основе факторов знания и биометрии_
- В) _двухфакторная на основе факторов знания и владения_

Задание 40. При выдаче посетителям МФЦ документов, дающих право на льготы или денежные выплаты, сотрудники должны проходить следующую процедуру. Для создания документа сотрудник должен ввести свои фамилию и должность. Подтвердить создание требуется вводом личного пароля доступа, обновляемого ежемесячно. Дальнейшие операции с документом требуют ввода личного секретного кода сотрудника и

подключения к системе внешнего носителя с секретным ключом. Какой тип аутентификации используется для создания особо важных документов?

- А) _однофакторная на основе фактора владения_
- Б) _двухфакторная на основе факторов знания и владения_
- В) _двухфакторная на основе факторов знания и биометрии_
- Г) _трёхфакторная_

Рекомендации для выполнения задания №41:

Достаточным является лаконичный ответ, содержащий ответы на пункты 1–3 в сочетании «информация (конкретные данные из приведённых в условии) – канал утечки – момент времени (действия пилотов или этапы полёта) – способ реализации угрозы (средство)», например: «Паспортные данные посетителя банка могут быть похищены по оптическому каналу в момент предъявления паспорта охране при помощи скрытой камеры, установленной рядом с постом охраны; телефонный номер может быть похищен по акустическому каналу в момент сообщения его оператору банка при помощи подслушивающего устройства («жучка»), размещённого рядом с рабочим местом оператора». Рассмотрите все возможные сочетания похищаемой информации и каналов утечки.

Задание 41. Инновационная компания разрабатывает беспилотные автомобили-такси. Для использования в качестве такси каждое транспортное средство будет снабжено системой, получающей сведения о поступающих заказах (точка подачи такси и пункт назначения), а также системой для приёма оплаты поездки при помощи банковских карт или получения уведомления об оплате от сервера (в случае оплаты через мобильное приложение).

Недавно появились сведения об утечках информации из систем беспилотных такси этой компании.

1. Оцените, какие сведения о поездках или оплате могут быть перехвачены злоумышленниками из системы беспилотного такси по побочным физическим каналам.
2. Оцените, приведя аргументы, какие каналы могли быть задействованы для совершения перехвата такой информации.

3. Приведите примеры устройств для каждой пары «канал – сведения», которые могли быть использованы для реализации таких угроз безопасности информации. Уточните, в какой момент (при каких действиях пассажира или в какие моменты поездки беспилотного такси) эти угрозы могут быть реализованы. Аргументируйте свою оценку.