

Предмет	Технология - Информационная безопасность
Автор	Четвергов А.Б., Дерягин А.В., Седов С.А. и др.
Класс	7-8
Описание	<p><i>Верхний = 1 дюйм (пт)</i>  <i>Левый = 0,75 дюйм (пт)</i>  <i>Нижний = 1 дюйм (пт)</i>  <i>Правый = 0,75 дюйм (пт)</i>  <i>Ширина = 11,69 дюйм (пт) ЛИСТА</i>  <i>Высота = 8,27 дюйм (пт) ЛИСТА</i>  <i>2 колонки = 2*35,63</i>  <i>Интервал м/у колонками = 2,14</i>  <i>Межстрочный интервал = 1 ИЛИ 1,5</i></p>
Шрифт*	<i>Times New Roman</i>
Размер шрифта*	<i>11</i>
Формат документа*	<i>word</i>
Технический специалист ГАОУ РОЦ*	<i>Бадертдинов Салават Ришатович,  <a href="mailto:3325173080@qq.com">3325173080@qq.com</a>  telegram: badert14</i>

<p><b>Инструкция по выполнению работы на олимпиаде</b>  <b>Всероссийская олимпиада школьников по технологии</b>  <b>профиль «Информационная безопасность»</b>  <b>Муниципальный этап</b>  <b>7-8 классы</b></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>





Задание 11. Для обеспечения контроля пропуска сотрудников была нанята охрана и установлены пропускные турникеты, при этом руководитель отдела информационной безопасности решил заменить пропуск на универсальный ключ доступа. Какой тип аутентификации тут предусмотрен?

- А) \_однофакторная аутентификация\_
- Б) \_двухфакторная аутентификация\_
- В) \_многофакторная аутентификация\_

**Условие (описание ситуации) для заданий №№ 12-15:**

***В компании «N» 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 12. 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) \_доступность похищенных данных\_
- Б) \_конфиденциальность похищенных данных\_
- В) \_целостность похищенных данных\_

Задание 13. Обнаружив пропажу, системный администратор немедленно заблокировал учётные записи пользователей, чьи пароли были на похищенном носителе, тем самым

- А) \_нарушил доступность информации, к которой имели доступ пользователи\_
- Б) \_предотвратил угрозу нарушения конфиденциальности информации на носителе\_
- В) \_нарушил целостность информации в системе компании\_

Задание 14. 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) \_доступность данных\_
- Б) \_конфиденциальность данных\_
- В) \_целостность данных\_

Задание 15. 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) \_доступность данных\_
- Б) \_конфиденциальность данных\_
- В) \_целостность данных\_

**Условие (описание ситуации) для заданий №№ 16-19:**

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

Задание 16. 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) \_доступность похищенных данных\_
- Б) \_конфиденциальность похищенных данных\_
- В) \_целостность похищенных данных\_

Задание 17. 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) \_доступность похищенных данных\_
- Б) \_конфиденциальность похищенных данных\_
- В) \_целостность похищенных данных\_

Задание 18. 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) \_доступность хранимых данных\_
- Б) \_конфиденциальность хранимых данных\_
- В) \_целостность хранимых данных\_

Задание 19. 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) \_не нарушили безопасность передаваемой информации\_
- Б) \_нарушили достоверность передаваемой информации\_
- В) \_нарушили доступность передаваемой информации\_
- Г) \_нарушили целостность передаваемой информации\_

**Условие (описание ситуации) для заданий №№ 20-23:**

**Компании «М» требуется уделять внимание обеспечению целостности обрабатываемой информации.**

Задание 20. 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) \_надежные цифровые водяные знаки\_
- Б) \_функции хэширования\_
- В) \_хрупкие цифровые водяные знаки\_
- Г) \_электронная подпись\_

Задание 21. Укажите меру из перечисленных ниже, которая наиболее предпочтительна для клиентов облачного хранилища с целью контроля целостности хранимых в нём данных.

- А) \_надежные цифровые водяные знаки\_
- Б) \_функции хэширования\_
- В) \_хрупкие цифровые водяные знаки\_
- Г) \_электронная подпись\_

Задание 22. Передавая партнёрам программные продукты, дальнейшее распространение которых не допускается лицензионным соглашением, компании следует использовать для отслеживания несанкционированного распространения

- А) \_надежные цифровые водяные знаки\_
- Б) \_функции хэширования\_
- В) \_хрупкие цифровые водяные знаки\_
- Г) \_электронная подпись\_

Задание 23. Укажите две меры, которые компания может использовать для подтверждения внесения клиентами изменений в библиотеки распространённого по лицензии программного обеспечения.

- А) \_надежные цифровые водяные знаки\_
- Б) \_функции хэширования\_
- В) \_хрупкие цифровые водяные знаки\_
- Г) \_электронная подпись\_

**Условие (описание ситуации) для заданий №№ 24-27:**

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

Задание 24. 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) \_вычисление контрольной суммы\_
- Б) \_система хэширования\_
- В) \_надежные цифровые водяные знаки\_
- Г) \_электронная подпись\_

Задание 25. 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) \_обеспечение контроля достоверности поступающих сообщений\_
- Б) \_контроль неизменности отправляемых сообщений\_
- В) \_обеспечение целостности хранимых на сервере файлов\_

Задание 26. Для функций хэширования коллизией называется

- А) \_входное значение, для которого не определено выходное значение функции\_
- Б) \_значение функции, для которого не определено ни одного входного значения\_
- В) \_пара входных значений, для которых значения функции совпадают\_
- Г) \_ситуация, когда невозможно корректно вычислить значение функции хэширования\_

Задание 27. В отдельных случаях для контроля целостности могут применяться цифровые водяные знаки. Для решения какой задачи они используются?

- А) \_контроль неизменности данных, хранимых на сервере\_
- Б) \_контроль неизменности продуктов, распространяемых по лицензии\_
- В) \_контроль целостности записей в базе данных\_

**Условие (описание ситуации) для заданий №№ 28-30:**

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

Задание 28. 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) \_аутентификация на основе фактора владения\_
- Б) \_аутентификация по ЭЦП\_
- В) \_двухфакторная аутентификация\_
- Г) \_однофакторная аутентификация\_

Задание 29. 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 на основе фактора знания\_
- Б) \_аутентификация по ЭЦП\_
- В) \_аутентификация по GPS\_
- Г) \_биометрическая аутентификация\_

Задание 30. 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) \_однофакторная аутентификация\_
- Б) \_двухфакторная аутентификация\_
- В) \_трёхфакторная аутентификация\_

**Условие (описание ситуации) для заданий №№ 31-34:**

**Компания «V» 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 31. Выберите все правильные ответы. На начальном этапе атаки нарушители внедрили в базы данных систем, в которых было развёрнуто решение от компании «V», вредоносную программу, которая могла блокировать или исказить (каждое из этих действий было реализовано примерно в половине заражённых систем) записи о действиях пользователей. Реализация такой угрозы нарушила

- А) \_доступность похищенных данных\_
- Б) \_конфиденциальность похищенных данных\_
- В) \_целостность похищенных данных\_

Задание 32. 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) \_не нарушили информационную безопасность\_
- Б) \_нарушили доступность удаленных данных\_
- В) \_нарушили конфиденциальность удаленных данных\_
- Г) \_нарушили целостность удаленных данных\_

Задание 33. Выберите все правильные ответы. Другие клиенты компании «V» приняли решение передать собранные данные на хранение в облачное хранилище, уже контролирующееся нарушителями. Что могут нарушить злоумышленники, полностью контролируя такое хранилище?

- А) \_доступность хранимых данных\_
- Б) \_конфиденциальность хранимых данных\_
- В) \_целостность хранимых данных\_

Задание 34. 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) \_обеспечило конфиденциальность собираемой информации\_
- Б) \_нарушило конфиденциальность собираемой информации\_
- В) \_нарушило доступность собираемой информации\_
- Г) \_никак не повлияло на информационную безопасность\_
- Д) \_обеспечило целостность собираемой информации\_

**Условие (описание ситуации) для заданий №№ 35-38:**

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

Задание 35. Укажите меру из предложенных ниже, подходящую для контроля целостности записей на сервере, сохраняемых в виде файлов, в которые не производится запись.

- А) \_система контроля версий\_
- Б) \_функции хэширования\_
- В) \_цифровая подпись\_
- Г) \_электронная подпись\_

Задание 36. Для схем цифровой подписи открытый (публичный) ключ используется для

- А) \_вычисления значения функции хэширования\_
- Б) \_для формирования электронной подписи\_
- В) \_зашифрования отправляемых сообщений\_
- Г) \_проверки электронной подписи\_

Задание 37. Строя коллизию для известной функции хэширования, нарушитель стремится

- А) \_нарушить целостность отправляемого сообщения\_
- Б) \_не дать возможность заметить внесённые в передаваемую информацию изменения\_
- В) \_осуществить подмену информации, от которой вычислена функция\_
- Г) \_подобрать входное значение функции, для которой известен результат вычисления функции\_

Задание 38. Для качественной функции хэширования одним из требований является

- А) \_отсутствие коллизий, вычисляемых при известной размерности выходного значения\_
- Б) \_простота вычисления прообраза\_
- В) \_простота вычисления значения функции\_
- Г) \_существенное изменение значения функции при внесении изменений во входное значение\_

**Условие (описание ситуации) для заданий №№ 39-40:**

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

Задание 39. 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?

- А) \_двухфакторная на основе факторов знания и владения\_
- Б) \_двухфакторная на основе факторов знания и биометрии\_
- В) \_двухфакторная на основе факторов владения и биометрии\_

Задание 40. 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 на основе факторов знания и владения\_
- Б) \_двухфакторная биометрическая на основе факторов знания и владения\_
- В) \_двухфакторная на основе факторов знания и биометрии\_

***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. На вокзале установлены терминалы самообслуживания. Пассажиру для приобретения билета требуется самостоятельно ввести дату отправления и номер поезда, на который требуется билет, ввести при помощи экранной клавиатуры и встроенного сканера паспортные данные, выбрать место, отсканировать документы, дающие право на приобретение льготного билета, после чего осуществить оплату банковской картой, вставив её в соответствующий разъем терминала и введя PIN-код.

Спустя некоторое время были обнаружены утечки персональных данных пассажиров (паспортных данных и данных других личных документов, сведений о приобретённых билетах) и сведений их банковских карт (номеров карт, сведений о владельцах карт, PIN-кодов и CVV-кодов).

1. Оцените, по каким из физических каналов утечки информации – оптическому, акустическому, радиоэлектронному – нарушители могут перехватить информацию из документов или карты пассажира.
2. Оцените, в какой момент, то есть при совершении пассажиром каких действий, это может произойти.
3. Для каждой определённой вами возможности перехвата информации (в т.ч.: а) паспортные данные; б) данные прочих документов, дающих право на льготные билеты; в) открытую информацию о банковской карте; г) CVV-код; д) PIN-код) по какому-то конкретному каналу приведите пример того, как (возможно, с помощью каких средств) это может быть совершено. Подтвердите свои оценки и выводы аргументами.

**Бланк ответов**

Общая часть

Задание 1. \_\_\_\_\_.

Задание 2. 1 – \_\_\_\_\_,

2 – \_\_\_\_\_.

Задание 3.

						И	
--	--	--	--	--	--	---	--

Задание 4.



Задание 5.

– А) \_\_\_\_\_

– Б) \_\_\_\_\_

– В) \_\_\_\_\_

Специальная часть

Задание 6. Ответ \_\_\_\_\_.

Задание 7. Ответ \_\_\_\_\_.

Задание 8. Ответ \_\_\_\_\_.

Задание 9. Ответ \_\_\_\_\_.

Задание 10. Ответ \_\_\_\_\_.

Задание 11. Ответ \_\_\_\_\_.

Задание 12. Ответ \_\_\_\_\_.

Задание 13. Ответ \_\_\_\_\_.

Задание 14. Ответ \_\_\_\_\_.

Задание 15. Ответ \_\_\_\_\_.

Задание 16. Ответ \_\_\_\_\_.

Задание 17. Ответ \_\_\_\_\_.

Задание 18. Ответ \_\_\_\_\_.

Задание 19. Ответ \_\_\_\_\_.

Задание 20. Ответ \_\_\_\_\_.

Шифр участника ИБ\_7-8 — \_\_\_\_\_

Задание 21. Ответ \_\_\_\_\_.

Задание 22. Ответ \_\_\_\_\_.

Задание 23. Ответ \_\_\_\_\_.

Задание 24. Ответ \_\_\_\_\_.

Задание 25. Ответ \_\_\_\_\_.

Задание 26. Ответ \_\_\_\_\_.

Задание 27. Ответ \_\_\_\_\_.

Задание 28. Ответ \_\_\_\_\_.

Задание 29. Ответ \_\_\_\_\_.

Задание 30. Ответ \_\_\_\_\_.

Задание 31. Ответ \_\_\_\_\_.

Задание 32. Ответ \_\_\_\_\_.

Задание 33. Ответ \_\_\_\_\_.

Задание 34. Ответ \_\_\_\_\_.

Задание 35. Ответ \_\_\_\_\_.

Задание 36. Ответ \_\_\_\_\_.

Задание 37. Ответ \_\_\_\_\_.

Задание 38. Ответ \_\_\_\_\_.

Задание 39. Ответ \_\_\_\_\_.

Задание 40. Ответ \_\_\_\_\_.

Задание 41. Ответ:

Шифр участника ИБ\_7-8 — \_\_\_\_\_

Задание 41. Лист для ответа

### Ключи

## МАКСИМАЛЬНЫЙ БАЛЛ ЗА ВСЕ ЗАДАНИЯ – 100.

### Общая часть

#### ЗАДАНИЯ №№ 1-5 ОЦЕНИВАЮТСЯ В 2 БАЛЛА (ставить 0 или 2)

Задание 1.

Обычно промышленные технологии состоят из нескольких частей, которые называются **производственными** технологиями.

Задание 2. **ОТВЕТ ОЦЕНИВАЕТСЯ ПО ОБЩЕМУ СМЫСЛУ**

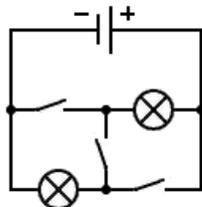
1 – **строительная основа** (оформление стен, пола, потолка)

2 – **предметная наполненность** (мебель, бытовая техника)

Задание 3.

К	О	М	П	О	З	И	Т
---	---	---	---	---	---	---	---

Задание 4.



Задание 5.

– А) 30

– Б) 130

### Специальная часть

#### ЗАДАНИЯ №№ 6-40 ОЦЕНИВАЮТСЯ В 2 БАЛЛА (ставить 0 или 2)

Задание 6. 2.

Задание 7. СОВЕЩАНИЯ

Задание 8. 26316251

Задание 9. – Б) РЕНОВАЦИЯ.

Задание 10. 44

Задание 11. – А) однофакторная аутентификация

Задание 12. – А) доступность похищенных данных

– Б) конфиденциальность похищенных данных

Задание 13. – А) нарушил доступность информации, к которой имели доступ пользователи

Задание 14. – А) доступность данных

– Б) конфиденциальность данных

– В) целостность данных

Задание 15. – А) доступность данных

– В) целостность данных

Задание 16. – Б) конфиденциальность похищенных данных

Задание 17. – Б) конфиденциальность похищенных данных

– В) целостность похищенных данных

Задание 18. – А) доступность хранимых данных

– В) целостность хранимых данных

Задание 19. – А) не нарушили безопасность передаваемой информации

Задание 20. – Б) функции хэширования

Задание 21. – Г) электронная подпись

Задание 22. – А) надежные цифровые водяные знаки

Задание 23. – Б) функции хэширования

– В) хрупкие цифровые водяные знаки

- Задание 24. – Г) \_электронная подпись\_
- Задание 25. – В) \_обеспечение целостности хранимых на сервере файлов\_
- Задание 26. – В) \_пара входных значений, для которых значения функции совпадают\_
- Задание 27. – Б) \_контроль неизменности продуктов, распространяемых по лицензии\_
- Задание 28. – А) \_аутентификация на основе фактора владения\_  
– Г) \_однофакторная аутентификация\_
- Задание 29. – Г) \_биометрическая аутентификация
- Задание 30. – В) \_трёхфакторная аутентификация\_
- Задание 31. – А) \_доступность похищенных данных\_  
– В) \_целостность похищенных данных\_
- Задание 32. – А) \_не нарушили информационную безопасность\_
- Задание 33. – А) \_доступность хранимых данных\_  
– Б) \_конфиденциальность хранимых данных\_  
– В) \_целостность хранимых данных\_
- Задание 34. – Б) \_нарушило конфиденциальность собираемой информации\_
- Задание 35. – Б) \_функции хэширования\_
- Задание 36. – Г) \_проверки электронной подписи\_
- Задание 37. – В) \_осуществить подмену информации, от которой вычислена функция\_

Задание 38. – Г) \_существенное изменение значения функции при внесении изменений во входное значение\_

Задание 39. – В) \_двухфакторная на основе факторов владения и биометрии

Задание 40. – Б) \_двухфакторная биометрическая на основе факторов знания и владения\_

### МАКСИМАЛЬНЫЙ БАЛЛ ЗА ЗАДАНИЕ № 41 – 20.

Задание 41. В ответе могут присутствовать следующие предусмотренные сочетания:

- 1) паспортные данные пассажиров – оптический канал – сканирование паспорта или ввод данных с клавиатуры – скрытая камера, установленная рядом с терминалом (допустимо любое иное устройство, позволяющее подсмотреть информацию с документа или при вводе с клавиатуры) **К1**;
- 2) паспортные данные пассажиров – радиоэлектронный канал – сканирование паспорта или ввод данных с клавиатуры – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) или его общее описание **К2**;
- 3) паспортные данные пассажиров – акустический канал – ввод данных с клавиатуры – подслушивающее устройство, установленное рядом с терминалом (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш **К3**;
- 4) данные других документов пассажиров – оптический канал – сканирование документа – скрытая камера, установленная рядом с терминалом (допустимо любое иное устройство, позволяющее подсмотреть информацию с документа) **К4**;
- 5) данные других документов пассажиров – радиоэлектронный канал – сканирование документа – устройство перехвата ПЭМИН (побочных

электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) или его общее описание **К5**;

6) номер, срок действия и владелец карты (напечатаны на лицевой стороне карты) – оптический канал – момент вставки карты в терминал/получения карты из терминала – скрытая камера, установленная рядом с терминалом (допустимо любое иное устройство, позволяющее подсмотреть информацию с лицевой стороны карты) **К6**;

7) номер, срок действия и владелец карты – радиоэлектронный канал – операции с картой через терминал – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу, или его общее описание) **К7**;

8) CVV-код (напечатан на оборотной стороне карты) – оптический канал – момент вставки карты в терминал/получения карты из терминала – скрытая камера, установленная рядом с терминалом (допустимо любое иное устройство, позволяющее подсмотреть информацию с лицевой стороны карты) **К8**;

9) PIN-код – оптический канал – ввод PIN-кода – скрытая камера, установленная рядом с терминалом (допустимо любое иное устройство, позволяющее подсмотреть информацию с клавиатуры) **К9**;

10) PIN-код – акустический канал – ввод PIN-кода – подслушивающее устройство, установленное рядом с терминалом (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш) **К10**;

11) PIN-код – радиоэлектронный канал – ввод PIN-кода – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) **К11**.

Каждое корректно описанное сочетание – **2 балла** (частичных баллов не предусмотрено, 10 сочетаний из предусмотренных 11 достаточно для получения максимального балла).

Если сумма баллов за корректные сочетания меньше 20, то могут быть начислены бонусные баллы (**К12**):

- за каждое корректное сочетание вне списка предусмотренных – **2 балла**;
- за рассмотрение каждого дополнительного способа или устройства реализации несанкционированного доступа к информации для уже засчитанного сочетания – **1 балл**.

**МАКСИМАЛЬНЫЙ БАЛЛ ЗА ЗАДАНИЕ № 41 – 20.**

Предмет	Технология - Информационная безопасность
Автор	Четвергов А.Б., Дерягин А.В., Седов С.А. и др.
Класс	9
Описание	<p><i>Верхний = 1 дюйм (пт)</i>  <i>Левый = 0,75 дюйм (пт)</i>  <i>Нижний = 1 дюйм (пт)</i>  <i>Правый = 0,75 дюйм (пт)</i>  <i>Ширина = 11,69 дюйм (пт) ЛИСТА</i>  <i>Высота = 8,27 дюйм (пт) ЛИСТА</i>  <i>2 колонки = 2*35,63</i>  <i>Интервал м/у колонками = 2,14</i>  <i>Межстрочный интервал = 1 ИЛИ 1,5</i></p>
Шрифт*	<i>Times New Roman</i>
Размер шрифта*	<i>11</i>
Формат документа*	<i>word</i>
Технический специалист ГАОУ РОЦ*	<i>Бадертдинов Салават Ришатович,  <a href="mailto:3325173080@qq.com">3325173080@qq.com</a>  telegram: badert14</i>

Инструкция олимпиаде
<p><b>Всероссийская олимпиада школьников по технологии</b>  <b>профиль «Информационная безопасность»</b>  <b>Муниципальный этап</b>  <b>9 класс</b></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

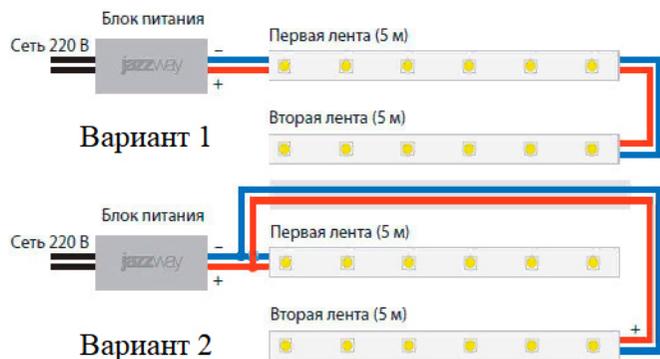
Задание 1. Это устройство, устанавливаемое под кухонной мойкой между сливом и сифоном, которое размалывает пищевые отходы на достаточно мелкие кусочки – обычно менее 2 мм – проходящие через канализационные трубы. Впишите слово (одна ячейка = одна буква).

Задание 2. По двум видам (главному виду и виду слева) построить вид сверху.



Задание 3. Внутри помещения устанавливают светодиодную подсветку длиной 10 метров.

- А) какой вариант подключения двух светодиодных лент к одному блоку питания правильный? В ответе укажите только цифру (1 или 2).
- Б) поясните свой ответ в пункте «А».
- В) для чего светодиодную ленту крепят на алюминиевый профиль?
- Г) какой мощности блок питания следует выбрать, если известно, что мощность светодиодной ленты 4,8 Вт на один метр? В решении считайте коэффициент запаса мощности равным 20%. В ответе запишите мощность, выбрав из следующего списка: 50 Вт, 60 Вт, 80 Вт, 100 Вт, 120 Вт, 150 Вт.



Задание 4. На городских фотографиях США к. XIX – н. XX-го вв. можно увидеть гигантские – до 90 метров в высоту – осветительные вышки. На них ставили дуговые лампы, которые были экономичнее других ламп того времени (газовых и масляных) и давали очень яркий белый свет. На каждой вышке монтировали от 4 до 6 ламп, которые зажигались каждую ночь (за исключением полнолуния) и горели до утра. Один такой светильник давал минимум столько же света, сколько 10 современных 100-ваттных ламп накаливания. Как назывались такие вышки?



Задание 5.

Фирма реализовала товар/услугу за 600 руб. (с НДС 20%). Определите:

- А) Сумму налога на добавленную стоимость (НДС) к уплате. Ответ запишите числом в рублях.
- Б) Сумму налога на прибыль к уплате. Ответ запишите числом в рублях.
- В) Сумму денег, которая осталась у компании после уплаты НДС и налога на прибыль. Ответ запишите числом в рублях.

### 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 «Т» зашифрована сочетанием цифр «42», а слово «ТРУД» – «42 36 43 15».

	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	.	,	?

Таким шифром зашифрован некоторый текст (без пробелов, но с сохранением знаков препинания – точки, запятой и вопросительного знака):

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 41 34 13 16 53 11 33 24 63 34 42 32 16 33 16 33 55 64

Установите, сколько слов зашифровано в сообщении.

Задание 7. Напишите третье слово открытого текста (*смотрите зашифрованное сообщение в задании 6*) без изменения его написания.

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

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

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

Задание 10. Установите шифробозначение (замену) буквы «С» в шифртексте 35 34 23 42 43 35 34 26

Задание 11. Для обеспечения контроля пропуска сотрудников была нанята охрана и установлены пропускные турникеты, при этом руководитель отдела информационной безопасности решил заменить пропуск на универсальный ключ доступа. Какой тип аутентификации тут предусмотрен?

- А) \_однофакторная аутентификация\_
- Б) \_двухфакторная аутентификация\_
- В) \_многофакторная аутентификация\_

*Условие (описание ситуации) для заданий №№ 12-14:*

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

Задание 12. 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) \_однофакторная аутентификация\_
- Б) \_аутентификация на основе фактора владения\_
- В) \_аутентификация по ЭЦП\_
- Г) \_двухфакторная аутентификация\_

Задание 13. 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) \_биометрическая аутентификация\_
- Б) \_аутентификация на основе фактора знания\_
- В) \_аутентификация по ЭЦП\_

– Г) \_аутентификация по GPS\_

Задание 14. 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) \_трёхфакторная аутентификация\_
- Б) \_однофакторная аутентификация\_
- В) \_двухфакторная аутентификация\_

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

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

Задание 15. 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) \_целостность похищенных данных\_
- Б) \_доступность похищенных данных\_
- В) \_конфиденциальность похищенных данных\_

Задание 16. 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) \_целостность похищенных данных\_
- Б) \_доступность похищенных данных\_
- В) \_конфиденциальность похищенных данных\_

Задание 17. 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) \_целостность хранимых данных\_
- Б) \_доступность хранимых данных\_
- В) \_конфиденциальность хранимых данных\_

Задание 18. 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 целостность передаваемой информации\_
- Б) \_не нарушили безопасность передаваемой информации\_
- В) \_нарушили достоверность передаваемой информации\_
- Г) \_нарушили доступность передаваемой информации\_

**Условие (описание ситуации) для заданий №№ 19-22:**

**В компании «E» 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 19. 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) \_целостность похищенных данных\_
- Б) \_доступность похищенных данных\_
- В) \_конфиденциальность похищенных данных\_

Задание 20. Обнаружив пропажу, системный администратор немедленно заблокировал учётные записи пользователей, чьи пароли были на похищенном носителе, тем самым

- А) \_нарушил целостность информации в системе компании\_
- Б) \_нарушил доступность информации, к которой имели доступ пользователи\_
- В) \_предотвратил угрозу нарушения конфиденциальности информации на носителе\_

Задание 21. 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) \_целостность данных\_
- Б) \_доступность данных\_
- В) \_конфиденциальность данных\_

Задание 22. 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) \_целостность данных\_
- Б) \_доступность данных\_
- В) \_конфиденциальность данных\_

**Условие (описание ситуации) для заданий №№ 23-26:**

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

Задание 23. 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) \_электронная подпись\_
- Б) \_вычисление контрольной суммы\_
- В) \_система хэширования\_
- Г) \_надёжные цифровые водяные знаки\_

Задание 24. 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) \_обеспечение целостности хранимых на сервере файлов\_
- Б) \_обеспечение контроля достоверности поступающих сообщений\_
- В) \_контроль неизменности отправляемых сообщений\_

Задание 25. Для функций хэширования коллизией называется

- А) \_ситуация, когда невозможно корректно вычислить значение функции хэширования\_
- Б) \_входное значение, для которого не определено выходное значение функции\_
- В) \_значение функции, для которого не определено ни одного входного значения\_
- Г) \_пара входных значений, для которых значения функции совпадают\_

Задание 26. В отдельных случаях для контроля целостности могут применяться цифровые водяные знаки. Для решения какой задачи они используются?

- А) \_контроль целостности записей в базе данных\_
- Б) \_контроль неизменности данных, хранимых на сервере\_
- В) \_контроль неизменности продуктов, распространяемых по лицензии\_

**Условие (описание ситуации) для заданий №№ 27-30:**

**Компании «О» требуется уделять внимание обеспечению целостности обрабатываемой информации.**

Задание 27. 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 клиентам в зашифрованном виде.

- А) \_электронная подпись\_
- Б) \_надежные цифровые водяные знаки\_
- В) \_функции хэширования\_
- Г) \_хрупкие цифровые водяные знаки\_

Задание 28. Укажите меру из перечисленных ниже, которая наиболее предпочтительна для клиентов облачного хранилища с целью контроля целостности хранимых в нём данных.

- А) \_электронная подпись\_
- Б) \_надежные цифровые водяные знаки\_
- В) \_функции хэширования\_
- Г) \_хрупкие цифровые водяные знаки\_

Задание 29. Передавая партнёрам программные продукты, дальнейшее распространение которых не допускается лицензионным соглашением, компании следует использовать для отслеживания несанкционированного распространения

- А) \_электронная подпись\_
- Б) \_надежные цифровые водяные знаки\_
- В) \_функции хэширования\_
- Г) \_хрупкие цифровые водяные знаки\_

Задание 30. Укажите две меры, которые компания может использовать для подтверждения внесения клиентами изменений в библиотеку распространённого по лицензии программного обеспечения.

- А) \_электронная подпись\_
- Б) \_надежные цифровые водяные знаки\_
- В) \_функции хэширования\_
- Г) \_хрупкие цифровые водяные знаки\_

**Условие (описание ситуации) для заданий №№ 31-32:**

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

Задание 31. 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?

- А) \_двухфакторная на основе факторов владения и биометрии\_
- Б) \_двухфакторная на основе факторов знания и владения\_
- В) \_двухфакторная на основе факторов знания и биометрии\_

Задание 32. 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 на основе факторов знания и биометрии\_
- Б) \_двухфакторная на основе факторов знания и владения\_
- В) \_двухфакторная биометрическая на основе факторов знания и владения\_

**Условие (описание ситуации) для заданий №№ 33-36:**

***Компания «Z» 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 33. Выберите все правильные ответы. На начальном этапе атаки нарушители внедрили в базы данных систем, в которых было развёрнуто

решение от компании «Z», вредоносную программу, которая могла заблокировать или исказить (каждое из этих действий было реализовано примерно в половине заражённых систем) записи о действиях пользователей. Реализация такой угрозы нарушила

- А) \_целостность похищенных данных\_
- Б) \_доступность похищенных данных\_
- В) \_конфиденциальность похищенных данных\_

Задание 34. 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 целостность удаленных данных\_
- Б) \_не нарушили информационную безопасность\_
- В) \_нарушили доступность удаленных данных\_
- Г) \_нарушили конфиденциальность удаленных данных\_

Задание 35. Выберите все правильные ответы. Другие клиенты компании «Z» приняли решение передать собранные данные на хранение в облачное хранилище, уже контролирующееся нарушителями. Что могут нарушить злоумышленники, полностью контролируя такое хранилище?

- А) \_целостность хранимых данных\_
- Б) \_доступность хранимых данных\_
- В) \_конфиденциальность хранимых данных\_

Задание 36. 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) \_обеспечило целостность собираемой информации\_
- Б) \_обеспечило конфиденциальность собираемой информации\_
- В) \_нарушило конфиденциальность собираемой информации\_
- Г) \_нарушило доступность собираемой информации\_
- Д) \_никак не повлияло на информационную безопасность\_

**Условие (описание ситуации) для заданий №№ 37-38:**

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

Задание 37. Укажите меру из предложенных ниже, подходящую для контроля целостности записей на сервере, сохраняемых в виде файлов, в которые не производится запись.

- А) \_электронная подпись\_
- Б) \_система контроля версий\_
- В) \_функции хэширования\_
- Г) \_цифровая подпись\_

Задание 38. Для схем цифровой подписи открытый (публичный) ключ используется для

- А) \_проверки электронной подписи\_
- Б) \_вычисления значения функции хэширования\_
- В) \_для формирования электронной подписи\_
- Г) \_зашифрования отправляемых сообщений\_

Задание 39. Строя коллизию для известной функции хэширования, нарушитель стремится

- А) \_подобрать входное значение функции, для которой известен результат вычисления функции\_
- Б) \_нарушить целостность отправляемого сообщения\_
- В) \_не дать возможность заметить внесённые в передаваемую информацию изменения\_
- Г) \_осуществить подмену информации, от которой вычислена функция\_

Задание 40. Для качественной функции хэширования одним из требований является

- А) \_существенное изменение значения функции при внесении изменений во входное значение\_
- Б) \_отсутствие коллизий, вычисляемых при известной размерности выходного значения\_
- В) \_простота вычисления прообраза\_
- Г) \_простота вычисления значения функции\_

**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. Авиакомпания для облегчения пилотирования самолётов устанавливает на них системы автоматического управления (автопилот). Для запуска работы такой системы пилот должен ввести координаты пунктов отправления и назначения, параметры самолёта, а также авторизационные данные для связи с наземными диспетчерскими службами по пути следования.

Недавно были обнаружены случаи перехвата вводимой пилотами информации (пункты отправления и назначения не являются секретными, но точный маршрут и промежуточные точки следования, а также служебные сведения компания желает сохранить конфиденциальными для обеспечения безопасности перелёта).

1. Оцените, какие сведения о перелёте могут быть перехвачены злоумышленниками из системы автоматического управления 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 пилота или в какие моменты работы автопилота) эти угрозы могут быть реализованы. Аргументируйте свою оценку.



Задание 19. Ответ \_\_\_\_\_.

Задание 20. Ответ \_\_\_\_\_.

Задание 21. Ответ \_\_\_\_\_.

Задание 22. Ответ \_\_\_\_\_.

Задание 23. Ответ \_\_\_\_\_.

Задание 24. Ответ \_\_\_\_\_.

Задание 25. Ответ \_\_\_\_\_.

Задание 26. Ответ \_\_\_\_\_.

Задание 27. Ответ \_\_\_\_\_.

Задание 28. Ответ \_\_\_\_\_.

Задание 29. Ответ \_\_\_\_\_.

Задание 30. Ответ \_\_\_\_\_.

Задание 31. Ответ \_\_\_\_\_.

Задание 32. Ответ \_\_\_\_\_.

Задание 33. Ответ \_\_\_\_\_.

Задание 34. Ответ \_\_\_\_\_.

Задание 35. Ответ \_\_\_\_\_.

Задание 36. Ответ \_\_\_\_\_.

Задание 37. Ответ \_\_\_\_\_.

Задание 38. Ответ \_\_\_\_\_.

Задание 39. Ответ \_\_\_\_\_.

Задание 40. Ответ \_\_\_\_\_.

Задание 41. Ответ:

Задание 41. Лист для ответа

### Ключи

**МАКСИМАЛЬНЫЙ БАЛЛ ЗА ВСЕ ЗАДАНИЯ – 100.**

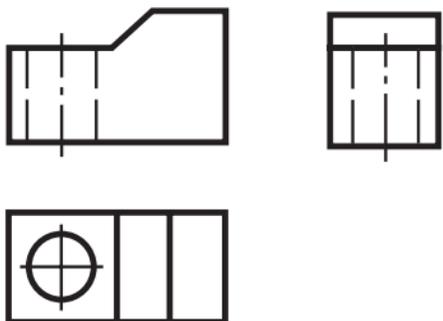
#### Общая часть

**ЗАДАНИЯ №№ 1-5 ОЦЕНИВАЮТСЯ В 2 БАЛЛА (ставить 0 или 2)**

Задание 1.

Д	И	С	П	О	У	З	Е	Р
---	---	---	---	---	---	---	---	---

Задание 2.



Задание 3.

– А) 1.

– Б) **ОТВЕТ ОЦЕНИВАЕТСЯ ПО ОБЩЕМУ СМЫСЛУ**

Потому что пять метров – это расчетная длина, которую могут выдержать токоведущие дорожки ленты. При большей длине, нагрузка будет превышать допустимую и лента обязательно выйдет из строя.

*Кроме того, будет наблюдаться неравномерность свечения. В начале ленты светодиоды будут светить ярко, а в конце гораздо тусклее.*

– В) Алюминиевый профиль выполняет роль теплоотвода.

– Г) 60\*

\*Прим. для жюри:  $4,8 \text{ (Вт/м)} \times 10 \text{ (м)} \times 0,2 = 57,6 \text{ Вт}$ . Выбираем блок 60 Вт.

Задание 4. Башни лунного света (лунные башни)

Задание 5.

– А) 100\*

– Б) 100\*

– В) 400

\*Прим. для жюри:

НДС считаем по формуле  $600 \times 20 / 120$ . Т.е. 600 это не 100 %, а 120 %.  
После уплаты НДС остается 500 рублей.

Налог на прибыль считаем по формуле  $500 \times 20 / 100$ . Т.е. 500 это 100 %.

#### Специальная часть

**ЗАДАНИЯ №№ 6-40 ОЦЕНИВАЮТСЯ В 2 БАЛЛА (ставить 0 или 2)**

Задание 6. 6

Задание 7. ТОЛЬКО

Задание 8. 42164533343134142463.

Задание 9. – В) РЕПЕТИЦИЯ

Задание 10. 23

Задание 11. – А) однофакторная аутентификация

Задание 12. – А) однофакторная аутентификация

– Б) аутентификация на основе фактора владения

Задание 13. – А) биометрическая аутентификация

Задание 14. – А) трёхфакторная аутентификация

Задание 15. – В) конфиденциальность похищенных данных

Задание 16. – А) целостность похищенных данных

– В) конфиденциальность похищенных данных

Задание 17. – А) целостность хранимых данных

– Б) доступность хранимых данных

- Задание 18. – Б) не нарушили безопасность передаваемой информации
- Задание 19. – Б) доступность похищенных данных  
– В) конфиденциальность похищенных данных
- Задание 20. – Б) нарушил доступность информации, к которой имели доступ пользователи
- Задание 21. – А) целостность данных  
– Б) доступность данных  
– В) конфиденциальность данных
- Задание 22. – А) целостность данных  
– Б) доступность данных
- Задание 23. – А) электронная подпись
- Задание 24. – А) обеспечение целостности хранимых на сервере файлов
- Задание 25. – Г) пара входных значений, для которых значения функции совпадают
- Задание 26. – В) контроль неизменности продуктов, распространяемых по лицензии
- Задание 27. – В) функции хэширования
- Задание 28. – А) электронная подпись
- Задание 29. – Б) надежные цифровые водяные знаки
- Задание 30. – В) функции хэширования  
– Г) хрупкие цифровые водяные знаки
- Задание 31. – А) двухфакторная на основе факторов владения и биометрии
- Задание 32. – В) двухфакторная биометрическая на основе факторов знания и владения
- Задание 33. – А) целостность похищенных данных  
– Б) доступность похищенных данных
- Задание 34. – Б) не нарушили информационную безопасность
- Задание 35. – А) целостность хранимых данных  
– Б) доступность хранимых данных  
– В) конфиденциальность хранимых данных
- Задание 36. – В) нарушило конфиденциальность собираемой информации
- Задание 37. – В) функции хэширования
- Задание 38. – А) проверки электронной подписи
- Задание 39. – Г) осуществить подмену информации, от которой вычислена функция
- Задание 40. – А) существенное изменение значения функции при внесении изменений во входное значение
- Задание 41. В ответе должны присутствовать следующие предусмотренные сочетания:
- 1) маршрут перелёта – оптический канал – ввод пунктов следования пилотом/отображение маршрута на экране в процессе полёта – скрытая камера, установленная рядом с пультом управления пилота (допустимо любое иное устройство, позволяющее подсмотреть информацию при вводе илис экрана места пилота) **K1**;

2) маршрут перелёта – акустический канал – ввод пунктов следования пилотом – подслушивающее устройство, установленное рядом с пультом управления пилота (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш) **К2**;

3) маршрут перелёта – радиоэлектронный канал – ввод пунктов следования пилотом/работа автопилота с маршрутом перелёта – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу **К3**;

4) параметры (технические данные) самолёта – ввод пилотом в начале полёта – скрытая камера, установленная рядом с пультом управления пилота (допустимо любое иное устройство, позволяющее подсмотреть информацию при вводе или с экрана места пилота) **К4**;

5) параметры (технические данные) самолёта – ввод пилотом в начале полёта/ работа автопилота – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу **К5**;

6) авторизационные данные для связи с наземными службами – ввод пилотом в начале полёта – скрытая камера, установленная рядом с пультом управления пилота (допустимо любое иное устройство, позволяющее подсмотреть информацию при вводе) **К6**;

7) авторизационные данные для связи с наземными службами – ввод пилотом в начале полёта – подслушивающее устройство, установленное рядом с пультом управления пилота (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш) **К7**;

8) авторизационные данные для связи с наземными службами – ввод пилотом в начале полёта/связь на протяжении перелёта – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) **К8**.

Каждое корректно описанное сочетание – **2 балла** (частичных баллов не предусмотрено).

Могут быть начислены бонусные баллы в пределах 20 баллов за всё задание (**К9**):

- каждое корректное сочетание вне списка предусмотренных – **2 балла**;
- приведено более одного устройства для уже засчитанного сочетания – **1 балл**.

**МАКСИМАЛЬНЫЙ БАЛЛ ЗА ЗАДАНИЕ № 41 – 20.**

Предмет	Технология - Информационная безопасность
Автор	Четвергов А.Б., Дерягин А.В., Седов С.А. и др.
Класс	10-11
Описание	<p><i>Верхний = 1 дюйм (пт)</i>  <i>Левый = 0,75 дюйм (пт)</i>  <i>Нижний = 1 дюйм (пт)</i>  <i>Правый = 0,75 дюйм (пт)</i>  <i>Ширина = 11,69 дюйм (пт) ЛИСТА</i>  <i>Высота = 8,27 дюйм (пт) ЛИСТА</i>  <i>2 колонки = 2*35,63</i>  <i>Интервал м/у колонками = 2,14</i>  <i>Межстрочный интервал = 1 ИЛИ 1,5</i></p>
Шрифт*	<i>Times New Roman</i>
Размер шрифта*	<i>11</i>
Формат документа*	<i>word</i>
Технический специалист ГАОУ РОЦ*	<i>Бадертдинов Салават Ришатович,  <a href="mailto:3325173080@qq.com">3325173080@qq.com</a>  telegram: badert14</i>

Инструкция олимпиаде
<p><b>Всероссийская олимпиада школьников по технологии  профиль «Информационная безопасность»  Муниципальный этап  10-11 классы</b></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:

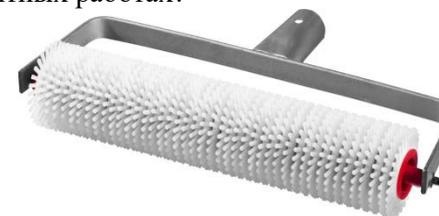
– А) Сколько денег останется у организации после уплаты (вычета) НДС?

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 клиентам 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?

- Б) \_двухфакторная биометрическая на основе факторов знания и владения\_
- В) \_двухфакторная на основе факторов знания и биометрии\_
- А) \_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.

**Бланк ответов**

Общая часть

Специальная часть

Задание 1. Решение \_\_\_\_\_

\_\_\_\_\_

Ответ \_\_\_\_\_

Задание 2. Решение \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Ответ \_\_\_\_\_

Задание 3.

– А) \_\_\_\_\_

– Б) \_\_\_\_\_

– В) \_\_\_\_\_

Задание 4. \_\_\_\_\_

\_\_\_\_\_

Задание 5.

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

Задание 6. Ответ \_\_\_\_\_.

Задание 7. Ответ \_\_\_\_\_.

Задание 8. Ответ \_\_\_\_\_.

Задание 9. Ответ \_\_\_\_\_.

Задание 10. Ответ \_\_\_\_\_.

Задание 11. Ответ \_\_\_\_\_.

Задание 12. Ответ \_\_\_\_\_.

Задание 13. Ответ \_\_\_\_\_.

Задание 14. Ответ \_\_\_\_\_.

Задание 15. Ответ \_\_\_\_\_.

Задание 16. Ответ \_\_\_\_\_.

Задание 17. Ответ \_\_\_\_\_.

Задание 18. Ответ \_\_\_\_\_.

Шифр участника ИБ\_10-11 — \_\_\_\_\_

Задание 19. Ответ \_\_\_\_\_.

Задание 20. Ответ \_\_\_\_\_.

Задание 21. Ответ \_\_\_\_\_.

Задание 22. Ответ \_\_\_\_\_.

Задание 23. Ответ \_\_\_\_\_.

Задание 24. Ответ \_\_\_\_\_.

Задание 25. Ответ \_\_\_\_\_.

Задание 26. Ответ \_\_\_\_\_.

Задание 27. Ответ \_\_\_\_\_.

Задание 28. Ответ \_\_\_\_\_.

Задание 29. Ответ \_\_\_\_\_.

Задание 30. Ответ \_\_\_\_\_.

Задание 31. Ответ \_\_\_\_\_.

Задание 32. Ответ \_\_\_\_\_.

Задание 33. Ответ \_\_\_\_\_.

Задание 34. Ответ \_\_\_\_\_.

Задание 35. Ответ \_\_\_\_\_.

Задание 36. Ответ \_\_\_\_\_.

Задание 37. Ответ \_\_\_\_\_.

Задание 38. Ответ \_\_\_\_\_.

Задание 39. Ответ \_\_\_\_\_.

Задание 40. Ответ \_\_\_\_\_.

Задание 41. Ответ:

Задание 41. Лист для ответа

### Ключи

## МАКСИМАЛЬНЫЙ БАЛЛ ЗА ВСЕ ЗАДАНИЯ – 100.

### Общая часть

#### ЗАДАНИЯ №№ 1-5 ОЦЕНИВАЮТСЯ В 2 БАЛЛА (ставить 0 или 2)

Задание 1. Решение: посчитаем экономию в кВт.

$$(60-5) \times 3 \text{ лампы} \times 8 \text{ часов} \times 30 \text{ дней} = 39600 \text{ Вт} = 39,6 \text{ кВт}$$

Вычислим экономию в руб.:  $39,6 \times 3,58 = 141,77$  руб.

Ответ: 141,77 руб.

Задание 2. Решение: Если площадь по полу 30 кв.м, а одна из стен 5 м,

то другая стена д.б. 6 м. Т.о. периметр =  $5 \times 2 + 6 \times 2 = 22$  м.

Площадь окрашенных стен =  $22 \times 2,75 - 5,5 = 55$  кв.м

Вычислим расход краски  $55 \times 0,15 \text{ кг} \times 2 \text{ слоя} = 16,5$  кг

Краска продается в банках по 2,5 кг, т.е. понадобилось 7 банок краски

( $16,5 / 2,5 = 6,6 = 7$ ). Определим расходы  $7 \times 1000 = 7000$  руб.

Ответ: 7000 руб.

Задание 3.

– А) 125\*

– Б) 25\*

– В) 100

\*Прим. для жюри: Организация купила НДС на сумму  $600 \times 20 / 120 = 100$ .

Организация продала НДС на сумму  $450 \times 20 / 120 = 75$ .

Таким образом, к уплате подлежит  $100 - 75 = 25$  руб. НДС

После покупки-продажи у организации осталось 150 руб. ( $600 - 450$ ).

После уплаты НДС в налоговую у организации останется  $150 - 25 = 125$ .

Сумма налога на прибыль к уплате организацией рассчитывается от 125.

Налог на прибыль считаем по формуле  $125 \times 20 / 100 = 25$ .

Сумма денег, которая останется у организации после уплаты НДС и налога на прибыль,  $150 - 25 - 25 = 100$ .

Задание 4. **ОТВЕТ ОЦЕНИВАЕТСЯ ПО ОБЩЕМУ СМЫСЛУ**

Валик используется для наливного пола - для устранения образовавшихся там пузырьков воздуха (позволяет выпустить лишний воздух из стяжки еще на этапе, когда состав не высох)

Задание 5.

– Б) Y	– Е) R
– В) W	– Ж) S
– Г) F	– З) Q

### Специальная часть

#### ЗАДАНИЯ №№ 6-40 ОЦЕНИВАЮТСЯ В 2 БАЛЛА (ставить 0 или 2)

Задание 6. 17

Задание 7. ОТМЕНЕНЫ

Задание 8. 42164533344144163611

Задание 9. – А) РЕПУТАЦИЯ

Задание 10. 31

Задание 11. – Г) функции хэширования

Задание 12. – Б) электронная подпись

Задание 13. – В) надежные цифровые водяные знаки

Задание 14. – А) хрупкие цифровые водяные знаки  
– Г) функции хэширования

Задание 15. – Б) электронная подпись

- Задание 16. – Б) \_обеспечение целостности хранимых на сервере файлов\_
- Задание 17. – А) \_пара входных значений, для которых значения функции совпадают\_
- Задание 18. – А) \_контроль неизменности продуктов, распространяемых по лицензии\_
- Задание 19. – Б) \_однофакторная аутентификация\_  
– В) \_аутентификация на основе фактора владения\_
- Задание 20. – Б) \_биометрическая аутентификация
- Задание 21. – Б) \_трёхфакторная аутентификация\_
- Задание 22. – А) \_конфиденциальность похищенных данных\_  
– В) \_доступность похищенных данных\_
- Задание 23. – В) \_нарушил доступность информации, к которой имели доступ пользователи\_
- Задание 24. – А) \_конфиденциальность данных\_  
– Б) \_целостность данных\_  
– В) \_доступность данных\_
- Задание 25. – Б) \_целостность данных\_  
– В) \_доступность данных\_
- Задание 26. – А) \_конфиденциальность похищенных данных\_
- Задание 27. – А) \_конфиденциальность похищенных данных\_  
– Б) \_целостность похищенных данных\_
- Задание 28. – Б) \_целостность хранимых данных\_  
– В) \_доступность хранимых данных\_
- Задание 29. – В) \_не нарушили безопасность передаваемой информации\_
- Задание 30. – Б) \_целостность похищенных данных\_  
– В) \_доступность похищенных данных\_
- Задание 31. – В) \_не нарушили информационную безопасность\_
- Задание 32. – А) \_конфиденциальность хранимых данных\_  
– Б) \_целостность хранимых данных\_  
– В) \_доступность хранимых данных\_
- Задание 33. – Г) \_нарушило конфиденциальность собираемой информации\_
- Задание 34. – Г) \_функции хэширования\_
- Задание 35. – Б) \_проверки электронной подписи\_
- Задание 36. – А) \_осуществить подмену информации, от которой вычислена функция\_
- Задание 37. – Б) \_существенное изменение значения функции при внесении изменений во входное значение\_
- Задание 38. – В) \_двухфакторная на основе факторов владения и биометрии
- Задание 39. – Б) \_двухфакторная биометрическая на основе факторов знания и владения\_
- Задание 40. – Б) \_двухфакторная на основе факторов знания и владения\_

### МАКСИМАЛЬНЫЙ БАЛЛ ЗА ЗАДАНИЕ № 41 – 20.

Задание 41. В ответе должны присутствовать следующие предусмотренные сочетания:

1) маршрут поездки – радиоэлектронный канал – работа устройства управления автомобиля с маршрутом поездки – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) **К1**;

2) номер, срок действия и владелец карты (напечатаны на лицевой стороне карты) – оптический канал – момент вставки карты в систему приёма оплаты/получения карты из системы/контакта карты с системой – скрытая камера, установленная рядом с устройством приёма оплаты (допустимо любое иное устройство, позволяющее подсмотреть информацию с лицевой стороны карты) **К2**;

3) номер, срок действия и владелец карты (напечатаны на лицевой стороне карты) – радиоэлектронный канал – операции с картой в устройстве приёма оплаты/оплата в мобильном приложении – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу, или его общее описание) **К3**;

4) CVV-код (напечатан на оборотной стороне карты) – оптический канал – момент вставки карты в систему приёма оплаты/получения карты из системы/контакта карты с системой – скрытая камера, установленная рядом с устройством приёма оплаты (допустимо любое иное устройство, позволяющее подсмотреть информацию с обратной стороны карты) **К4**;

5) PIN-код – оптический канал – ввод PIN-кода – скрытая камера, установленная рядом с устройством приёма оплаты (допустимо любое иное устройство, позволяющее подсмотреть информацию с клавиатуры) **К5**;

6) PIN-код – акустический канал – ввод PIN-кода – подслушивающее устройство, установленное рядом с устройством приёма оплаты (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш) **К6**;

7) PIN-код – радиоэлектронный канал – ввод PIN-кода – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу) **К7**.

Каждое корректно описанное сочетание – **2 балла** (частичных баллов не предусмотрено).

За полноту рассмотрения описанной в задаче ситуации

- рассмотрены все каналы утечки информации хотя бы в одном сочетании – **1 балл**;

- рассмотрены все предусмотренные виды информации – **1 балл**.

Могут быть начислены бонусные баллы в пределах 20 баллов за всё задание (**К9**):

- каждое корректное сочетание вне списка предусмотренных – **2 балла**;

- приведено более одного устройства для уже засчитанного сочетания – **1 балл**.

### МАКСИМАЛЬНЫЙ БАЛЛ ЗА ЗАДАНИЕ № 41 – 20.