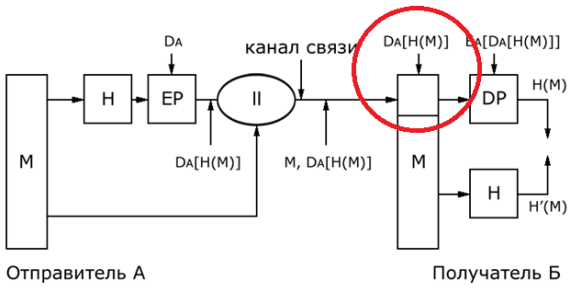
Ключи к теоретическим заданиям по профилю «Информационная безопасность»

10-11 классы

Вопрос	Ответ	
	Общая часть	
1	ж	1 балл
2	3505+1206+5050+ +580+907 =11248	1 балл
3	(2500000-2000000) х 0,2 = 500000 х 0,2 = 100000 руб. 100000 + (500000 + 200000) х 0,2 + (500000 + 200000 + 350000) х 0,2 = 450000 руб. ОТВЕТ: 450 тыс. руб.	1 балл
4	а	1 балл
5	Wi-Fi, Z-Wave, Zigbee, Thread, Bluetooth, ИК порт	1 балл
	Специальная часть	
6	**Сведения** — это знания, передаваемые в виде сообщений, уведомлений и сигналов.	2 балла
7	Информационная безопасность	1 балл
8	идентификации	2 балла
9	Рассмотрим сумму нового пароля **SARCL** и известного старого пароля СВЕЧА, от числовых значений которого взяты остатки от деления на 26. От значений полученной суммы также возьмём остатки от деления на 26: S A R C L + 19 1 18 3 12 = 12 4 24 2 13. С В Е Ч А 19 3 6 25 1 Таким образом, получено зашифрованное сообщение, переданное Катей и искаженное на приемном конце программой Юры. На самом деле зашифровывание осуществлялось в русском алфавите, поэтому для некоторых числовых значений зашифрованного сообщения возможны варианты: 12 (4, 4+26) 24 (2, 2+26) 13 – 12 (4, 30) 24 (2, 28) 13. Вычтем теперь из полученных числовых вариантов зашифрованного пароля числовые значения старого пароля в русском алфавите 19 3 6 25 1: –7 (1, 27) 18 (–23, 3) 12 и возьмём от полученных разностей остатки от деления на 33, получим: 26 (1, 27) 18 (10, 3) 12 = Ш (А, Щ) Р (И, В) К Единственный читаемый вариант – ШАРИК. Ответ: **ШАРИК**	10 баллов
10	В -передачи или копирования легальными пользователями секретной информации за пределы защищаемой системы	2балла
11	В современных системах цифровой связи для борьбы с потерей информации при передаче часто применяется следующий прием. Все сообщение разбивается на порции — блоки. Для каждого блока вычисляется **контрольная сумма** (сумма двоичных цифр), которая передается вместе с данным блоком. В месте приема заново вычисляется контрольная сумма принятого блока и, если она не совпадает с первоначальной суммой, передача данного блока повторяется. Так происходит до тех пор, пока исходная и конечная контрольные суммы не совпадут.	6 баллов
12	1-А, 2 – В, 3 – Г, 4 - Б	8 баллов (по 2

<table>
<tr><td></td><td></td><td>балла за каждую верную пару)</td></tr>
<tr><td>13</td><td>
<table>
<tr><th></th><th>этапы инновационной деятельности</th><th>этапы жизненного цикла инновации</th></tr>
<tr><td>I</td><td>опытно-конструкторские работы</td><td>фундаментальные исследования</td></tr>
<tr><td>II</td><td>опытно-конструкторские работы</td><td>прикладные исследования</td></tr>
<tr><td>III</td><td>изготовление опытного образца</td><td>коммерциализация новации</td></tr>
<tr><td>IV</td><td>изготовление головного образца</td><td>коммерциализация новации</td></tr>
<tr><td>V</td><td>организация производства опытных партий новой техники</td><td></td></tr>
</table>
</td><td>2 балла</td></tr>
<tr><td>14</td><td>N=90 K=389 Ответ 1 9 89
N=91 K=89 Ответ 10
N=161 K=10 Ответ 0
N=200 K=60 Ответ 1 39</td><td>8 баллов (за каждый правильный ответ по 2балла)</td></tr>
<tr><td>15</td><td>Криптография с открытым ключом имеет недостаток в низкой скорости, а поэтому применяется при шифровании/дешифровании коротких сообщений (ключа симметричного шифрования, хеш-кода).</td><td>4 балла</td></tr>
<tr><td>16</td><td> 
</td><td>10 баллов</td></tr>
<tr><td>17</td><td>a); d)</td><td>4 балла (по 2 балла за ответ)</td></tr>
<tr><td>18</td><td>источники угроз безопасности информации включают работников офиса, сбои самого компьютера, вредоносные программы</td><td>1 балл</td></tr>
<tr><td>19</td><td>Перечислены компоненты системы «Умный дом».
«Умный дом» – это совокупность электронных и электронно-механических компонентов, которые предоставляют человеку возможность дистанционного управления и отслеживания всего происходящего в квартире или доме. Система автоматизации работы бытовых устройств, выполняющих рутинные домашние дела. В неё могут входить инженерные системы, бытовая, мультимедийная, климатическая техника и системы безопасности.
Основные принципы защиты:
Первый шаг – создать отдельную сеть для устройств умного</td><td>9 баллов
(3)

(3)</td></tr>
</table>

	дома. Это довольно просто: нужно просто настроить для них гостевые сети. Так вы не защитите само IoT-устройство: ваш холодильник по-прежнему можно будет взломать и сделать частью ботнета, который рассылает спам или майнит криптовалюты. Но преступники не смогут добраться до вашей электронной почты или банковского счета – ведь взломанный холодильник хранит данные в гостевой сети, из которой нельзя попасть в домашнюю. Гостевые сети помогут защитить ваш Wi-Fi и от других угроз. Второй шаг – защитить все устройства, которые обрабатывают ваши данные: умные колонки, роутер, компьютер, смартфон и другую умную технику. Если ваш смартфон взломают или украдут, вся ваша домашняя сеть может быть скомпрометирована. А ее безопасность – главный приоритет.	(3)
20	В	1 балл
21	**Творческое задание.** Достаточным является лаконичный ответ, содержащий ответы на пункты 1–3 в сочетании «информация (конкретные данные из приведённых в условии) – канал утечки – момент времени (действия клиента банка) – способ реализации угрозы (средство)» В ответе должны присутствовать следующие предусмотренные сочетания: 1) номер, срок действия и владелец карты (напечатаны на лицевой стороне карты) – оптический канал – вставление карты в банкомат/получение карты из банкомата – скрытая камера, установленная рядом с банкоматом (допустимо любое иное устройство, позволяющее подсмотреть информацию с лицевой стороны карты, например, так называемый скимер); 2) номер, срок действия и владелец карты – радиоэлектронный канал – совершение операций на экране банкомата – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу, например, так называемый скимер или его общее описание); 3) CVV-код (напечатан на оборотной стороне карты) – оптический канал – вставление карты в банкомат/получение карты из банкомата – скрытая камера, установленная рядом с банкоматом (допустимо любое иное устройство, позволяющее подсмотреть информацию с лицевой стороны карты, например, так называемый скимер); 4) PIN-код – оптический канал – ввод PIN-кода – скрытая камера, установленная рядом с банкоматом (допустимо любое иное устройство, позволяющее подсмотреть информацию с клавиатуры); 5) PIN-код – акустический канал – ввод PIN-кода – подслушивающее устройство, установленное рядом с банкоматом (допустимо любое иное устройство, позволяющее подслушать нажатия клавиш); 6) PIN-код – радиоэлектронный канал – ввод PIN-кода – устройство перехвата ПЭМИН (побочных электромагнитных излучений и наводок) (допустимо любое устройство, действующее по такому принципу, например, так называемый скимер или его общее описание). □ Каждое корректно описанное сочетание: +1 балл. □ Рассмотрены все каналы утечки информации хотя бы в одном сочетании: +1 балл. □ Рассмотрены все предусмотренные виды информации: +1 балл.	

	□ Перечислены все предусмотренные варианты: +1 балл. □ Каждое некорректное сочетание: –1 балл. □ Каждое корректное сочетание вне списка предусмотренных: +1 балл. □ Приведено более одного устройства для уже засчитанного сочетания: +1 балл. □ **Максимальное количество баллов: 25**	
	итого	**100 баллов**