

ВСЕРОССИЙСКАЯ ОЛИМПИАДА ШКОЛЬНИКОВ ПО ТЕХНОЛОГИИ
РЕГИОНАЛЬНЫЙ ЭТАП
ТЕОРЕТИЧЕСКИЙ ТУР
10 класс

Профиль «Информационная безопасность»

Уважаемый участник олимпиады!

Вам предстоит выполнить теоретические и тестовые задания.

Время выполнения заданий теоретического тура 2 академических часа (120 минут).

Выполнение тестовых заданий целесообразно организовать следующим образом:

- не спеша, внимательно прочитайте тестовое задание;
- обратите внимание, что задания, в которых варианты ответа являются продолжением текста задания, предполагают единственный ответ; задания, в которых имеется инструкция «укажите все», предполагает несколько верных ответов;
- определите, какой (или какие) из предложенных вариантов ответа наиболее верный и полный; другие варианты ответа могут быть частично верными, верными, но неточными или неполными, верными без учета условий конкретного задания – такие ответы признаются неверными при наличии более точного, полного или учитывающего условия варианта;
- напишите букву (или набор букв), соответствующую выбранному Вами ответу;
- продолжайте таким образом работу до завершения выполнения тестовых заданий;
- после выполнения всех предложенных заданий еще раз удостоверьтесь в правильности ваших ответов;
- если потребуется корректировка выбранного Вами варианта ответа, то неправильный вариант ответа зачеркните крестиком, и рядом напишите новый.

Выполнение теоретических (письменных, творческих) заданий целесообразно организовать следующим образом:

- не спеша, внимательно прочитайте задание и определите, наиболее верный и полный ответ;
- отвечая на теоретический вопрос, обдумайте и сформулируйте конкретный ответ только на поставленный вопрос;
- если Вы выполняете задание, связанное с заполнением таблицы или схемы, формализованным описанием указанного объекта не старайтесь детализировать информацию, вписывайте только те сведения или данные, которые указаны в вопросе;
- после выполнения всех предложенных заданий еще раз удостоверьтесь в правильности выбранных Вами ответов и решений.

Предупреждаем Вас, что:

- при оценке тестовых заданий, где необходимо определить один правильный ответ, 0 баллов выставляется за неверный ответ и в случае, если участником отмечены несколько ответов (в том числе правильный), или все ответы;
- при оценке тестовых заданий, где необходимо определить все правильные ответы, 0 баллов выставляется, если участником отмечены неверные ответы, большее количество ответов, чем предусмотрено в задании (в том числе правильные ответы) или все ответы.

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

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

Общая часть

1. На решение какой экологической проблемы направлены следующие меры: сокращение выбросов фреона, использование новых видов авиатоплива, выбрасывание восстанавливающих добавок – жидких смесей водорода и кислорода?

2. Вставьте пропущенное слово и число, выбрав из скобок правильные варианты.

Биоцемент может самостоятельно восстанавливаться благодаря бактериям, компонентам лактата кальция, азота и ____1____ (свинца, фосфора, магния), которые смешиваются с материалом. Эти компоненты могут оставаться активными в биоцементе до __2__ (50, 100, 150, 200, 250) лет. Биоцемент, как и любой другой бетон, может треснуть из-за внешних сил и напряжений. Однако, в отличие от обычного бетона, микроорганизмы в биоцементе могут прорасти при попадании в воду.

3. Установите соответствие между терминами и определениями.

1	Акция	а	Фиксированный доход, получаемый дольщиком компании в результате распределения чистой прибыли
2	Бюджет	б	Имущество, которое служит гарантией возврата займа или кредита
3	Выручка	в	Несовершенная конкуренция, при которой на рынке доминирует небольшое количество организаций
4	Дивиденд	г	Долевая ценная бумага, дающая право голоса при принятии управленческих решений и получение фиксированного дохода по итогам финансового года
5	Залог	д	Финансовый документ, отражающий баланс доходов и расходов организации, физического лица
6	Олигополия	е	Вид интернет-мошенничества, целью которого является похищение платежных реквизитов и паролей пользователей компьютеров
7	Фишинг	ж	Совокупная сумма денежных средств, полученных от основных видов деятельности организации до вычета себестоимости, прочих расходов и налогов

4. Установите соответствие между масштабами изображений и их обозначениями

на чертежах всех отраслей промышленности и строительства, согласно ГОСТ 2.302-68 «ЕСКД. Масштабы»

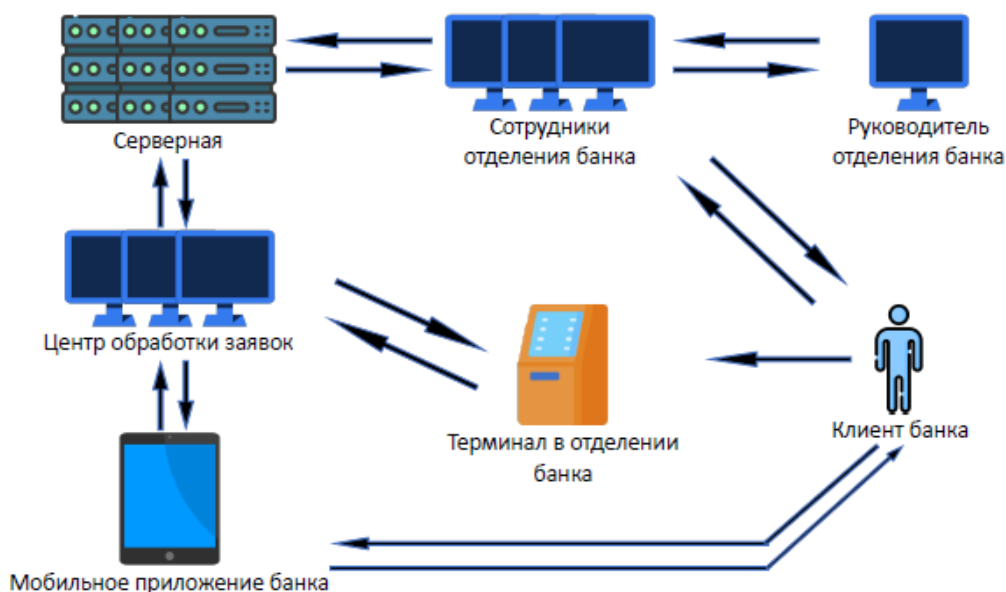
1	Масштабы увеличения	а	1:2; 1:3; 1:4; 1:5; 1:10; 1:15; 1:20; 1:25; 1:40; 1:50; 1:75; 1:100; 1:200; 1:400; 1:500; 1:800; 1:1000
2	Масштабы уменьшения	б	1:1
3	Нет такого ряда в стандарте «ГОСТ 2.302-68»	в	2:1; 2,5:1; 4:1; 5:1; 10:1; 20:1; 40:1; 50:1; 100:1
4	Натуральная величина	г	1:2; 1:2,5; 1:4; 1:5; 1:10; 1:15; 1:20; 1:25; 1:40; 1:50; 1:75; 1:100; 1:200; 1:400; 1:500; 1:800; 1:1000
		д	2:1; 3:1; 4:1; 5:1; 10:1; 20:1; 40:1; 50:1; 100:1

5. Выберите из предложенного списка примеры процессов биотехнологий. Укажите буквы правильных ответов.

- а. – выполнение хирургических операций;
- б. – производство инсулина;
- в. – создание генетически модифицированных продуктов;
- г. – получение кефира из молока;
- д. – разработка плаща–невидимки;
- е. – изготовление чипа-биосенсора.

Специальная часть

Перед Вами схема информационной системы банка. Клиенты банка могут взаимодействовать с центром обработки заявок через мобильное приложение, а также через терминал в отделении банка или непосредственно с сотрудниками отделения. Координация осуществляемых операций производится через сервер банка, а в исключительных случаях сотрудники отделения могут обращаться за принятием решений к руководителю отделения банка, который также может по своему решению взаимодействовать с сотрудниками банка, передавать им индивидуальные распоряжения, поручения и инструкции.



Локальная сеть кафе быстрого питания недавно была реорганизована. Известно, что в ней настроена статическая маршрутизация. У вас есть удалённый доступ к маршрутизаторам компании. С помощью команды **show ip route** можно узнать о подключенных к маршрутизатору сетях. Существует три типа записей:

1) **directly connected** (непосредственно-подключенные) – сети, которые подключены непосредственно к маршрутизатору и на маршрутизаторе настроен интерфейс с адресом из этой сети. Проверяются в первую очередь. Если адрес в ip-пакете принадлежит непосредственно подключённой сети, то он посылается на интерфейс, находящийся в этой сети

2) **static** (статический) маршрут. Если сеть непосредственно не подключена к маршрутизатору, то ему необходимо понимать, на какой соседний маршрутизатор нужно послать пакет, чтобы он дошёл до адресата. Записи данного вида содержат три поля – адрес сети назначения, маска сети, и сетевой адрес следующего маршрутизатора (**next hop**). Разумеется, текущий маршрутизатор должен сам иметь интерфейс в той же сети, что и **next hop**. Чаще всего его обозначают в консольном выводе с помощью «**via**».

3) Маршрут по умолчанию (**gateway of last resort**) – если маршрутизатор не нашёл записей предыдущих типов, то любой пакет отправляется на маршрут по умолчанию. Выглядит он следующим образом – 0.0.0.0/0 **via** 12.13.14.15 (адрес **next hop**).

При попытке проведения анализа защищенности сети выяснилось, что документация по топологии сети была утеряна. Для качественного аудита её требуется восстановить.

Вам удалось посмотреть записи о маршрутизации со всех маршрутизаторов компании. Известно, что их семь, а также то, что сеть имеет три локальных подсети из диапазона адресов 192.168.0.0/16. Для внутренней маршрутизации используются адреса из диапазона 10.0.0.0/8. В сети имеется пограничный

маршрутизатор, который обеспечивает связь с глобальной сетью Интернет (пограничный маршрутизатор – маршрутизатор, связанный как с локальной сетью, так и с глобальной сетью Интернет). Известно, что на маршрутизаторах нет настроенных, но не подключенных интерфейсов, а также то, что если присутствует маршрут по умолчанию, то резервного маршрута нет.

В качестве сокращений для маршрутов и сетей на маршрутизаторах используются следующие обозначения:

Codes: C - connected, S - static, R - RIP, M - mobile, B – BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route

Консольный вывод маршрутизаторов сети:

R1#show ip route

```
Gateway of last resort is 10.10.11.6 to network 0.0.0.0
 10.0.0.0/30 is subnetted, 1 subnets
C    10.10.11.4 is directly connected, FastEthernet0/0
 192.168.1.0/25 is subnetted, 1 subnets
C    192.168.1.0 is directly connected, FastEthernet3/1
S*  0.0.0.0/0 [1/0] via 10.10.11.6
```

R2#show ip route

```
Gateway of last resort is 10.10.1.10 to network 0.0.0.0
 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.10.1.8/29 is directly connected, FastEthernet0/0
C    10.10.11.0/30 is directly connected, FastEthernet1/0
 192.168.1.0/25 is subnetted, 2 subnets
S    192.168.1.0 [1/0] via 10.10.1.11
S    192.168.1.128 [1/0] via 10.10.1.1
S*  0.0.0.0/0 [1/0] via 10.10.1.10
```

R3#show ip route

```
Gateway of last resort is 84.201.172.234 to network 0.0.0.0
 84.0.0.0/30 is subnetted, 1 subnets
C    84.201.172.232 is directly connected, FastEthernet3/1
 10.0.0.0/29 is subnetted, 1 subnets
C    10.10.1.0 is directly connected, FastEthernet0/0
```

```
S 192.168.1.0/24 [1/0] via 10.10.1.1
S 192.168.2.0/24 [1/0] via 10.10.1.2
S* 0.0.0.0/0 [1/0] via 84.201.172.234
```

R4#show ip route

```
Gateway of last resort is 10.10.1.3 to network 0.0.0.0
 10.0.0.0/29 is subnetted, 2 subnets
C    10.10.1.0 is directly connected, FastEthernet1/0
C    10.10.1.8 is directly connected, FastEthernet0/0
 192.168.1.0/25 is subnetted, 2 subnets
S    192.168.1.0 [1/0] via 10.10.1.11
S    192.168.1.128 [1/0] via 10.10.1.9
S   192.168.2.0/24 [1/0] via 10.10.1.2
S* 0.0.0.0/0 [1/0] via 10.10.1.3
```

R5#show ip route

```
Gateway of last resort is 10.10.1.3 to network 0.0.0.0
 10.0.0.0/29 is subnetted, 1 subnets
C    10.10.1.0 is directly connected, FastEthernet0/0
S   192.168.1.0/24 [1/0] via 10.10.1.1
C   192.168.2.0/24 is directly connected, FastEthernet3/1
S* 0.0.0.0/0 [1/0] via 10.10.1.3
```

R6#show ip route

```
Gateway of last resort is 10.10.11.2 to network 0.0.0.0
 10.0.0.0/30 is subnetted, 1 subnets
C    10.10.11.0 is directly connected, FastEthernet0/0
 192.168.1.0/25 is subnetted, 1 subnets
C    192.168.1.128 is directly connected, FastEthernet3/1
S* 0.0.0.0/0 [1/0] via 10.10.11.2
```


R7#show ip route

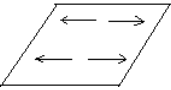
```
Gateway of last resort is 10.10.1.10 to network 0.0.0.0
 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.10.1.8/29 is directly connected, FastEthernet0/0
C    10.10.11.4/30 is directly connected, FastEthernet1/0
 192.168.1.0/25 is subnetted, 2 subnets
S    192.168.1.0 [1/0] via 10.10.11.5
S    192.168.1.128 [1/0] via 10.10.1.9
S* 0.0.0.0/0 [1/0] via 10.10.1.10
```

6. Определите, какой из маршрутизаторов сети является пограничным. Укажите в ответе его номер, соответствующий указанному в заголовке соответствующего консольного вывода.
7. Определите глобальный IP-адрес компании, выданный провайдером. Известно, что он связан только с одним соседним маршрутизатором из глобальной сети. Для их адресации используется сеть с маской длины /30.
8. Восстановите топологию сети, изобразив ее в виде схемы, отражающей связи маршрутизаторов, коммутаторов и присоединенных локальных сетей.

Обозначьте подсети прямоугольниками с адресом сети внутри - 123.231.0.0/16

Обозначьте подключение в глобальную сеть как подсеть. Вместо адреса сети пропишите внутри «Интернет»/«Internet».

Обозначьте маршрутизаторы перечеркнутым кругом  с обозначением «М» («Маршрутизатор») или «R» («Router») и номером

коммутатор –  «К» («Коммутатор») или «S» («Switch»), если их несколько, то номер указывать не надо.

Соединения обозначаются прямыми линиями между элементами схемы.

Для обеспечения безопасности сведений, составляющих банковскую тайну, руководитель отделения банка принял решение внедрить систему разграничения доступа. В системе обрабатываются следующие виды информации:

- сведения об очереди к сотрудникам отделения банка и доступных банковских продуктах должны быть доступны всем желающим, включая клиентов, использующих терминал, не проходя авторизацию (не вставляя банковскую карту и не вводя PIN-код);
- сведения о собственных банковских продуктах, хранящиеся в мобильном приложении, должны быть доступны авторизованным пользователям мобильного приложения;
- сведения об активных заявках клиентов банка должны быть доступны центру обработки заявок, а также сотрудникам и руководителю отделения банка;
- сведения о числе обработанных заявок и оформленных банковских продуктах должны быть доступны руководителю отделения;

- сведения об активных продуктах и заказах конкретных клиентов должны быть доступны сотрудникам банка, ведущим прием соответствующих клиентов;
- сведения о регламенте работы банка (порядок приема заявок, оформления документов клиентами, предоставления банковских продуктов) должны быть доступны всем сотрудникам банка;

Доступ к персональным данным клиентов, переданным через мобильное приложение, должны быть доступны центру обработки заявок и сотрудникам отделения банка, обрабатывающим заявки соответствующих клиентов, а также руководителю отделения;

Доступ к персональным данным клиентам, переданным при личном визите, должны быть доступны сотрудникам отделения банка, ведущим прием соответствующих клиентов, и руководителю отделения банка.

9. За основу была взята мандатная модель. Укажите номера категорий информации, к которым невозможно организовать доступ в рамках такой модели (потребуется использовать дополнительные механизмы разграничения доступа).
10. Укажите, сколько уровней мандатной модели потребуется для организации доступа к остальным категориям информации.
11. Укажите уровень доступа (при минимальном количестве уровней доступа), который требуется назначить центру обработки заявок, где 1 – наименьший уровень.
12. Укажите номера категорий информации, которым требуется назначить наивысший уровень секретности.

Для обеспечения целостности передаваемой информации и ее защиты от возможных искажений из-за случайных ошибок могут применяться коды Грея.

Код Грея – двоичный код, в котором соседние кодовые слова различаются значением только в одном двоичном разряде с учетом цикличности (если расположить исходное множество бинарных команд в лексикографическом порядке).

Пример:

Десятичное значение	Двоичное значение (2 бита)	Код Грея
0	00	00
1	01	01
2	10	11
3	11	10

В рассматриваемой организации коды Грея используются для кодирования номеров дорожек жестких дисков сервера. В результате случившего сбоя настройки оборудования сбились, в связи с чем возникает риск нарушения доступности хранящейся на них информации. Сохранились следующие значения:

Десятичное значение	Двоичное значение (4 бита)	Код Грея
0	0000	0000
1	0001	
2	0010	
3	0011	
4	0100	0110
5	0101	
6	0110	
7	0111	
8	1000	1100
9	1001	
10	1010	
11	1011	
12	1100	1010
13	1101	
14	1110	
15	1111	1000

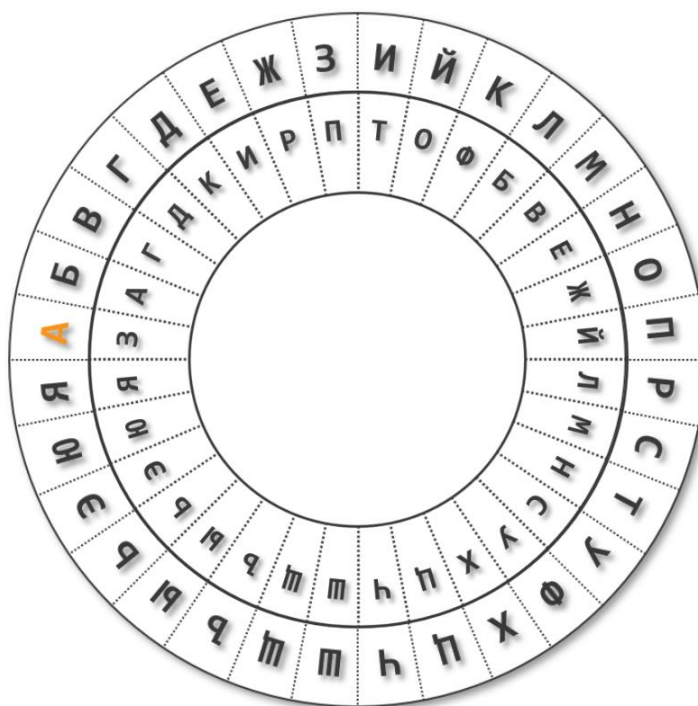
13. Восстановите значение кода Грея для десятичного значения 6.
14. Восстановите значение кода Грея для десятичного значения 10.
15. Укажите десятичное значение, которому соответствует код Грея 0011.
16. Укажите двоичное значение, которому соответствует код Грея 1011.

Для обеспечения конфиденциальности информации, передаваемой от терминала в центр обработки заявок, руководитель отделения банка принял решение ввести шифрование передаваемых данных. Для выбора наилучшей меры защиты им

рассматривается ряд предлагаемых решений, одно из которых основано на шифре, известном как «Диск Альберти».

Такой шифр основан на использовании устройства, состоящего из двух дисков, имеющих единую ось. Оба диска имеют секторы, на которые нанесены буквы алфавита открытого текста и шифртекста. Внешний диск неподвижен, буквы расположены на нем в алфавитном порядке. Внутренний диск может вращаться вокруг оси для установки в различные положения, буквы на нем нанесены в произвольном порядке. Расположение букв на внутреннем диске является ключом данного шифра.

Для зашифрования внутренний диск устанавливается таким образом, чтобы заранее согласованная отправителем и получателем буква внутреннего диска (назовем ее индикаторной буквой), оказалась напротив буквы «А» на внешнем диске. После этого первая буква открытого текста отыскивается на внешнем диске, а в качестве символа замены для нее берется буква внутреннего диска, находящаяся напротив нее (например, на приведенной иллюстрации буква «И» будет зашифрована буквой «Т», «О» – «Ж»).

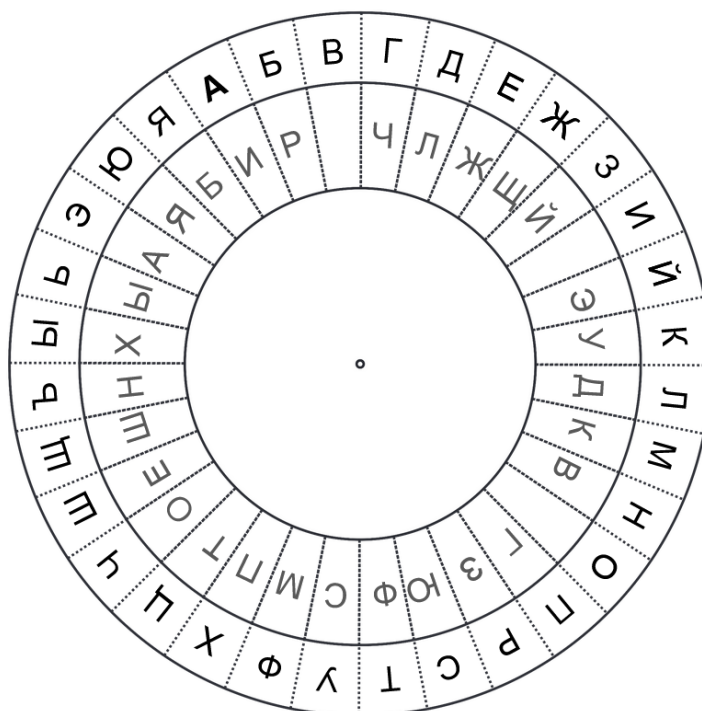


Затем положение диска меняется на 1 сектор по часовой стрелке, происходит зашифрование следующей буквы, после чего эта процедура повторяется до полного зашифрования всего открытого текста.

Таким способом был зашифрован некоторый проверочный текст:

ВЙЬМВБРЬЙФААКЮНЧММГЧММСЗЭЗБФБЭАЯОПРАИСРШТТЯЗНПЗМЩЗ
ЩММРЬХЗЫИИХЯУЖЕЪФАФРЬБЫНТЕГЗЩДЗИЗАВРБЭАЭКЪЖ

Использованный ключ приведен на иллюстрации ниже.



17. Установите индикаторную букву, использованную для зашифрования данного сообщения.
18. Определите первые 10 букв открытого текста.
19. Укажите, какие буквы пропущены на внутреннем диске, расположив их (пропущенные буквы) в порядке следования от буквы «А» внутреннего диска по часовой стрелке.
20. Зашифруйте с той же индикаторной буквой слово «транспарентность».

Угрозы информационной безопасности, согласно Методике оценки угроз безопасности информации (ФСТЭК России), описываются в следующем формате:

УБИ_і = [нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия].

21. Сформулируйте для рассмотренного выше банка 5 различных угроз, рассматривая источники угроз различных классов и категорий. В каждой угрозе рассмотрите единственный источник, объект воздействия и способ

реализации. В качестве объектов воздействия рассматривайте только элементы приведенной схемы или объекты, наличие которых очевидно и логично вытекает из нее. В качестве способов реализации угроз указывайте подходящие из следующего перечня:

- использование уязвимостей (требуется указать, уязвимостей какого рода и какого объекта (например, «уязвимостей реализации системы управления базой данных» или «уязвимостей конфигурации системы управления доступом»);
- внедрение вредоносного программного обеспечения;
- формирование и использование скрытых каналов передачи конфиденциальных данных;
- перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации;
- нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, администрированию, обслуживанию;
- ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств;
- физическое воздействие на объект угрозы.

В качестве негативных последствий укажите в краткой, лаконичной формулировке, последствия, к которым может привести успешная реализация угрозы нарушителем для всего объекта информатизации (например, «Отсутствие доступа к государственной услуге», «Прекращение или нарушение функционирования объектов транспортной инфраструктуры» и т. п.)

Для получения максимального балла стремитесь рассмотреть угрозы, реализуемые источниками различных категорий, четко и конкретно указать все параметры угроз, связать их с предложенной схемой банка, учесть реалии функционирования организаций, аналогичных представленной. По желанию можно дополнить формализованное описание угроз пояснениями в свободной форме, приведенными ниже, способствующими однозначному и точному пониманию рассмотренных угроз.