ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕВЫСШЕГО ОБРАЗОВАНИЯ
«АМУРСКИЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «АмГПГУ»)

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ,
МАТЕМАТИКИ и ФИЗИКИ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ,
ИНФОРМАЦИОННЫХ СИСТЕМ и ФИЗИКИ

УТВЕРЖДАЮ:
Проректор
по учебной работе
Дегтяренко В. А.
_____
«05» 02 2024 г.

ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ, ПРОВОДИМЫХ УНИВЕРСИТЕТОМ САМОСТОЯТЕЛЬНО

по предмету: ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Комсомольск-на-Амуре, 2024 г.

1. Пояснительная записка

Назначение вступительного испытания – оценить общеобразовательную подготовку по «Основам информационной безопасности» выпускников общеобразовательных учреждений с целью их аттестации и конкурсного отбора в высшее профессиональное образование.

Содержание и структура работы определяется целями единого государственного экзамена: обеспечение объективной оценки качества подготовки лиц, освоивших образовательные программы среднего (полного) общего образования, с использованием заданий стандартизированной формы.

1.1. Цели и задачи вступительного испытания

Цель вступительного испытания – оценка качества подготовки выпускников образовательных организаций среднего общего образования по «Основам информационной безопасности», способности к обучению и усвоению ООП ВПО по направлению подготовки 10.03.01 «Информационная безопасность» профессионально-образовательный профиль «Техническая защита информации».

Задачи проведения вступительного испытания:

1) должны отражать основы системного подхода к организации защиты конфиденциальной информации, передаваемой и обрабатываемой техническими средствами;

2) выявить владение знаниями о основных нормативно-правовых актах международного, федерального и ведомственно-отраслевого уровней, определяющих организационные и правовые аспекты в области информационной безопасности;

3) должны отражать владение методами формирования политики информационной безопасности организации;

4) выявить владение методами анализа деятельности организации с целью определения информационно-технологических ресурсов, подлежащих защите;

5) показать владение необходимыми прикладными умениями и навыками применения знаний в области информационной безопасности.

1.2. Форма проведения вступительного испытания

Вступительные испытания по «Основам информационной безопасности» проводятся университетом в форме комплексного тестирования (в том числе с применением дистанционных компьютерных технологий).

1.3. Требования к подготовке абитуриента

На вступительном экзамене по «Основам информационной безопасности» поступающий в высшее учебное заведение должен:

знать:

- нормативные правовые акты, методические документы, международные и национальные стандарты в области защиты информации;
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны
- виды конфиденциальной информации;
- перечни сведений конфиденциального характера, основные требования и рекомендации по их защите;
- типовые угрозы безопасности информации;
- классификацию и характеристики технических каналов утечки информации;
- основные способы и средства контроля защищенности информации;

уметь:

- работать с действующей нормативной правовой и методической базой в области защиты информации;
- определять типовые угрозы информации;
- систематизировать, анализировать и оценивать информацию в области информационной безопасности.

2. Продолжительность проведения вступительного испытания

Продолжительность вступительного испытания составляет 3,55 академических часа.

Примерное время выполнения отдельных заданий составляет:
1) для каждого задания части 1 – 1–10 минут;
2) для каждого задания части 2 – 5–35 минут.

3. Содержание программы вступительных испытаний по «Основам информационной безопасности»

№ п/п	Раздел, тема и краткое содержание
1.	**Раздел 1. Теоретические основы информационной безопасности**
1.1.	*Тема «Основные понятия и задачи информационной безопасности»* Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем..
1.2.	*Тема «Угрозы и риски информационной безопасности»* Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
1.3.	*Тема «Основы защиты информации»* Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации.
1.4.	*Тема «Политика информационной безопасности»* Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности. Определение объектов защиты на типовом объекте информатизации. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.
1.5.	*Тема «Угрозы безопасности защищаемой информации»* Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации Определение угроз объекта информатизации и их классификация
2	**Раздел 2. Методология защиты информации**
2.1.	*Тема «Методологические подходы к защите информации».* Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый

	уровень защиты информации. Виды мер и основные принципы защиты информации.
2.2.	*Тема «Нормативно правовое регулирование защиты информации».* Организационная структура системы защиты информации. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации..
2.3.	*Тема «Вредоносные программы и компьютерные вирусы».* Способы распространения вредоносных программ. Последствия заражений вредоносной программой. Классификации вредоносных программ и вирусов. Примеры угроз безопасности информации реализуемых вредоносными программами. Ответственность за написание и распространение вредоносных программ
2.4.	*Тема «Защита информации в автоматизированных (информационных) системах».* Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в информационных системах. Программные и програмно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Выбор мер защиты информации для автоматизированного рабочего места.

4. Критерии оценивания экзаменационной работы по «Основам информационной безопасности»

Каждый экзаменационный билет по «Основам информационной безопасности» состоит из двух частей. Часть 1 содержит 18 заданий с кратким ответом. Предложены следующие разновидности заданий с кратким ответом:

- задания на выбор и запись одного правильного ответа из предложенного перечня ответов;
- задания на определение последовательности расположения данных элементов;
- задания на установление соответствия элементов, данных в нескольких информационных рядах;
- задания на определение по указанным признакам и запись в виде слова (словосочетания) термина, названия, имени, века, года и т.п.

Часть 2 содержит задание с развернутым ответом, выявляющих и оценивающих освоение выпускниками различных комплексных умений. Предложены следующие разновидности заданий:

- задание, предполагающие знание и анализ законов РФ в области обеспечения информационной безопасности;
- задания, связанные с анализом какой-либо проблемы или ситуации при обеспечении информационной безопасности;
- задания, связанные с применением приемов причинно-следственного, структурно-функционального, пространственного и технического анализа при решении задач обеспечения информационной безопасности.

Все задания отражают учебный материал по основным разделам программы вступительного экзамена: раздел 1. Стратегические цели и основные направления обеспечения информационной безопасности; раздел 2. Угрозы безопасности

конфиденциальной информации; раздел 3. Основы политики информационно безопасности.

Задание части 1 с кратким ответом считается выполненным верно, если правильно указаны цифра или последовательность цифр, требуемое слово (словосочетание). Полный правильный ответ на задания 1–15 оценивается 3 баллами; неполный, неверный ответ или его отсутствие – 0 баллов. Полный правильный ответ на задания 16–18 оценивается 10 баллами; если допущена одна ошибка (в т.ч. отсутствует одна из цифр или имеется одна лишняя цифра) – 5 баллами; если допущено две и более ошибок (в т.ч. отсутствуют две и более цифры или имеются две и более лишних цифр) или ответ отсутствует – 0 баллов.

Задание части 2 - задание 19 оценивается в зависимости от полноты и правильности ответа. За выполнение заданий ставится от 0 до 25 баллов.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Основная и дополнительная литература:

Основная литература:

1. Внуков А.А. Защита информации. Учебное пособие для бакалавриата и магистратуры. – М.: Юрайт. 2018 г.
2. Расторгуев С.П. Основы информационной безопасности : учебное пособие. - М.: Академия, 2007. - 192 с.
3. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации: учебное пособие. - М.: Академия, 2006. - 256 с.
4. Мельников В.П., Петраков А.М., Клейменов С.А. Информационная безопасность и защита информации: учебное пособие. - 4-е изд. - М.: Академия, 2009. - 336 с.
5. Щеглов А.Ю., Щеглов К.А. Защита информации: основы теории: учебник для бакалавриата и магистратуры. - /М.: Юрайт, 2018 . – 309 с.

Дополнительная литература:

6. Галатенко В.А. Основы информационной безопасности: учебное пособие. - М.: БИНОМ. Лаборатория знаний, 2011. - 205с.
7. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры /под ред. Т.А. Поляковой, А.А. Стрельцова. - М.: Юрайт, 2018. - 325с.
8. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие. - 2-е изд., стер. - М.: Академия, 2006. - 256с.
9. Ярочкин В.И. Информационная безопасность: учебник для вузов. - М.: Академический проект, 2008. - 544 с.
10. Специальные требования и рекомендации по защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 02.03.01 г. № 282.
11. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России. 2002.

5.2. Интернет-ресурсы

1. Интернет-портал системы «Гарант», предоставляющий правовую информацию http://www.garant.ru
2. Федеральное агентство по техническому регулированию и метрологии Росстандарт http://www.gost.ru/wps/portal/tk362
3. Сайт ФСТЭК РФ. http://www.fstec.ru
4. Информационная система по науке и технологиям Европейского Сообщества // http://www.cordis.lu/.

5. Научная электронная библиотека http://elibrary.ru/defaultx.asp.
6. Российская государственная библиотека (РГБ) // http://www.rsl.ru/.
7. Российская Национальная Библиотека http:// www.nlr.ru.

Типовые задания экзамена по основам информационной безопасности

Вариант 1

A00001_1 Укажите сведения, которые не могут быть отнесены к государственной тайне.
A) о фактах нарушения прав и свобод человека и гражданина;

B) о директивах, планах, указаниях делегациям и должностным лицам по вопросам внешнеполитической и внешнеэкономической деятельности;

C) об экспорте и импорте вооружения, военной техники, отдельных стратегических видов сырья и продукции;

D) об использовании транспорта, связи, других отраслей и объектов инфраструктуры страны в интересах обеспечения ее безопасности;

A00001_2 Укажите правильное утверждение:
Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.
Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами:
A) наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев;
B) исправительные работы на срок до 1 года;
C) наказываются лишением свободы на срок от трех до семи лет;
D) наказываются лишением свободы на срок от 7 до 20 лет;

A00001_3 Укажите неправильное утверждение:
Статья 275. Государственная измена
Государственная измена, то есть шпионаж, выдача государственной тайны либо иное оказание помощи иностранному государству, иностранной организации или их представителям в проведении враждебной деятельности в ущерб внешней безопасности Российской Федерации, совершенная гражданином Российской Федерации, -
наказывается:
A) лишением свободы на срок от двенадцати до двадцати лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осуждённого за период до трех лет либо без такового;
B) лишение свободы на срок от 3 до 10 лет;
C) лишение свободы на срок до 3 лет.
D) наказываются лишением свободы на срок от 10 до 20 лет;

A00001_4 Укажите неправильное утверждение: Статья 272. Неправомерный доступ к компьютерной информации. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение,

блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети: влечет:
A) штраф до 200 000 рублей;

B) либо обязательные работы на срок от 120 до 180 часов;

C) либо исправительными работами на срок от 6 месяцев до 1 года;

D) либо лишением свободы на срок до 2 лет.

A00001_5 Укажите, к какой модели относится политика безопасности организации, если выполняются следующие условия:
- Вся информация рассматривается как принадлежащая организации, а не пользователю, ее создавшему.
- Решение о разрешении или отказе в доступе принимается на основе информации о той функции, которую пользователь выполняет в организации
A) мандатная
B) избирательная
C) ролевая
D) все ответы верны

A00001_6 К правовым методам, обеспечивающим информационную безопасность, относятся:
A) разработка аппаратных средств обеспечения правовых данных
B) разработка и установка во всех компьютерных правовых сетях журналов учета действий
C) разработка и конкретизация правовых нормативных актов обеспечения безопасности
D) разработка программных средств обеспечения правовых данных

A00001_7 Основными источниками угроз информационной безопасности являются все указанное в списке:
A) хищение жестких дисков, подключение к сети, инсайдерство
B) перехват данных, хищение данных, изменение архитектуры системы
C) хищение данных, подкуп системных администраторов, нарушение регламента работы
D) перехват данных, инсайдерство, нарушение регламента работы

A00001_8 Виды информационной безопасности:
A) персональная, корпоративная, государственная
B) клиентская, серверная, сетевая
C) локальная, глобальная, смешанная
D) локальная, серверная, государственная

A00001_9 Цели информационной безопасности – своевременное обнаружение, предупреждение:
A) несанкционированного доступа, воздействия в сети
B) инсайдерства в организации
C) чрезвычайных ситуаций
D) подкупа системных администраторов

A00001_10 Принципом информационной безопасности является принцип недопущения:

A) неоправданных ограничений при работе в сети (системе)

B) рисков безопасности сети, системы

C) презумпции секретности

D) полного доступа пользователей ко всем ресурсам сети, системы

A00001_11 Основные объекты информационной безопасности:

A) компьютерные сети, базы данных

B) информационные системы, психологическое состояние пользователей

C) бизнес-ориентированные, коммерческие системы

D) стационарно установленные ЭВМ

A00001_12 Основными рисками информационной безопасности являются:

A) искажение, уменьшение объема, перекодировка информации

B) техническое вмешательство, выведение из строя оборудования сети

C) потеря, искажение, утечка информации

D) стихийные бедствия

A00001_13 К основным функциям системы безопасности можно отнести все перечисленное:

A) установление регламента, аудит системы, выявление рисков

B) установка новых офисных приложений, смена хостинг-компании

C) внедрение аутентификации, проверки контактных данных пользователей

D) ликвидация последствий несанкционированных вторжений

A00001_14 Принципом политики информационной безопасности является принцип:

A) невозможности миновать защитные средства сети (системы)

B) усиления основного звена сети, системы

C) полного блокирования доступа при риск-ситуациях

D) полного доступа пользователей ко всем ресурсам сети, системы

A00001_15 Когда получен спам по e-mail с приложенным файлом, следует:

A) прочитать приложение (файл), если оно не содержит ничего ценного – удалить

B) сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

C) удалить письмо с приложением, не раскрывая (не читая) его

D) не обращать внимание на письмо

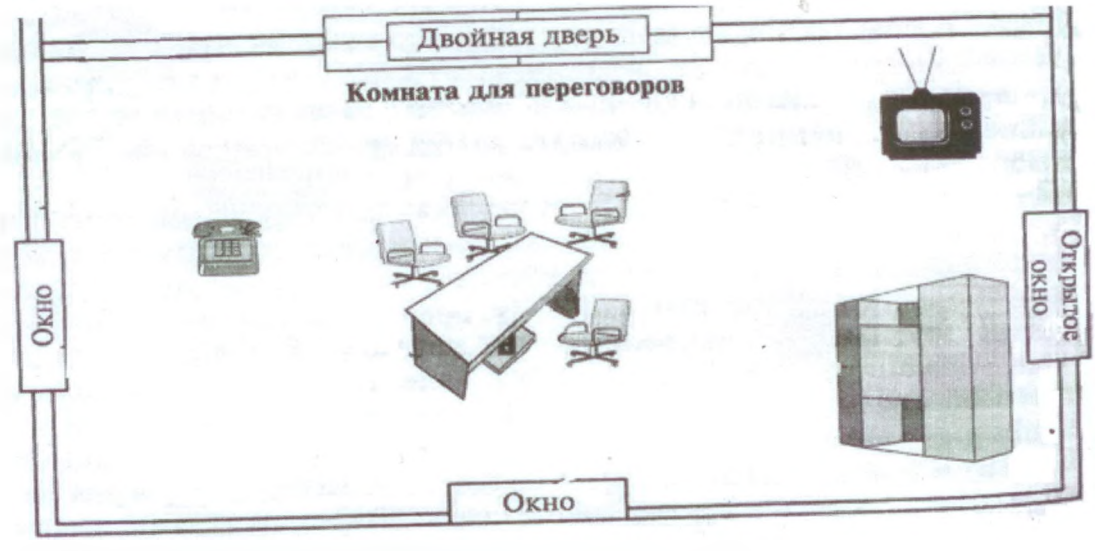
B00001_16 Установите соответствия

1. сведения составляющие тайну следствия и судопроизводства;	A) сведения, составляющие коммерческую тайну;
2. Сведения в области экономики, науки и техники;	B) сведения конфиденциального характера;
3. Сведения, позволяющие ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов;	C) сведения, составляющие государственную тайну.

B00001_17 Дайте определение. Вредоносная программа- это…..

B00001_18 При разработке технического проекта по защите объекта информатизации 2 документа имеют гриф «для служебного пользования», 10 документов имеют гриф «секретно» и 1 документ относится к категории «совершенно секретно». Какой гриф должен стоять на техническом проекте?

C00001_19 Дана схема расположения в кабинете оборудования и ЭВМ, в которой происходят переговоры. Укажите, какие угрозы безопасности информации являются актуальными.



Вариант 2

A00002_1 Укажите сведения, которые не могут быть отнесены к коммерческой тайне.
A) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

B) о научно-технической составляющей производственного процесса;

C) о финансово-экономическом состоянии предприятия;

D) о секретах производства «ноу-хау».

A00002_2 Укажите правильное утверждение:
Статья 283. Разглашение государственной тайны
Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены влечет:
A) административный штраф;
B) исправительные работы на срок до 1 года;
C) арест на срок до 4 месяцев;
D) арест на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

A00002_3 Укажите правильное утверждение:
Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений
Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан влечет:
A) обязательные работы на срок от 120 до 180 часов;
B) арест на срок до 4 месяцев;
C) лишение свободы на срок до 2 лет;
D) лишение свободы на срок до 4 лет;

A00002_4 Укажите неправильное утверждение:
Статья 272. Неправомерный доступ к компьютерной информации. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети: влечет:
A) штраф до 200 000 рублей;

B) либо обязательные работы на срок от 120 до 180 часов;

C) либо исправительными работами на срок от 6 месяцев до 1 года;

D) либо лишением свободы на срок до 2 лет;

A00002_5 Укажите, к какой модели относится политика безопасности организации, если выполняются следующие условия:

- Все субъекты и объекты идентифицированы;
- Права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила;

A) мандатная
B) избирательная
C) ролевая
D) все ответы верны

A00002_6 Принципом политики информационной безопасности является принцип:
A) усиления защищенности самого незащищенного звена сети (системы)
B) перехода в безопасное состояние работы сети, системы
C) полного доступа пользователей ко всем ресурсам сети, системы
D) все ответы верны

A00002_7 В информационной безопасности по аббревиатурой ЭЦП понимают:
A) электронно-цифровой преобразователь
B) электронно-цифровая подпись
C) электронно-цифровой процессор
D) такого понятия не существует

A00002_8 Наиболее распространены угрозы информационной безопасности корпоративной системы:
A) покупка нелицензионного ПО
B) ошибки эксплуатации и неумышленного изменения режима работы системы
C) сознательное внедрение компьютерных вирусов
D) подкуп системных администраторов

A00002_9 Наиболее распространены угрозы информационной безопасности сети:
A) распределенный доступ клиент, отказ оборудования
B) моральный износ сети, инсайдерство
C) сбой (отказ) оборудования, нелегальное копирование данных
D) стихийные бедствия

A00002_10 Утечкой информации в системе называется ситуация, характеризуемая:
A) потерей данных в системе
B) изменением формы информации
C) изменением содержания информации
D) изменением качества информации

A00002_11 Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
A) целостность
B) доступность
C) актуальность
D) релевантность

A00002_12 Угроза информационной системе (компьютерной сети) – это:
A) вероятное событие
B) детерминированное (всегда определенное) событие
C) событие, происходящее периодически
D) неизбежное событие

A00002_13 Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

A) программные, технические, организационные, технологические

B) серверные, клиентские, спутниковые, наземные

C) личные, корпоративные, социальные, национальные

D) региональные, отраслевые, международные, клиентские

A00002_14 Окончательно, ответственность за защищенность данных в компьютерной сети несет:

A) владелец сети

B) администратор сети

C) пользователь сети

D) клиент сети

A00002_15 Принципом политики информационной безопасности является принцип:

A) разделения доступа (обязанностей, привилегий) клиентам сети (системы)

B) создание одноуровневой защиты сети, системы

C) создание совместимых, однотипных программно-технических средств сети, системы

D) полного доступа пользователей ко всем ресурсам сети, системы

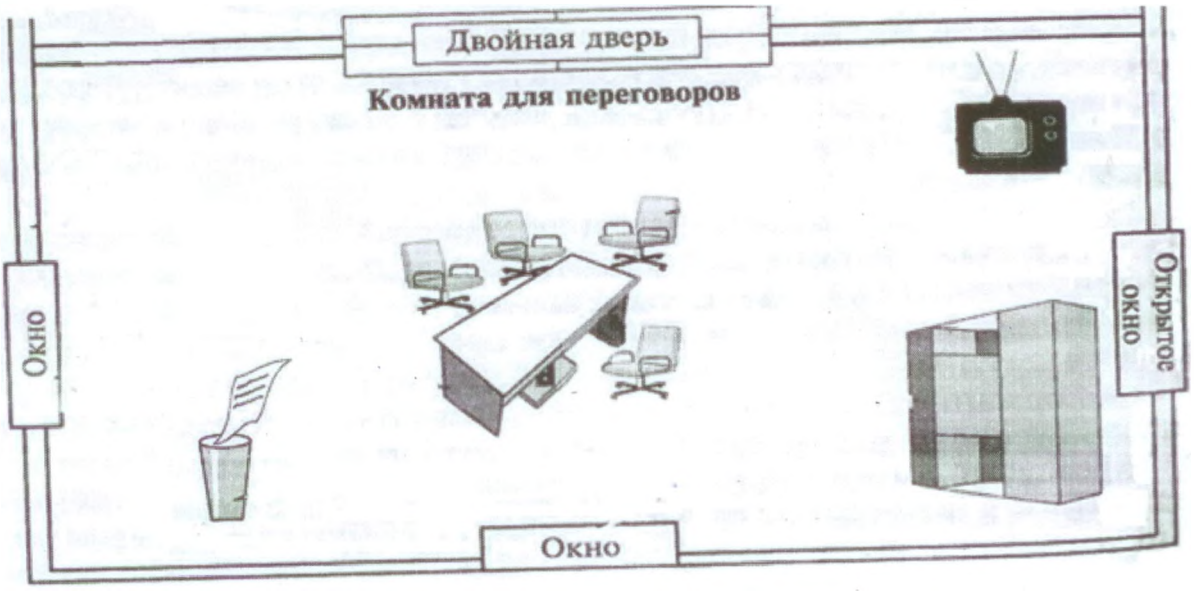
B00002_16 Установите соответствия

1. Сведения, касающиеся деятельности организаций, ограничения на распространение которой диктуется служебной необходимостью;	A) сведения, составляющие банковскую тайну;
2. Сведения о планах, объемах и других важнейших характеристиках добычи, производства и реализации отдельных стратегических видов сырья и продукции;	B) сведения, составляющие служебную тайну;
3. Сведения о счетах клиентов и корреспондентов и действиях с ними в кредитной организации;	C) сведения, составляющие государственную тайну.

B00002_17 Дайте определение. Искусственные угрозы - это……..

B00002_18 При разработке технического проекта по защите объекта информатизации 2 документа не имеют грифа, 10 документов имеют гриф «для служебного пользования». Какой гриф должен стоять на техническом проекте?

C00002_19 Дана схема расположения в кабинете оборудования и ЭВМ, в которой происходят переговоры. Укажите, какие угрозы безопасности информации являются актуальными.



Вариант 3

A00003_1 Укажите признаки, которые свидетельствую, что коммерческая информация получена законно.
A) полученная информация составляет коммерческую тайну и получатель умышленно преодолевал меры по ее охране;

B) получатель информации знал, что получает информацию от лица, не имеющего право на ее передачу получателю;

C) информация, составляющая коммерческую тайну, получена от ее обладателя на основании договора;

D) получатель информации не знал, что получает информацию от лица, не имеющего право на ее передачу получателю.

A00003_2 Укажите в каких случаях требуется согласия субъекта персональных данных на обработку персональных данных:
A) обработка ПД осуществляется на основании федерального закона, устанавливающего ее цель, условия получения ПД и круг субъектов, ПД, которых подлежат обработке, а также определяющего полномочия оператора;
B) обработка ПД осуществляется для статистических или иных научных целей при условии обязательного обезличивания ПД;
C) обработка ПД осуществляется в целях исполнения договора, одной из сторон которого является субъект ПД;
D) обработка персональных данных осуществляется с целью создания баз данных обучающихся или работников образовательной организации.

A00003_3 Укажите неправильное утверждение:
Статья 137. Нарушение неприкосновенности частной жизни.
1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации влечет:

A) обязательные работы на срок от 120 до 180 часов;
B) исправительные работы на срок до 1 года;
C) арест на срок до 4 месяцев;
D) лишение свободы на срок до 2 лет.

A00003_4 Укажите неправильное утверждение:
Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, наказывается:
A) штраф до 200 000 рублей;
B) либо обязательные работы на срок от 120 до 180 часов;
C) либо ограничение свободы на срок до 2 лет.
D) наказываются лишением свободы на срок от 7 до 20 лет;

A00003_5 Укажите, к какой модели относится политика безопасности организации, если выполняются следующие условия:

- Все субъекты и объекты идентифицированы;
- Задан линейно упорядоченный набор меток секретности;
- Каждому объекту системы присвоена метка секретности - его уровень секретности;
- Каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему - его уровень доступа;
- Решение о разрешении доступа субъекта к объекту принимается исходя из типа доступа и сравнения метки субъекта и объекта

A) мандатная;
B) избирательная;
C) ролевая.
D) все ответы верны

A00003_6 Политика безопасности в системе (сети) – это комплекс:
A) руководств, требований обеспечения необходимого уровня безопасности
B) инструкций, алгоритмов поведения пользователя в сети
C) норм информационного права, соблюдаемые в сети
D) все ответы верны

A00003_7 Утечка информации – это …
A) несанкционированный процесс переноса информации от источника к злоумышленнику
B) непреднамеренная утрата носителя информации
C) процесс раскрытия секретной информации
D) процесс уничтожения информации

A00003_8 Информация, составляющая государственную тайну не может иметь гриф…
A) «совершенно секретно»
B) «особой важности»
C) «секретно»
D) «для служебного пользования»

A00003_9 Под угрозой удаленного администрирования в компьютерной сети понимается угроза…
A) перехвата или подмены данных на путях транспортировки

B) поставки неприемлемого содержания
C) вмешательства в личную жизнь
D) несанкционированного управления удаленным компьютером

A00003_10 К преднамеренной угрозе безопасности информации можно отнести
A) повреждение кабеля, по которому идет передача, в связи с погодными условиями
B) наводнение
C) кражу информации
D) ошибку разработчика

A00003_11 Наиболее эффективное средство для защиты от сетевых атак
A) посещение только «надёжных» Интернет-узлов
B) использование антивирусных программ
C) использование только сертифицированных программ-браузеров при доступе к сети Интернет
D) использование сетевых экранов или «firewall»

A00003_12 Концепция системы защиты от информационного оружия не должна включать…
A) процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей
B) механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
C) признаки, сигнализирующие о возможном нападении
D) средства нанесения контратаки с помощью информационного оружия

A00003_13 К формам защиты информации не относится…
A) страховая
B) организационно-техническая
C) программно-аппаратная
D) правовая

A00003_14 Методы повышения достоверности входных данных
A) отказ от использования данных
B) использование вместо ввода значения его считывание с машиночитаемого носителя
C) проведение комплекса регламентных работ
D) многократный ввод данных и сличение введенных значений

A00003_15 Суть компрометации информации заключается во
A) внесении изменений в базу данных, в результате чего пользователь лишается доступа к информации
B) внесении несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений
C) несанкционированном доступе к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
D) достоверную информацию невозможно скомпрометировать

B00003_16 Установите соответствия

1. Сведения, о принятии и зачислении поступающих на счет клиента денежных средств;
2. Сведения о директивах, планах, указаниях делегациям и должностным лицам по вопросам внешнеполитической и внешнеэкономической деятельности;
3. Сведения, позволяющие ее обладателю при существующих или возможных обстоятельствах сохранить положение на рынке товаров, работ, услуг.

A) сведения, составляющие коммерческую тайну;

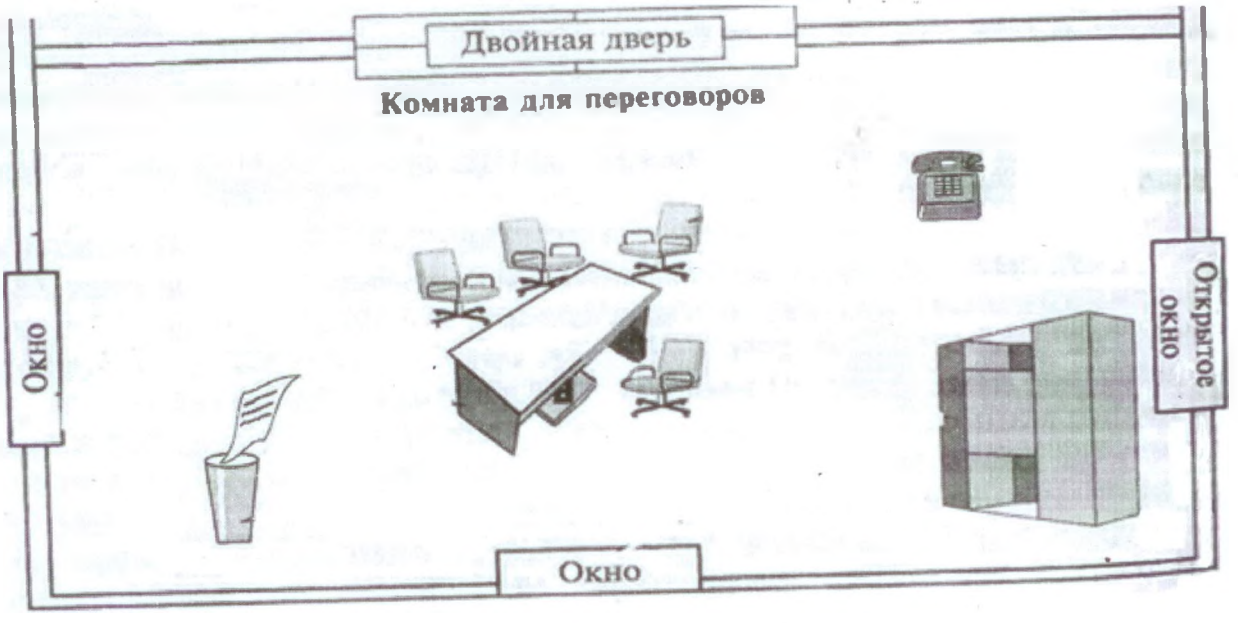
B) сведения, составляющие банковскую тайну;

C) сведения, составляющие государственную тайну.

B00003_17 Дайте определение. Обработка персональных данных - это……..

B00003_18 При разработке технического проекта по защите объекта информатизации 2 документа имеют гриф «секретно», 5 документов имеют гриф «для служебного пользования», один документ имеет гриф «особой важности». Какой гриф должен стоять на техническом проекте?

C00003_19 Дана схема расположения в кабинете оборудования и ЭВМ, в которой происходят переговоры. Укажите, какие угрозы безопасности информации являются актуальными.



Вариант 4

A00004_1 Укажите сведения, которые могут быть отнесены к государственной тайне.
A) о фактах нарушения прав и свобод человека и гражданина;
B) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях;

C) об экспорте и импорте вооружения, военной техники, отдельных стратегических видов сырья и продукции;
D) о состоянии здоровья высших должностных лиц Российской Федерации;

A00004_2 Укажите правильное утверждение:
Статья 276. Шпионаж. Передача, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки иных сведений для использования их в ущерб внешней безопасности РФ, если эти деяния совершены иностранным гражданином или лицом без гражданства, - наказывается
A) лишением свободы на срок от десяти до двадцати лет;
B) исправительные работы на срок до 1 года;
C) не наказываются лишением свободы;
D) наказываются штрафом;

A00004_3 Укажите правильное утверждение:
Статья 325. Похищение или повреждение документов, штампов, печатей. Похищение, уничтожение, повреждение или сокрытие официальных документов, штампов или печатей, совершенные из корыстной или личной заинтересованности, - наказывается
A) штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда, либо исправительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до одного года;
B) не наказывается лишением свободы;
C) наказываются лишением свободы на срок до 10 лет;
D) наказываются лишением свободы на срок от 10 до 20 лет;

A00004_4 Укажите правильное утверждение:
Статья 13.14 Кодекса об административных правонарушениях Разглашение информации, доступ к которой ограничен ФЗ (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет
A) наложение административного штрафа;

B) не наказывается;

C) лишение свободы на срок до 10 лет;
D) лишение свободы на срок от 10 до 20 лет;

A00004_5 Укажите не правильное утверждение:
Административные меры защиты информации - это меры организационного характера. Они регламентируют:
A) порядок уголовного преследования нарушителей;

B) процессы функционирования системы обработки данных;
C) деятельность персонала;
D) порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности;

A00004_6 Принципом политики информационной безопасности является принцип:
A) разделения доступа (обязанностей, привилегий) клиентам сети (системы);

B) одноуровневой защиты сети, системы;
C) совместимых, однотипных программно-технических средств сети, системы;
D) неотвратимости наказания;

A00004_7 Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
A) регламентированной;
B) правовой;
C) защищаемой;
D) служебной;

A00004_8 Основные угрозы доступности информации:
A) непреднамеренные ошибки пользователей;
B) перехват данных;
C) злонамеренное изменение данных;
D) отказ программного и аппаратно обеспечения;

A00004_9 Причины возникновения ошибки в данных
A) преднамеренное искажение данных;
B) неустранимые причины природного характера;
C) ошибки при переносе данных с промежуточного документа в компьютер;
D) отказ программного и аппаратно обеспечения;

A00004_10 Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)
A) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения атак;
B) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты;
C) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом;
D) принципиального отличия нет;

A00004_11 Основные угрозы конфиденциальности информации:
A) маскарад;
B) перехват данных;
C) блокирование;
D) переадресовка;

A00004_12 Назовите вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование
A) пассивная угроза;
B) активная угроза;
C) значительная угроза;
D) критическая угроза;

A00004_13 Кто является основным ответственным за определение уровня классификации информации в организации?
A) руководитель среднего звена;
B) никто не отвечает;
C) руководитель организации;
D) пользователь информации;

A00004_14 Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
A) сотрудники;
B) хакеры;
C) атакующие;
D) контрагенты (лица, работающие по договору);

A00004_15 Защита информации это:
A) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
B) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
C) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
D) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

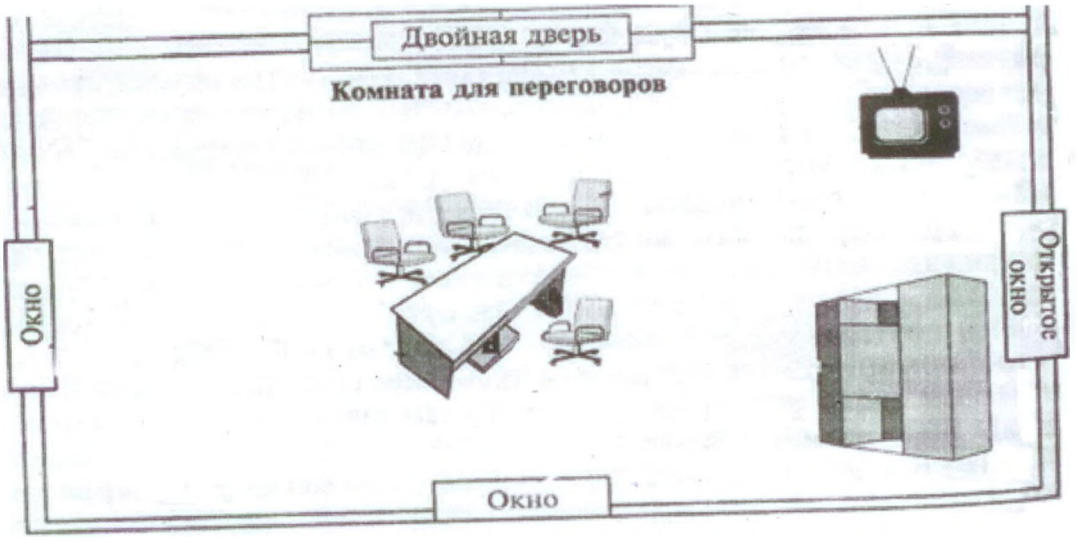
B00004_16 Установите соответствия

1. сведения составляющие врачебную тайну;	A) сведения, составляющие коммерческую тайну;
2. Сведения в области экономики, науки и техники;	B) сведения конфиденциального характера;
3. Сведения, позволяющие ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов;	C) сведения, составляющие государственную тайну.

B00004_17 Дайте определение. Угроза безопасности информации - это…..

B00004_18 При разработке технического проекта по защите объекта информатизации 22 документа имеют гриф «для служебного пользования», 10 документов имеют гриф «секретно» и 1 документ относится к категории «совершенно секретно». Какой гриф должен стоять на техническом проекте?

C00004_19 Дана схема расположения в кабинете оборудования и ЭВМ, в которой происходят переговоры. Укажите, какие угрозы безопасности информации являются актуальными.



Вариант 5

A00005_1 Укажите сведения, которые не могут быть отнесены к коммерческой тайне.
A) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

B) о научно-технической составляющей производственного процесса;

C) о методах и средствах защиты секретной информации;

D) о содержании, объеме, финансировании и выполнении государственного оборонного заказа;

A00005_2 Федеральный закон "О персональных данных" от 27.07.2006 обозначен под номером
A) 152-ФЗ;
B) 52-ФЗ;
C) 2153-ФЗ;
D) 1-ФЗ;

A00005_3 Укажите правильное утверждение:
Статья 275. Государственная измена влечет:
A) обязательные работы на срок от 120 до 180 часов;
B) административный арест на срок до 1 месяца;
C) лишение свободы на срок от 12 до 20 лет;
D) штраф до 1000 руб;

A00005_4 Укажите правильное утверждение:
Согласно статье 276 Шпионаж. Под шпионажем понимают
A) передачу, а равно собирание, похищение или хранение в целях передачи иностранному государству, иностранной организации или их представителям сведений, составляющих государственную тайну;

B) опубликование сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц;

C) разглашение сведений, составляющих коммерческую тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц;

D) собирание или хранение информации, составляющей государственную тайну;

A00005_5 Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

Варианты ответа:

A) активный перехват;

B) видеоперехват;

C) аудиоперехват;

D) просмотр мусора.

A00005_6 Что из перечисленного не относится к числу основных аспектов информационной безопасности:

A) доступность;

B) масштабируемость;

C) целостность;

D) конфиденциальность;

A00005_7 Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

A) снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования;

B) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации;

C) улучшить контроль за безопасностью этой информации;

D) снизить уровень классификации этой информации;

A00005_8 Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

A) владельцы данных;

B) пользователи;

C) администраторы;

D) руководство;

A00005_9 Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

A) никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски;

B) когда риски не могут быть приняты во внимание по политическим соображениям;

C) когда необходимые защитные меры слишком сложны;

D) когда стоимость контрмер превышает ценность актива и потенциальные потери;

A00005_10 Что такое политика безопасности?

A) пошаговая инструкция по выполнению задач безопасности;

B) конкретизированные руководящие требования по достижению определенного уровня безопасности;

C) широкие, высокоуровневые заявления руководства;

D) детализированные документы по обработке инцидентов безопасности;

A00005_11 Эффективная программа безопасности требует сбалансированного применения:

A) технических и нетехнических методов защиты;

B) контрмер;

C) физической безопасности информации;

D) процедур безопасности и шифрования;

A00005_12 Государственный стандарт ГОСТ Р ИСО 27799-2015 Информатизация здоровья предназначен в качестве

A) руководства для медицинских организаций и других хранителей персональной медицинской информации;

B) руководства для учебных организаций и других хранителей персональной медицинской информации;

C) руководства для государственных организаций и других хранителей персональной информации;

D) руководства для учебных организаций и других хранителей персональной информации;

A00005_13 Защита информации это:

A) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

B) преобразование информации, в результате которого содержание информации становится непонятным для субъекта;

C) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

D) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

A00005_14 Естественные угрозы безопасности информации вызваны:

A) деятельностью человека;

B) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

C) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

D) корыстными устремлениями злоумышленников;

A00005_15 Антивирус, который не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние, называется:

A) детектор;

B) доктор;

C) сканер;

D) сторож.

B00005_16 Установите соответствия

1. Сведения, касающиеся деятельности организаций, ограничения на распространение которой диктуется служебной необходимостью;
2. Сведения о планах, объемах и других важнейших характеристиках добычи стратегических видов сырья и продукции;
3. Сведения о данных пациентов и действиях с ними в медицинской организации;

A) сведения, составляющие медицинскую тайну;

B) сведения, составляющие служебную тайну;

C) сведения, составляющие государственную тайну.

B00005_17 Дайте определение. Естественные угрозы информационной безопасности - это……..

B00005_18 При разработке технического проекта по защите объекта информатизации 12 документов не имеют грифа, 1 документ имеет гриф «для служебного пользования». Какой гриф должен стоять на техническом проекте?

C00005_19 Дана схема расположения в кабинете оборудования и ЭВМ, в которой происходят переговоры. Укажите, какие угрозы безопасности информации являются актуальными.