МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« *29* » *августа* 2023 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Нормативно-правовое регулирование в сфере информационной безопасности
(наименование учебной дисциплины)

10.04.01 Информационная безопасность, направленность (профиль) «Защищенные информационные системы»
(код и наименование ОПОП ВО)

Курск – 2023

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема №1 «Информация, информационные системы как объект правового регулирования информационной безопасности»

1. Раскрыть содержание понятия информационной системы как правовой категории.
2. Перечислить отличительные черты информационной системы от других систем
3. Каковы основные результаты внедрения ИС? Дать определения структуры ИС.
4. Что описывают физическая, логическая, топологическая структуры ИС?
5. Перечислить и раскрыть содержание требований к архитектуре ИС.
6. Раскрыть содержание схем информационных потоков и методологии построения баз данных, как правовых категорий.
7. Показать роль и место видов обеспечения ИС, определяющих информационные отношения, подлежащие правовому регулированию.
8. Раскрыть содержание понятий различных видов обеспечения ИС, системной программы, операционной системы, прикладной программы.
9. Дать определение понятий документированной информации, (документа), конфиденциальной информации, информационных ресурсов, информационного продукта (продукции), государственной тайны, компьютерной информации.
10. Раскрыть соотношение понятий информации как отражения действительности объектом окружающего мира и как объект права собственности.
11. С чем связано содержание понятия информации как объекта правового регулирования различных сфер деятельности личности, общества и государства?
12. Раскрыть содержание понятия угрозы информации как правовой категории, обусловливающей заданное качество правовой и иной информации подлежащей правовому регулированию.

Тема №2 «Правовая основа допуска и доступа персонала к защищаемым сведениям»

1. Понятие государственных информационных ресурсов.
2. История и причины возникновения проблемы законодательного обеспечения защиты государственной тайны.
3. Основные направления разработка проблемы правового обеспечения защиты информации?
4. В чем сущность комплексной защиты информации?

5. Структура системы защиты государственной тайны.
6. Основные задачи и функции Государственной технической комиссии при Президенте РФ?
7. Основные направления деятельности федеральных органов правительственной связи и информации по защите государственной тайны.
8. Понятие персональных данных и проблемы их правовой регламентации.
9. Правовая охрана и защита прав на неприкосновенность частной жизни.
10. Государственная тайна в системе информационной безопасности РФ.
11. Общая характеристика правовых основ защиты государственной тайны.

Тема №3 «Правовые основы защиты коммерческой тайны»

1. Дайте определение понятия «коммерческая тайна» и укажите на ее отличия от государственной тайны.
2. В чем отличие коммерческой тайны от профессиональной, личной, семейной, служебной?
3. Какими свойствами характеризуется коммерческая тайна?
4. Какие факторы обусловили появление института коммерческой тайны в нашей стране ранее и сейчас?
5. Каков механизм правой защиты коммерческой тайны?
6. Сформулируйте основной вопрос проблемы защиты информации в процессе реализации коммерческой деятельности и раскройте его.
7. Расскажите о двухуровневой системе правовой защиты коммерческой тайны.
8. Назовите основные группы сведений, которые могут быть отнесены к сведениям, составляющим коммерческую тайну.
9. Назовите методологические основы рассмотрения содержания понятия «коммерческая тайна».
10. Что такое предмет и объект защиты коммерческой тайны?
11. В чем разница между объектом защиты и сведениями, составляющими коммерческую тайну?
12. Основы организации системы зашиты коммерческой тайны.

Тема №4 «Компьютерная информация – как объект информатизации»

1. Классификация видов противоправных деяний в отношении компьютерной информации.
2. Особенности компьютерных преступлений.
3. Особенности компьютерных преступлений.
4. Классификация компьютерных преступников.
5. Способы и механизмы совершения компьютерных преступлений.
6. Способы несанкционированного доступа к ЭВТ

7. Этапы проведения расследования в сфере компьютерных преступлений.
8. Тактика и особенности проведения следственных действий.
9. Виды экспертиз, назначаемых при расследовании преступлений в сфере компьютерных преступлений.
10. Перечень сведений, составляющих государственную тайну.

Тема №5 «Лицензирование в области защиты информации»

1. Структура системы государственного лицензирования деятельности в области защиты информации.
2. Порядок лицензирования деятельности предприятий.
3. Дайте определение лицензионного договора.
4. Определите особенности заключения лицензионного договора.
5. Основные нормативные акты в области лицензирования ЗИ.
6. Дайте понятие сертификации.
7. Определите особенности проведения государственной аттестации руководителей предприятий.
8. Какие нормативные правовые акты по сертификации средств защиты информации?
9. Что составляет организационную структуру системы сертификации средств защиты информации по требованиям ее безопасности?
10. Назовите порядок проведения сертификации и контроля средств защиты информации.

Тема №6 «Сертификация в области защиты информации»

1. Что такое сертификация в области защиты информации и какие цели она преследует?
2. Какие организации или структуры отвечают за проведение сертификации в области защиты информации?
3. Каков процесс получения сертификата в области защиты информации? Какие требования и этапы включает этот процесс?
4. Какие стандарты и нормативы применяются при сертификации в области защиты информации?
5. Как определить, какой уровень сертификации необходим для конкретной организации или системы?
6. Какие преимущества и привилегии получает организация с сертифицированной системой защиты информации?
7. Какие типы сертификации существуют в области защиты информации? Как они отличаются друг от друга?
8. Что такое сертификационная схема и как она связана с процессом сертификации в области защиты информации?
9. Какие меры сопровождения требуются после получения сертификата в области защиты информации?
10. Какие вызовы и проблемы могут возникнуть при процессе сертификации в области защиты информации? Как их преодолеть?

Тема №7 «Система правовой ответственности за утечку информации и утрату носителей информации»

1. Виды юридической ответственности за нарушение правовых норм по защите информации.
2. Классификация характера сохраняемой тайны.
3. Проблемы уголовной ответственности за нарушение правовых норм по защите информации.
4. Уголовный кодекс РФ о наказаниях за правонарушения в области информационной безопасности.
5. Уголовный кодекс РФ о наказаниях за правонарушения в области информационной безопасности.
6. Административные взыскания за нарушения правовых норм по защите информации.
7. Проведение административного расследования по фактам нарушения установленного порядка защиты информации.
8. Особенности трудовых отношений при нарушении правовых норм в сфере информационной безопасности.
9. Особенности гражданско-правовых отношений при нарушении правовых норм в сфере информационной безопасности.
10. Особенности и основные направления международного сотрудничества в области обеспечения информационной безопасности РФ.

Тема №8 «Правовые основы деятельности подразделений защиты информации»

1. Объекты, подлежащие защите.
2. Особенности обеспечения безопасности объекта.
3. Организация и возможная структура службы безопасности объекта.
4. Классификация форм, методов и средств обеспечения безопасности.
5. Особенности закрытого делопроизводства как основного мероприятия по обеспечению режима секретности.
6. Соотношение пропускного и внутриобъектового режимов.
7. Особенности организации пропускного режима.
8. Организация внутриобъектового режима на территориях с ограниченным доступом.
9. Понятие, признаки, виды и общая характеристика преступлений в информационной сфере.
10. Признаки, состав и характеристика правонарушений в информационной сфере.

Тема №9 «Правовые основы защиты персональных данных»

1. Дайте определение понятия «персональные данные».
2. К какой категории сведений относятся персональные данные?

3. Каким федеральным законом регулируются права в области персональных данных?

4. Какие виды персональных данных вы можете назвать?

5. В каких формах государство регулирует работу с персональными данными?

6. Чем характеризуется обработка специальной категории персональных данных?

7. Каковы особенности обработки персональных данных в государственных или муниципальных информационных системах?

8. Какие требования выдвигает закон к деятельности организаций по обеспечению безопасности персональных данных?

9. Федеральный закон №152-ФЗ "О персональных данных"

10. Какие могут быть правовые основания обработки персональных данных?

Критерии оценки:

9-16 баллов выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1-8 баллов выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРАКТИЧЕСКИМ РАБОТАМ

Контрольные вопросы для защиты практической работы №1 «Организационно-правовые механизмы обеспечения информационной безопасности».

1. Что включают в себя каналы распространения информации?

2. Как вы понимаете термин «канал несанкционированного получения информации»?

3. В чем отличие третьего лица от злоумышленника?

4. Какие каналы несанкционированного доступа вы знаете?
5. Основные угрозы безопасности информации в компьютерных системах.
6. Дайте определение «Организационные каналы».
7. По каким признакам классифицируются «Организационные каналы утечки конфиденциальной информации».
8. Назовите основные организационные каналы утечки и несанкционированного доступа к информации.
9. Понятие, признаки, виды и общая характеристика преступлений в информационной сфере.
10. Признаки, состав и характеристика правонарушений в информационной сфере.

Контрольные вопросы для защиты практической работы №2 «Технические средства защиты информации».

1. На какие группы можно разделить средства защиты информации в части предотвращения преднамеренных действий.
2. Опишите каждую группу средств защиты информации в части предотвращения преднамеренных действий.
3. Какой следующий этап защиты информации, после проведения комиссии и составления, утверждения акта?
4. Что нужно сделать до составления план всего здания, его помещений, зон контроля?
5. Что включают в себя правовые средства обеспечения защиты информации?
6. Что включают в себя инженерно-технические средства защиты информации?
7. Что включают в себя программно-аппаратные средства защиты информации?
8. Перечислите требования, предъявляемые к системам защиты информации.
9. Какие существуют модели защиты информации?
10. Перечислите основные мероприятия организации работ по обеспечению защиты информации.

Контрольные вопросы для защиты практической работы №3 «Защита персональных данных».

1. Назовите этапы работ по защите персональных данных.
2. Что включают обязательные (в том числе предварительные) этапы работ по защите персональных данных?
3. Какие бизнес-процессы, в которых обрабатываются персональные данные, вы знаете?
4. На какие категории делятся персональные данные?

5. Нужно ли брать согласие на обработку ПД у субъектов при их защите?
6. Чем характеризуется обработка специальной категории персональных данных?
7. Каковы особенности обработки персональных данных в государственных или муниципальных информационных системах?
8. Какие требования выдвигает закон к деятельности организаций по обеспечению безопасности персональных данных?
9. Федеральный закон №152-ФЗ "О персональных данных"
10. Какие могут быть правовые основания обработки персональных данных?

Контрольные вопросы для защиты практической работы №4 «Разработка организационно-распорядительной документации для объекта информации».

1. Какие виды организационно-распорядительной документации вы знаете?
2. Назовите требования к оформлению организационно-распорядительной документации.
3. Назовите назначение основных видов организационно-распорядительных документов.
4. Состав реквизитов организационно-распорядительной документации.
5. Какая информация является конфиденциальной?
6. Что относится к защищаемой информации?
7. Что понимается под политикой безопасности?
8. Что понимается под несанкционированным воздействием на защищаемую информацию?
9. Дайте понятие конфиденциальности, целостности и доступности информации.
10. Нормативные документы, регламентирующие порядок разработки документации для объекта информации.

Контрольные вопросы для защиты практической работы №5 «Анализ эффективности применения средств защиты информации на объекте информатизации».

1. Назовите основные организационно-технические мероприятия по защите информации.
2. Назовите основные угрозы для системы электронного документооборота.
3. Что подразумевает «угроза доступности информации»?
4. Что подразумевает «угроза конфиденциальности»?

5. Перечислите основные методы и средства обеспечения защиты информации.
6. Что включают в себя организационные средства обеспечения защиты информации?
7. Что включают в себя правовые средства обеспечения защиты информации?
8. Какие существуют модели защиты информации?
9. Перечислите основные мероприятия организации работ по обеспечению защиты информации.
10. Приведите структуру и содержание цикла работ по защите информации.

Контрольные вопросы для защиты практической работы №6 «Разработка модели угроз информационной безопасности».

1. Что вы понимаете под моделью угроз информационной безопасности?
2. Назовите шаги построения модели угроз информационной безопасности.
3. В модели должны учитываться все актуальные угрозы на всех стадиях их жизненного цикла? Если нет, то какие?
4. Содержание модели угроз»?
5. Определение источников угроз.
6. Выявление критических объектов информационной системы.
7. Определение перечня угроз для каждого критического объекта.
8. Выявление способов реализации угроз.
9. Кто должен разрабатывать модель угроз?
10. Как строится модель угроз?

Критерии оценки:

9-16 баллов выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1-8 баллов выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не

отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.3 ПРОИЗВОДСТВЕННЫЕ ЗАДАЧИ

1. Ваша компания собирается начать работу с новым контрагентом, который занимается обработкой конфиденциальной информации. Какие нормативные акты необходимо изучить, чтобы обеспечить безопасность обмена информацией с этим контрагентом?

2. На производственной площадке был установлен новый оборудование, связанное с обработкой персональных данных. Какие нормативно-правовые требования необходимо выполнить для обеспечения безопасности обработки персональных данных на данном оборудовании?

3. В вашей компании был обнаружен случай утечки конфиденциальной информации. Какие нормативно-правовые требования необходимо выполнить для уведомления компетентных органов и пострадавших лиц о случившемся?

4. Ваша компания работает с персональными данными клиентов. Какие нормативно-правовые акты нужно соблюдать при обработке и хранении таких данных?

5. На производстве было обнаружено нарушение правил доступа к информационной системе. Какие нормативно-правовые требования необходимо выполнить для расследования этого инцидента и принятия мер по обеспечению безопасности информации?

6. Компания разрабатывает новый продукт, который будет обрабатывать и хранить конфиденциальную информацию клиентов. Какие законодательные акты в области информационной безопасности необходимо учесть при разработке и внедрении продукта?

7. В организации возник конфликт между необходимостью обеспечения информационной безопасности и требованиями к свободному доступу к информации. Какие нормативно-правовые акты могут помочь решить этот конфликт?

8. Компания проводит аудит информационной безопасности и выявляет нарушения требований законодательства в области защиты персональных данных. Какие меры необходимо принять для устранения нарушений и соблюдения нормативно-правовых актов?

9. В компании необходимо обеспечить защиту от утечки конфиденциальной информации. Какие законодательные акты в области информационной безопасности необходимо учесть при разработке и внедрении системы защиты информации?

10. Компания собирается начать работу с персональными данными граждан Европейского Союза. Какие требования к защите персональных данных установлены законодательством ЕС, и как их необходимо учесть при организации работы с данными?

Критерии оценки:

7-8 баллов выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1-4 баллов выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.4 КЕЙС-ЗАДАЧИ

1. Компания "Альфа" занимается разработкой программного обеспечения для крупных банков. В связи с этим у компании имеются конфиденциальные данные клиентов банков. Недавно компания получила запрос на разработку ПО от нового клиента - банка "Бета". Однако, в условиях договора с "Бета", необходимо соблюдать требования по защите информации о клиентах банка на всех этапах разработки и хранения ПО.

Компания "Альфа" решает приступить к разработке ПО для "Бета", но не уверена, что полностью соответствует всем требованиям по защите информации. Кроме того, "Альфа" знает, что имеет ряд законодательных ограничений в области обработки конфиденциальных данных.

Какие действия должна предпринять компания "Альфа" для соблюдения нормативно-правового регулирования в сфере информационной безопасности и защиты конфиденциальной информации клиентов банка "Бета"?

2. Компания, занимающаяся онлайн-торговлей, получила уведомление о том, что на одном из ее серверов был обнаружен вредоносный код. Дальнейшее расследование показало, что причиной инцидента стало нарушение нормативно-правового регулирования в сфере информационной

безопасности. Компания не принимала меры по регулярной проверке своих систем на наличие уязвимостей и отсутствовала процедура реагирования на инциденты информационной безопасности.

Задача: Ваша задача состоит в том, чтобы помочь компании разработать план действий для исправления ситуации и предотвращения подобных инцидентов в будущем.

1) Какие конкретные нарушения нормативно-правового регулирования в сфере информационной безопасности были допущены компанией?

2) Какие дополнительные меры компании необходимо предпринять, чтобы исправить ситуацию?

3) Какие дополнительные меры компании необходимо предпринять, чтобы предотвратить подобные инциденты в будущем?

4) Какие законодательные акты и нормы регулируют информационную безопасность в данной ситуации, и какие санкции могут быть применены в случае нарушения этих актов?

5) Какую роль в данной ситуации могут сыграть сторонние эксперты по информационной безопасности, и какие задачи они могут выполнить?

3. В компании "Альфа" разрабатывается новая информационная система, которая будет обрабатывать и хранить большое количество конфиденциальных данных клиентов. Компания хочет обеспечить полную безопасность этих данных и соответствовать нормативно-правовым требованиям.

Одним из главных требований является соблюдение стандартов и правил, установленных в области информационной безопасности. В частности, необходимо соблюдать требования по защите информации, установленные федеральными законами Российской Федерации.

Ваша задача как специалиста по информационной безопасности состоит в том, чтобы провести анализ текущей ситуации в компании "Альфа" и подготовить рекомендации по обеспечению надежной защиты информации в соответствии с нормативно-правовыми требованиями.

1) Оцените текущую систему защиты информации в компании "Альфа", включая систему аутентификации и авторизации пользователей, уровень шифрования данных, механизмы защиты от вторжений и другие аспекты информационной безопасности.

2) Составьте список всех требований по защите информации, установленных федеральными законами Российской Федерации, которые должна соблюдать компания "Альфа".

3) Подготовьте план мероприятий по усилению защиты информации в компании "Альфа" в соответствии с требованиями законодательства, включая рекомендации по установке дополнительных механизмов защиты, обучению сотрудников и т.д.

4) Проведите анализ рисков и угроз для информационной системы компании "Альфа" и подготовьте план по их минимизации.

5) Подготовьте рекомендации по управлению доступом к информации, включая установку правил доступа для различных групп пользователей, а также механизмы мониторинга и анализа действий пользователей.

6) Подготовьте доклад для руководства компании "Альфа" о текущей ситуации в области информационной безопасности и предложенных мерах по усилению защиты информации в соответствии с нормативно-прав

4. Вы являетесь ответственным за информационную безопасность в крупной компании, которая занимается разработкой программного обеспечения. Однажды вы узнали, что один из ваших сотрудников, не имеющий необходимых полномочий, имел доступ к базе данных клиентов, содержащей конфиденциальную информацию.

Вы обратились к руководству компании и сообщили о нарушении нормативно-правового регулирования в сфере информационной безопасности. Однако, руководство компании проигнорировало ваше сообщение и не предприняло никаких мер для устранения нарушения.

Как вы будете действовать в данной ситуации?

Задачи:

1) Составьте план действий для устранения нарушения нормативно-правового регулирования в сфере информационной безопасности в компании.

2) Определите, какие нормативные документы были нарушены, и какие меры должны быть предприняты для исправления нарушений.

3) Подготовьте отчет для руководства компании, в котором обоснуйте необходимость устранения нарушений, перечислите все риски, связанные с невыполнением нормативных требований, и предложите конкретные меры по исправлению ситуации.

4) Рассмотрите возможность обратиться к правоохранительным органам для привлечения ответственных лиц к ответственности за нарушение нормативно-правового регулирования в сфере информационной безопасности.

5. Вы работаете руководителем отдела информационной безопасности в крупной финансовой компании. Компания регулярно собирает, обрабатывает и хранит конфиденциальную информацию своих клиентов, поэтому защита данных является критически важной задачей.

Недавно вступили в силу новые нормативные акты, предписывающие использование определенных методов и технологий для обеспечения безопасности персональных данных. Ваша компания должна выполнить эти требования, чтобы избежать штрафов и возможных репутационных потерь.

Ваша задача: разработать план действий для обеспечения соответствия нормативным актам и провести аудит системы информационной безопасности компании для выявления недостатков и рисков.

Ключевые шаги:

1) Изучите нормативные акты и требования, связанные с обеспечением безопасности персональных данных.

2) Оцените текущую систему информационной безопасности компании, чтобы выявить недостатки и определить, какие меры необходимо принять для соответствия требованиям.

3) Разработайте план действий, который будет содержать необходимые меры, сроки и ответственных за их выполнение.

4) Проведите аудит системы информационной безопасности компании, чтобы проверить соответствие ее нормативным требованиям и обнаружить любые потенциальные риски и уязвимости.

5) Оцените результаты аудита и разработайте план действий по устранению выявленных недостатков и уязвимостей.

6) Разработайте процедуры и инструкции для обеспечения надлежащего управления информационной безопасностью в соответствии с нормативными требованиями.

7) Обеспечьте тренинг и обучение сотрудников компании по вопросам информационной безопасности, чтобы гарантировать, что они понимают свои обязанности и могут помочь предотвратить нарушения безопасности данных.

8) Регулярно проверяйте систему информационной безопасности компании, чтобы убедиться в ее соответствии нормативным требованиям и выявить любые новые уязвимости или риски.

Критерии оценки:

7-8 баллов выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

1-4 баллов выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Субъектами информационных отношений в области коммерческой тайны являются:

1) -физические лица;
2) - юридические лица всех форм собственности;
3) - органы государственной власти;
4) - должностные лица;

2. Коммерческую тайну субъекта хозяйствования не могут составлять:

А) учредительные документы, а также документы, дающие право на занятие предпринимательской деятельностью и отдельными видами хозяйственной деятельности;

Б) сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные данные, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей;

1) А-верно, Б-не верно
2) А-не верно, Б-верно
3) -оба верны
4) оба не верны

3. Коммерческая тайна - это

1) -информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которой нет свободного доступа на законном основании, обладатель которой принимает меры к охране ее конфиденциальности.
2) сведения, доступ к которым ограничен госорганами в соответствии с ГК РФ и федеральными законами.
3) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами.
4) правовое, социально-этическое понятие, представляющее собой запрет медицинскому работнику сообщать третьим лицам информацию о состоянии здоровья пациента.

4. Тайны делятся на:

1) -Государственные,
2) Международные
3) -служебные
4) -личная тайна.

5. К профессиональной тайне относится информация:

1) -ставшая известной лицу определенной профессии в силу исполнения им профессиональных обязанностей;
2) являющаяся государственной или коммерческой тайной;
3) не защищаемая законом;
4) связанная с государственной или муниципальной службой;
5) -распространение которой может нанести ущерб ее исходному владельцу.

6. Служебная тайна —это…

1) -сведения, доступ к которым ограничен госорганами в соответствии с ГК РФ и федеральными законами;
2) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами.
3) информация, имеющая действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которой нет свободного доступа на законном основании, обладатель которой принимает меры к охране ее конфиденциальности.
4) правовое, социально-этическое понятие, представляющее собой запрет медицинскому работнику сообщать третьим лицам информацию о состоянии здоровья пациента,

7. Принципы, не относящиеся к построению комплексной системы защиты информации

1) принцип законности
2) принцип превентивности
3) принцип полноты состава защищаемой информации
4) принцип обоснованности защиты информации
5) -принцип доступности

8. Комплексная система защиты информации – это

1) -система, полно и всесторонне охватывающая все предметы, процессы и факторы, которые обеспечивают безопасность всей защищаемой информации.
2) это комплекс мер, которые предназначены для безопасного хранения и защиты информации от нежелательных пользователей.
3) деятельность по предотвращению утечки, хищения, утраты, модификации (подделки), несанкционированных и непреднамеренных воздействий на защищаемую информацию.

9. Назначение комплексности защиты информации состоит:

А) в объединении локальных систем защиты;

Б) обеспечении полноты всех составляющих системы защиты;

1) А-верно,Б-не верно
2) А-не верно,Б-верно
3) -оба верны
4) оба не верны

10. Комплекс – это…

1) -совокупность предметов и явлений, составляющих одно целое.
2) один из основополагающих принципов защиты информации.
3) метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

11. Комплексность – это…

1) -один из основополагающих принципов защиты информации.
2) совокупность предметов и явлений, составляющих одно целое.
3) система, полно и всесторонне охватывающая все предметы, процессы и факторы, которые обеспечивают безопасность всей защищаемой информации».

12. Что называют защитой информации?

1) - Все ответы верны
2) Называют деятельность по предотвращению утечки защищаемой информации
3) Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию
4) Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

13. На основе персональных компьютеров построены сети ЭВМ:

1) - локальные,
2) региональные
3) городские,
4) –транснациональные

14. Современное предприятие представляет собой сложную систему, в рамках которой осуществляется защита информации. Выберите основные особенности такого сложного современного предприятия:

1) -сложная организационная структура;
2) -многоаспектность функционирования;
3) -высокая техническая оснащённость;

4) -непрерывно расширяющаяся доступность;

15. Системный подход – это …

1) -принцип рассмотрения проекта, при котором анализируется система в целом, а не её отдельные части.
2) -система, полно и всесторонне охватывающая все предметы, процессы и факторы, которые обеспечивают безопасность всей защищаемой информации
3) один из основополагающих принципов защиты
4) принцип улучшения эффективности отдельных частей системы

16. Системный подход к построению любой системы включает в себя:

1) изучение объекта внедряемой системы;
2) оценку угроз безопасности объекта;
3) анализ средств, которыми будем оперировать при построении системы;
4) оценку экономической целесообразности;
5) -Все варианты ответов являются верными.

17. Под системностью как основной частью системно-концептуального подхода информационной безопасности понимается:

А) системность целевая, т.е. защищённость информации рассматривается как основная часть общего понятия качества информации;
Б) системность пространственная, предлагающая взаимоувязанное решение всех вопросов защиты на всех компонентах предприятия;

1) а-верно, б-не верно
2) а-не верно, б-верно
3) -оба верны
4) оба не верны

18. К произведениям, не являющимся объектами авторского права (п. 6 ст. 1259 ГК) не относится:

1) официальные документы государственных органов и органов местного самоуправления муниципальных образований, в том числе законы, другие нормативные акты, судебные решения, иные материалы законодательного, административного и судебного характера, официальные документы международных организаций, а также их официальные переводы;
2) государственные символы и знаки (флаги, гербы, ордена, денежные знаки и тому подобно, а также символы и знаки муниципальных образований;
3) произведения народного творчества (фольклор), не имеющие конкретных авторов;
4) -Изобретения, промышленные образцы, полезные модели

19. К объективной форме интеллектуальной собственности не относится

1) рукопись, машинопись, нотная запись
2) публичное произнесение
3) звуко- или видеозаписи
4) -официальные документы государственных органов

20. К принципам авторского права не относится:
1) принцип свободы творчества
2) принцип сочетания личных интересов автора с интересами общества
3) принцип не отчуждаемости личных неимущественных прав автора
4) -принцип уникальности

21. Субъекты патентного права не являются:
1) -Патент выдающие органы
2) авторы (соавторы) изобретений, полезных моделей и промышленных образцов;
3) патентообладатели;
4) иные лица, приобретающие определенные патентные права на основании закона или договора (наследники и иные правопреемники авторов и патентообладателей).

22. Признаются промышленными образцами:
1) решения, обусловленные исключительно технической функцией изделия (гайки, болты и пр.);
2) объекты архитектуры;
3) промышленные, гидротехнические и иные стационарные сооружения;
4) -художественно-конструкторские решения

23. Товарный знак – это…
1) -средство индивидуализации товаров
2) средство индивидуализации работ и услуг, иными словами, нематериальных благ
3) средство индивидуализации коммерческих юридических лиц, представляющее собой название организации
4) обозначение, служащее для различения товаров, услуг, предприятий, организаций и других объектов в сфере хозяйственного оборота

24. К средствам индивидуализации не относятся:
1) фирменное наименование, наименование некоммерческой организации,
2) товарный знак, знак обслуживания,
3) коммерческое обозначение,
4) -наименование места происхождения товара,
5) девизы, логотипы, слоганы,

25. К коммерческой тайне не относятся информация, которая:

1) имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее другим;
2) -Не может быть использована в корыстных целях
3) не является общедоступной на законном основании;
4) не содержит государственной тайны .

26. Основные признаки изобретения, отвечающие за эффективность патентования:

1) -мировая новизна,
2) -изобретательский уровень,
3) Сложность конструкции
4) Стоимость изобретения

27. Различные правонарушения интеллектуальной собственности

1) -Торговля контрафактной продукцией через Интернет-магазины.
2) -Плагиат
3) Копирование
4) Цитирование

28. Выберите НЕверный вариант ответа. Нормативное правовое обеспечение функционирования системы обеспечения информационной безопасности Российской Федерации.

1) Координации деятельности федеральных органов исполнительной власти по решению задач противодействия угрозам национальным интересам в информационной сфере;
2) Разграничения компетенции федеральных органов исполнительной власти в области обеспечения информационной безопасности Российской Федерации
3) Согласования деятельности федеральных органов исполнительной власти и деятельности органов исполнительной власти субъектов Российской Федерации по решению задач обеспечения информационной безопасности в рамках установленного законодательством разграничения предметов ведения и полномочий.
4) -План счетов бухгалтерского учета и порядок его применения.

29. Какая статья УК РФ относиться к правовой защите информации.

a) -Статья 146. Нарушение авторских и смежных прав.
b) Статья 110. Доведение до самоубийства.
c) Статья 128.1. Клевета.
d) Статья 143. Нарушение требований охраны труда.
e) Статья 159. Мошенничество.

30. К какой отрасли права относиться информационной система?

a) Гражданское право.
b) Уголовное право.
c) -Информационное право.
d) Компьютерное право.
e) Электронно-производственное право.

31. Режим защиты информации не устанавливается в отношении сведений, относящихся к …

1. государственной тайне.
2. конфиденциальной информации.
3. персональным данным.
4. -деятельности государственных деятелей.

32. В регистрации средства массовой информации не может быть отказано…

1. -по мотивам нецелесообразности
2. если регистрирующий орган уже зарегистрировал другое средство массовой информации с тем же названием и формой распространения
3. когда заявление подано не соответствующим лицом
4. даже если сведения в заявлении не соответствуют действительности

33. Засекречиванию подлежат сведения о …

1. состоянии демографии
2. состоянии преступности
3. -силах и средствах гражданской обороны
4. фактах нарушения прав и свобод человека и гражданина

34. Проверить электронно-цифровую подпись под документом может…

1. только эксперт, преобразуя электронный образец документа и открытый ключ отправителя
2. только эксперт с помощью преобразований электронного образца документа, открытого ключа отправителя и собственно значения электронно-цифровой подписи
3. только отправитель электронного документа
4. -любое заинтересованное лицо, преобразуя электронный образец документа, открытый
5. -ключ отправителя и собственно значение электронно-цифровой подписи

35. Режим документированной информации – это …

1. выделенная информация по определенной цели
2. выделенная информация в любой знаковой форме
3. электронная информация, позволяющая ее идентифицировать

4. - электронный документ с электронно-цифровой подписью

36. Согласие субъекта персональных данных на их обработку требуется, когда обработка персональных данных осуществляется …

1) для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно
2) для доставки почтовых отправлений
3) в целях профессиональной деятельности журналиста
4) -в целях профессиональной деятельности оператора

37. Режим **общественного** достояния устанавливается для …

1. для государственных органов и муниципальных образований
2. любой общедоступной информации
3. -сведений, которые являются уникальными, незаменимыми по своей природе
4. любой общественной организации

38. Учредителями средства массовой информации могут выступать…

1. -власти.
2. -граждане, достигшие 18 лет, объединения граждан, организаций, органы государственной
3. только юридические лица
4. граждане, достигшие 18 лет и лица без гражданства, постоянно проживающие на территории российской Федерации
5. граждане, достигшие 16 лет и юридические лица
6. граждане другого государства, постоянно не проживающие в Российской Федерации, юридические лица и органы государственной власти

39. Чтобы обеспечить доказательства при возникновении спора, редакция радио-, телепрограммы обязана сохранять в записи материалы собственных передач, вышедших в эфир (не менее … со дня выхода в эфир) и фиксировать передачи, вышедшие в эфир в регистрационном журнале, который хранится не менее … с даты последней записи.

1. -1 месяца, 1 года
2. 1 года, 3 лет
3. 7 месяцев, полгода

40. С точки зрения информационного права информация – это …

1. форма выражения объективных знаний

2. сведения о законодательстве, правовых явлениях, правоприменительной деятельности
3. -сведения независимо от формы их представления
4. данные о развитии конкретной правовой науки и ее практическом применении

41. Не являются объектами информационного правоотношения …

1. -обладатели информации
2. элементы информационной системы
3. информационные продукты
4. неправовая информация
5. информационные системы
6. -недокументированная информация

42. Общее управление информационной сферой не вправе осуществлять …

1. министерство информационных технологий
2. -экспертные советы
3. федеральное агентство по науке и инновациям
4. федеральные службы

43. Открытость информации в архивных фондах обеспечивается…

1. различными режимами доступа к информации
2. -различными режимами доступа к информации и переходом информации из одной
3. переходом информации из одной категории доступа в другую
4. категории доступа в другую
5. правовым статусом архивного фонда

44. Под периодическим печатным изданием понимается альманах, бюллетень, имеющие…

1. постоянное название и выходящие в свет не реже одного раза в месяц
2. постоянное название и текущий номер
3. -постоянное название, текущий номер и выходящие в свет не реже одного раза в год
4. постоянное название, текущий номер и выходящие в свет не реже одного раза в месяц

45. Признак, не относящийся к коммерческой тайне

1. отсутствует свободный доступ к информации
2. обладатель информации принимает меры к охране ее конфиденциальности
3. информация имеет действительную или потенциальную коммерческую ценность
4. -сведения, содержащие коммерческую тайну, устанавливаются учредительными
5. -документами

46. Основные объекты обеспечения информационной безопасности России

1. квалифицированные кадры в области информационных технологий
2. информационные продукты
3. -информационные ресурсы, содержащие сведения, которые относятся к государственной
4. -помещения, предназначенные для ведения закрытых переговоров
5. -тайне и конфиденциальной информации

47. Предмет информационного права на современном этапе развития законодательства – это …

1. -общественные отношения в информационной сфере
2. информационные отношения, возникающие в процессе производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления информации
3. совокупность результатов труда, воплощенных в информации, информационных ресурсов, информационных технологий, средств и технологий коммуникации информации по сетям связи
4. продукты, производные от информации и деятельность, связанная с ними

48. К служебной тайне не относится …

1. тайна деятельности соответствующего органа
2. профессиональная тайна
3. -вред, причиненный здоровью работника в связи с производственной травмой

49. Как называется информация, к которой ограничен доступ?

1) Противозаконная
2) Открытая
3) - Конфиденциальная
4) Недоступная

50. В правовой режим документированной информации входит …

1. тайна частной жизни

2. банковская тайна
3. персональные данные
4. государственная тайна
5. -электронная цифровая подпись

51. Исключите неправильный постулат:

1. информация не связана с определенным конкретным носителем
2. информация не существует без материального носителя
3. -содержание информации меняется одновременно со сменой материального носителя

52. Редакция обязана…

1. в любом случае соблюдать в тайне источник информации с условием неразглашения его имени
2. -если затронуты честь, достоинство или деловая репутация гражданина
3. отвечать на письма граждан и пересылать письма тем органам, в чью компетенцию входит их рассмотрение
4. -исключением случая, когда соответствующее требование поступило от суда в связи с
5. -соблюдать авторские права на результаты интеллектуальной деятельности
6. -находящимся в его производстве делом
7. -распространить опровержение или предоставить гражданину право зачитать его самому,
8. -соблюдать в тайне источник информации с условием неразглашения его имени за

53. К государственной тайне не относятся сведения, защищаемые государством …, распространение которых может нанести ущерб государству.

1. в экономической области
2. в оперативно-розыскной деятельности
3. в контрразведывательной деятельности
4. -о частной жизни политических деятелей

54. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений…

1. -неоправданных расходов
2. -которые составляют финансово-экономическую информацию и позволяют избежать

3. безопасности пищевых продуктов
4. о показателях производственного травматизма, профессиональной заболеваемости
5. о системе оплаты и условиях труда

55. Ответственность за создание вредоносной программы наступает в…

1. -совокупности с ответственностью за ее использование
2. случаях, установленных законодательством
3. любом случае

56. Обработка специальных категорий персональных данных в отношении религиозных или философских убеждений допускается в случае, когда обработка персональных данных…

1. необходима в соответствии с оперативно-розыскной деятельностью
2. -необходима в связи с выездом за пределы Российской Федерации
3. осуществляется в медицинских целях для установления диагноза при условии, что ее осуществляет профессиональный медицинский работник
4. необходима в связи с осуществлением правосудия

57. Субъектами информационных отношений могут (может) быть …

1. -трансграничные информационно-телекоммуникационные сети
2. муниципальные образования
3. Российская Федерация
4. трудовой коллектив

58. Не является признаком информационного общества …

1. массовое подключение персональных компьютеров к трансграничным информационно-телекоммуникационным сетям
2. общедоступность и постоянное обновление информационных данных
3. мгновенная коммуникация членов общества друг с другом, вне зависимости от времени и от расстояния
4. -приоритетное развитие сельского хозяйства и промышленности на основе нанотехнологий

59. Признак, не относящийся к охраноспособной информации – это …:

1. доступ к охраноспособной информации ограничен только законом
2. защита охраноспособной информации устанавливается Законом
3. -доступ к охраноспособной информации ограничен владельцем информационных ресурсов
4. охране подлежит только документированная информация

60. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений…

1. -об использовании новых технологий, позволяющих получить коммерческую выгоду
2. об оплате труда работников некоммерческих организаций
3. об использовании безвозмездного труда граждан в деятельности некоммерческой организации
4. о размере и составе имущества некоммерческих организаций

61. Не являются принципами информационного права …

1. принцип равноправия языков
2. принцип оборотоспособности
3. -принцип преимущества применения нанотехнологий в промышленности
4. - принцип свободы слова
5. принцип распространяемости
6. -принцип имущественной ответственности

62. Федеральный закон «О персональных данных» от 27 июля 2006 г. не регулирует отношения, возникающие при…

1. -обработке персональных данных, отнесенных к служебной тайне
2. хранении, комплектовании, учете и использовании архивных документов
3. обработке персональных данных, отнесенных к государственной тайне
4. включении в Единый государственный реестр индивидуальных предпринимателей
5. обработке персональных данных физическими лицами исключительно для личных и семейных нужд

63. Основное средство антивирусной защиты

1. -резервное копирование ценных данных
2. подготовка квалифицированных кадров в сфере информационной безопасности
3. регулярное сканирование жестких дисков

64. Дети до 6 лет не вправе…

1. с разрешения законных представителей выходить в Интернет
2. с согласия законных представителей пользоваться телефонными услугами
3. -с согласия законных представителей совершать сделки с компьютерной техникой

65. Владелец информационных ресурсов не обязан …

1. бесплатно опубликовывать библиографическую информацию
2. -использовать информацию по своему усмотрению
3. хранить производственные документы
4. включать библиографическую информацию в международные автоматизированные банки данных

66. Основные предметные направления Защиты Информации?

1) -охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
2) Охрана золотого фонда страны
3) Определение ценности информации
4) Усовершенствование скорости передачи информации

67. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

1) - защищенные КС
2) небезопасные КС
3) Само достаточные КС
4) Саморегулирующиеся КС

68. Какими путями может быть получена информация?

1) - проведением, покупкой и противоправным добыванием информации научных исследований
2) захватом и взломом ПК информации научных исследований
3) добыванием информации из внешних источников и скремблированием информации научных исследовании
4) захватом и взломом защитной системы для информации научных исследований

69. Как называется информация, к которой ограничен доступ?

1. - Конфиденциальная
2. Противозаконная
3. Открытая
4. Недоступная

70. Сертификация –

1) -процедура подтверждения соответствия, посредством которой независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация удостоверяет в письменной форме, что продукция соответствует установленным требованиям.
2) подтверждение квалификации, уровня знаний и умений человека — отзыв, характеристика

3) повторная аттестация работников на предмет их соответствия профессии (должности)

71. ФСТЭК организует обязательную аттестацию объектов информатики:

1) -создает системы аттестации и устанавливает правила проведения аттестации в этих системах;
2) -устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;
3) -утверждает нормативные и методические документы по аттестации.

72. Государственные органы по лицензированию:

организуют обязательное государственное лицензирование деятельности предприятий;
выдают государственные лицензии предприятиям-заявителям;

1) А-верно ,Б-не верно
2) А-не верно,Б-верно
3) -оба верны
4) оба не верны

73. Организационную структуру системы государственного лицензирования деятельности предприятий в области защиты информации образуют:

1) областные органы по лицензированию;
2) Лицевые центры
3) -лицензионные центры;
4) -предприятия-заявители.

74. Криптографические средства

1) -средства защиты с помощью преобразования информации (шифровани.
2) правовые акты страны, которые регламентируют правила использования, обработки и передачи информации ограниченного доступа и которые устанавливают меры ответственности за нарушение этих правил.
3) нормы, традиции в обществе**.**

75. Аппаратно-программные средства защиты -

1) -средства, в которых программные (микропрограммны и аппаратные части полностью взаимосвязаны и неразделимы.
2) средства защиты с помощью преобразования информации (шифровани.
3) это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для

внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.

4) предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем

76. Программные средства защиты –

1) -предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.

2) предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем

3) это электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками. Они предназначены для внутренней защиты структурных элементов средств и систем вычислительной техники: терминалов, процессоров, периферийного оборудования, линий связи и т.д.

77. Физические средства защиты -

1) -предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем.

2) предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.

3) средства, в которых программные (микропрограммны и аппаратные части полностью взаимосвязаны и неразделимы.

78. Маскировка –это…

1) метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

2) -метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

3) метод защиты информации в автоматизированной информационной системе предприятия путем ее хеширования.

79. Коммерческая тайна это…

1) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
2) - ограничения доступа в отдельные отрасли экономики или на конкретные производства
3) защищаемые банками и иными кредитными организациями сведения о банковских операциях
4) защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

80. Какая из перечисленных атак на поток информации является пассивной:
1) - перехват.
2) имитация.
3) модификация.
4) фальсификация.
5) Прерывание

81. К открытым источникам информация относятся.
1) -Газеты, Радио, Новости
2) Информация украденная у спецслужб
3) Из вскрытого сейфа
4) Украденная из правительственной организации

82. Врачебная тайна - информация, содержащая:
1) -результаты обследования лица, вступающего в брак;
2) -сведения о факте обращения за медицинской помощью, о состоянии здоровья, диагнозе заболевания и иные сведения, полученные при обследовании и лечении гражданина;
3) -сведения о проведенных искусственном оплодотворении и имплантации эмбриона, а также о личности донора;
4) -сведения о доноре и реципиенте при трансплантации органов и (или) тканей человека;

83. Что такое политика информационной безопасности
1) Методология защиты информации
2) -Идеология информационной безопасности
3) Концепция защиты информации

84. Какой федеральный закон считается рамочным по защите информации?
1) ФЗ «О коммерческой тайне»
2) ФЗ «О персональных данных»

3) -ФЗ «Об информации, информационных технологиях и о защите информации»

85. Номер ФЗ «Об информации, информационных технологиях и о защите информации» является:

1) 188 ФЗ
2) 152 ФЗ
3) -149 ФЗ
4) 214 ФЗ

86. Лицензирование деятельности по распространению криптографических средств, осуществляет:

1) –ФСБ.
2) ФСТЭК.
3) Роскомнадзор.
4) Ростехнадзор.

87. Подключение ИС, обрабатывающих служебную тайну к сети Интернет:

1) допускается.
2) не допускается.
3) -допускается только с использованием специально предназначенных для этого средств.
4) допускается только с использованием средств защиты известных производителей.

88. Специальная проверка это

1) выявление возможных каналов утечки информации Российскими техническими средствами.
2) определение соответствия условий эксплуатации ОИ требованиям аттестатов соответствия объектам защиты.
3) -проверки технических средств на наличие возможно внедренных электронных устройств перехвата информации.

89. Каким документов определяются права человека на доступ к информации?

1) Доктриной ИБ
2) -Конституцией
3) ФЗ «О коммерческой тайне»

90. В соответствии с каким Гостом производится аттестация объекта информатизации?

1) -ГОСТ РО 0043-004-2013.
2) ГОСТ ISO 17799.
3) BS 7799.

91. Источниками угроз несанкционированного доступа являются:

1) -нарушители
2) природные факторы
3) -носители вредоносных программ
4) -аппаратные закладки
5) отказы оборудования
6) отказы программного обеспечения

92. Основные направления обеспечения информационной безопасности указанные в Доктрине ИБ

1) стратегическое развитие военных конфликтов, которые могут возникнуть в результате применения информационных технологий;
2) совершенствование Вооруженных Сил Российской Федерации;
3) -прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;
4) -содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере.

93. Техническими каналами утечки информации, приводящими к возникновению угроз безопасности персональных данных являются:

1) кражи технических средств информационной системы
2) -утечки акустической (речевой) информации
3) утечки информации реализуемые через общедоступные информационные сети
4) -утечки видовой информации
5) -утечки информации по каналам побочных электромагнитных излучений
6) утечки информации реализуемые через интернет

94. Документом, определяющим лицензируемые виды деятельности, является:

1) Постановление правительства РФ от 26 января 2006 г. № 45 Об организации лицензирования отдельных видов деятельности.
2) Постановление Правительство РФ от 15 августа 2006 г. № 504 О лицензировании деятельности по технической защите конфиденциальной информации.
3) Постановление Правительства РФ от 31 августа 2006 г. № 532 О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации.
4) -ФЗ «О лицензировании отдельных видов деятельности» 99-ФЗ от 4 мая 2011 г.
5) ФЗ «О техническом регулировании» 184-ФЗ от 27 декабря 2002 г.

95. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

1) -противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;
2) осуществление контроля за населением РФ с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;
3) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления;

96. Перечислить нормативно-методические документы по анализу угроз и уязвимостей
1) -BS 7799-3
2) -ISO 27005
3) -BSI IT Baseline Protection Manual
4) ГОСТ 3328

97. «Информационная система» это:
1) -совокупность информации, информационных технологий и технических средств.
2) совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему.
3) совокупность информационных технологий и технических средств.
4) совокупность информации, технических средств и персонала, обслуживающего информационную систему.
5) совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему.

98. Количество категорий внутренних нарушителей для ИСПДн, определяемых нормативными документами ФСТЭК:
1) 4
2) 6
3) -8
4) 9

99. Основными элементами ИС являются:
1) помещения для размещения технических средств
2) -персональные данные, содержащиеся в базах данных
3) -контролируемая зона
4) -информационные технологии

5) обслуживающий персонал
6) -технические средства обработки информации
7) ограждающие конструкции
8) технические средства перевозки материальных носителей информации

100. Каким нормативными документами регламентируется деятельность по выявлению угроз

1) -BS 7799
2) -ISO 27005
3) -BSI IT Baseline Protection Manual
4) ГОСТ 3328
5) Приказ ФСТЭК № 31

Задания в открытой форме

1) При внедрении организационных мер защиты информации осуществляются: введение … на действия персонала.

2) Ущерб от реализации риска может быть - ... и … .

3) При проектировании системы защиты автоматизированной системы управления необходимо: определять типы … и … , являющихся объектами защиты .

4) Основные требования к системе защиты автоматизированной системы управления должны содержать - … .

5) Классификация угроз информационной безопасности, по виду активов делиться на угрозы, направленные против … и угрозы, направленные против … .

6) … критерии предъявляются к действиям разработчика системы, документам для оценивания и работе самой организации. Включают требования доверия к мерам к СЗИ в информационных системах, а также к их разработке и эксплуатации.

7) … — положения политик безопасности.

8) К методам и способам защиты информации в информационных системах относятся методы и способы защиты информации от … и методы и способы защиты информации от … .

9) Основным ответственным лицом за определение уровня классификации информации является …

10) Основным ответственным лицом за определение уровня классификации информации является …

11) Действия третьей стороны, цель которых подтвердить (с помощью сертификата соответствия) то, что изделие (в том числе программное средство) или услуга соответствует определенным стандартам или другим нормативным документам– это …

12) Потенциальная причина инцидента, который может нанести ущерб системе или организации, это – …

13) Эффективная программа безопасности требует сбалансированного применения организационных и … методов.

14) Субъект персональных данных может отозвать свое согласие на обработку …

15) Концепция защиты информации, циркулирующая в помещениях или технических системах коммерческого объекта, требует не периодического, а … контроля в зоне расположения объекта.

16) …. - представляет собой совокупность управленческих решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению информационной безопасности, так и создание и функционирование систем защиты информации на конкретных объектах.

17) … информации отличаются большим разнообразием видов и основаны на установлении разнообразных, в том числе законных, взаимоотношений злоумышленника с фирмой или ее сотрудником для последующего несанкционированного доступа к интересующей информации.

18) Согласно законодательству информация представляет собой …, независимо от формы их представления..

19) ... средства. Это различные по типу, которые аппаратными средствами решают задачи защиты информации.

20) … — комплекс мероприятий, направленных на обеспечение установленного режима секретности непосредственно в структурных подразделениях, на объектах и в служебных помещениях предприятия.

Задание на установление правильной последовательности

1. Установите правильную последовательность комплекса мероприятий, проводимых на предприятии по определению сведений, являющихся коммерческой тайной (КТ):

а) вырабатывается первоначальный вариант Перечня сведений, составляющих КТ предприятия;

б) перечень утверждается руководителем предприятия и доводится до исполнителей в полном объеме или в части их касающейся;

в) анализируются поступившие предложения по формировании. Перечня сведений, составляющих КТ предприятия, и готовится окончательный вариант Перечня сведений.

г) создается комиссия из числа квалифицированных специалистов ведущих структурных подразделений, которая будет выполнять экспертные функции;

д) выделяется ответственный за работу по определению сведений, являющихся КТ, который совместно со службой безопасности (СБ) организует и осуществляет весь комплекс работ

2. Установите последовательность способов уменьшения риска (в порядке приоритетов):

а) Защитные устройства и персональное защитное оборудование

б) Обучение

в) Разработка безопасного в своей основе проекта

г) Информация по установке и применению

3. Установите этапы анализа защищенности:

1) Анализ полученных данных и уязвимостей.

2) Выработка рекомендаций.

3) Подготовка отчетных документов.

4) Инициирование и планирование Определение области и границ аудита.

5) Обследование, документирование и сбор информации.

4. Установите последовательность способов уменьшения риска (в порядке приоритетов):

а) Защитные устройства и персональное защитное оборудование

б) Обучение

в) Разработка безопасного в своей основе проекта

г) Информация по установке и применению

5. Установите последовательность порядка проведения аттестации объектов информатизации:

а) Подача заявки на рассмотрение и проведение аттестации;

б) Проведение предварительного специального обследования аттестуемого объекта информатизации;

в) Разработка программы и методики аттестационных испытаний;

г) Проведение специальных проверок на наличие возможно внедренных электронных устройств перехвата информации;

д) Проведение аттестационных испытаний объекта информатизации;

6. Расположите этапы развития информационных технологий в соответствии с проблемами, стоящими на пути информатизации общества.

1) Максимальное удовлетворение потребностей пользователя и создание соответствующего интерфейса работы в компьютерной среде.

2) Обработка больших объемов данных в условиях ограниченных возможностей аппаратных средств.

3) Отставание программного обеспечения от уровня развития аппаратных средств.

4) Выработка соглашений и установление стандартов, протоколов для компьютерной связи; организация доступа к стратегической информации; организация защиты и безопасности информации.

7. Установите последовательность процессов в системе менеджмента информационной безопасности (СМИБ) в соответствии с моделью PDCA

а) Разработка СМИБ

б) Внедрение и функционирование СМИБ

в) Проведение мониторинга и анализа СМИБ

г) Поддержка и улучшение СМИБ

8. Установите последовательность мер по защите персональных данных при их обработке, которые должен принимать оператор в соответствии с федеральным законом от 27 июля 2007 152-ФЗ.

а) Назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных.

б) Издание оператором, являющимся юридическим лицом, локальных актов по вопросам обработки персональных данных.

в) Применение правовых, организационных и технических мер по обеспечению безопасности персональных данных.

г) Осуществление внутреннего контроля или аудита соответствия обработки персональных данных требованиям 152-ФЗ и принятым в соответствии с ним нормативным правовым актам.

д) Оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения 152-ФЗ.

е) Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, локальными актами по вопросам обработки персональных данных, и обучение указанных работников.

9. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:

1) Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов

2) Реализация защитных мер по противодействию скрытых каналов

3) Организация контроля за противодействием скрытых каналов.

4) Выявление скрытых каналов и оценка их опасности для активов организации

10. Установите последовательность разработки модели угроз ИСПДн:

а) Описать ИСПДн

б) Определить пользователей ИСПДн

в) Определить тип ИСПДн

г) Определить исходный уровень защищенности ИСПДн
д) Определить вероятность реализации угроз в ИСПДн
е) Определить возможность реализации угроз в ИСПДн
ж) Оценить опасность угроз
з) Определить актуальность угроз в ИСПДн

11. Установите правильный порядок засекречивания информации, составляющей государственную тайну (ГТ):

а) правительство вносит предложение о Перечне должностных лиц органов государственной власти и управления, наделенных полномочиями по отнесению сведений к ГТ;

б) правительство разрабатывает Правила отнесения сведений, составляющих ГТ, к различным степеням секретности;

в) закон определяет категории сведений, отнесенных к ГТ;

г) руководители ведомств на основании соответствующих документов издают приказы, вводящие в действие и детализирующие в перечни засекречиваемых сведений;

д) межведомственная комиссия по защите государственной тайны разрабатывает Перечень сведений, отнесенных к ГТ;

е) руководители органов власти и управления, наделенные соответствующими полномочиями по засекречиванию информации, осуществляют политику государства в области защиты информации; ж) президент РФ утверждает Перечень сведений, отнесенных к ГТ и Перечень должностных лиц органов государственной власти и управления, наделенных полномочиями по отнесению сведений к государственной тайне.

12. Выберите последовательность приоритетных этапов защиты информации:

1) Защита информации от несанкционированного доступа;
2) Защита информации в системах связи;
3) Защита юридической значимости электронных документов;
4) Защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок;
5) Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;
6) Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации.

13. Выберите правильную последовательность этапов работы по обеспечению режима ИБ:

1) Выявление максимально полного множества потенциальных угроз, способов и каналов их осуществления;
2) Определение и выработка политики информационной безопасности;

3) Определение совокупности целей создания системы иб и сферы (границ) ее функционирования;

4) Выявление уязвимостей, проведение оценки рисков, формирование методик управление рисками;

5) Выберите правильную последовательность этапов работы по обеспечению режима ИБ:

14. Установите последовательность этапов работы по обеспечению информационной безопасности:

1) Определение требований к системе защиты информации;

2) Выбор контрмер, обеспечивающих режим иб, и средств защиты;

3) Разработка, внедрение и организация использования выбранных мер, способов и средств защиты;

4) Осуществление текущего контроля целостности информационных ресурсов и средств защиты и плановый аудит системы управления информационной безопасностью.

15. Выберите правильную последовательность этапов процесса управления рисками:

1) Идентификация активов и ценности ресурсов, нуждающихся в защите;

2) Анализ угроз и их последствий, определение слабостей в защите;

3) Классификация рисков, выбор методологии оценки рисков и проведение оценки;

4) Выбор, реализация и проверка защитных мер;

5) Оценка остаточного риска;

6) Выбор анализируемых объектов и степени детальности их рассмотрения;

16. Выберите правильную последовательность этапов обеспечения информационной безопасности:

1) Оценка стоимости;

2) Реализация политики;

3) Квалифицированная подготовка специалистов;

4) Аудит;

5) Разработка политики безопасности;

17. Выберите последовательность уровней безопасности информации:

1) Административный уровень

2) Процедурный уровень

3) Программно-технический уровень

4) Законодательный уровень

18. Установите правильную последовательность комплекса мероприятий, проводимых на предприятии по определению сведений, являющихся коммерческой тайной (КТ):

а) вырабатывается первоначальный вариант Перечня сведений, составляющих КТ предприятия;

б) перечень утверждается руководителем предприятия и доводится до исполнителей в полном объеме или в части их касающейся;

в) анализируются поступившие предложения по формировании. Перечня сведений, составляющих КТ предприятия, и готовится окончательный вариант перечня сведений.

г) создается комиссия из числа квалифицированных специалистов ведущих структурных подразделений, которая будет выполнять экспертные функции;

д) выделяется ответственный за работу по определению сведений, являющихся КТ, который совместно со службой безопасности (СБ) организует и осуществляет весь комплекс работ.

19. Выберите правильную последовательность этапов оценки угроз безопасности информации:

1) Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

2) Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;

3) Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

4) Оценка способов реализации (возникновения) угроз безопасности информации;

5) Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

6) Оценка сценариев реализации угроз безопасности информации в системах и сетях.

20. Выберите правильную последовательность этапов построения политики безопасности:

1) Выбор и установка средств защиты;

2) Организация обслуживания по вопросам информационной безопасности;

3) Создание системы периодического контроля информационной безопасности

4) Обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;

5) Подготовка персонала работе со средствами защиты;

Задание на установление соответствия

1. Установить соответствие типа организации его характеристике:

1) Аттестация	a) Проверка, выполняемая компетентным органом (лицом) с целью обеспечения независимой оценки степени соответствия программных продуктов или процессов установленным требованиям
2) Аудит	b) Объединение нескольких рисков в один риск, направленное на более глубокое понимание совокупного риска
3) Аккредитация	c) Официальное признание правомочий осуществлять какую-либо деятельность
	d) Подтверждение экспертизой и представлением объективных доказательств того, что конкретные требования к конкретным объектам полностью реализован

2. Установить соответствие типа организации его характеристике:

1) Производственный кооператив	a) Имущество является неделимым и не может быть распределено по вкладам (долям), в том числе между работниками предприятия
2) Государственное (муниципальное) унитарное предприятие	b) Основано на личном трудовом или ином участии и объединении его членов
3) Общество с ограниченной ответственностью	c) Участники не отвечают по обязательствам и несут риск убытков, связанных с деятельностью общества, в

	пределах стоимости внесенных ими вкладов
	d) Участники несут солидарную ответственность по его обязательствам своим имуществом в одинаковом для всех кратном размере стоимости их вкладов

3. Установить соответствие:

1) Межсетевой экран	a) Обеспечивает сохранность информации.
2) Программа шифрования	b) Фильтрует трафик между компьютером и сетью.
3) Антивирусная программа	c) Ищет и удаляет вредоносный код.
	d) Устанавливает соединения в локальной сети.

4. Установить соответствие:

1) Dlp-система (data leak prevention)	a) Отслеживает пересылку и распечатку файлов, внезапные всплески интернет-общения, посещение нехарактерных для работы сайтов и т. Д.
2) Тренинг	b) Сотрудники имеют полный доступ к информации на компьютерах работников, а в случае разглашения коммерческой тайны будут требовать возмещения убытков. Эти меры являются мощным сдерживающим психологическим фактором.
3) Трудовой договор.	c) Сотрудникам рассылают письма с вирусами, просят по телефону выдать конфиденциальные сведения и т. П. В результате теста выясняется, как персонал реагирует на такие действия, и разрабатываются меры защиты.
	d) Массовая рассылка нежелательной и несанкционированной электронной почты или других форм электронных сообщений

5. Установить соответствие:

1) Целостность	a) Неизменность информации, при выполнении некоторых операций над ней
2) Конфиденциальность	b) Возможность субъектов воспользоваться чужими правами доступа к информации.
3) Доступность	c) Требование не передавать информацию третьим лицам
	d) Возможность субъектов воспользоваться своими правами доступа к информации.

6. Установить соответствие:

1) Риск	a) Это вероятный ущерб, который зависит от защищенности системы.
2) Угроза доступности	b) Это стоимость потерь, которые понесет компания в случае реализации угрозы конфиденциальности, целостности или доступности по каждому виду ценной информации.
3) Ущерб	c) Это угроза нарушения работоспособности системы при доступе к информации.
	d) Это угроза изменения информации.

7. Установить соответствие:

1) Доступность	a) Подразумевает единство организации всех работ по защите информации и их управления.
2) Системность пространственная	b) Защищенность информации рассматривается как составная часть общего понятия качества информации.
3) Системность временная	c) Защищенность основанная на принципе непрерывности функционирования системы защиты
	d) Защищенность рассматривается как увязка вопросов защиты информации

8. Установить соответствие:

1) Основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования системы защиты включают:	a) Мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АСОД (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности средств вычислительной техники, носителей информации и т.п.).
2) Разовые мероприятия включают:	b) Распределение реквизитов разграничения доступа (пароли, ключи шифрования и т.д.).
3) Периодически проводимые мероприятия включают:	c) Общесистемные мероприятия по созданию научно-технических и методологических основ защиты АСОД.
	d) Мероприятия проводимые и повторяемые только при полном пересмотре принятых решений.

9. Установить соответствие:

1) Администраторы сервисов	a) Построение защиты в соответствии с общей политикой безопасности
2) Администраторы локальной сети	b) Выполнение правил и процедур политики безопасности
3) Руководитель подразделения	c) Доведение положений политики безопасности до пользователей и за контакты с ними
	d) Обеспечение непрерывного функционирования сети и реализация технических мер безопасности

10. Установить соответствие:

1) Правовой документ	a) Инструкция администратора безопасности
2) Организационно распорядительный документ	b) ГОСТ РФ
3) Нормативный документ	c) Кодекс РФ
	d) Акт ввода в эксплуатацию СЗИ

11. Установите соответствие между названием закона, номером и датой его принятия:

1) "О персональных данных"	a) 149-ФЗ от 27 июля 2006
2) "О лицензировании отдельных видов деятельности"	b) 152-ФЗ от 27 июля 2006
3) "Об информации, информационных технологиях и о защите информации"	c) 99-ФЗ от 04 мая 2011
	d) 5485-1 от 21 июля 1993

12. Установить соответствие нарушителей по уровням:

1) 1 уровень	a) Знает структуру, функции и механизмы действия средств защиты, их слабые и сильные стороны.
2) 2 уровень	b) Знает функциональные особенности, основные закономерности формирования в нестандартных массивах данных и потоков запросов к ним. Умеет пользоваться штатными средствами.
3) 3 уровень	c) Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и ее обслуживания.
	d) Обладает уровнем знаний в области программирования и вычислительных технологий, проектирования и эксплуатации.

13. Установить соответствие нарушителей по уровням возможностей (используемым методам и вопросам):

1) 1 уровень	a) Применяющие методы и действия активного воздействия (модификация и подключение дополнительных технических устройств).
2) 2 уровень	b) Применяющие только агентурные методы получения сведений

3) 3 уровень	c) Использующие только штатные средства и недостатки системы защиты, их сильные и слабые стороны.
	d) Применяющие пассивные средства (технические средства перехвата без модификации компонентов системы).

14. Установить соответствие оценки рисков в зависимости от факторов:

1) Уничтожение компьютерной информации	a) Это стирание ее в памяти ЭВМ, удаление с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие содержание.
2) Компрометация информации	b) это процесс создания копий всех файлов, находящихся на компьютере, и затем их удаление для освобождения места на жестком диске.
3) Блокирование компьютерной информации	c) Как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений.
	d) Это искусственное затруднение доступа пользователей к компьютерной информации.

15. Установить соответствие:

1) Правовая защита	a) Это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, которая исключает или ослабляет нанесение каких-либо убытков предприятию;
2) Организационная защита	b) Это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, которые обеспечивают защиту информации на правовой основе;

3) Инженерно-техническая защита	c) Это использование разнообразных технических средств, которые препятствуют нанесению убытков предприятию.
	d) Это использование разнообразных технических средств, для повышения безопасности персонала.

16. Установить соответствие:

1) Модификация компьютерной информации	a) Изготовление и устойчивое запечатление второго и последующих экземпляров базы данных, файлов в любой материальной форме, а также их запись на машинный носитель, в память ЭВМ.
2) Копирование компьютерной информации	b) Это внесение в нее любых изменений, кроме связанных с адаптацией программы для ЭВМ или базы данных.
3) Каналы передачи данных	c) Это изменение может включать в себя адаптацию программного обеспечения для ЭВМ или базы данных.
	d) Воздействие на пакеты данных может рассматриваться как атака на объекты сети, воздействие на передачу - специфический род атак, характерный для сети.

17. Установить соответствие:

1) Физические злоупотребления	a) Включают в себя: различные способы изменения системы математического обеспечения («логическая бомба»– введение в программу команды компьютеру проделать в определенный момент какое-либо несанкционированное действие; «троянский конь»– включение в обычную программу своего задания).
2) Операционные злоупотребления	b) Представляющие собой: мошенничество (выдача себя за другое лицо или использование прав другого лица); несанкционированное использование

	различных устройств.
3) Программные злоупотребления	c) Включают в себя разрушение оборудования; уничтожение данных или программ; ввод ложных данных, кражу информации, записанной на различных носителях.
	d) Незаконное использование привилегий доступа к операционной системе компьютера или сети

18. Установить соответствие:

1) «Маскарад»	a) Попытки злоумышленников угадать или получить доступ к паролю, используя автоматические программы для перебора возможных комбинаций символов.
2) «Неспешный выбор»	b) При данном способе преступником осуществляется конкретизация уязвимых мест в защите: определяются участки, имеющие ошибку или неудачную логику программного строения.
3) «Брешь»	c) Отличительной особенностью данного способа совершения преступления является то, что преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите.
	d) Данный способ состоит в том, что преступник проникает в компьютерную систему, выдавая себя за законного пользователя.

19. Установить соответствие степеней происхождения угрозы информационной безопасности:

1) Естественная	a) Данные угрозы, в свою очередь, делятся на 2 подкатегории: преднамеренная подкатегория — это действия хакеров, конкурентов, недобросовестных сотрудников и т. д., непреднамеренная — действия происходят из-за людей по их неосторожности.

2) Искусственная	b) Это те угрозы, которые не зависят от деятельности человека: землетрясения, ураганы, смерчи, дожди, молнии и т. д.
3) Внутренняя	c) Все угрозы, которые происходят вне системы.
	d) Угроза исходит изнутри самой системы.

20. Установить соответствие:

1) Политика использования электронной почты	a) Может определять границы использования технологий, позволяющих подключить компьютеры и информационные системы предприятия к информационным системам и коммуникационным каналам за его пределами.
2) Политика использования коммуникационных средств	b) Может включать в себя как общие ограничения на ее использование определенными категориями сотрудников, так и требования к управлению доступом и сохранению конфиденциальности сообщений, а также к администрированию почтовой системы и хранению электронных сообщений.
3) Политика использования мобильных аппаратных средств	c) Может относиться к различным устройствам, таким как мобильные ПК, КПК (PDA), переносные устройства хранения информации (дискеты, USB-flash, карты памяти, подключаемые жесткие диски и т.п.)
	d) Набор правил и рекомендаций, которые определяют, каким образом пароли должны создаваться, использоваться и управляться в организации или системе.

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по

промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1. Подготовить перечень защищаемых персональных данных согласно Приказа № 21 ФСТЭК в администрации г. Курск.
2. Подготовить перечень защищаемой информации на ООО «Курская недвижимость».
3. Разработать концепцию информационной безопасности для ООО «Курская недвижимость».
4. Разработать политику информационной безопасности для ЮЗГУ.
5. Подготовить частную модель угроз персональным данным на ООО «Курская недвижимость» исходя из «Базовой модели угроз персональным данным ФСТЭК».
6. Оценить уровни защищенности конфиденциальной информации ЮЗГУ.

7. Подготовить модель внутреннего нарушителя «Аппарата губернатора Курской Области».

8. Подготовить перечень защищаемой информации на ООО «Кварта-Л».

9. Разработать концепцию информационной безопасности для ООО «Кварта-Л».

10. Разработать политику информационной безопасности для КГУ.

11. Подготовить частную модель угроз персональным данным на ООО «Кварта-Л» исходя из «Базовой модели угроз персональным данным ФСТЭК».

12. Оценить уровни защищенности конфиденциальной информации КГУ.

13. Подготовить перечень защищаемой информации на ООО «КурсКлимат».

14. Разработать концепцию информационной безопасности для ООО «КурсКлимат».

15. Разработать политику информационной безопасности для КГМУ.

16. Подготовить частную модель угроз персональным данным на ООО «КурсКлимат» исходя из «Базовой модели угроз персональным данным ФСТЭК».

17. Оценить уровни защищенности конфиденциальной информации КГМУ.

18. Подготовить перечень защищаемой информации на ООО «Курс».

19. Разработать концепцию информационной безопасности для ООО «Курс».

20. Разработать политику информационной безопасности для РФЭИ.

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл

по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или)

значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.