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

Организация аудита 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. Структура службы информационной безопасности.

1. Приведите примерную структуру типовой службы защиты информации
2. Основные направления службы защиты информации
3. Место службы защиты информации в структуре предприятия
4. Подходы к созданию службы безопасности
5. Информационные угрозы, их виды и причины возникновения.
6. Информационные угрозы для государства.
7. Информационные угрозы для компании.
8. Информационные угрозы для личности (физического лица).
9. Действия и события, нарушающие информационную безопасность.
10. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.

Тема 2. Функции основных групп службы безопасности.

1. Функции группы режима
2. Функции группы охраны и сопровождения
3. Функции технической группы
4. Функции детективной группы
5. Деление сотрудников службы информационной безопасности по функциональным обязанностям
6. Функциональные обязанности сотрудников службы защиты информации
7. Структура типовой должностной инструкции сотрудника службы защиты информации.
8. Функции сотрудников службы информационной безопасности
9. Способы воздействия информационных угроз на объекты.
10. Внешние и внутренние субъекты информационных угроз.

Тема 3. Цели и задачи службы информационной безопасности.

1. Цели обеспечения безопасности предприятия
2. Задачи и функции службы
3. Функции различных подразделений службы информационной безопасности
4. Прогресс информационных технологий и необходимость обеспечения информационной
5. безопасности.
6. Основные понятия информационной безопасности. Структура понятия информационная безопасность.

7. Система защиты информации и ее структура.
8. Экономическая информация как товар и объект безопасности.
9. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
10. Персональные данные и их защита.

Тема 4. Организационные основы и принципы деятельности службы информационной безопасности.

1. Организация деятельности службы информационной безопасности
2. Правовое обеспечение службы.
3. Принципы организации службы.
4. В чём заключаются гарантии безопасности объектов защиты?
5. Назовите виды гарантий безопасности объектов защиты
6. Состав пакета документов для службы информационной безопасности
7. Назовите обязательные и необязательные документы, регламентирующие деятельность службы информационной безопасности
8. Понятие и система правовых основ информационной безопасности.
9. Международное информационное законодательство.
10. Понятие информационной безопасности РФ. Понятие национальных интересов РФ в информационной сфере и их обеспечение.

Тема 5. Лицензирование видов деятельности службы безопасности.

1. Виды деятельности службы информационной безопасности, подлежащие лицензированию
2. Органы государственной власти, отвечающие за лицензирование
3. Требования к лицензиату
4. Назовите причины отказа в получении лицензии для службы информационной безопасности.
5. Структура системы государственного лицензирования деятельности в области защиты информации.
6. Порядок лицензирования деятельности предприятий. Дайте определение лицензионного договора.
7. Основные нормативные акты в области лицензирования ЗИ.
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. Управление службой защиты информации.

1. Назовите варианты реализации организационной структуры службы информационной безопасности и условия выбора того или иного варианта.
2. Назовите вопросы, решение которых предворяет создание службы информационной безопасности
3. Назовите и охарактеризуйте методы управления службой информационной безопасности
4. Назовите и охарактеризуйте основные функции процессов управления
5. Назовите набор признаков, свидетельствующих о возможных условиях для реализации преступного замысла в отношении охраняемого объекта
6. Назовите элементы процесса установления постоянных и временных взаимоотношений между всеми подразделениями службы безопасности, определение порядка и условий ее функционирования
7. Назовите потребности, которые обладают конкретными мотивационно-трудовыми значениями.
8. Назовете принципы управления службой защиты информации
9. Назовете принципы управления службой защиты информации в критических ситуациях.
10. Доктрина информационной безопасности России

Тема 7. Организация информационно-аналитической работы.

1. Цели и задачи информационно-аналитической работы
2. Задачи, возникающие при выполнении информационно-аналитической работы
3. Направления и методы аналитической работы
4. Что включает в себя такое направление, как обнаружение каналов несанкционированного доступа к информации?
5. Что предусматривает аналитическая работа с источником угрозы конфиденциальной информации?
6. Назовите этапы выполнения информационно-аналитических исследований производственных ситуаций
7. Методы выполнения аналитических исследований
8. Государственное регулирование информационной безопасности.
9. Деятельность международных организаций в сфере информационной безопасности.
10. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации

Тема 8. Организация работы с персоналом предприятия.

1. Перечислите группы лиц, от которых могут исходить угрозы информационной безопасности
2. Перечислите этапы процедуры отбора персонала

3. Как следует выполнять сравнительный анализе нескольких кандидатур?

4. Какие вопросы следует затронуть на итоговом собеседовании?

5. Как осуществляется проверка на благонадежность?

6. Особенности проверки руководящих кадров.

7. Особенности увольнения сотрудников, владеющих конфиденциальной информацией.

8. Какую информацию целесообразно собрать об увольняемом сотруднике?

9. Уголовно-правовой контроль над компьютерной преступностью в России. Федеральные законы по ИБ в РФ.

10. Политика безопасности и ее принципы.

Критерии оценки:

7-12 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.

1-6 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 (или оценка «неудовлетворительно») 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 ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Контрольные вопросы к практической работе №1 «Определение класса государственной информационной системы (ГИС)»:

1. Какие исходные данные необходимы для проведения классификации?

2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?

3. Какова специфика проведения классификации?

4. Каковы суть и содержание нормативной основы организации ЗСИ?

5. Понятие и виды угроз информационной безопасности РФ.
6. Классификация угроз информационной безопасности РФ.
7. Понятие и классификация общих методы обеспечения информационной безопасности РФ.
8. Основные направления обеспечения информационной безопасности в области внешней и внутренней политики РФ.
9. Особенности и основные направления международного сотрудничества в области обеспечения информационной безопасности РФ.
10. Основные положения государственной политики обеспечения информационной безопасности РФ.

Контрольные вопросы к практической работе №2 «Разработка структуры государственных и международных стандартов в Российской Федерации в области информационной безопасности и защиты информации»:

1. Дать полное определение ГОСТ
2. Дать полное определение ИСО
3. Как проводится сертификация средств защиты информации?
4. Что показывают характеристики данного средства защиты?
5. Какая основная информация содержится в сертификате?
6. Основные положения государственной политики обеспечения информационной безопасности РФ.
7. Принципы государственной политики обеспечения информационной безопасности РФ.
8. Основные функции системы обеспечения информационной безопасности РФ.
9. Основные элементы организационной основы системы обеспечения информационной безопасности РФ
10. Государственная тайна в системе информационной безопасности РФ. Общая характеристика правовых основ защиты государственной тайны.

Контрольные вопросы к практической работе №3 «Техническое задание на создание информационной системы и системы защиты информации»

1. Где необходима электронная подпись документов?
2. Какие могут быть альтернативные наборы вариантов решения?
3. Как определялась схема рассадки людей?
4. Какой перечень документов по которым готовился?
5. Какой регулятор контролирует данную область информационной безопасности?
6. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.
7. Доктрина информационной безопасности России.
8. Уголовно-правовой контроль над компьютерной преступностью в России.
9. Федеральные законы по ИБ в РФ.

10. Политика безопасности и ее принципы.

Контрольные вопросы к практической работе №4 «Основные методы управления информационной безопасностью в ГИС»

1. Что такое плановая документация?
2. Что такое информационно-справочная и справочно-аналитическая документация?
3. Что такое отчетная документация?
4. Что такое документация по обеспечению кадрами?
5. Что такое финансовая документация?
6. Что такое материально-техническое снабжение?
7. Что такое договорная документация?
8. Государственная тайна в системе информационной безопасности РФ. Общая характеристика правовых основ защиты государственной тайны.
9. Полномочия органов государственной власти и должностных лиц в области отнесения сведений к государственной тайне и их защиты.
10. Перечень сведений, составляющих государственную тайну.
11. Защита государственной тайны. Органы защиты государственной тайны.

Критерии оценки:

3-4 балла (или оценка «отлично») 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.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») 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 (или оценка «неудовлетворительно») 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 КЕЙС-ЗАДАЧИ

1. Вы являетесь ответственным за информационную безопасность в небольшой компании, занимающейся продажей электроники. Компания имеет офисное помещение, где работают 15 сотрудников, и интернет-магазин. Компания хранит конфиденциальную информацию клиентов, включая персональные данные и данные о покупках. Вам поручили организацию аудита информационной безопасности компании.

Какие шаги вы предпримете для организации аудита информационной безопасности в компании? Какие аспекты безопасности вы будете оценивать? Какие рекомендации вы дадите компании на основе результатов аудита?

Для решения задачи, необходимо провести анализ угроз и оценку рисков, выработать систему мер по защите информации, разработать процедуры управления безопасностью, определить необходимость проведения аудита и выбрать квалифицированного аудитора, осуществляющего оценку соответствия требованиям нормативно-правовых документов, а также провести внутренний аудит безопасности информации в компании.

В ходе аудита нужно оценить уровень доступности, конфиденциальности и целостности информации, проверить соответствие действующих правил информационной безопасности, наличие угроз и возможности их реализации, наличие защитных мероприятий и их эффективность.

На основании результатов аудита, необходимо дать рекомендации компании по обеспечению безопасности информации, улучшению политики и процедур управления безопасностью, обеспечению соответствия требованиям законодательства, а также проводить периодические аудиты для поддержания высокого уровня безопасности информации.

2. Вы являетесь руководителем отдела информационной безопасности в крупной компании. Ваша компания занимается производством и продажей товаров, а также оказывает услуги. Компания имеет собственные производственные и складские помещения, офисы, сеть интернет-магазинов, а также ряд сайтов с различным функционалом.

Последнее время вы заметили увеличение случаев кибератак на компанию, а также утечек конфиденциальной информации. Вы считаете, что необходимо провести аудит информационной безопасности компании для выявления уязвимостей и усиления мер безопасности.

Кейс задача:

1) Составьте план проведения аудита информационной безопасности компании, учитывая ее особенности.

2) Опишите методы и инструменты, которые вы будете использовать во время аудита.

3) Какие рекомендации вы можете дать руководству компании на основании результатов аудита?

4) Какие меры безопасности можно реализовать в компании, чтобы предотвратить подобные инциденты в будущем?

3. Вы работаете инженером по информационной безопасности в крупной IT-компании. Ваша задача - провести аудит информационной безопасности сети офиса компании, состоящей из 200 компьютеров. В рамках аудита необходимо проверить уровень защиты информации, обеспечить контроль доступа и предотвратить утечку данных.

Компьютеры в офисе работают на различных операционных системах, включая Windows, MacOS и Linux. В сети компании используются различные программы и сервисы, включая облачное хранилище, мессенджеры и электронную почту.

В рамках аудита вам необходимо:

1) Проверить наличие и корректность установки антивирусного ПО на всех компьютерах и серверах сети.

2) Проверить уровень доступа к информации на серверах и рабочих станциях, а также наличие резервного копирования.

3) Проверить наличие защищенного соединения (SSL) для доступа к облачному хранилищу и проверить, какие данные хранятся в облаке.

4) Проверить, какие мессенджеры используются в компании, и определить, какую информацию можно передавать по ним.

5) Проверить наличие политики паролей в компании и настроить контроль доступа на основе паролей для сети.

6) Проверить наличие мер защиты от вредоносного ПО на компьютерах и серверах, а также наличие защиты от несанкционированного доступа к данным.

4. Крупная компания, занимающаяся разработкой программного обеспечения, решила провести аудит информационной безопасности своей IT-инфраструктуры. На предприятии работает более 1000 сотрудников, у каждого из которых есть доступ к корпоративной сети и часто используемым программам. Кроме того, компания хранит большое количество конфиденциальной информации о своих клиентах и партнерах.

Ваша задача как аудитора - провести аудит информационной безопасности и выявить потенциальные уязвимости и угрозы для компании. Какие шаги вы предпримете для достижения этой цели? Какие инструменты и методы вы используете? Какие рекомендации вы дадите компании для улучшения информационной безопасности?

5. Компания "Альфа" является крупным производителем товаров и услуг в своей отрасли. Она хранит и обрабатывает большое количество

конфиденциальной информации о своих клиентах, поэтому безопасность данных является ее приоритетной задачей.

Для обеспечения безопасности данных компания применяет ряд технологий и политик, включая защиту периметра, системы мониторинга, контроля доступа, шифрования и политики паролей. Однако, компания осознает, что безопасность должна регулярно аудитироваться, чтобы обнаруживать и исправлять слабые места в системе.

Компания наняла вас как эксперта по безопасности, чтобы провести аудит ее системы информационной безопасности. Ваша задача состоит в том, чтобы выполнить следующие шаги:

1) Оценить текущее состояние системы безопасности компании, провести анализ рисков и выявить слабые места.

2) Составить рекомендации по улучшению системы безопасности компании, сделать акцент на наиболее критических уязвимостях.

3) Разработать план действий по устранению выявленных проблем и слабых мест в системе безопасности, определить ответственных за каждое действие.

4) Представить отчет об аудите компании и рекомендации по улучшению системы безопасности ее информации.

В качестве эксперта по безопасности, вам нужно работать в тесном сотрудничестве с командой ИТ-специалистов компании, а также проводить интервью с представителями различных отделов, чтобы понять, как используется информация и какие требования к безопасности нужно учитывать в каждом конкретном случае.

6. Вы назначены ответственным за информационную безопасность в небольшой компании, которая занимается продажей товаров в Интернете. Компания находится в стадии быстрого развития, и вы обеспокоены возможными уязвимостями в системах безопасности компании.

Компания использует несколько серверов для обработки заказов, хранения данных клиентов и выполнения других задач. В компании также есть несколько рабочих станций для работы с данными и электронной почтой, а также Wi-Fi сеть для доступа к Интернету.

Ваша задача - провести аудит информационной безопасности компании, чтобы идентифицировать уязвимости в системах безопасности, а также разработать план мероприятий по их устранению.

1) Какие этапы аудита информационной безопасности вы проведете?

2) Какие инструменты и технологии вы будете использовать для проведения аудита?

3) Как вы оцените уровень уязвимостей в системах безопасности компании?

4) Какие меры безопасности вы предложите для устранения уязвимостей?

5) Как вы оцените эффективность мероприятий, предпринятых после аудита?

Критерии оценки:

7-12 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.

1-6 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 (или оценка «неудовлетворительно») 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 ПРОИЗВОДСТВЕННЫЕ ЗАДАЧИ

1. Компания X обнаружила, что ее ИС была скомпрометирована. Какие конкретные действия вы бы предприняли, чтобы расследовать инцидент и вернуть ИС в рабочее состояние? Какие меры безопасности вы предпринимаете, чтобы предотвратить подобные инциденты в будущем?
2. Как бы вы провели аудит безопасности ИС в компании Y? Какие инструменты и методы вы бы использовали для обнаружения потенциальных уязвимостей в ИС? Как бы вы определили критические уязвимости и разработали план мероприятий по устранению этих уязвимостей?
3. Компания Z планирует перевести свою ИС на облачную платформу. Какие меры безопасности вы бы рекомендовали принять компании Z перед переносом данных в облако? Как бы вы оценили безопасность выбранного облачного провайдера и как бы вы защитили данные, хранящиеся в облаке, от потенциальных угроз?
4. Ваша компания получила угрозу распространения вредоносного ПО. Как бы вы организовали обучение сотрудников по безопасности ИС и какие меры безопасности вы бы рекомендовали принять, чтобы

предотвратить распространение вредоносного ПО? Как бы вы оценили эффективность ваших мер безопасности?

5. Как бы вы разработали и реализовали план управления рисками безопасности ИС в компании? Как бы вы определили потенциальные угрозы и оценили их влияние на бизнес компании? Как бы вы определили наиболее критические области ИС и как бы вы защитили их от угроз?

6. Компания А решила провести реструктуризацию своих информационных систем для повышения безопасности данных. Какие компетенции необходимо иметь у специалистов, занимающихся этим проектом?

7. Сотрудник компании Б обнаружил утечку конфиденциальной информации. Какие компетенции он должен проявить, чтобы правильно и своевременно сообщить об этом инциденте и помочь минимизировать его последствия?

8. Компания В решила перевести свои информационные системы на облачные платформы. Какие компетенции должны иметь сотрудники, которые будут заниматься реализацией этого проекта, чтобы обеспечить максимальную безопасность данных?

9. Специалист по информационной безопасности в компании Г заметил некоторые аномальные действия в системе и подозревает, что произошла атака хакеров. Какие компетенции ему необходимо проявить, чтобы быстро и эффективно реагировать на инцидент и предотвратить утечку конфиденциальной информации?

10. Компания Д решила создать отдел по информационной безопасности. Какие компетенции должны быть у новых сотрудников, чтобы эффективно защищать ИС компании и принимать меры по предотвращению угроз?

11. Ваша компания переживает серьезный инцидент безопасности, который привел к утечке конфиденциальной информации. Вам поручено возглавить расследование и принять меры для предотвращения подобных инцидентов в будущем. Какие конкретные действия вы будете предпринимать, чтобы выполнить это задание и продемонстрировать свою компетентность в области безопасности информационных систем?

12. Ваша компания готовится к запуску нового веб-приложения. Ваша задача - убедиться, что приложение безопасно и не подвержено риску взлома или кражи данных. Какие шаги вы будете предпринимать, чтобы проверить безопасность приложения и дать рекомендации по усовершенствованию его безопасности?

13. Ваша компания рассматривает возможность перехода на облачные технологии. Ваша задача - провести анализ рисков и предложить конкретные меры для обеспечения безопасности данных и приложений в облачной среде. Какие действия вы будете предпринимать, чтобы выполнить это задание и продемонстрировать свою компетентность в области облачных технологий и безопасности информационных систем?

14. Ваша компания недавно была атакована злоумышленниками, которые украли данные и вымогали выкуп. Ваша задача - разработать стратегию обеспечения безопасности информационных систем компании, чтобы избежать подобных инцидентов в будущем. Какие действия вы будете предпринимать, чтобы выполнить это задание и продемонстрировать свою компетентность в области безопасности информационных систем и управления рисками?

15. Вы работаете в отделе информационной безопасности крупной компании. Ваша задача - разработать и реализовать программу обучения по безопасности информационных систем для всех сотрудников компании. Какие методы обучения и материалы вы будете использовать, чтобы обеспечить эффективность программы обучения и продемонстрировать свою компетентность в области обучения и безопасности информационных систем?

Критерии оценки:

5-8 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 (или оценка «неудовлетворительно») 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. Что представляет с собой термин «Информационные ресурсы»?
   A. Отдельные документы и массивы документов.
   B. Слитые документы и массивы документов.
   C. Архивы и информационные системы.
   D. Программные средства.
   E. Вычислительные данные и библиотека.
2. К какому классу относятся компьютерно-машинные системы?
   A. Машинные системы.
   B. Компьютерные и вычислительные машинные системы.
   C. Человеко-машинные системы.
   D. Электронные системы.
   E. Вычислительные техники систем.
3. Взаимосвязанная совокупность средств, методов и персонала которые используются для хранения, обработки передачи и получения информации в интересах достижения поставленной цели.
   A. Объект защиты.
   B. Системы защиты.
   C. Информационная безопасность.
   D. Информационные системы.
   E. Программные защиты системы.
4. Что представляет с собой понимание под системой защиты информации в ИС?
   A. состояние всех компонент информационной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне.
   B. единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности.
   C. Обслуживающий персонал и пользователи могут быть как объектом, так и источником несанкционированного воздействия на информацию.
   D. Цели политики информационной безопасности и основные направления решения задач защиты информации в ИС.
   E. Целью защиты информации становится уменьшение размеров ущерба до допустимых значений.
5. Основными задачами и составляющими ИБ является?
   A. Доступность, субъективность, конфиденциальность

B. Целостность, доступность, динамичность
C. Конфиденциальность, целостность, субъективность
D. Динамичность, субъективность, доступность
E. Доступность, конфиденциальность, целостность

6. Понятие «целостности» в ИБ?
   A. Это возможность за приемлемое время получить требуемую информационную услугу.
   B. Это защита от несанкционированного доступа к информации.
   C. Это ее защищенность от разрушения и несанкционированного изменения.
   D. Это возможность за приемлемое время получить требуемую информационную услугу и защищенность от разрушения.
   E. Это обеспечение информационных ресурсов и поддерживающей инфраструктуры.
7. Что включают в себя системы управления ИБ?
   A. Политика, планирование, должностные обязанности, процедуры, процессы и ресурсы.
   B. Организационную структуру, политики, планирование, должностные обязанности, практики,
   C. Организационную структуру, политики, планирование, должностные обязанности, практики.
   D. Организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.
   E. Организационную структуру, политики, должностные обязанности, практики, процессы и ресурсы.
8. Как называется действие, которое потенциально может привести к нарушению информационной безопасности.
   A. Уязвимость
   B. Угроза
   C. Критичность
   D. Окно опасности
   E. Выведывание
9. Какое определение правильно с термином «уязвимость»?
   A. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется,
   B. Действие, которое потенциально может привести к нарушению информационной безопасности
   C. Перечень и характеристики основных (актуальных) угроз безопасности
   D. Слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы

E. Степень возможности реализации угрозы через данную уязвимость в тех или иных условиях

10. Документ, определяющий перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей при их обработке в ИС, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищенности ИС
    A. Модель угроз
    B. Модель уязвимости
    C. Модель структуры
    D. Модель потерь
    E. Модель убыток
11. Угрозы можно классифицировать по нескольким критериям.
    A. По аспектам, компонентам, эксплуатации
    B. По аспектам, происхождению и способу осуществления, концептуальной ошибке
    C. По аспектам, компонентам, происхождению и способу осуществления
    D. По происхождению и способу осуществления, эксплуатации, концептуальной ошибке.
    E. По компонентам, аспектам, концептуальной ошибке
12. Возможность за приемлемое время получить требуемую информационную услугу.
    A. Целостность
    B. Объективность
    C. Доступность
    D. Конфиденциальность
    E. Безопасность
13. К какой угрозе относятся нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений
    A. Угроза динамической конфиденциальности
    B. Угроза динамической тайны
    C. Угроза динамической доступности
    D. Угроза динамической безопасности
    E. Угроза динамической целостности
14. Конфиденциальную информацию можно разделить на:
    A. Предметная и документированная
    B. Предметная и служебная
    C. Служебная и записная
    D. Документированная и защитная
    E. Служебная и защитная
15. На какие механизмы действия делятся вредоносные программы?
    A. Логические бомбы, Арифметические черви, Компьютерные вирусы, Нано-вирусы

B. Логические бомбы, Троянские кони, Черви, Компьютерные вирусы
C. Логические бомбы, Нано-вирусы, Троянские кони, Паразитные черви
D. Нано вирусы, Троянские кони, Компьютерные вирусы, Паразитные черви
E. Арифметические черви, Компьютерные вирусы, Нано вирусы, логические бомбы

16. Какой из этих вредителей постоянно находятся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условий?
    A. Логическая бомба
    B. Червь
    C. Троянский конь
    D. Компьютерный вирус
    E. Нано вирус
17. Найдите определения вредителя под названием «червь»
    A. Полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.
    B. Небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС
    C. Программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условий.
    D. Программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.
    E. Программы или их части, постоянно находящиеся в ЭВМ, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии.
18. Стандартизация в области ИБ необходимо по ….. причинам
    A. 4
    B. 5
    C. 2
    D. 7
    E. 3
19. Какие стандарты причины необходимы в ИБ?

A. Единых характеристик, единых требовании
B. Единых требовании, единых конфиденциальности, единых подходов, единых стандартов
C. Единых требовании, единых подходов, единых качественных показателей для оценки безопасности
D. Единых характеристик, единых требовании, единых качественных показателей для оценки безопасности
E. Единых подходов, единых качественных показателей для оценки безопасности

20. Зачем нужны стандарты экспертам по ИБ?
A. Уровня защиты
B. Уровня оценки ценных документов
C. Уровня информации
D. Уровня безопасности
E. Уровня ответственности

21. Министерством обороны США в 1983 году была разработана книга:
A. Оранжевая книга
B. Желтая книга
C. Белая книга
D. Черная книга
E. Зеленая книга

22. Сколько групп имеет данная книга по стандартизации?
A. 3
B. 6
C. 1
D. 5
E. 4

23.Что с собой представляет термин «Программно-техническая среда»?
A. меры физической защиты, персонал и его специфика
B. назначение оценочного объекта(ОО), предполагаемые области его применения.
C. положения политик безопасности, затрагивающих ОО и учитывающих его особенности;
D. законы и нормативны акты, затрагивающие ОО
E. Меры физической защиты и положения политик безопасности

24. При подготовке к оценке формализуются следующие аспекты среды оценочного объекта(ОО):
A. Предположения безопасности, угрозы безопасности, политика конфиденциальности
B. Предположения безопасности, требования доверия, политика безопасности
C. Функциональные требования безопасности, угрозы безопасности, политика безопасности

D. Предположения безопасности, угрозы безопасности, политика безопасности
E. Предположения безопасности, Функциональные требования безопасности, требования доверия

25. Какие два документа могут быть разработаны при формулировании к требованиям Оценочного объекта(ОО)?
A. Профиль защиты, требования доверия
B. Задание по безопасности, Предположение безопасности
C. Профиль защиты, Задание по безопасности
D. Требования доверия, предположение безопасности
E. Задание по безопасности, требования доверия

26. Британский Институт Стандартов при поддержке группы коммерческих организаций приступил к разработке стандарта управления информационной безопасностью. Как называется этот стандарт
A. BA 7799
B. BB 7788
C. BS 7799
D. BB 7799
E. BS 7788

27. Политика безопасности, организационная защита, классификация ресурсов и контроль, безопасность персонала, управление доступом к системе. К чему относятся перечисленные прилагательные?
A. К системе стандарта
B. К Политике безопасности
C. К подразделениям стандарта
D. К основам стандарта
E. К структуре стандарта

28. В «ISO 27001» для описания СУИБ процессная модель предусматривает непрерывный цикл мероприятий
A. Определение, реализация, проверка, действие
B. Планирование, реализация, проверка, действие
C. Планирование, реализация, изготовление, действие
D. Планирование, реализация, проверка.
E. Планирование, создание проверка, действие

29. В соответствии с процессной моделью, стандарт определяет … этапа создания СУИБ
A. 4
B. 3
C. 5
D. 2
E. 8

30. Какому этапу относится «проведение мониторинга и анализа системы управления информационной безопасности»?
A. К шестому
B. Ко второму

C. К четвертому
D. К третьему
E. К первому

31. Для создания СУИБ на предприятии и подготовке к ее сертификации на соответствие требованиям стандарта делится на 2 основных этапа:
    A. Разработку системы управления и внедрение системы управление
    B. Разработку системы управления и внедрение выбранных мер обработки рисков
    C. Разработку системы и оценка информационных рисков
    D. Разработку системы и моделирование программ
    E. Разработку системы и контроль выполнения рисков
32. Как определяют оценку критичности активов?
    A. Оценка в ущербах единиц и уровня
    B. Оценка в товарах единиц и уровня
    C. Оценка в денежных единиц и уровня
    D. Оценка в металлах единиц и уровня
    E. Оценка в активах единиц и уровня
33. Какие уровни шкалы достаточны для базовой оценки рисков?
    A. Низкий, высокий предельно высокий
    B. Низкий , средний, высокий
    C. Ниже среднего, средний, высокий
    D. Низкий и высокий
    E. Шкала от 1 до 3
34. Оценка информационных рисков заключается в расчете рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей. Укажите формулу оценки рисков:
    A. R=D + P(C)
    B. R=D - P(V)
    C. R=D / P(A)
    D. R=D * P(E)
    E. R=D * P(V)
35. Результаты оценки рисков как правило, представляются в «…»
    A. В этапах об оценке информационных рисков компаний
    B. В обработке об оценке информационных рисков компаний
    C. В уровнях об оценке информационных рисков компаний
    D. В отчете об оценке информационных рисков компаний
    E. В расчетах об оценке информационных рисков компаний
36. Какой буквой отмечено «критичность актива(ущерб)» в формуле оценки рисков?
    A. R
    B. A
    C. D
    D. P(A)

E. P(V)

37. Что означает данный термин «уклонение от рисков»
    A. Перенесение ответственности за риск на третьи лица
    B. Полное устранение источника риска
    C. Выбор и внедрение мер по снижению риска
    D. Определение уровня риска
    E. Уклонение от риска по целесообразным мерам
38. Перенесение ответственности за риск на третьи лица, без устранение источника риска:
    A. Передача риска
    B. Снижение риска
    C. Принятие риска
    D. Уклонение от риска
    E. Передача и снижение риска
39. Какие основные документы являются по управлению ИБ?
    A. Доктрина и политика ИБ
    B. Законы и Политика управления ИБ
    C. Статья и законы ИБ
    D. Политика управления ИБ
    E. Политика ИБ и Политика управления ИБ
40. Как по другому называется модель Шухарта-Деминга?
    A. PDCA
    B. PPCA
    C. PDDA
    D. PCCA
    E. PPAA
41. Сколько этапов модели Шухарта-Деминга?
    A. 3
    B. 5
    C. 8
    D. 9
    E. 4
42. Укажите критичность реализации угрозы
    A. Tmax
    B. P(V)
    C. Dc
    D. ER
    E. Th
43. Укажите правильный алгоритм уровня угрозы по уязвимости
    A. $Th = \frac{ER}{100} \times \frac{CTh}{100}$
    B. $Th = \frac{ER}{100} \times \frac{T\max}{100}$
    C. $P(\mathrm{V}) = \frac{ER}{100} \times \frac{T\max}{100}$

D. $Th = \frac{P(\mathrm{V})}{100} \times \frac{ER}{100}$

E. $Th_{c,1,a} = \frac{ER_{c,1,a}}{100} \times \frac{P(\mathrm{V})_{c,1,a}}{100}$

44. Как рассчитывается риск по ресурсу R, для режима с одной базовой угрозой ?

A. $R = CThR \times D$

B. $R = CThR - D$

C. $R = CThR - \frac{D}{100}$

D. $R = CThR \times \frac{D}{100}$

E. $R = CThR \div D$

45. Как рассчитывается риск по информационной системе CR для режима с одной базовой угрозой, для работы в деньгах?

A. $CR = (0 \times \prod_{i=1}^{n} (0 \div \frac{R_i}{100})) - 100 \qquad V(\mathrm{P}) = \sum_{i=1}^{n} R_i$

B. $CR = \sum_{i=1}^{n} R_i$

C. $CR = \sum_{i=1}^{n}$

D. $CR = \sum_{i=1}^{m+1} R_i$

E. $V(\mathrm{P}) = \sum_{i=1}^{m+1} R_i$

46. Как рассчитывается риск по информационной системе CR для режима с одной базовой угрозой, для работы в уровнях?

A. $CR = (1 - \prod_{i=1}^{n} (1 + \frac{R_i}{100})) \div 100$

B. $CR = (0 - \prod_{i=1}^{n} (1 \times \frac{R_i}{100})) \div 100$

C. $CR = (1 - \prod_{i=1}^{n} (1 - \frac{R_i}{100})) \times 100$

D. $CR = (1 \times \prod_{i=1}^{n} (1 \div \frac{R_i}{100})) - 100$

E. $CR = (0 \times \prod_{i=1}^{n} (0 \div \frac{R_i}{100})) - 100$

47. Эффективность контрмеры рассчитывается по следующей формуле:

A. $E = \frac{R_{old} - R_{new}}{R_{old}}$

B. $E = \frac{R_{old} + R_{new}}{R_{old}}$

C. $E = \frac{R_{old} \times R_{new}}{R_{old}}$

D. $E = \frac{R_{old} \div R_{new}}{R_{old}}$

E. $E = \frac{R_{old} \pm R_{new}}{R_{old}}$

48. Почему при локальном доступе VPN не учитывается, при передаче информации?
    A. Локальная сеть использует другой шифроватор
    B. Локальную сеть шифруют в сервере
    C. Для этого нужен отдельный кабель
    D. Локальная сеть не используется для передачи информации
    E. Трудно взломать локальную сеть
49. Как работает методика по оценке информационными рисками под названием COBRA?
    A. В виде внедрение своих проблем в специальную программу
    B. В виде тематических вопросников, после которого данные автоматически обрабатываются
    C. Приглашение специалиста по работе COBRA
    D. Отправление вопросов на почту специалисту COBRA
    E. Скачивание дополнительных утилит на сервер, после которого программа автоматически начинает работу
50. В 1985 году Центральное агентство по компьютерам и телекоммуникациям Великобритании начало исследования существующих методов управления ИБ для выдачи рекомендации по их использованию в правительственных организациях. Но не подошел ни один из них. Какой метод был создан на тот момент?
    A. Метод COBRA
    B. Метод SSADM
    C. Метод RA Software Tool
    D. Метод Software
    E. Метод CRAMM
51. Назовите какие этапы есть в методе CRAMM?
    A. Initiation, Risk analysis, Risk initiation, Identification Assets
    B. Risk analysis, Threat and Vulnerability Assessment, Risk initiation, Risk identification
    C. Initiation, Identification and Valuation of Assets, Threat and Vulnerability Assessment, Risk Analysis, Risk management
    D. Risk management, Risk analysis, Initiation, Risk initiation, Identification and Valuation of Assets
    E. Threat and Vulnerability Assessment, Identification and Valuation of Assets, Risk management, risk initiation
52. Что с собой значит термин «Risk management»?
    A. Предлагаются меры и средства уменьшения или уклонения рисков
    B. Позволяет получить качественные и количественные оценки

C. Идентифицируются и оцениваются угрозы и уязвимости информационных активов компании
D. Определяются границы исследуемой информационной системы компании, состав и структура ее основных информационных активов и транзакции
E. Четко идентифицируются активы, и определяются их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты

53. Что с собой представляет значение термина «Threat and Vulnerability Assessment»?
A. Предлагаются меры и средства уменьшения или уклонения рисков
B. Позволяет получить качественные и количественные оценки
C. Идентифицируются и оцениваются угрозы и уязвимости информационных активов компании
D. Определяются границы исследуемой информационной системы компании, состав и структура ее основных информационных активов и транзакции
E. Четко идентифицируются активы, и определяются их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты

54. Идентификация ресурсов и построение модели системы с точки зрения ИБ. Какие идентификации ресурсов проводятся?
A. Материальных, моральных, психологических
B. Материальных, программных, политических
C. Программных, политических и информационных
D. Материальных, программных, информационных
E. Политических, материальных, информационных

55. Недоступность ресурса в течении определенного времени, разрушение ресурса – потеря информации, полученной со времени последнего резервного копирования, нарушение конфиденциальности в случаях несанкционированного доступа, ошибки, связанные с передачей информации. К какому типу относятся вышеперечисленные ценности
A. Ценность информации
B. Ценность безопасности
C. Ценность политики ИБ
D. Ценность документирования
E. Ценность ресурса

56. Нарушение целостности может произойти не только вследствие преднамеренных действий, но и по ряду других причин:
A. Сбой системы, сбой сервера
B. Сбоев оборудования, ведущих к потере или искажению информации, стихийных бедствий, ошибок в программном обеспечении.

C. Сбой данных в программирований
D. Сбой серверных процессоров
E. Сбой в электричестве

57. Анализ риска можно проводить согласно методике по сценарию, Сколько этапов имеет анализ риска?
A. 6
B. 7
C. 4
D. 5
E. 9

58. По какой шкале определяется уровень риска?
A. От 0 - до 10
B. 0-5
C. 0-3
D. 0-8
E. 0-6

59. По статистике, самым большим препятствием на пути принятия каких-либо мер по обеспечению информационной безопасности в компании являются 2 причины:
A. Ограничение служебных мест
B. Ограничение бюджета и отсутствие поддержки сос стороны руководства
C. Ограничение баз данных
D. Ограничении ИТ специалистов
E. Ограничение финансирование и ИТ специалистов

60. Кем разработана методика FRAPP ?
A. Томас Шелби
B. Генри Форд
C. Густав Клинтвуд
D. Стефано Розино
E. Томас Пелтиер

61. Основные 2 Этапа оценки риска:
A. Сопоставление документов и политика конфиденциальности
B. Политика конфиденциальности и политика управление ИБ
C. Политика конфиденциальности и идентификация угроз
D. Определение защищаемых угроз и политика управление ИБ
E. Определение защищаемых активов и идентификация угроз

62. Какая методика поведения оценки рисков разработана Инженерным Институтом Программного Обеспечения (SEI) при университете Карнеги Меллон?
A. CRAMM
B. OCTAVE
C. SDSS
D. FRAPP
E. COBRA

63.Сколько фаз предполагает методика OCTAVE?

A. 4
B. 3
C. 2
D. 6
E. 7

64. Укажите правильную формулу возврата инвестиций от Risk Watch

A. $ROI = \sum_i NVP(Benefits_i) - \sum_i NVP(Costs_i)$
B. $ROI = \sum_i \text{NVP} + \sum_i NVP + Benefits_i + Costs_i$
C. $ROI = \sum_i NVP(Benefits_i) + \sum_i NVP(Costs_i)$
D. $ROI = \sum_i (Benefits_i) + \sum_i (Costs_i)$
E. $ROI = \sum_i \text{NVP} + \sum_i NVP$

$ROI = \sum_i \text{NVP} + \sum_i NVP + Benefits_i + Costs_i$

65. Оценка пользы (т.е. ожидаемого снижения потерь) который принесет внедрение данной меры защиты:

A. Costs_i
B. NPV
C. Benefists_i
D. ROI
E. LAFE

66. Затраты на внедрение и поддержание *j*–меры защиты

A. ROI
B. Benefits_i
C. NPV
D. Costs_i
E. LAFE

67. Чистая текущая стоимость в Risk Watch

A. ROI
B. LAFE
C. NPV
D. Costs_i
E. Benefits_i

68. Специальные законы, другие нормативные акты, правила, процедуры, и мероприятия, которые обеспечивают защиту информации на правовой основе

A. Организационная защита
B. Инженерно- техническая защита
C. Информационная защита
D. Конфиденциальная защита
E. Правовая защита

69. Регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, которая исключает или ослабляет нанесение каких либо убытков предприятию
    A. Организационная защита
    B. Правовая защита
    C. Инженерно-техническая защита
    D. Конфиденциальная защита
    E. Информационная защита
70. Использование разнообразных технических средств, которые препятствуют нанесению убытков предприятию
    A. Организационная защита
    B. Правовая защита
    C. Конфиденциальная защита
    D. Инженерно-техническая защита
    E. Информационная защита
71. Какой документ является основным по ИБ современного коммерческого предприятия ?
    A. Правовая защита ИБ
    B. Политика ИБ предприятия
    C. Политика конфиденциальности ИБ
    D. Статья ИБ
    E. Доктрина ИБ
72. Что такое «Политика безопасности организации»?
    A. обеспечение развития организации в области ИБ
    B. совокупность руководящих принципов, правил, процедур и практических приёмов
    C. Подход к управлению рисками и выбора контрмер для минимизации рисков информационной безопасности
    D. Краткое объяснение принципов информационной безопасности
    E. комплекс превентивных мер по защите информации на предприятии и содержит требования в адрес персонала, менеджеров и технических служб
73. Цель политики информационной безопасности
    A. Обеспечение развития организации в области ИБ
    B. Совокупность руководящих принципов, правил, процедур и практических приемов
    C. Подход к управлению рисками и выбора контрмер для минимизации рисков ИБ
    D. Краткое объяснение принципов ИБ
    E. Комплекс превентивных мер по защите информации на предприятии и содержит требования в адрес персонала, менеджеров и технических служб
74. Авторское право-
    A. Сведения которые не являются государственными тайнами секретами

B. Сведения которые являются государственными тайнами и секретами
C. Прибегают при широкой публикации своей информации, в то время как коммерческую тайну и держат в секрете
D. Не прибегают при широкой публикации своей информации, в то время как коммерческую тайну и не держат секрете
E. Разрешение выданное государством на проведение некоторых видов хозяйственной деятельности

75. Лицензия-
A. Сведения которые не являются государственными тайнами секретами
B. Сведения которые являются государственными тайнами и секретами
C. Прибегают при широкой публикации своей информации, в то время как коммерческую тайну и держат в секрете
D. Не прибегают при широкой публикации своей информации, в то время как коммерческую тайну и держат в секрете
E. Разрешение выданное государством на проведение некоторых видов хозяйственной деятельности

76. Создавая систему информационной безопасности, необходимо четко понимать что, …… защиты информации какие-либо претензии к недобросовестному сотруднику, клиенту, конкуренту и должностному лицу будут просто безосновательными
A. Без политики конфиденциальности
B. Без правового обеспечения
C. Без защиты информации
D. Без учредительных документов
E. Без организационных и функциональных документов

77. Правовые нормы обеспечения безопасности и защиты информации на конкретном предприятии отображаются в совокупности:
A. Политика конфиденциальности, правовое обеспечение, защита информации
B. Учредительные документы, Правовое обеспечение
C. Организационные и функциональные документы, Защита информации
D. Учредительные, организационные, функциональные документы
E. Защита информации, Политика конфиденциальности, Функциональные документы

78. В каком договоре предусматриваются требования правового обеспечения защиты информации
A. Политика конфиденциальности
B. Коллективный договор
C. Учредительные документы
D. Предмет договора
E. Функциональные документы

79. Регламентация производственной деятельности и взаимоотношений исполнителей на нормативной основе, что исключает или существенно осложняет неправомерное овладение конфиденциальной информацией и проявления внутренних и внешних угроз
    A. Организационная защита
    B. Информационная защита
    C. Информационная безопасность
    D. Служба безопасности
    E. Политика конфиденциальности
80. Сколько основных организационных мероприятии
    A. 4
    B. 6
    C. 5
    D. 8
    E. 3
81. Организация работы с документами и документируемой информацией:
    A. Внутренние и внешние угрозы конфиденциальной информации и разработка мероприятий по обеспечению ее защиты
    B. Использования технических средств сбора, обработки и хранение и конфиденциальной информации
    C. Проведение систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.
    D. Организация разработки и использование, возврат, хранение и уничтожение
    E. Организация и поддержка надежного пропускного режима
82. Организация режима и охраны
    A. Внутренние и внешние угрозы конфиденциальной информации и разработка мероприятий по обеспечению ее защиты
    B. Использование технических средств сбора, обработки и хранение и конфиденциальной информации
    C. Проведение систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.
    D. Организация разработки и использование, возврат, хранение и уничтожение
    E. Организация и поддержка надежного пропускного режима
83. Организация использования технических средств:
    A. Внутренние и внешние угрозы конфиденциальной информации и разработка мероприятий по обеспечению ее защиты
    B. Использование технических средств сбора, обработки и хранение и конфиденциальной информации
    C. Проведение систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

D. Организация разработки и использование, возврат, хранение и уничтожение
E. Организация и поддержка надежного пропускного режима

84. Организация работы по анализу внутренних и внешних угроз
A. Внутренние и внешние угрозы конфиденциальной информации и разработка мероприятий по обеспечению ее защиты
B. Использование технических средств сбора, обработки и хранение и конфиденциальной информации
C. Проведение систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.
D. Организация разработки и использование, возврат, хранение и уничтожение
E. Организация и поддержка надежного пропускного режима

85. Организация работы по проведению систематического контроля:
A. Внутренние и внешние угрозы конфиденциальной информации и разработка мероприятий по обеспечению ее защиты
B. Использование технических средств сбора, обработки и хранение и конфиденциальной информации
C. Проведение систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.
D. Организация разработки и использование, возврат, хранение и уничтожение
E. Организация и поддержка надежного пропускного режима

86. Какие организационные средства защиты компьютерных информационных систем и сетей чаще всего применяются?
A. При проектировании, при подборе и подготовке персонала, при хранении и использования документов, при соблюдении надежного пропускного контроля, при подготовке и контроле за работой
B. При копировании документов, при подборе и подготовке персонала, при хранении и использования документов, при соблюдении надежного пропускного контроля, при подготовке и контроле за работой
C. При проектировании, При защите конфиденциальной информации , при хранении и использования документов, при соблюдении надежного пропускного контроля, при подготовке и контроле за работой
D. При проектировании, при подборе и подготовке персонала, при хранении и использования документов, при соблюдении надежного пропускного контроля, При проверке новых сотрудников
E. При проектировании, при подборе и подготовке персонала, при хранении и использования документов, При составлении

политики конфиденциальности, при подготовке и контроле за работой

87. Что составляет контроль за процессом печати информации, учет печатных документов, учет съемных носителей, учет технических средств, ведение учетных карточек пользователей?
    A. Политика конфиденциальности
    B. Защита Информации
    C. Государственная тайна
    D. Политика управления
    E. Защита данных
88. Большинство сервисов безопасности направлено на предупреждение нарушений:
    A. Аудит и контроль
    B. Идентификация, аутентификация, управление доступом, шифрование, экранирование
    C. Обеспечение безопасности, аудит, контроль данных, шифрование
    D. Туннелирование, идентификация, шифрование
    E. Активный аудит, Уязвимые места, аутентификация
89. Что такое конвертирование одних протоколов передачи пакетов через сеть, в другие протоколы
    A. Аудит
    B. Контроль
    C. Консоль
    D. Туннелирование
    E. Аутентификация
90. Что позволяет идентификация субъекту
    A. Убеждается что субъект действительно тот за кого себя принимает
    B. Запрашивает у пользователя его имя и пароль
    C. Защищает данные и генерирует его
    D. Проверяет подлинность документов
    E. Позволяет субъекту, действующему от имени определенного пользователя, назвать себя
91. Наиболее известный программный генератор одноразовых паролей
    A. True key
    B. Bellcore
    C. Keyloger
    D. SKEY
    E. Printcode
92. Как называется серверный аутентификактор разработанный в середине 1980-х в Массачусетском технологическом институте
    A. SKEY
    B. Bellcore
    C. Kerberos
    D. Keyloger

E. True key

93. Что с собой представляет с собой совокупность автоматизированных методов идентификации и аутентификации людей на основе их физиологических и поведенческих характеров
    A. База данных
    B. Хранилище доступа
    C. Серверные
    D. 3D анимирование
    E. Биометрия
94. Что делает средства управления доступом?
    A. Контролировать действия которые субъекты могут выполнять над объектами
    B. Контролировать лицевой счет
    C. Контролировать ПК
    D. Контролировать базы данных
    E. Контролировать системными блоками
95. Основной механизм многопользовательских систем, призванный обеспечить конфиденциальность, целостность объектов и до некоторой степени их доступность:
    A. Управление доступом
    B. Логическое управление доступом
    C. Многопользовательские доступы
    D. Объективный доступ
    E. Субъективный доступ
96. Что понимается при слове протоколирование?
    A. Анализирование накопленной информаций
    B. Разделение на внешние и внутренние сервисы
    C. Сбор и накопление информации о событиях, происходящих в информационной системе
    D. Аудит с автоматическим реагированием на выявленные не штатные ситуации
    E. Обеспечение возможности реконструкции последовательности событий
97. Анализ накопленной информации:
    A. Учет
    B. Протоколирование
    C. Активация
    D. Аудит
    E. Лояльность
98. Что представляет с собой задача активного аудита?
    A. Незаконное получение полномочии
    B. Совокупность условии при выполнении которых атака считается имеющей место
    C. Поведение пользователя или компонента информационной системы

D. Оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее
E. Выявлять подозрительную активность и предоставлять средства для механического реагирования на нее

99. Совокупность условий (действий), при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию:
A. Активная атака
B. Злоупотребления полномочиями
C. Системная атака
D. Подозрительная атака
E. Сигнатурная атака

100. Что такое «шифрование»
A. Мощное средство обеспечения конфиденциальности
B. Аутентификация данных
C. Секретный код
D. Доступ к данным
E. Контроль целостности

Задания в открытой форме

1) … - самый ценный ресурс в компании, а в некоторых случаях является и производственным ресурсом, от сохранности которого зависят важные технологические процессы.

2) … – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

3) … — это комплекс мероприятий, направленных на обеспечение информационной безопасности.

4) … защиты информации является информационная система (предприятия, коммерческой организации) или автоматизированная система обработки данных.

5) … система — взаимосвязанная совокупность средств, методов и персонала, которые используются для хранения, обработки, передачи и получения информации в интересах достижения поставленной цели.

6) … информации в ИС – это такое состояние всех компонент информационной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне.

7) Под … в ИС понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности.

8) Цель …. – обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством их предотвращения и сведения последствий к минимуму.

9) … — это защита от несанкционированного доступа к информации

10) Под .. информации подразумевается, ее защищенность от разрушения и несанкционированного изменения.

11) … — это возможность за приемлемое время получить требуемую информационную услугу.

12) … можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)).

13) … — законы и нормативны акты, затрагивающие ОО;

14) … — положения политик безопасности, затрагивающих ОО и учитывающих его особенности;

15) … — меры физической защиты, персонал и его специфика;

16) … — назначение ОО, предполагаемые области его применения.

17) … — типовой набор требований для некоторой категории ОО.

18) … — документ, содержащий требования безопасности для конкретной разработки, выполнение которых обеспечивает достижение поставленных целей безопасности.

19) … – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер).

20) … – действие, которое потенциально может привести к нарушению безопасности

21) … – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

22) …– ущерб, который понесет компания от потери ресурса

23) … – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса.

Задание на установление соответствия

1. Установить соответствие этапов CRAMM:

1) «Identification and Valuation of Assets»	a) — идентифицируются и оцениваются угрозы и уязвимости информационных активов компании.
2) «Threat and Vulnerability Assessment»	b) — четко идентифицируются активы, и определяется их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты.

3) «Risk Analysis»	c) — предлагаются меры и средства уменьшения или уклонения от риска.
	d) — позволяет получить качественные и количественные оценки рисков.

2. Установить соответствие ущерба репутации организации:

1) 2	a) — критика в средствах массовой информации, имеющая последствия в виде крупных скандалов, парламентских слушаний, широкомасштабных проверок и т. п.;
2) 4	b) — негативная реакция отдельных депутатов;
3) 6	c) — негативная реакция отдельных чиновников, общественных деятелей;
4) 8	d) — критика в средствах массовой информации, не имеющая широкого общественного резонанса;
	e) — негативная реакция на уровне Президента и Правительства.

3. Установить соответствие ущерба здоровью персонала:

1) 2	a) — ущерб среднего размера (необходимо лечение для одного или нескольких сотрудников, но длительных отрицательных последствий нет);
2) 4	b) — минимальный ущерб (последствия не связаны с госпитализаций или длительным лечением);
3) 6	c) — гибель людей.
	d) — серьезные последствия (длительная госпитализация, инвалидность одного

	или нескольких сотрудников);

4. Установить соответствие финансовых потерь, связанных с восстановлением ресурсов:

1) 2	a) — от $1000 до $10 000;
2) 4	b) — менее $1000;
3) 6	c) — от $10 000 до $100 000;
	d) — свыше $100 000.

5. Установить соответствие дезорганизации деятельности в связи с недоступностью данных::

1) 2	a) — отсутствие доступа к информации до 1 часа;
2) 4	b) — отсутствие доступа к информации до 15 минут;
3) 6	c) — отсутствие доступа к информации от 12 часов;
4) 8	d) — отсутствие доступа к информации до 3 часов;
	e) — отсутствие доступа к информации более суток.

6. Установить соответствие оценки уровня угрозы:

1) Очень высокий	a) Инцидент происходит в среднем, не чаще, чем каждые 10 лет
2) Высокий	b) Инцидент происходит в среднем один раз в 3 года
3) Средний	c) Инцидент происходит в среднем раз в год
4) Низкий	d) Инцидент происходит в среднем один раз в четыре месяца

	e) Инцидент происходит в среднем раз в месяц

7. Установить соответствие оценки рисков в зависимости от факторов:

1) Высокий риск	a) Предполагается, что без снижения таких рисков обращение к информационной системе предприятия может оказать отрицательное влияние на бизнес;
2) Существенный риск	b) Здесь требуется эффективная стратегия управления рисками, которая позволит уменьшить или полностью исключить отрицательные последствия нападения;
3) Умеренный риск	c) Усилия по управлению рисками в данном случае не будут играть важной роли.
	d) В отношении рисков, попавших в эту область, достаточно применить основные процедуры управления рисками;

8. Установить соответствие:

1) Угроза безопасности	a) Это некая неудачная характеристика системы, которая делает возможным возникновение угрозы.
2) Уязвимость	b) Это угроза раскрытия информации.
3) Атака	c) Это потенциально возможное происшествие, которое может оказать воздействие на информацию в системе.
	d) Это действие по использованию уязвимости; реализация угрозы.

9. Установить соответствие:

1) Угроза целостности	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.

10. Установить соответствие:

1) High-severity vulnerabilities	a) Список уязвимостей, которые надо устранить в ближайшее время
2) Middle-severity vulnerabilities	b) Список уязвимостей, в отношении которых не требуется немедленных действий
3) Low-severity vulnerabilities	c) Список уязвимостей, которые можно не устранять
	d) Список уязвимостей, которые надо устранить немедленно

11. Установить соответствие:

1) Командный интерфейс	a) Движения

2) SILK	b) Последовательности символов
3) WIMP	c) Манипулятор
	d) Аудио

12. Установить соответствие этапов RiskWatch:

1) Первый этап	a) ввод данных, описывающих конкретные характеристики системы.
2) Второй этап	b) Определение предмета исследования.
3) Третий этап	c) Генерация отчетов.
	d) Количественная оценка риска

13. 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) Защищает информацию путем использования технических мер, таких как пароли, шифрование, брандмауэры и другие средства защиты информации на уровне программного обеспечения.

14. Установить соответствие:

1) OLE-automation или просто Automation	a) Технология, организующая доступ к данным разных компьютеров с учетом балансировки нагрузки сети.
2) ActiveX	b) Технология, обеспечивающая безопасность и стабильную работу распределенных приложений при больших объемах передаваемых данных.
3) MIDAS	c) Технология предназначена для создания программного обеспечения как сосредоточенного на одном компьютере, так и распределенного в сети.
	d) Технология создания программируемых приложений, обеспечивающая программируемый доступ к внутренним службам этих приложений

15. Установить соответствие:

1) Режим государственной	a) Совокупность правил въезда (прохода), временного пребывания лиц

границы	и транспортных средств в пограничной полосе; осуществление в ее пределах хозяйственной, промысловой и тон деятельности; проведение массовых общественно-политических, культурных и других мероприятий
2) Пограничный режим	b) Совокупность правил, устанавливающих порядок ее содержания, пересечения гражданами и транспортными средствами; перемещения через границу товаров и животных; ведения на ней хозяйственной, промысловой и иной деятельности;
3) Пограничная полоса	c) Часть территории российской федерации, непосредственно прилегающей к государственной границе на всем ее протяжении.
	d) Линия, которая отделяет одно государство от другого и может быть определена на местности, на карте или в законодательстве.

16. Установить соответствие:

1) Линейная структура процесса вычислений	a) Предполагает, что для получения результата некоторые действия необходимо выполнить несколько раз.
2) Разветвленная структура процесса вычислений	b) Предполагает, что конкретная последовательность операций зависит от значений одной или нескольких переменных.
3) Циклическая структура	c) Предполагает, что для получения результата необходимо выполнить

процесса вычислений	некоторые операции в определенной последовательности.
	d) Процесс вычислений вызывает сам себя.

17. Установить соответствие:

1) Правильность	a) Возможность проверки получаемых результатов;
2) Универсальность	b) Обеспечение полной повторяемости результатов, т. Е. Обеспечение их правильности при наличии различного рода сбоев;
3) Надежность	c) Обеспечение правильной работы при любых допустимых данных и защиты от неправильных данных;
	d) Функционирование в соответствии с техническим заданием;

18. Установить соответствие:

1) Точность результатов	a) Возможность совместного функционирования с некоторым оборудованием
2) Защищенность	b) Возможность совместного функционирования с другим программным обеспечением
3) Программная совместимость	c) Обеспечение конфиденциальности инф ормации;

	d) Обеспечение погрешности результатов не выше заданной;

19. Установить соответствие:

1) Превентивные	a) Меры безопасности, направленные на обнаружение инцидентов. Например, антивирусная защита или система обнаружения вторжений.
2) Восстановительные	b) Меры безопасности, которые предотвращают появление инцидента информационной безопасности. Например, распределение прав доступа.
3) Обнаруживающие	c) Меры безопасности, направленные на уменьшение потенциального ущерба в случае инцидента. Например, резервное копирование.
4) Подавляющие	d) Меры безопасности, направленные на восстановления после инцидента. Например, восстановление резервных копий, откат на предыдущее рабочее состояние и т.п.
	e) Меры безопасности, которые противодействуют попыткам реализации угрозы, то есть инцидентам.

20. Установить соответствие:

1. Сертификат ключа подписи	a) Документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи

	установленным требованиям.
2. Сертификат средств электронной цифровой подписи	b) Документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра.
3. Электронная цифровая подпись	c) Документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа
	d) Уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Задание на установление правильной последовательности

1. Установить этапы системы управления:
   1) Планирование.
   2) внедрение.
   3) мониторинг и анализ.
   4) совершенствование.

2. Основные этапы разработки системы управления информационной безопасностью:

1) обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов);
2) контроль выполнения и эффективности выбранных мер.
3) оценка защищенности информационной системы;
4) оценка информационных рисков;
5) инвентаризация активов;
6) внедрение выбранных мер обработки рисков;
7) категорирование активов;

3. Установить предпочтительную последовательность этапов внедрения межсетевого экрана:
   1) конфигурирование
   2) планирование
   3) тестирование
   4) развертывание
   5) управление

4. Установите основные этапы оценки риска:
   1) Сопоставление вероятности возникновения
   2) Определение контрмер
   3) Документирование
   4) Идентификация угроз
   5) Определение защищаемых активов

5. Установите фазы анализа OCTAVE:
   1) разработка профиля угроз, связанных с активом;
   2) идентификация инфраструктурных уязвимостей;
   3) разработка стратегии и планов безопасности.

6. Установите этапы PDCA:
   1) планирование
   2) проверка
   3) действие
   4) выполнение
7. Установите этапы этапы создания СУИБ:
   1) Внедрение и функционирование системы управления информационной безопасности.
   2) Проведение мониторинга и анализа системы управления информационной безопасности.
   3) Разработка системы управления информационной безопасности.
   4) Поддержка и улучшение системы управления информационной безопасности.

8. Установить этапы разработки:
    1) Проектирование
    2) Реализация
    3) Внедрение
    4) Анализ и планирование требований пользователей

9. Установить этапы разработки программной документации:
    1) Разработка технического проекта.
    2) Комплексное внедрение программной документации.
    3) Подготовка технического специального задания.
    4) Составление подробного эскизного варианта проекта.
    5) Оформление рабочего документа.

10. Установите этапы процесса управления рисками:
    1) Выбор анализируемых объектов и уровня детализации их рассмотрения.
    2) Инвентаризация активов.
    3) Анализ угроз и их последствий, выявление уязвимых мест в защите.
    4) Оценка рисков.
    5) Выбор методики оценки рисков.
11. Установите этапы процесса управления рисками:
    1) Реализация и проверка выбранных мер.
    2) Выбор защитных мер.
    3) Обработка рисков.
    4) Оценка остаточного риска.

12. Установите этапы стратегии управления рисками Microsoft:
    1) – определение допустимого уровня рисков (то есть того уровня рисков,
    2) который приемлем);
    3) – оценка вероятности возникновения каждого риска;
    4) – присвоение стоимости каждому риску;
    5) – расстановка приоритетов.

13. Выберите правильную последовательность этапов по созданию системы защиты персональных данных:
    1) Опытная и промышленная эксплуатация
    2) Проектный этап
    3) Аттестация или декларирование
    4) Предпроектный этап

14. Выберите правильную последовательность этапов разработки профиля защиты.
    1) Анализ среды применения ИТ-продукта с точки зрения

2) безопасности.
3) Выбор профиля-прототипа.
4) Синтез требований.

15. 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

16. 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;

17. Выберите последовательность проведения моделирования угроз:
    1) Определение негативных последствий от угроз безопасности информации.
    2) Определение объектов воздействия угроз безопасности информации.
    3) Оценка возможности реализации угроз и их актуальности.

18. Установите этапы процессной модели:
    1) Проверка.
    2) Планирование.
    3) Реализация
    4) Действие.

19. Установите этапы методики анализа рисков Microsoft:
    1) Распознавание (идентификация) рисков.
    2) Определение размера риска.
    3) Разработка плана управления рисками.
    4) Текущий контроль и управление рисками.

20. Установите этапы процесса управления рисками в методике CRAMM:
    1) «Initiation».
    2) «Identification and Valuation of Assets».
    3) «Risk Analysis».
    4) «Threat and Vulnerability Assessment».

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. Компания хочет провести аудит информационной безопасности. Какие шаги вы предпримете для подготовки к аудиту? Какие процессы в вашей организации вы будете аудитировать и какие меры безопасности вы проверите?

2. Вы работаете в компании, которая хочет подготовиться к сертификации по стандарту ISO 27001. Какой процесс вы предпримете для оценки текущего состояния безопасности в вашей компании? Какие меры безопасности вы будете проверять и какие документы вы будете анализировать?

3. Компания столкнулась с нарушением информационной безопасности, и вам поручили провести аудит, чтобы выяснить, как это произошло. Какие шаги вы предпримете для проведения аудита? Какие меры безопасности вы проверите и какие документы вы запросите?

4. Компания хочет убедиться, что ее персонал полностью соответствует политике информационной безопасности. Как вы определите, какие требования политики безопасности могут быть нарушены? Как вы будете проверять соответствие персонала этим требованиям?

5. Ваша компания хочет провести аудит информационной безопасности своих вендоров и партнеров. Как вы определите, какие компании следует аудитировать? Какие меры безопасности вы проверите и как вы будете использовать результаты аудита для обеспечения безопасности вашей компании?

6. Компания решила провести аудит информационной безопасности. Какие этапы вы предложите для проведения аудита? Какую методику аудита выберете и почему?

7. Компания была подвержена кибератаке, которая привела к утечке конфиденциальной информации. Какие меры по организации аудита информационной безопасности вы предложите для предотвращения подобных инцидентов в будущем?

8. Компания реализует проект по переходу на облачные технологии. Какие шаги вы предпримете для проведения аудита информационной безопасности в связи с этим проектом?

9. Компания планирует провести аудит информационной безопасности внутри организации. Какие методы и инструменты для проведения аудита вы будете использовать? Какие результаты вы ожидаете от проведения аудита?

10. Компания реализует проект по внедрению новой системы хранения данных. Какие меры по организации аудита информационной

безопасности вы примените для проверки безопасности новой системы хранения данных?

11. Вы работаете в IT-отделе компании и ответственны за аудит информационной безопасности. Какие методы и инструменты вы будете использовать для проведения аудита и обеспечения безопасности сети и данных компании?

12. Вы являетесь аудитором информационной безопасности и назначены для проведения аудита в организации. Какие этапы вы будете проходить в ходе аудита, чтобы обеспечить полноту и достоверность аудиторской информации?

13. Компания была подвержена кибератаке, которая привела к утечке конфиденциальной информации. Как вы организуете аудит информационной безопасности, чтобы выявить уязвимости в системе безопасности и предотвратить подобные инциденты в будущем?

14. Компания компания перешла на удаленную работу, и теперь большинство сотрудников работает из дома. Как вы организуете аудит информационной безопасности в такой среде, чтобы обеспечить безопасность данных компании и соблюдение стандартов безопасности?

15. Вы были назначены руководителем проекта по организации аудита информационной безопасности в организации. Как вы организуете команду для проведения аудита и как будете оценивать результаты аудита?

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.