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

Методы и средства защиты информации в системах электронного документооборота
(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. Введение в курс «Методы и средства защиты информации в системах электронного документооборота.

1. Что такое система электронного документооборота?
2. Какая цель и задача курса?
3. Что такое электронно-цифровая подпись?
4. Какие существуют этапы документооборота?
5. Что такое документ?
6. Что подразумевается под системами электронного документооборота?
7. Какие методы защиты информации используются в системах электронного документооборота?
8. Каковы основные принципы обеспечения безопасности информации в системах электронного документооборота?
9. Какие средства защиты информации применяются для обеспечения безопасности систем электронного документооборота?
10. Какие потенциальные угрозы могут возникнуть при использовании систем электронного документооборота и как можно их предотвратить?

Тема 2. Аудит информационной безопасности СЭД. Методы и средства защиты информации в СЭД.

1. Классификация информации.
2. Как обеспечить подлинность документов?
3. Какие существуют виды разграничения доступа?
4. Что такое конфиденциальность?
5. Какие существуют угрозы для системы электронного документооборота?
6. Что подразумевается под аудитом информационной безопасности в системе электронного документооборота?
7. Какая роль аудита информационной безопасности СЭД в обеспечении безопасности информации?
8. Какие методы и инструменты используются при проведении аудита информационной безопасности СЭД?
9. Какие основные аспекты и параметры проверяются в рамках аудита информационной безопасности СЭД?
10. Какие рекомендации и меры безопасности могут быть предложены на основе результатов аудита информационной безопасности СЭД?
11. Какие методы защиты информации применяются в системах электронного документооборота?

12. Какие технические средства используются для обеспечения безопасности информации в СЭД?
13. Какие организационные средства применяются для защиты информации в СЭД?
14. Какие законодательные механизмы существуют для обеспечения информационной безопасности СЭД?
15. Какие преимущества и ограничения имеют различные методы и средства защиты информации в СЭД?

Тема 3. Технические средства защиты информации в СЭД. Организационные средства защиты информации. Законодательные средства защиты информации.

1. Что такое регламенты управления?
2. Как осуществляется защита персональных данных в информационных системах?
3. В каком законе дано определение персональных данных?
4. Какие нужны исходные данные при проведении классификации информационной системы?
5. Сколько существует основных категорий персональных данных?
6. Какие технические средства используются для защиты информации в системах электронного документооборота?
7. Какие средства шифрования и аутентификации могут быть применены в СЭД?
8. Какие механизмы контроля доступа и защиты от несанкционированного доступа применяются в СЭД?
9. Каким образом системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS) влияют на безопасность СЭД?
10. Какие средства мониторинга и анализа используются для обеспечения безопасности информации в СЭД?
11. Какие технические средства используются для защиты информации в системах электронного документооборота?
12. Какие средства шифрования и аутентификации могут быть применены в СЭД?
13. Какие механизмы контроля доступа и защиты от несанкционированного доступа применяются в СЭД?
14. Каким образом системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS) влияют на безопасность СЭД?
15. Какие средства мониторинга и анализа используются для обеспечения безопасности информации в СЭД?

Тема 4. Система защиты электронного документооборота организации. Организация работы с персоналом по обеспечению защиты информации в СЭД.

1. Что такое целостность информации?

2. Как осуществляется комплексный метод защиты информации?
3. Что такое шифрование информации?
4. Какие существуют проблемы распределения и хранения ключей?
5. Что такое ЭЦП?
6. Какие основные функции выполняет система защиты электронного документооборота в организации?
7. Как осуществляется аутентификация пользователей в системе электронного документооборота?
8. Какие меры предпринимаются для обеспечения конфиденциальности и целостности данных в системе электронного документооборота?
9. Как организуется управление доступом к документам и информации в системе электронного документооборота?
10. Какие меры обеспечивают безопасность передачи данных в рамках системы электронного документооборота?
11. Как организуется работа с персоналом по обеспечению защиты информации в системе электронного документооборота?
12. Какие обязанности и роли определены для сотрудников, ответственных за защиту информации в системе электронного документооборота?
13. Как проводится обучение и осведомление персонала о правилах и политике информационной безопасности в рамках системы электронного документооборота?
14. Каковы процедуры слежения за действиями персонала в системе электронного документооборота с целью предотвращения несанкционированного доступа или утечек информации?
15. Как осуществляется контроль и обновление прав доступа персонала в системе электронного документооборота для обеспечения минимизации рисков безопасности?

Тема 5. Развитие международного законодательства в области защиты информации и информационной безопасности.

1. Назовите проект, который позволил организовать электронный архив конструкторской документации?
2. Какую выбрали систему для реализации внедрения в оперативном режиме?
3. Какие стояли задачи перед проектом?
4. За какое время проект был реализован?
5. Для какой цели создаются государственные информационные системы?
6. Какие основные международные организации занимаются развитием законодательства в области защиты информации и информационной безопасности?
7. Какие ключевые международные договоры и соглашения существуют для защиты информации и информационной безопасности?

8. Какова роль ООН в развитии международного законодательства в области защиты информации и информационной безопасности?
9. Какие существуют проблемы и вызовы при разработке и принятии международного законодательства в области защиты информации и информационной безопасности?
10. Какие тенденции и новшества можно наблюдать в развитии международного законодательства в области защиты информации и информационной безопасности?

Критерии оценки:

3-4 балла 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.

1-2 балла 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 ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа№1 «Механизмы обеспечения информационной безопасности электронных документов»

1. Что такое ECM?
2. Что такое система электронного документооборота?
3. Назовите недостатки бумажного документооборота?
4. Что такое документооборот?
5. Назовите преимущества электронного документооборота?
6. Какие основные механизмы обеспечения конфиденциальности электронных документов можно применить?
7. Какие средства защиты доступа используются для обеспечения целостности электронных документов?
8. Какие методы аутентификации могут быть использованы для обеспечения безопасности электронных документов?

9. Какие технические меры могут быть применены для обеспечения защиты от несанкционированного доступа к электронным документам?

10. Какие процедуры контроля и мониторинга могут быть использованы для обнаружения нарушений информационной безопасности электронных документов?

Лабораторная работа№2 «Защищенные системы электронного документооборота»

1. Что такое СЭД?
2. Главные особенности российского делопроизводства влияющих на специфику отечественных СЭД?
3. Основные черты переносимости СЭД?
4. Какие существуют целы физической реализации СЭД?
5. Кто несет ответственность за содержание и оформление документа?
6. Какие основные принципы обеспечения безопасности могут быть применены в системе электронного документооборота?
7. Каким образом могут быть защищены электронные документы от утраты или повреждения?
8. Какие меры могут быть предприняты для защиты от вредоносного программного обеспечения в системе электронного документооборота?
9. Какие процедуры резервного копирования и восстановления могут быть применены для обеспечения надежности системы электронного документооборота?
10. Каким образом может осуществляться контроль доступа к системе электронного документооборота и ее компонентам?

Лабораторная работа№3 «Применение электронной подписи в системах электронного документооборота»

1. Что такое электронная подпись?
2. Основные свойства ЭЦП?
3. Для чего нужна ЭЦП?
4. Дайте определение электронного документооборота.
5. Какие существуют проблемы при использовании электронного документооборота?
6. Как работает электронная подпись и какие преимущества она может предоставить в системе электронного документооборота?
7. Какие требования и правила существуют для использования электронной подписи в системах электронного документооборота?
8. Каким образом можно проверить подлинность электронной подписи в системе электронного документооборота?
9. Какие технические и организационные меры могут быть применены для защиты от подделки или несанкционированного использования электронной подписи?

10. Какие существуют стандарты и законодательные нормы относительно использования электронной подписи в системах электронного документооборота?

Лабораторная работа№4 «Настройка межсетевого взаимодействия»

1. Для чего предназначено межсетевое взаимодействие?
2. Виды межсетевых мастер ключей.
3. Какими принципами следует руководствоваться при выборе межсетевого мастер ключа?
4. Для чего необходимо прекращение взаимодействия между сетями?
5. Перечислите по порядку основные действия при настройке взаимодействия между сетями?
6. Какие протоколы и стандарты обеспечивают безопасное межсетевое взаимодействие?
7. Каким образом может быть обеспечена конфиденциальность данных при передаче между сетями?
8. Какие меры могут быть применены для обеспечения целостности данных при межсетевом взаимодействии?
9. Каким образом может быть организован контроль доступа и аутентификация при настройке межсетевого взаимодействия?
10. Какие существуют методы обнаружения и предотвращения атак при межсетевом взаимодействии?

Лабораторная работа№5 «ViPNet Деловая почта»

1. Перечислите функциональные возможности деловой почты?
2. Что такое автопрессинг?
3. Что создает УКЦ и ЦУС для абонентского пункта?
4. Перечислите уровни адресации и поясните каждый из них.
5. Для чего необходимо подписывать письмо с помощью сертификата пользователя?
6. ак работает ViPNet Деловая почта и какие функции она предоставляет?
7. Какие меры безопасности и шифрования применяются в ViPNet Деловой почте?
8. Каким образом обеспечивается конфиденциальность и целостность сообщений при использовании ViPNet Деловой почты?
9. Какие механизмы аутентификации могут быть использованы для обеспечения безопасности при работе с ViPNet Деловой почтой?
10. Какие преимущества и ограничения имеет использование ViPNet Деловой почты в системах электронного документооборота?

Критерии оценки:

3-4 балла 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.

1-2 балла 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. Разработка и внедрение системы шифрования: Ваша задача состоит в разработке и внедрении системы шифрования, которая будет обеспечивать конфиденциальность информации в системе электронного документооборота. Используйте различные методы шифрования, такие как симметричное или асимметричное шифрование, для защиты документов от несанкционированного доступа.

2. Реализация механизмов аутентификации пользователей: Ваша задача - реализовать механизмы аутентификации пользователей в системе электронного документооборота. Используйте методы, такие как парольная аутентификация, двухфакторная аутентификация или биометрическая аутентификация, для обеспечения безопасности доступа к системе.

3. Создание системы контроля доступа: Вам предстоит создать систему контроля доступа, которая будет регулировать права пользователей на просмотр, редактирование и распространение документов в системе электронного документооборота. Разработайте гибкую систему, которая будет учитывать различные уровни доступа, роли пользователей и условия доступа к документам.

4. Разработка системы обнаружения и предотвращения утечки данных: Ваша задача - разработать систему, способную обнаруживать и предотвращать утечку конфиденциальной информации в системе электронного документооборота. Используйте методы обнаружения угроз, мониторинга активности пользователей и контроля передачи данных для предотвращения утечек и несанкционированного распространения информации.

5. Проведение аудита безопасности системы: Организуйте аудит безопасности системы электронного документооборота, чтобы оценить ее

уязвимости и эффективность методов и средств защиты информации. Проведите проверку на соответствие стандартам безопасности, анализ уязвимых мест и рекомендуйте меры по усовершенствованию безопасности системы

6. Внедрение системы электронной подписи: Ваша компания решила внедрить систему электронной подписи для обеспечения аутентичности и целостности документов в системе электронного документооборота. Ваша задача - выбрать подходящий метод электронной подписи, провести пилотное тестирование и реализовать систему в производственной среде.

7. Разработка и внедрение системы контроля доступа: Вам предстоит разработать и внедрить систему контроля доступа к документам в системе электронного документооборота. Задача включает определение уровней доступа, реализацию механизмов аутентификации и авторизации, а также контроль действий пользователей в системе.

8. Создание системы обнаружения и предотвращения утечки информации: Ваша задача - разработать и внедрить систему, которая будет обнаруживать и предотвращать утечку конфиденциальной информации из системы электронного документооборота. Используйте методы контроля данных, мониторинга сетевого трафика и анализа поведения пользователей для обнаружения подозрительной активности и утечек данных.

9. Разработка системы резервного копирования и восстановления: Ваша задача - разработать и внедрить систему резервного копирования и восстановления данных в системе электронного документооборота. Разработайте методы регулярного создания резервных копий, хранения и восстановления данных, а также проведите тестирование системы для проверки ее надежности и эффективности.

10. Обучение сотрудников в области информационной безопасности: Ваша задача - разработать и провести обучающие программы для сотрудников, связанные с методами и средствами защиты информации в системах электронного документооборота. Подготовьте материалы, организуйте обучающие сессии и проверьте уровень понимания и применения безопасных практик сотрудниками в процессе работы с документами.

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 балла 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. Как называется бланк, содержащий одинаковый набор реквизитов для всех видов документов

1) бланк конкретного документа
2) единый бланк
3) общий бланк

2. В каком НПА указаны основные требования в области гостайны?

1) Конституция РФ
2) Доктрина информационной безопасности РФ
3) для выяснения готовности предприятия к автоматизации
4) Закон о государственной тайне

3. Бланк документа – это

1) лист бумаги с заранее воспроизведенными реквизитами, содержащими постоянную информацию об организации — авторе документа
2) лист бумаги с заранее воспроизведенными реквизитами, содержащими постоянную и переменную информацию об организации
3) государственная бумага, обязательная для применения в организации
4) государственная бумага, необязательная для применения в организации

4. В объеме документооборота следует учитывать:

1) все входящие и исходящие документы за определенный период времени
2) все внутренние документы и все копии за определенный период времени
3) все входящие и исходящие документы за определенный период времени
4) все входящие, исходящие и внутренние документы, а также все копии за определенный период времени

5. Ответственность за разглашения государственной тайны будет:

1) административной
2) гражданско-правовой
3) дисциплинарной
4) уголовной

6. Абстрактное описание системы, без связи с ее реализацией, дает модель политики безопасности

1) Белла-ЛаПадула
2) С полным перекрытием
3) Лендвера
4) С частичным перекрытием

7. Сколько грифов секретности существует?

1) 1
2) 3
3) 4
4) 5
5) 2

8. Группы доступа необходимы

1) для предоставления прав контролера сотрудникам, обязанным следить за действиями пользователей системы
2) в случае отсутствия сотрудника ответственного за работу над документом и необходимостью ее продолжение в его отсутствие
3) для организации доступа к документам для отделов организации, коллектива сотрудников, работающих над отдельным проектом

9. Для реализации технологии RAID создается:

1) специальный процесс
2) компилятор
3) интерпретатор
4) псевдодрайвер

10. Определение допустимых для пользователя ресурсов ОС происходит на уровне ОС

1) сетевом
2) внешнем
3) приложений
4) системном

11. Делегирование прав доступа необходимо:

1) в случае отсутствия сотрудника ответственного за работу над документом и необходимостью ее продолжение в его отсутствие

2) для предоставления прав контролера сотрудникам, обязанным следить за действиями пользователей системы
3) для организации доступа к документам для отделов организации, коллектива сотрудников, работающих над отдельным проектом

12. За разглашение служебной тайны наступает ответственность по статье:

1) УК РФ Статья 283. Разглашение государственной тайны
2) УК РФ Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну
3) КоАП РФ Статья 13.14. Разглашение информации с ограниченным доступом
4) Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

13. Такой документопоток состоит из документов, создаваемых в данной организации и отправляемых за ее пределы:

1) Входящий
2) Внешний
3) Внутренний
4) Исходящий

14. Документ имеет две сущности:

1) информационную и материальную
2) общую и специальную
3) информационную и коммуникационную
4) информационную и специальную

15. нет такого вида цифровой подписи как:

1) простая электронная подпись
2) усиленная электронная подпись
3) квалифицированная электронная подпись
4) неквалифицированная электронная подпись
5) защищенная цифровая подпись

16. Документопотоки по направлению делятся на такие потоки:

1) параллельные и пересекающиеся
2) горизонтальные и вертикальные
3) входящие и уходящие

17. Из перечисленного, подсистема управления доступом системы защиты информации должна обеспечивать:

1) управление потоками информации
2) оповещение о попытках нарушения защиты
3) учет носителей информации
4) идентификация
5) аутентификация

18. Что из перечисленного относится к числу основных аспектов информационной безопасности:

1) подотчетность - полнота регистрационной информации о действиях субъектов
2) приватность - сокрытие информации о личности пользователя
3) конфиденциальность - защита от несанкционированного ознакомления

19. Компьютерная преступность в мире:

1) остается на одном уровне
2) снижается
3) растет

20. По документам ГТК количество классов защищенности АС от НСД:

1) 6
2) 9
3) 7
4) 8

21. Укажите, с какой целью строятся диаграммы для экспозиции (FEO).

1) для иллюстрации отдельных фрагментов модели
2) для иллюстрации альтернативной точки зрения
3) для иллюстрации специальных целей
4) для иллюстрации взаимосвязи между работами

22. Общепринятая методика подсчета документооборота предусматривает выражение его объема дробью, в числителе которой указывается количество:

1) копий, а в знаменателе – количество всех документов организации
2) подлинников, а в знаменателе – количество копий
3) копий, а в знаменателе – количество подлинников

23. Укажите, что входит в определение контекста модели.

1) определение субъекта моделирования
2) определение цели моделирования
3) определение точки зрения
4) определение количества уровней декомпозиции

24. Согласно "Оранжевой книге" верифицированную защиту имеет группа критериев

1) B
2) C
3) A
4) D

25. Верно ли следующее утверждение?

Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые:
позволяют установить факт изменения подписанного электронного документа после момента его подписания

1) да
2) скорее да
3) скорее нет
4) нет

26. Сформулируйте цель методологии проектирования ИС

1) регламентация процесса проектирования ИС и обеспечение управления этим процессом с тем, чтобы гарантировать выполнение требований как к самой ИС, так и к характеристикам процесса разработки
2) формирование требований, направленных на обеспечение возможности комплексного использования корпоративных данных в управлении и планировании деятельности предприятия
3) автоматизация ведения бухгалтерского аналитического учета и технологических процессов

27. Восстановление данных является дополнительной функцией услуги защиты

1) целостность
2) контроль доступа
3) аутентификация

4) причастность

28. Верно ли следующее утверждение?
Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые: не позволяют установить факт изменения подписанного электронного документа после момента его подписания;

1) да
2) нет
3) скорее да
4) скорее нет

29. Каким термином обозначается анализ регистрационной информации системы защиты?

1) мониторинг
2) аудит
3) аккредитация
4) сертификация

30. В модели политики безопасности Лендвера одноуровневый блок информации называется:

1) объектом
2) контейнером
3) множеством
4) массивом

31. Основными видами срокового контроля являются:

1) еженедельный, ежемесячный и ежеквартальный
2) текущий, предупредительный и итоговый
3) ручной и автоматизированный

32. Верно ли следующее утверждение?
Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые: обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки

1) да
2) скорее да

3) нет
4) скорее нет

33. Проверка подлинности пользователя по предъявленному им идентификатору — это:

1) идентификация
2) аутентификация
3) авторизация
4) аудит

34. Официальный документ – это:

1) любая информация, внесенная в базу данных
2) любой бумажный документ
3) информация, зафиксированная на каком-либо носителе, пригодном для достаточно долговременного хранения, и оформленная по действующим законодательным правилам

35. Защищенность системы защиты определяется как величина…

1) обратная суммарному количеству рисков
2) обратная остаточному риску
3) обратная уязвимости
4) равная сумме всех уязвимостей

36. Подготовка документа к сканированию включает в себя такие операции:

1) предварительную обработку изображений, нахождение полей, проверку распознанной информации
2) описание настройки системы и непосредственную подготовку документа
3) сканирование, контроль качества и возможное повторное сканирование

37. Под таким контролем понимают подготовку сведений о документах, срок исполнения которых истекает сегодня:

1) предупредительным
2) грамотным
3) финансовым
4) текущим

38. Верно ли следующее утверждение?
Для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые: позволяют создать электронную

подпись в формате, устанавливаемом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, и обеспечивающем возможность ее проверки всеми средствами электронной подписи.

1) да
2) скорее да
3) нет
4) скорее нет

39. Под таким контролем понимают аналитическое обобщение электронного документооборота, исполнительской дисциплины в организации и ее структурных подразделениях:

1) финансовым
2) итоговым
3) текущим
4) грамотным

40. Что из нижеперечисленного относится к оперативным методам повышения безопасности?

1) систематическое тестирование
2) предотвращение ошибок в CASE-технологиях
3) обязательная сертификация
4) программная избыточность

41. К сведениям в области государственной тайны НЕ относится:

1) об организации и о фактическом состоянии защиты государственной тайны
2) о мерах по обеспечению безопасности критической информационной инфраструктуры Российской Федерации и о состоянии ее защищенности от компьютерных атак
3) о фактах нарушения законности органами государственной власти и их должностными лицами
4) о методах и средствах защиты секретной информации
5) о результатах финансового мониторинга в отношении организаций и физических лиц, полученных в связи с проверкой их возможной причастности к террористической деятельности

42. Выделите внутренние по отношению к объекту уязвимости дестабилизирующие факторы и угрозы безопасности:

1) ошибки персонала при эксплуатации
2) ошибки программирования
3) сбой и отказы аппаратуры ЭВМ
4) ошибки алгоритмизации задач

43. Под таким контролем понимают подготовку сведений о документах, срок исполнения которых истекает через 2 — 3 дня:

1) предупредительным
2) текущим
3) грамотным
4) финансовым

44. Под электронной цифровой подписью понимается:

1) средство защиты от подделок или потерн данных в рукописных документах
2) реквизит электронного документа, предназначенный для его защиты от подделки и позволяющий идентифицировать владельца подписи
3) традиционная рукописная подпись, содержащая информацию об отправителе сообщения

45. Какой орган исполнительной власти в настоящее время выполняет функции Гостехкомиссиии России в области технической защиты информации?

1) ФСТЭК России
2) ФСБ России
3) МВД России
4) Роскомнадзор

46. В каком документе описан порядок проведения плановых и внеплановых проверок?

1) ФЗ “О государственной тайне”
2) Указ Президента “О проверках”
3) ФЗ “О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля”

4) ФЗ “О информации, информационных технологиях и о защите информации”

47. Верны ли следующие суждения?

Основными угрозами для системы электронного документооборота, как и для любой другой информационной системы, являются:
Угроза целостности информации – повреждение, искажение или уничтожение информации;
Угроза доступности информации – ошибки пользователей, внешние сетевые атаки, вредоносное ПО.

1) Верны оба
2) Неверны оба
3) Верна только 1 угроза
4) Верна только 2 угроза

48. В соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» для защиты информации используются правовые, организационные и технические меры, обеспечивающие:

1) истечение года со дня получения лицензии
2) истечение трех лет со дня получения лицензии
3) истечение года со дня проведения последней плановой проверки
4) истечение трех лет со дня проведения последней плановой проверки

49. Получение изображения документа включает в себя операции:

1) описание настройки системы и непосредственную подготовку документа
2) предварительную обработку изображений, нахождение полей, проверку распознанной информации
3) сканирование, контроль качества и возможное повторное сканирование

50. Как называется проверка соблюдения лицензиатом лицензионных требований, осуществляющаяся на территории лицензиата?

1) документальная
2) выездная
3) плановая
4) внеплановая

51. Наиболее надежным механизмом для защиты содержания сообщений является:

1) криптография
2) дополнительный хост
3) специальный аппаратный модуль
4) специальный режим передачи сообщения

52. Как называются методы защиты акустической информации, предусматривающие подавление технических средств разведки?

1) активные
2) пассивные
3) проактивные
4) превентивные

53. Как называется процесс приведения чего-либо к единой системе, форме, единообразию:

1) классификация
2) унификация
3) стандартизация

54. Распознавание предполагает выполнение следующих операций:

1) описание настройки системы и непосредственную подготовку документа
2) сканирование, контроль качества и возможное повторное сканирование
3) предварительную обработку изображений, нахождение полей, проверку распознанной информации

55. К информации ограниченного доступа НЕ относится:

1) адвокатская тайна
2) государственная тайна
3) врачебная тайна
4) тайна завещания
5) тайна свободы мысли

56. Гарантия сохранности данными правильных значений, которая обеспечивается запретом для
неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные — это:

1) целостность
2) конфиденциальность
3) доступность

57. Какой из приведенных ниже документов содержит требования и рекомендации в области технической защиты конфиденциальной информации?

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

2) ФЗ «О техническом регулировании»
3) СТР-К
4) Доктрина информационной безопасности Российской Федерации

58. Выберите рекомендации верные для защищаемых помещений (ЗП) в соответствии с СТР-К:

1) ЗП должны располагаться на первом этаже
2) ЗП не должны располагаться на первом этаже
3) ЗП должны находиться максимально близко к границам контролируемой зоны
4) ЗП должны быть удалены от границ контролируемой зоны
5) Ограждающие конструкции ЗП не должны быть смежными с помещениями других организаций
6) В ЗП не должно быть окон

59. Регистрации подлежат:

1) все документы, требующие специального учета, исполнения и использования в справочных целях, независимо от способа получения
2) только входящие и исходящие документы
3) только письма и обращения граждан

60. Перечисленные выше свойства электронной цифровой подписи НЕ позволяют использовать её в следующих основных целях электронной экономики и электронного документального и денежного обращения:

1) Использование в банковских платежных системах
2) Электронная коммерция (торговля)
3) Электронная регистрация сделок по объектам недвижимости
4) Для снятия информации с технических каналов связи
5) Таможенное декларирование товаров и услуг (таможенные декларации). Контролирующие функции исполнения государственного бюджета (если речь идет о стране) и исполнения сметных назначений и лимитов бюджетных обязательств (в данном случае если разговор идет об отрасли или о конкретном бюджетном учреждении). Управление государственными заказами

61. Реквизит документа – это:

1) обязательный символ в документе, расположенный в правом верхнем углу
2) логотип на официальном документе
3) обязательный элемент официального документа

62. Маршрутизаторы с фильтрацией пакетов осуществляют управление

доступом методом проверки

1) содержания сообщений
2) адресов отправителя и получателя
3) структуры данных
4) электронной подписи

63. Недостатком дискретных моделей политики безопасности является:

1) необходимость дополнительного обучения персонала
2) сложный механизм реализации
3) изначальное допущение вскрываемости системы
4) статичность

64. Если средства защиты могут быть преодолены только государственной спецслужбой, то согласно "Европейским критериям" безопасность считается:

1) стандартной
2) базовой
3) высокой
4) сверхвысокой

65. К информации ограниченного доступа НЕ относится

1) Секрет производства (ноу-хау)
2) Банковская тайна
3) Тайна перевода
4) Аудиторская тайна
5) Тайна следствия
6) Сведения о населении, содержащиеся в переписных листах

66. С точки зрения ГТК основной задачей средств безопасности является обеспечение:

1) защиты от НСД
2) простоты реализации
3) сохранности информации
4) надежности функционирования

67. Из перечисленного электронная почта состоит из:

1) прикрепленных файлов
2) тела письма
3) электронного ключа
4) расширенного содержания письма

5) краткого содержания письма

68. Верны ли следующие определения?

1. информация - сведения (сообщения, данные) независимо от формы их представления
2. электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

1) верны оба
2) неверны оба
3) верно 1
4) верно 2

69. Из перечисленного для аутентификации по личной подписи терминальных пользователей используются методы:

1) исследование динамических характеристик движения руки
2) фрагментарное сканирование
3) визуальное сканирование
4) исследование траектории движения руки

70. Как называется реквизит, отражающий основное содержание электронного документа:

1) текст
2) приложение
3) регистрационный номер

71. Модели политики безопасности на основе анализа угроз системе исследуют вероятность преодоления системы защиты

1) за определенное время
2) фиксированными затратами
3) ограниченной компетенцией злоумышленника
4) фиксированным ресурсом

72. Верны ли следующие определения?

доступ к информации - возможность получения информации и ее использования

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц

1) верны оба
2) неверны оба
3) верно 1
4) верно 2

73. В многоуровневой модели, если субъект доступа формирует запрос на чтение-запись, то уровень безопасности субъекта относительно уровня безопасности объекта должен:

1) доминировать
2) быть меньше
3) специально оговариваться
4) быть равен

74. Из перечисленного услуга обеспечения доступности реализуется на уровнях:

1) канальном
2) сетевом
3) прикладном
4) физическом
5) транспортном

75. К информации, которая может быть засекречена НЕ относится:

1) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях
2) о фактах нарушения законности органами государственной власти и их должностными лицами
3) о лицах, оказывающих содействие контрразведывательным органам
4) о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям
5) составляющие информацию о состоянии окружающей среды (экологическую информацию)

76. Стандарт DES основан на базовом классе

1) гаммирование
2) блочные шифры

3) замещения
4) перестановки

77. Реквизиты характерные только для бланка письма – это:

1) справочные данные об организации
2) трафаретные части реквизитов «дата», «номер документа»
3) эмблема организации

78. К информации которая может быть засекречена относится:

1) об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства
2) о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, об их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов
3) о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
4) составляющие информацию о состоянии окружающей среды (экологическую информацию)

79. Организационные меры включают:

1) документированные процедуры и правила работы с разными видами информации, IT-сервисами, средствами защиты
2) подбор персонала и его инструктаж
3) обеспечение режимности объекта
4) заключение соглашений

80. Процесс определения риска, применения средств защиты для сокращения риска с последующим определением приемлемости остаточного риска, называется:

1) оптимизацией средств защиты
2) мониторингом средств защиты
3) управлением риском
4) минимизацией риска

81. При качественном подходе риск измеряется в терминах

1) оценок экспертов
2) денежных потерь
3) заданных с помощью шкалы или ранжирования
4) объема информации

82. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство

1) восстанавливаемость
2) детермированность
3) доступность
4) целостность

83. К Службам, организующим защиту информации на уровне предприятий (банков и др.) не относится:

1) отдел экономической безопасности
2) служба безопасности персонала (режимный отдел)
3) службы информационной безопасности
4) отдел кадров
5) юридический отдел

84. Из перечисленного формами причастности являются:

1) аутентификация
2) контроль доступа
3) к посылке сообщения
4) подтверждение получения сообщения

85. Из перечисленного, различают модели воздействия программных закладок на компьютеры:

1) уборка мусора
2) наблюдение и компрометация
3) перехват
4) внедрение
5) искажение

86. Действие программных закладок основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютере в рамках модели

1) компрометация
2) искажение
3) перехват
4) наблюдение

87. С использованием прикладных ресурсов ИС связан уровень ОС:

1) приложений
2) системный
3) внешний
4) сетевой

88. верно ли следующее утверждение:
Организационно-технические меры предусматривают использование звукопоглощающих средств. Пористые и мягкие материалы типа ваты, ворсистые ковры, пенобетон, пористая сухая штукатурка являются хорошими звукоизолирующими и звукопоглощающими материалами - в них очень много поверхностей раздела между воздухом и твердым телом, что приводит к многократному отражению и поглощению звуковых колебаний.

1) верно
2) неверно
3) скорее верно
4) скорее неверно

89. Конкретизацией модели Белла-ЛаПадула является модель политики безопасности

1) С полным перекрытием
2) Лендвера
3) На основе анализа угроз
4) LWM

90. Как предотвращение неавторизованного использования ресурсов определена услуга защиты

1) причастность
2) контроль доступа
3) целостность
4) аутентификация

91. Из перечисленного в обязанности сотрудников группы информационной безопасности входят:

1) устранение дефектов аппаратной части
2) управление доступом пользователей к данным
3) исправление ошибок в программном обеспечении
4) расследование причин нарушения защиты

92. Система защиты должна гарантировать, что любое движение данных

1) контролируется, кодируется, фиксируется, шифруется

2) копируется, шифруется, проектируется, авторизуется
3) анализируется, идентифицируется, шифруется, учитывается
4) идентифицируется, авторизуется, обнаруживается, документируется

93. При полномочной политике безопасности совокупность меток с одинаковыми значениями образует:

1) область равной критичности
2) уровень безопасности
3) область равного доступа
4) уровень доступности

Задания в открытой форме

1. Документооборот – это…
2. Аутентификация – это…
3.Проверка подлинности пользователя по предъявленному им идентификатору — это:
4. Реквизит документа – это:
5. Применение услуги причастности рекомендуется на _____ уровне модели OSI.
6. Формирование пакетов данных реализуется на _____ уровне модели взаимодействия открытых систем.
7. В модели политики безопасности Лендвера ссылка на сущность, если это идентификатор сущности, называется ...
8. Реквизиты характерные только для бланка письма – это:
9. Регистрация – это:
10. При передаче по каналам связи на канальном уровне избыточность вводится для:
11. Официальный документ – это:
12. По умолчанию право на подключение к общей базе данных предоставляется:
13. Хэш-значение – это … сообщения, т.е. сжатое двоичное представление основного сообщения произвольной длины, формируемое функцией хэширования:
14. В модели политики безопасности Лендвера ссылка на сущность, если это последовательность имен сущностей, называется ...
15. Гарантия сохранности данными правильных значений, которая обеспечивается запретом для
неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные — это:
16. ACL-список ассоциируется с каждым…
17. Маршрутизация и управление потоками данных реализуются на ______ уровне модели взаимодействия открытых систем.

18. Обеспечение взаимодействия удаленных процессов реализуется на _____ уровне модели взаимодействия открытых систем.
19. Поддержка диалога между удаленными процессами реализуется на _____ уровне модели взаимодействия открытых систем.
20. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это:

Задания на установление соответствия

1. Установите взаимно однозначное соответствие

1	Биометрические персональные данные	А	Информация о личности человека: расовая и национальная принадлежность, политические, религиозные и философские взгляды, состояние здоровья, подробности интимной жизни, информация о судимостях.
2	Общие персональные данные	Б	Это физиологические или биологические особенности человека, которые используют для установления его личности. К ним могут относиться фотографии, отпечатки пальцев, группа крови, генетическая информация.
3	Специальные персональные данные	В	К ним законодательство о персональных данных относит базовые личные данные: ФИО, место регистрации, информация о месте работы, номер телефона, email.

2. Установите взаимно однозначное соответствие

1	ИС управления технологическими процессами	А	предназначены для автоматизации функций инженеров-проектировщиков, конструкторов, архитекторов, дизайнеров при создании новой техники или технологии.
2	ИС автоматизированного проектирования	Б	используются для автоматизации всех функций фирмы и охватывают весь цикл работ от планирования деятельности до сбыта

			продукции.
3	Интегрированные (корпоративные) ИС	В	оказывает устойчивую тенденцию роста спроса на информационные системы организационного управления.
4	Анализ современного состояния рынка ИС	Г	служат для автоматизации функций производственного персонала по контролю и управлению производственными операциями.

3. Установите взаимно однозначное соответствие

1	Гибкость системы-	А	определяется как частное от деления фактического количества группировок на величину емкости системы.
2	Емкость системы-	Б	это способность допускать включение новых признаков, объектов без разрушения структуры классификатора.
3	Степень заполненности системы-	В	это наибольшее количество классификационных группировок, допускаемое в данной системе классификации.

4. Установите взаимно однозначное соответствие

1.	Целостность	А	свойство информации, гарантирующее, что доступ к информации имеет доступ только определенные лица.
2	Конфиденциальность	Б	свойство информации, гарантирующее, что только определенные лица могут менять информацию.
3	Доступность	В	свойство информации, гарантирующее, что лица имеющие доступ к информации в нужный момент смогут получить доступ.

5. Установите взаимно однозначное соответствие

1	Конфиденциальный аспект	А	Это комплексная работа при защите данных, которая

			обеспечит защиту от сбоев в работе и уничтожения самих данных.
2	Целостностный аспект	Б	Включает в себя обеспечение надежного и эффективного доступа к защищаемой информации только проверенных лиц.
2	Аспект доступности	В	Означает, что нужно тщательно контролировать работу с данными, чтобы устранить возможность их утечки, а также предотвратить несанкционированный доступ к ним со стороны неизвестных людей

6. Установите взаимно однозначное соответствие

1	Форма собственности	А	Майоров Юрий Станиславович
2	Вид деятельности	Б	18
3	Руководитель	В	"Торговый дом "Демидовский"
4	Количество штатных единиц	Г	Общество с ограниченной ответственностью

7. Установите взаимно однозначное соответствие

1	Антивирусная программа-	А	специализированное программное обеспечение, предназначенное для защиты компании от утечек информации
2	CloudAV-	Б	специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ .
3	DLP-решения-	В	заключается в преобразовании ее составных частей (слов, букв, слогов, цифр) с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду
4	Криптографическое	Г	одно из облачных решений

	преобразование-		информационной безопасности, что применяет легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдер

8. Установите взаимно однозначное соответствие

1.	Автоматизированная обработка персональных данных	А	с помощью средств вычислительной техники. Это компьютеры, телефоны и другие электронные устройства, базы данных, криптографические средства защиты, программы, скрипты.
2	Смешанная обработка персональных данных	Б	без автоматизации.
3	Неавтоматизированная обработка персональных данных	В	обработка человеком при участии средств вычислительной техники. Например, когда в бухгалтерии вбивают в программу данные из бумажного заявления на отпуск.

9. Средства ИБ ЭД и решаемые ими задачи

1	Технические	А	Разграничение прав пользователей к конфиденциальной информации, Контроль целостности информации, Подлинность информации, Защита информации в случаи кражи или утечки по каналам связи
2	Программные	Б	Создание резервных копий на случай выхода оборудования из строя, Разграничение локального и сетевого трафика предприятия, Средства аутентификации и авторизации пользователей к

			ресурсам сети
3	Организационно-правовые	В	Уменьшение количества допускаемых ошибок в процессе обработки информации
4	Криптографические	Г	Защиту ПО и информации от вирусов, Защиту от НСД, Аутентификация и авторизация пользователей

10. Установите взаимно однозначное соответствие

1	Идентификация	А	это процедура проверки подлинности
2	Аутентификация	Б	это процедура распознавания субъекта по его идентификатору
3	Авторизация	В	это предоставление доступа к какому-либо ресурсу

11. Установите взаимно однозначное соответствие

1	Пароль	А	пластиковая карта, ключ от замка, USB-ключ
2	Устройство	Б	отпечаток пальца, портрет, сетчатка глаза
3	Биометрика	В	слово, PIN-код, код для замка, графический ключ

12. Установите взаимно однозначное соответствие

1	Операционная гарантированность	А	охватывает весь жизненный цикл ИС, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения.
2	Технологическая гарантированность	Б	это совокупность защитных механизмов ИС
3	Доверенная вычислительная база	В	относится к архитектурным и реализационным аспектам системы

13. Установите взаимно однозначное соответствие

1	Произвольное управление доступом-	А	Представляют собой свойства (характеристики) объектов и (или) субъектов доступа
2	Безопасность повторного использования объектов-	Б	основано на сопоставлении меток безопасности субъекта и объекта.
3	Метки безопасности-	В	это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит.
4	Принудительное (или мандатное) управление доступом-	Г	важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора"

14. Основные средства обеспечения ИБ ЭД и их методы

1	Технические	А	Использования криптографических средств шифрования конфиденциальной информации
2	Программные	Б	введения учета ознакомления сотрудников с информацией ограниченного распространения
3	Организационно-правовые	В	физическое разграничение сетевого оборудования
4	Криптографические	Г	использование программных средств идентификации и аутентификации пользователей

15. Установите взаимно однозначное соответствие

1	Математическое и программное обеспечение	А	совокупность правовых норм, определяющих создание,

	(МО, ПО)-		юридический статус и функционирование информационных систем, регламентирующих порядок получения, преобразования и использования информации
2	Организационное обеспечение (ОО)-	Б	совокупность математических методов, моделей, алгоритмов и программ для реализации целей и задач информационной системы, а также нормального функционирования комплекса технических средств
3	Правовое обеспечение (Пр.О) -	В	совокупность методов и средств, регламентирующих взаимодействие работников с техническими средствами и между собой в процессе разработки и эксплуатации информационной системы.

16. Соотнести основные угрозы СЭД со способом нейтрализации угроз.

1	Угроза целостности	А	Ошибки пользователя, компьютерные атаки, вредоносное ПО
2	Искажение информации	Б	Повреждение или уничтожение информации.
3	Угроза работоспособности системы	В	Кража информации, подмена маршрутов следования, НСД
4	Угроза конфиденциальности	Г	Сбои и ошибки, повреждение, подмена.

17. Установите взаимно однозначное соответствие

1	Утрата информации	А	результат такого воздействия, последствием которого является постоянное или временное отсутствие возможности осуществлять над компьютерной информацией операции
2	Блокировка информации	Б	Нарушение целостности переданных данных путем

			несанкционированного удаления, вставки, изменения, изменения порядка следования, повторного использования или задержки.
3	Искажение информации	В	физическое уничтожение информации. Цель защиты информации – противодействие угрозам безопасности информации.
4	Несанкционированное копирование информации	Г	воспроизведение, с превышением предоставленных собственником прав доступа, компьютерной информации с ограниченным доступом с сохранением исходной информации.

18. Установите взаимно однозначное соответствие

1	CRM-	А	программная система, охватывающая ключевые процессы деятельности и управления, позволяющая получить самый общий взгляд на работу предприятия
2	SCM-	Б	система планирования потребностей в материалах, одна из наиболее популярных в мире логистических концепций, на основе которой разработано и функционирует большое число микрологистических систем
3	MRP-	В	управления цепочками поставок
4	ERP-	Г	управление отношениями с клиентами - бизнес-стратегия, предназначенная для оптимизации доходов, прибыльности и

			удовлетворенности клиентов

19. Установите взаимно однозначное соответствие

1	Аппаратный RAID	А	микрочип, установленный на материнскую плату, который берет на себя часть функционала аппаратного RAID-контроллера, работая в паре с центральным процессором. Этот подход работает чуть быстрее, чем программный RAID, но надежность у такого массива оставляет желать лучшего.
2	Интегрированный аппаратный RAID	Б	отдельный контроллер с собственным процессором и кэширующей памятью, полностью забирающий на себя выполнение всех дисковых операций. Наиболее затратный, однако, самый производительный и надежный вариант для использования.
3	Программный RAID	В	наименее затратный вариант, но и наименее производительный. Массив создается средствами операционной системы, вся нагрузка по обработке данных «ложится на плечи» центрального процессора.

20. Установите взаимно однозначное соответствие

1	Соответствие направлению импортозамещения-	А	наличие и состав индивидуально настраиваемых параметров, гибкость настройки позволят оценить применимость решения к принятой парадигме развития процессов обеспечения ИБ
2	Функциональные	Б	наличие развитых встроенных

	особенности-		и интегрируемых подсистем позволит в начальном периоде эксплуатации ограничиться использованием одного продукта, без увеличения количества используемых интерфейсов
3	Интеграционные возможности-	В	отчетность, и удобство, и глубина погружения при навигации в рамках интерфейса системы
4	Дополнительные критерии-	Г	позволит оценить, можно ли использовать решение в рамках государственных инициатив по поддержке отечественного производителя и борьбе с санкциями.

Задания на установление правильной последовательности

1. При подготовке к внедрению электронного документооборота необходимо

1. Анализ бизнес-процессов организации
2. Анализ возможных конфигураций аппаратно-программных средств, необходимых для внедрения СЭД
3. Состояние используемого оборудования и технологий
4. Разработка информационно-функциональной модели предприятия, реинжиниринг бизнес-процессов

2. Установить последовательность этапов внедрения системы безопасности
1. Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта
2. Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению
3. Установка и настройка средств защиты информации
4. Испытания и опытная эксплуатации системы защиты информации

3. Установить порядок проведения аттестации информационных систем по требованиям безопасности информации

1. Проведение аттестационных испытаний объекта
2. Предварительное ознакомление с аттестуемым объектом (при необходимости)
3. Оформление, регистрация и выдача аттестата соответствия
4. Подача и рассмотрение заявки на аттестацию
5. Разработка программы и методики аттестационных испытаний

4. Определить этапы уровня защищенности персональных данных
1. классификация информационной системы
2. сбор и анализ исходных данных по информационной системе
3. установление уровня защищенности персональных данных и его документальное оформление
4. формирование модели угроз и определение категории нарушителя

5. Процесс документооборота
1. Создание документа
2. Исполнение документа
3. Отправка документа
4. Получение документа

6. Установить последовательность этапов методического процесса построения корпоративной системы защиты от вирусов

1. Разработка политики антивирусной безопасности
2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности
3. Реализация плана антивирусной безопасности
4. Разработка плана обеспечения антивирусной безопасности

7. Установить порядок обеспечения защиты информации

1. Проверяется эффективность принятых мер
2. Составляется перечень коммерческих тайн и сведений, не подлежащих разглашению
3. Разрабатываются способы хранения информации (использование электронных носителей, бумажных документов, технических средств обработки)

8. Установить последовательность клиент-серверной архитектуры

1. клиентские компьютеры выступают потребителями

2. серверы являются поставщиками услуг (сервисов)
3. информационная система

9. Установить последовательность многозвенной архитектуры

1. Уровень данных
2. Представление
3. Уровень логики
4. Данные
5. Уровень представления

10. Установить последовательность этапов архитектуры распределенных систем с репликацией

1. Репликация
2. Сервер без данных
3. Клиентская ЭВМ
4. Репликация

11. Установить последовательность итерационного процесса разработки и реализации политики ИБ

1. Принципы контроля состояния систем защиты информации
2. Вопросы резервного копирования данных и информации
3. Принципы администрирования системы ИБ и управление доступом к вычислительным и телекоммуникационным средствам, программам и информационным ресурсам,
4. Принципы использования информационных ресурсов персоналом компании и внешними пользователями
5. антивирусную защиту и защиту против действий хакеров

12. Установить последовательность распределения ответственности за обеспечение безопасности

1. Назначение для каждого ресурса (или процесса) ответственного сотрудника из числа руководителей
2. Определение и документальное закрепление для каждого ресурса списка прав доступа (матрицы доступа)
3. Определение ресурсов, имеющих отношение к информационной безопасности по каждой системе

13. Установить последовательность ролевого управления доступом

1. Сеанс работы пользователя
2. Объект

3. Пользователь
4. Роль
5. Операция

14. Установить последовательность Метода OCTAVE

1. Осуществляется оценка организационных аспектов
2. Проводится разработка стратегии обеспечения безопасности
3. Высокоуровневый анализ ИТ-инфраструктуры организации
4. Определяются требования безопасности
5. Сроится профиль угроз для каждого критического ресурса

15. Установить последовательность возникновения плана обработки рисков метода OCTAVE

1. Атака на данные системы электронного документооборота
2. Выход из строя системы эл. документооборота или изменение/уничтожение данных на ресурсе
3. Атака на данные сервера разработки
4. Выход из строя сервера разработки или уничтожение изменение данных на данном ресурсе

16. Установить последовательность полной обработки рисков

1. Выход из строя сервера разработки или изменение/ уничтожение данных
2. Выход из строя СЭД или изменение/уничтожение данных
3. Угроза
4. Атака на данные СЭД
5. Атака на данные сервера разработки

17. Установить последовательность этапов проектирования информационных систем

1. Требуемой пропускной способности системы
2. Определения цели проекта
3. Требуемой функциональности системы и уровня ее адаптивности к Изменяющимся условиям функционирования
4. Безотказной работы системы
5. Простоты эксплуатации и поддержки системы

18. Установить последовательность этапов ЖЦ построения и последовательного преобразования ряда согласованных моделей

1. Требований к приложениям

2. Организации
3. Проекта ИС
4. Требований к ИС

19. Установить последовательность этапов создания ИС

1. Реализация
2. Формирование требований к системе
3. Ввод в действие
4. Тестирование
5. Проектирование

20. Определить методы защиты информации в СЭД.

1. Выявить преимущества электронного документооборота на предприятии
2. Дать определение понятия электронный документооборот
3. Описать угрозы для СЭД
4. Описать структуру СЭД
5. Привести пример построение защищенной модели электронного документооборота организации.
6. Описать основные методы защиты информации в СЭД

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. Анализ уязвимостей системы электронного документооборота: Вам предстоит провести анализ системы электронного документооборота организации и выявить потенциальные уязвимости. Задача включает в себя исследование протоколов передачи данных, механизмов аутентификации и шифрования, а также методов контроля доступа. На основе анализа необходимо предложить меры по устранению уязвимостей и повышению уровня безопасности системы.

2. Разработка политики безопасности для системы электронного документооборота: Ваша задача - разработать политику безопасности, которая определит правила и процедуры защиты информации в системе электронного документооборота. Политика должна включать в себя требования к аутентификации пользователей, шифрованию данных, контролю доступа, резервному копированию и управлению уязвимостями. При разработке политики необходимо учесть специфику организации и соответствующие регуляторные требования.

3. Выбор и внедрение средств защиты информации: Вам предстоит выбрать и внедрить средства защиты информации в систему электронного документооборота. Задача включает в себя изучение различных методов и средств защиты, таких как межсетевые экраны, антивирусное программное обеспечение, системы обнаружения вторжений и системы контроля целостности данных. На основе анализа требований и бюджета организации необходимо выбрать оптимальные средства защиты и провести их внедрение.

4. Анализ уязвимостей системы электронного документооборота: Проведите анализ уязвимостей выбранной системы электронного документооборота. Определите потенциальные уязвимые места, которые могут быть использованы злоумышленниками для несанкционированного доступа, подделки документов или утечки конфиденциальной информации.

5. Разработка стратегии шифрования данных: Разработайте стратегию шифрования данных в системе электронного документооборота. Определите, какие данные требуют шифрования, выберите подходящие алгоритмы шифрования и разработайте ключевое управление для обеспечения конфиденциальности и целостности данных.

6. Внедрение системы электронной цифровой подписи: Разработайте и внедрите систему электронной цифровой подписи (ЭЦП) в систему электронного документооборота. Определите правила создания и проверки ЭЦП, выберите подходящие алгоритмы и сертификационные авторитеты, а также обеспечьте безопасное хранение и управление ключами ЭЦП.

7. Анализ системы электронного документооборота: Проведите анализ системы электронного документооборота в организации и определите ее уязвимости в области защиты информации. Используйте методы оценки рисков и угроз для выявления возможных уязвимостей, таких как незащищенные каналы связи, слабая аутентификация или недостаточные механизмы шифрования.

8. Разработка политики безопасности: Разработайте политику безопасности для системы электронного документооборота, включающую методы и средства защиты информации. Определите требования к шифрованию данных, аутентификации пользователей, контролю доступа и аудиту. Разработайте процедуры для реагирования на инциденты безопасности и обучения сотрудников правилам использования системы.

9. Внедрение системы электронной подписи: Вашей задачей является внедрение системы электронной подписи в систему электронного документооборота. Определите требования к сертификации и управлению ключами, выберите подходящий алгоритм электронной подписи и разработайте процедуры проверки подлинности документов.

10. Защита от несанкционированного доступа: Разработайте механизмы защиты от несанкционированного доступа к документам в системе электронного документооборота. Включите механизмы шифрования данных, контроль доступа на основе ролей и прав, а также систему мониторинга и обнаружения необычной активности.

11. Аудит и мониторинг системы: Разработайте механизмы аудита и мониторинга для системы электронного документооборота. Определите события, которые требуется отслеживать, и настройте систему для регистрации и анализа этих событий. Разработайте процедуры анализа логов и реагирования на возможные инциденты безопасности.

12. Анализ уязвимостей системы электронного документооборота: Ваша задача - провести анализ системы электронного документооборота и выявить потенциальные уязвимости. Используя знания о методах и средствах защиты информации, определите уязвимые места в системе, такие как неаутентифицированный доступ, утечка данных или возможности подмены документов.

13. Разработка политики безопасности системы: Вам необходимо разработать политику безопасности для системы электронного документооборота. Задача включает определение правил доступа к

документам, установку криптографической защиты, аутентификацию пользователей и управление ключами шифрования. Разработайте комплексную политику, учитывающую специфику системы и требования безопасности.

14. Выбор и реализация методов шифрования: Ваша задача - выбрать и реализовать подходящие методы шифрования для защиты информации в системе электронного документооборота. Используйте знания о симметричных и асимметричных алгоритмах шифрования, цифровых подписях и протоколах безопасной передачи данных. Разработайте систему шифрования, которая обеспечит конфиденциальность и целостность документов.

15. Оценка стойкости системы шифрования: Вам предстоит оценить стойкость системы шифрования в системе электронного документооборота. Используя математический анализ алгоритмов шифрования, проведите оценку стойкости относительно различных видов атак, таких как атаки перебором или криптоанализ. Предложите улучшения или замены алгоритмов, если это необходимо.

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.