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

Информационно-аналитические системы 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. Сущность, структура и задачи аналитики СБ.

1. Что представляет собой сущность аналитики в области безопасности (СБ)?
2. Каковы основные задачи аналитики СБ при обеспечении безопасности организации?
3. Какие компоненты входят в структуру аналитической работы в области СБ?
4. Каким образом аналитика СБ способствует выявлению и анализу угроз безопасности?
5. Как важна аналитика СБ для принятия эффективных решений и разработки стратегии безопасности организации?
6. Какие методы и техники используются аналитиками СБ для предотвращения инцидентов безопасности?
7. Каким образом аналитика СБ помогает в поиске и раскрытии внутренних угроз?
8. Как аналитическая работа в области СБ помогает в предсказании и прогнозировании возможных угроз безопасности?
9. Как влияет аналитика СБ на эффективность и результативность действий оперативных служб по обеспечению безопасности?
10. Какие навыки и компетенции требуются у аналитиков СБ для успешного выполнения своих задач?

Тема 2. Аналитика как интерфейс между теорией и практикой.

1. Как аналитика в области СБ выполняет роль интерфейса между теорией и практикой?
2. Как аналитика СБ помогает в переводе теоретических сведений в конкретные действия и решения?
3. Какие методы и инструменты используются аналитиками СБ для преобразования теории в практические рекомендации?
4. Как аналитика СБ связывает технические аспекты безопасности с бизнес-потребностями организации?
5. Как аналитика СБ помогает в оценке эффективности существующих политик и процедур безопасности и вносит рекомендации по их улучшению?
6. Каким образом аналитика СБ учитывает динамику развития технологий и угроз в своей работе?
7. Как аналитика СБ помогает в обучении и развитии персонала, осознавать значимость безопасности и соблюдать соответствующие процедуры?

8. Какие вызовы и проблемы возникают при переводе теории в практику через аналитический процесс СБ?

9. Как аналитика СБ содействует передаче знаний и опыта между различными уровнями и подразделениями организации?

10. Каким образом аналитика СБ способствует повышению информированности и осведомленности руководства о текущей ситуации с безопасностью?

Тема 3. Принципы организации аналитической деятельности в СБ.

1. Какие принципы лежат в основе организации аналитической деятельности в области СБ?

2. Как принцип коллективности влияет на эффективность аналитической работы в СБ?

3. Как принцип системности помогает обеспечить полноту и объективность аналитических исследований в СБ?

4. Как принцип актуальности обеспечивает своевременное выявление и реагирование на угрозы безопасности?

5. Как принцип конфиденциальности влияет на сохранение и защиту информации в аналитической деятельности СБ?

6. Как принцип независимости гарантирует объективность и непредвзятость аналитических выводов в СБ?

7. Как принцип постоянного обучения и развития способствует повышению профессионального уровня аналитиков СБ?

8. Каким образом принцип сегментации информации влияет на эффективность аналитической работы в СБ?

9. Как принцип оперативности и своевременности способствует эффективному реагированию на изменения среды и угроз безопасности?

10. Как принцип прозрачности и документирования помогает обеспечить юридическую значимость и анализируемости аналитической работы в СБ?

Тема 4. Технологический цикл информационно-аналитической работы.

1. Каковы этапы технологического цикла информационно-аналитической работы в области СБ?

2. Что включает первый этап технологического цикла - сбор информации в аналитике СБ?

3. Как осуществляется анализ и интерпретация собранных данных в информационно-аналитической работе СБ?

4. Каким образом принимаются решения и формулируются рекомендации на основе проведенного анализа в технологическом цикле СБ?

5. Каким способом осуществляется контроль и обратная связь на завершающем этапе технологического цикла информационно-аналитической работы в СБ?

6. Какие методы и инструменты используются на этапе сбора информации в аналитике СБ?

7. Как аналитика СБ выбирает и применяет методы структурирования и анализа данных на этапе обработки информации?

8. Как представление информации и ее визуализация влияют на эффективность аналитического процесса в СБ?

9. Какие подходы используются для автоматизации и оптимизации технологического цикла информационно-аналитической работы в аналитике СБ?

10. Как информационно-аналитическая работа в СБ учитывает требования по защите данных и конфиденциальности?

Тема 5. Аналитический режим потребления информации.

1. Что представляет собой аналитический режим потребления информации в области СБ?

2. Какой подход следует использовать для построения аналитического режима потребления информации в аналитике СБ?

3. Как аналитический режим помогает в обнаружении скрытых угроз и аномалий в информационной безопасности?

4. Каким образом аналитический режим способствует эффективному использованию информации для принятия решений в СБ?

5. Какие преимущества получает организация при внедрении аналитического режима потребления информации в аналитике СБ?

6. Какие навыки и инструменты необходимы аналитику СБ для эффективного использования аналитического режима?

7. Как аналитический режим помогает в прогнозировании и предотвращении инцидентов безопасности?

8. Как аналитический режим способствует постоянному мониторингу и анализу потенциальных угроз безопасности?

9. Каким образом аналитический режим фокусируется на поиске новых трендов и возможных уязвимостей?

10. Как аналитический режим потребления информации способствует принятию оперативных мер и реагированию на угрозы безопасности в реальном времени?

Тема 6. Синтез информационно-аналитических СБ.

1. Что означает синтез информационно-аналитических решений в области СБ?

2. Какие методы и подходы применяются для синтеза информационно-аналитических СБ?

3. Как синтез информационно-аналитических решений помогает преодолеть сложности и неопределенность в области безопасности?

4. Каким образом синтез информационно-аналитических СБ способствует выявлению скрытых связей и паттернов в данных?

5. Как аналитика СБ интегрирует различные источники информации и аналитические методы для синтеза полной картины безопасности?

6. Как синтез информационно-аналитических решений помогает прогнозированию и предотвращению будущих угроз безопасности?

7. Как аналитика СБ применяет синтез информационно-аналитических решений для разработки стратегии безопасности организации?

8. Какие вызовы и проблемы возникают при синтезе информационно-аналитических решений в области СБ?

9. Каким образом синтез информационно-аналитических СБ помогает в принятии комплексных и обоснованных решений в области безопасности?

10. Как аналитика СБ управляет информацией, полученной в результате синтеза, для предоставления ценных выводов и рекомендаций?

Тема 7. Информационно аналитические системы аутентификации.

1. Что представляют собой информационно-аналитические системы аутентификации?

2. Как работают информационно-аналитические системы аутентификации для обеспечения безопасности?

3. Какие основные методы и технологии используются в информационно-аналитических системах аутентификации?

4. Как информационно-аналитические системы аутентификации обеспечивают защиту от подделки или манипуляции идентификационных данных?

5. Каким образом информационно-аналитические системы аутентификации способствуют контролю и управлению доступом к информации?

6. Как информационно-аналитические системы аутентификации используют анализ поведения пользователей для определения аномалий и потенциальных угроз?

7. Каким образом информационно-аналитические системы аутентификации применяют многофакторную аутентификацию для повышения безопасности?

8. Как информационно-аналитические системы аутентификации обеспечивают учет и аудит доступа к информации?

9. Какие вызовы и проблемы возникают при разработке и использовании информационно-аналитических систем аутентификации?

10. Как информационно-аналитические системы аутентификации способствуют удовлетворению требований по безопасности данных и соответствию нормативным актам в области безопасности?

Тема 8. Информационно аналитические системы защиты от несанкционированного доступа (НСД).

1. Как работают информационно-аналитические системы НСД для обеспечения безопасности?
2. Какие методы и технологии используются в информационно-аналитических системах НСД для обнаружения и предотвращения атак?
3. Как информационно-аналитические системы НСД помогают в обнаружении уязвимостей и слабых мест в защите информации?
4. Как информационно-аналитические системы НСД реагируют на аномальное поведение и атаки в реальном времени?
5. Каким образом информационно-аналитические системы НСД анализируют события и логи для выявления инцидентов безопасности?
6. Как информационно-аналитические системы НСД используют искусственный интеллект и машинное обучение?
7. Какие информационно аналитические системы защиты от несанкционированного доступа (НСД)?
8. Какие преступления в области НСД в России Вам известны?
9. Что представляют собой информационно-аналитические системы защиты от несанкционированного доступа (НСД)?
10. Что такое НСД? Виды НСД.

Критерии оценки:

2 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 балл 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 ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1 «Анализ информации на предприятии»

1. Дать определение понятию « безопасность информации».

2. Какие действия понимаются под безответственностью пользователя?

3. Критерии оценки информационных систем.

4. Какие параметры защиты не учитываются концепцией защиты информации?

5. На чем основан механизм одобрения для защищенных систем?

6. Какие методы анализа информации на предприятии могут помочь в принятии стратегических решений?

7. Какие типы данных обычно анализируются на предприятии?

8. Какие преимущества может принести анализ информации на предприятии для улучшения операционной эффективности?

9. Как можно использовать анализ информации для выявления новых рыночных возможностей?

10. Какие инструменты и технологии используются в анализе информации на предприятии?

Практическая работа №2 «Применение навыков анализа на примере Business Objects»

1. Функциональные характеристики критериев
2. Что такое построение диаграмм ?
3. Что такое имитационное моделирование?
4. Что такое прототипирование?
5. Назовите общие функции.
6. Какие функции и возможности предоставляет Business Objects для анализа данных?
7. Какие типы отчетов можно создавать с помощью Business Objects?
8. Какие навыки анализа данных могут пригодиться при работе с Business Objects?
9. Какие инструменты и методы в Business Objects помогают в проведении мультимодального анализа данных?
10. Какие преимущества имеет использование Business Objects для анализа данных по сравнению с другими инструментами?

Практическая работа №3 «Основные понятие информационно-аналитических систем».

1. Что такое аналитика в целом?
2. Что такое информационно-аналитическая система? Приведите примеры.
3. Что такое OSINT?
4. В чем заключается сущность и задачи информации?
5. Основные схемы сертификации средств защиты информации.
6. Что такое информационно-аналитические системы и как они используются в бизнесе?

7. Какие основные компоненты входят в информационно-аналитическую систему?

8. Какие методы анализа данных применяются в информационно-аналитических системах?

9. Как информационно-аналитические системы помогают в выявлении трендов и паттернов в данных?

10. Какие преимущества имеют информационно-аналитические системы по сравнению с традиционными методами анализа данных?

Практическая работа №4 «Оперативный анализ данных»

1. В каких случаях обязательно выполнение рекомендаций регулятора?
2. Что регламентируют нормы ФСТЭК?
3. Что относится к документам государственной организации?
4. Методы проверки в ходе аттестации.
5. Какие функции осуществляет ФСТЭК России в пределах своей компетенции?
6. Что такое оперативный анализ данных и как он отличается от стратегического анализа данных?
7. Какие методы и инструменты используются для оперативного анализа данных?
8. Как оперативный анализ данных помогает в принятии оперативных решений?
9. Какие преимущества имеет использование реального времени в оперативном анализе данных?
10. Какие вызовы и проблемы могут возникнуть при оперативном анализе больших объемов данных?

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.

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. Задача по внедрению информационно-аналитической системы безопасности в производственное предприятие: Ваша задача - внедрить информационно-аналитическую систему безопасности в производственную среду. Определите требования предприятия, проведите анализ существующих систем безопасности, разработайте и внедрите систему, которая будет способна собирать, анализировать и визуализировать данные о безопасности в реальном времени.

2. Задача по разработке системы мониторинга производственной безопасности: Ваша задача - разработать систему мониторинга производственной безопасности с использованием информационно-аналитической системы. Определите ключевые параметры и показатели безопасности, такие как условия рабочей среды, работа оборудования, защитные меры и другие факторы. Разработайте систему мониторинга, которая будет предупреждать о потенциальных угрозах и обеспечивать быстрое реагирование на них.

3. Задача по анализу данных безопасности в производственной среде: Ваша задача - анализировать данные безопасности, собранные в производственной среде, с использованием информационно-аналитической системы. Исследуйте данные о происшествиях, авариях, нарушениях безопасности и других событиях. Выявите паттерны, тренды и корреляции в данных, чтобы определить основные причины и факторы, влияющие на безопасность производства. Предложите рекомендации и меры по улучшению безопасности.

4. Задача по оптимизации процессов безопасности с помощью информационно-аналитической системы: Ваша задача - оптимизировать процессы безопасности в производственной среде с помощью информационно-аналитической системы. Используя данные о безопасности, угрозах и инцидентах, проанализируйте существующие процессы безопасности и предложите улучшения. Разработайте систему мониторинга и предупреждения, которая будет автоматически обнаруживать потенциальные угрозы и предлагать эффективные меры по их устранению.

5. Задача по созданию системы управления безопасностью в производственной среде: Ваша задача - разработать информационно-аналитическую систему для управления безопасностью в производственной среде. Эта система должна включать в себя мониторинг уровня безопасности, анализ данных, принятие решений и автоматизацию мер безопасности. Разработайте процедуры и алгоритмы для эффективного управления безопасностью в режиме реального времени.

6. Задача по анализу безопасности внутренней сети производственной компании: Ваша задача - провести анализ безопасности внутренней сети производственной компании с помощью информационно-аналитической системы. Изучите сетевую инфраструктуру, обнаружите потенциальные уязвимости и риски, связанные с безопасностью. Предложите рекомендации и меры по усилению безопасности сети, включая сегментацию сети, установку брандмауэров, контроль доступа и мониторинг сетевого трафика.

7. Задача по оптимизации производственных процессов с использованием информационно-аналитической системы безопасности: Ваша задача - разработать информационно-аналитическую систему безопасности, которая поможет оптимизировать производственные процессы с учетом безопасности. Используйте данные о безопасности, событиях и угрозах, чтобы анализировать и предсказывать потенциальные риски для производства. Разработайте механизмы реагирования на угрозы и предложите рекомендации по улучшению безопасности и эффективности производства.

8. Задача по разработке системы мониторинга безопасности в производственной среде: Ваша задача - разработать систему мониторинга безопасности, специально адаптированную для производственной среды. Используйте информационно-аналитические методы для обнаружения потенциальных угроз и аномалий в производственных процессах. Разработайте систему оповещения и управления для своевременного реагирования на возможные проблемы безопасности.

9. Задача по анализу эффективности информационно-аналитической системы безопасности: Ваша задача - проанализировать эффективность информационно-аналитической системы безопасности в производственной среде. Оцените ее способность обнаруживать и предотвращать угрозы, а также ее влияние на производственные показатели, такие как безопасность персонала, снижение простоев и потерь. Предложите рекомендации по улучшению системы и ее интеграции в производственные процессы.

10. Задача по оптимизации процессов безопасности с использованием информационно-аналитической системы: Ваша задача - использовать информационно-аналитическую систему безопасности для оптимизации процессов безопасности в производственной среде. Используя данные о безопасности, анализируйте тренды, идентифицируйте уязвимые места и предлагайте улучшения в процедурах и мероприятиях безопасности. Цель состоит в повышении эффективности и эффективности системы безопасности.

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.

2-4 баллов выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

1.4 КЕЙС-ЗАДАЧИ

1.Ваша задача состоит в разработке и внедрении информационно-аналитической системы безопасности для производственных объектов компании. Вы должны определить необходимые функциональные возможности системы, провести анализ требований, разработать план внедрения и обеспечить эффективное использование системы в производственной среде.

Шаги кейса:

1. Анализ требований: Проведите анализ требований компании в отношении системы безопасности. Изучите производственные процессы, выявите потенциальные угрозы и риски, а также определите ожидания по мониторингу, аналитике и предупреждению безопасностных инцидентов.
2. Разработка функциональностей системы: На основе анализа требований разработайте список функциональностей, которые должна предоставлять информационно-аналитическая система безопасности. Это может включать сбор и хранение данных о безопасности, мониторинг событий, анализ данных, создание отчетов и дашбордов, интеграцию с другими системами и т.д.
3. Выбор технологий и инфраструктуры: Проанализируйте различные технологические решения и инфраструктуру, которые могут быть использованы для реализации информационно-аналитической системы безопасности. Учтите требования по масштабируемости, производительности, безопасности данных и интеграции с существующими системами.

2.Ваша задача состоит в создании информационно-аналитической системы безопасности, которая будет способна собирать, обрабатывать и анализировать данные о безопасности, предоставляя важную информацию для принятия решений и прогнозирования потенциальных угроз. Вам необходимо определить требования, разработать архитектуру системы, выбрать соответствующие инструменты и реализовать ее функциональность.

Шаги кейса:

1. Идентификация требований: Ваша задача - провести анализ потребностей и требований к информационно-аналитической системе безопасности. Обратитесь к заинтересованным сторонам, включая руководство организации и сотрудников, чтобы понять, какие данные и функциональности им требуются. Определите основные цели и задачи системы.
2. Разработка архитектуры системы: На основе идентифицированных требований разработайте архитектуру информационно-аналитической системы безопасности. Разделите систему на компоненты, определите их взаимодействие и функции. Учтите масштабируемость, гибкость и безопасность при проектировании архитектуры.
3. Выбор и интеграция инструментов: Определите необходимые инструменты и технологии для реализации информационно-аналитической системы безопасности. Это может включать инструменты для сбора и хранения данных, аналитики и визуализации данных, а также инструменты для обеспечения безопасности и защиты информации. Обеспечьте совместимость и интеграцию выбранных инструментов.

3.Ваша задача состоит в разработке и внедрении информационно-аналитической системы безопасности для компании. Система должна обеспечивать мониторинг и контроль безопасности в реальном времени, обнаруживать и реагировать на потенциальные угрозы и инциденты, а также предоставлять аналитическую информацию для принятия решений и оптимизации безопасности.

Шаги кейса:

1. Анализ требований безопасности: Проведите анализ требований безопасности компании. Взаимодействуйте с заинтересованными сторонами, такими как менеджеры филиалов и складов, аналитики безопасности и сотрудники службы безопасности, чтобы определить основные угрозы и требования к системе безопасности.
2. Проектирование информационно-аналитической системы безопасности: На основе проведенного анализа разработайте концепцию информационно-аналитической системы безопасности. Определите основные функциональные модули системы, такие как мониторинг безопасности, обнаружение угроз, аналитика безопасности и генерация отчетов. Разработайте архитектуру системы и определите необходимые интеграции с другими системами и источниками данных.

3. Разработка и внедрение системы безопасности: Разработайте и внедрите информационно-аналитическую систему безопасности для компании. Это может включать разработку программного обеспечения, установку аппаратного обеспечения, конфигурирование сетевых устройств и настройку интеграций. Удостоверьтесь, что система способна собирать и обрабатывать данные

4.Ваша задача состоит в обнаружении и предотвращении инцидентов безопасности на производственной площадке с помощью информационно-аналитической системы безопасности. Вам предоставляются данные о производственных операциях, событиях безопасности, авариях, инцидентах и других параметрах, связанных с безопасностью. Вам необходимо использовать эти данные для выявления потенциальных угроз, прогнозирования рисков и принятия мер для предотвращения инцидентов безопасности.

Шаги кейса:

1. Анализ данных безопасности: Изучите предоставленные данные о безопасности, включая события, инциденты, аварии и другие параметры. Проведите анализ данных, чтобы выявить общие тренды, паттерны и аномалии. Определите ключевые факторы, которые могут указывать на возможные угрозы безопасности.
2. Разработка моделей прогнозирования: Используя данные о безопасности, разработайте модели прогнозирования, которые позволят определить вероятность возникновения инцидентов безопасности на производственной площадке. Используйте методы машинного обучения и статистического анализа для создания моделей, которые могут предсказывать потенциальные угрозы и риски.
3. Мониторинг и обнаружение угроз: Настройте информационно-аналитическую систему безопасности для мониторинга и обнаружения потенциальных угроз безопасности. Используйте разработанные модели прогнозирования для идентификации аномалий и неправильных событий.

5.Ваша задача состоит в разработке и внедрении информационно-аналитической системы безопасности для организации. Система должна обеспечивать эффективное сбор, анализ и использование данных о безопасности, а также предоставлять инструменты для принятия решений и контроля безопасности в различных областях компании.

Шаги кейса:

1. Анализ безопасности: Проведите анализ безопасности в организации. Изучите существующие политики и процедуры безопасности, а также выявите уязвимые места и риски, связанные с безопасностью. Определите необходимые данные для мониторинга и управления безопасностью.
2. Разработка информационно-аналитической системы: На основе анализа безопасности разработайте информационно-аналитическую систему

безопасности. Определите необходимые функциональные возможности системы, такие как сбор данных, анализ и визуализация, мониторинг событий безопасности и предупреждение о потенциальных угрозах.

3. Интеграция данных: Разработайте механизмы для интеграции различных источников данных о безопасности в информационно-аналитическую систему. Это могут быть данные с камер видеонаблюдения, систем контроля доступа, журналов безопасности и других источников. Обеспечьте согласованность и целостность данных.

4. Анализ и визуализация данных: Разработайте алгоритмы и методы анализа данных для выявления паттернов, трендов и аномалий в безопасности. Используйте аналитические инструменты и техники, чтобы определить важные события и предупредить о возможных угрозах

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.

2-4 баллов выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Что отражает модель жизненного цикла информационной системы?

1) все события, происходящие с системой в процессе ее создания и использования

2) процесс создания системы

3) процессы, связанные с использованием системы

4) все события в системе во время ее эксплуатации

2. Для чего производится предварительное обследование объекта автоматизации?

1) для формирования концепции создания системы

2) для создания прототипа системы

3) для выяснения готовности предприятия к автоматизации

4) для формирования команды, которая будет работать над созданием системы

3. Укажите основную цель детального обследования объекта автоматизации.

1) формирование технического задания на систему

2) подбор исполнителя для создания системы

3) определение целей автоматизации

4) выбор технических и программных инструментов

4. Отметьте методы сбора информации при проведении обследования объекта автоматизации.

1) анкетирование

2) интервьюирование

3) метод аналогий

4) создание "фотографии рабочего дня"

5) метод проб и ошибок

6) метод Монте-Карло

5. Какие данные обрабатываются в фактографических информационных системах?

1) структурированные данные в виде текстов и чисел

2) любые изображения

3) только числовые

4) исторические факты

6. Какая методология моделирования систем использует понятие "Прецедент"?

1) методология объектно-ориентированного моделирования

2) структурное моделирование

3) визуальное моделирование

4) функциональное моделирование

7. В основе архитектурного проектирования лежат понятия:

1) Проектирование – как средство достижения поставленного результата

2) Архитектура – как результат

3) Архитектура – как видение

4) Проектирование – как инструмент планирования разработки

8. Проектирование - это

1) вид активности направленный на создание уникального продукта (услуги), последовательность этапов реализации которого, будет определяться «внешними» факторами, и определять его конечные преимущества и недостатки

2) видение конечного результата реализации информационной системы

3) процесс формирования структуры проекта

4) анализ текущего состояния структуры компании и предложение идей об улучшении бизнес-процессов

9. Архитектурное проектирование - это

1) процесс реализации пожеланий Стэйкхолдеров

2) работы по подготовке структуры взаимодействия систем в организации

3) вид активности, который своей целью ставит создание архитектуры в процессе выполнения проекта

4) вид работ по определению границ проекта

10. Архитектурное проектирование программного обеспечения, одной из задач ставит

1) бесперебойное функционирование информационных систем компании

2) поддержку и развитие существующих процессов и информационных систем компании

3) формирование особого видения, всех участников проекта, на конечный продукт

4) создание артефакта (архитектуры), который должен обеспечить достижение результатов деятельности организаций, использующих программные продукты для реализации своих процессов

11. Программные продукты – это

1) исполняемые процедуры

2) реализация требований Спонсоров проекта

3) взаимосвязанные информационные сущности, выполняющие запросы Пользователей

4) основной элемент большинства современных высокотехнологичных доменов деятельности

12. Причиной развития темы архитектуры программного обеспечения является

1) рост издержек предприятий

2) развитие технологий

3) нарастающая конкуренция

4) требования к качеству информационных продуктов

13. Шаблоны проектирования (design patterns) представляет собой

1) руководство по реализации

2) универсальный свод информации

3) проектная документация на разработку

4) ограничения по реализации

14. Архитектурные решения - это

1) соглашения, учитывающие и удовлетворяющие различные точки зрения, «силы», принципы, как технического, так и не технического характера

2) соглашения, между Архитектором и Командой по реализации

3) тип используемых методик проектирования

4) видение конечного результата реализации

15. Выбор стиля использования шаблонов производится на основании

1) имеющихся ресурсов

2) конкурентной среды

3) политики организации

4) требований

16. Сложность обеспечения информационной безопасности является следствием:

1) злого умысла разработчиков информационных систем

2) объективных проблем современной технологии программирования

3) происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы

17. Сложность обеспечения информационной безопасности является следствием:

1) невнимания широкой общественности к данной проблематике

2) все большей зависимости общества от информационных систем

3) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

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

1) доступность

2) целостность

3) защита от копирования

4) конфиденциальность

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. Укажите, что показывает диаграмма дерева узлов.

1) иерархическую зависимость работ

2) взаимосвязи между работами

3) глубины детализации

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. Какие типы элементарных моделей используются для построения организационно-функциональной структуры?

1) древовидные модели (классификаторы)

2) процессные модели

3) матричные модели

25. Какая модель отвечает на вопросы: *зачем* компания занимается именно этим бизнесом, *почему* предполагает быть конкурентоспособной, *какие* цели и стратегии для этого необходимо реализовать?

1) стратегическая модель целеполагания

2) организационно-функциональная модель

3) функционально-технологическая модель

4) процессно-ролевая модель

5) модель структуры данных

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. Выделите утверждение, верное в отношении защиты сетей.

1) уровень защищенности сети определяется уровнем защищенности ее самого «сильного» звена

2) уровень защищенности сети определяется суммой уровней защищенности ее звеньев

3) уровень защищенности сети определяется уровнем защищенности ее самого «слабого» звена

4) уровень защищенности сети не зависит напрямую от защищенности ее отдельных звеньев

28. Как называется мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы и методам управления её конфигурацией и целостностью?

1) эффективность безопасности

2) гарантированность безопасности

3) непрерывность безопасности

4) надежность безопасности

29. Каким термином обозначается анализ регистрационной информации системы защиты?

1) мониторинг

2) аудит

3) аккредитация

4) сертификация

30. Какие компоненты присутствуют в модели системы защиты с полным перекрытием?

1) область угроз

2) область рисков

3) защищаемая область

4) система защиты

5) область безопасности

31. Как называется возможность осуществления угрозы T в отношении объекта O?

1) слабость

2) неполнота

3) уязвимость

4) риск

32. Что означает система защиты с полным перекрытием?

1) для половины (и более) уязвимостей есть устраняющие барьеры

2) для любой уязвимости есть устраняющий ее барьер

3) у любой уязвимости есть риск ее реализации

4) количество уязвимостей меньше, чем количество препятствующих им барьеров

33. Чем характеризуется степень сопротивляемости механизма защиты?

1) вероятностью его преодоления

2) количеством угроз, которым этот механизм препятствует

3) величиной потерь в случае успешного прохождения

4) стоимостью механизма защиты

34. При отсутствии в системе барьеров, «перекрывающих» выявленные уязвимости, степень сопротивляемости механизма защиты принимается равной...

1) 0

2) 1

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. В чем заключается идеология открытых систем информационной безопасности?

1) в строгом соответствии систем информационной безопасности законодательству страны, котором они созданы

2) в строгом соблюдении совокупности профилей, протоколов и стандартов де-факто и де-юре

3) в открытости информации о стоимости реализации конкретной системы защиты

4) в открытости программных кодов средств защиты от производителей разных стран

37. Для чего в первую очередь нужна идеология открытых систем информационной безопасности?

1) для удешевления средств защиты информации

2) для минимизации рисков от реализации угроз

3) для совместимости компонент различных информационных систем

38. В чем заключается принцип минимизации привилегий?

1) выделение полных прав доступа только администраторам системы

2) выделение только тех прав, которые необходимы для реализации своих должностных обязанностей

3) выделение прав доступа в зависимости от величины возможного ущерба

39. В чем заключается принцип эшелонирования обороны?

1) в том, чтобы использовать максимально возможное количество защитных средств

2) в простоте и управляемости информационной системы

3) в усилении самого надежного защитного рубежа

4) в том, чтобы не полагаться на один защитный рубеж

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. то из нижеперечисленного относится к мерам предотвращения угроз безопасности?

1) систематическое тестирование

2) предотвращение ошибок в CASE-технологиях

3) обязательная сертификация

4) программная избыточность

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. На каких принципах должна строиться архитектура ИС?

1) проектирование на принципе закрытых систем

2) проектирование на принципе открытых систем

3) усиление самого сильного звена

4) усиление самого слабого звена

5) эшелонирование обороны

44. Какие органы исполнительной власти являются ключевыми в области технической защиты информации?

1) ФСТЭК России

2) ФСБ России

3) СВР России

4) МВД России

5) Роскомнадзор

45. Какой орган государственной власти осуществляет контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных?

1) ФСТЭК России

2) ФСБ России

3) СВР России

4) МВД России

5) Роскомнадзор

46. Какой орган исполнительной власти осуществляет контроль в области криптографической защиты информации?

1) ФСТЭК России

2) ФСБ России

3) МВД России

4) Роскомнадзор

47. Какой орган исполнительной власти осуществляет сертификацию средств защиты информации, систем и комплексов телекоммуникаций, технических средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?

1) ФСТЭК России

2) ФСБ России

3) МВД России

4) Роскомнадзор

48. 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

49. Какой орган исполнительной власти реализует контрольные функции в области обеспечения защиты (некриптографическими методами) информации?

1) ФСТЭК России

2) ФСБ России

3) МВД России

4) Роскомнадзор

50. Какой орган исполнительной власти проводит лицензирование деятельности по оказанию услуг в области защиты государственной тайны в части, касающейся противодействия техническим разведкам и/или технической защиты информации?

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

Задания в открытой форме

1. Информационная система-это…
2. Информационные системы можно классифицировать по признакам…
3. Подсистема-это…
4. Унифицированные системы документации-это…
5. В концепции обеспечения информационной безопасности предприятия определяются…
6. Конфиденциальную информацию обычно классифицируют…
7. Обеспечение безопасности должно основываться на…
8. Для обеспечения мероприятия для защиты информации необходимо произвести…
9.К принципам построения технической системы безопасности относятся…

10. Архитектура системы должна быть…
11. В качестве объектов уязвимости рассматриваются…
12. Наличие и полнота политики безопасности-это…
13. Механизм одобрения для защищенных систем основан на…
14. Владелец информации и владелец ресурсов могут быть…
15. Формирование защиты в ИС основывается на…
16. Организационное обеспечение-это…
17. В структуру информационного обеспечения входит…
18. На этапе хранения данных информационная система охватывает…
19. База данных-это…
20. На этапе публикации (представления) информации ИО включает…

Задания на установление соответствия

1. Установите взаимно однозначное соответствие

1	Информационная система (ИС)	А	предназначена для эффективной эксплуатации экономической ИС
2	Автоматизированная ИС	Б	система сбора, хранения, накопления, поиска и передачи информации, применяемая в процессе управления или принятия решений.
3	Автоматизированная ИС	В	совокупность информ., экономико-математических методов и моделей, аппаратных, программных, организационных, технологических средств и специалистов

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	В	оказывает устойчивую

	(корпоративные) ИС		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.	Выявление критически важной информации	А	на этом этапе выполняется непосредственно специалистами, проводящими аудит. От результатов этой работы зависит выбор схемы построения информационной безопасности
2	Выявление слабых мест в корпоративной безопасности	Б	Это завершающий этап аудита, в ходе которого на основании проведенного анализа составляется список конкретных мер, которые необходимо принять для охраны корпоративных секретов компании
3	Оценка возможностей защиты информации	В	на этом этапе происходит определение тех документов и данных, безопасность которых имеет огромное значение для

			компании, а утечка – несет огромные убытки.

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	Аппаратная угроза	А	есть вероятность некорректной работы программного обеспечения
2	Вероятность утечки	Б	существует вероятность нарушения работоспособности оборудования
3	Нестабильность ПО	В	возможен несанкционированный доступ к данным и их потеря

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 преобразование-	Г	одно из облачных решений 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.	Защита информации-	А	это желаемый результат защиты информации. Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.
2	Объект защиты-	Б	это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
3	Цель защиты информации-	В	степень соответствия результатов защиты информации поставленной цели
4	Эффективность защиты информации-	Г	информация, носитель информации или информационный процесс, в

			отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации

9. Установите взаимно однозначное соответствие

1	Защита информации от утечки-	А	деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.
2	Защита информации от разглашения-	Б	деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.
3	Защита информации от НСД-	В	Деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
4	Система защиты информации -	Г	совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-

			распорядительными и нормативными документами по защите информации.

10. Установите взаимно однозначное соответствие

1	Доступ к информации -	А	это способность информации или некоторого информационного ресурса быть доступными для конечного пользователя в соответствии с его оперативными потребностями.
2	Оперативность доступа к информации-	Б	субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.
3	Собственник информации-	В	получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.
4	Владелец информации -	Г	субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

11. Установите взаимно однозначное соответствие

1	Способ защиты информации -	А	совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности системы (сети).
2	Средство защиты информации-	Б	порядок и правила применения определенных принципов и средств защиты информации.
3	Комплекс средств защиты (КСЗ)-	В	средства защиты информации, средства контроля эффективности защиты информации, средства и

			системы управления, предназначенные для обеспечения защиты информации.
4	Техника защиты информации-	Г	Техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации

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. Установите взаимно однозначное соответствие

1	Ядро безопасности-	А	проверка подлинности идентификаторов сущностей с помощью различных (преимущественно криптографических) методов.
2	Аутентификация-	Б	показатель реально обеспечиваемого уровня безопасности, отражающий степень эффективности и надежности реализованных средств защиты и их соответствия поставленным задачам
3	Идентификация-	В	совокупность аппаратных, программных и специальных компонентов ВС, реализующих функции защиты и обеспечения безопасности.
4	Адекватность-	Г	процесс распознавания сущностей путем присвоения им уникальных меток

15. Установите взаимно однозначное соответствие

1	Математическое и программное обеспечение (МО, ПО)-	А	совокупность правовых норм, определяющих создание, 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. Установите взаимно однозначное соответствие

1	Сопровождение-	А	проверка функционального соответствия системы показателям, определенным на этапе анализа
2	Функционирование-	Б	обеспечение штатного процесса эксплуатации системы на предприятии заказчика.
3	Внедрение-	В	штатный процесс эксплуатации в соответствии с основными целями и задачами ИС
4	Тестирование-	Г	установка и ввод системы в действие

17. Установите взаимно однозначное соответствие

1	Принцип интеграции	А	заключается в том, что при декомпозиции должны быть установлены такие связи между структурными компонентами системы, которые обеспечивают цельность корпоративной системы и ее взаимодействие с другими системами
2	Принцип системности	Б	предполагает рассмотрение всех сторон объекта исследования в его связи и зависимости с другими процессами и явлениями
3	Принцип комплексности	В	заключается в том, что обрабатываемые данные (документы) вводятся в

			систему только один раз и затем многократно используются для решения возможно большего числа задач

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	Специальные категории ПДн-	А	данные, характеризующие биологические или физиологические особенности субъекта и используемые для установления личности, например, фотография или отпечатки пальцев
2	Биометрические ПДн-	Б	обработка персональных данных субъектов, не являющихся работниками

			вашей организации
3	Общедоступные ПДн-	В	относятся информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта
4	Иные категории ПДн-	Г	сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом

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 особенности-	Б	наличие развитых встроенных 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. Установить последовательность этапов стадии создания системы защиты информации

1. Внедрение системы защиты информации (этап установки, настройки, испытаний)
2. Формирование требований к системе защиты информации (предпроектный этап)
3. Подтверждение соответствия системы защиты информации (этап оценки)
4. Разработка системы защиты информации (этап проектирования)

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.Установить последовательность этапов принципа действия сетевых червей
1. Поиск "жертв»
2. Подготовка копий
3. Проникновение в систему
4. Распространение копий

5. Активация

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. Установить последовательность совокупности архитектурой программных систем

1. Выбор структурных элементов, составляющих систему и их интерфейсов
2. Объединение элементов в подсистемы
3. Организации программной системы
4. Поведение элементов во взаимодействии с другими элементами

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. Задача по разработке информационно-аналитической системы безопасности: Ваша задача - разработать информационно-аналитическую систему безопасности, которая будет собирать, анализировать и интерпретировать данные о безопасности в организации. Разработайте алгоритмы и методы обработки данных, чтобы система могла определять потенциальные угрозы и предлагать решения для их предотвращения.

2. Задача по интеграции различных источников данных в информационно-аналитическую систему безопасности: Ваша задача - разработать механизмы интеграции различных источников данных в информационно-аналитическую систему безопасности. Это может включать интеграцию данных с системами видеонаблюдения, системами контроля доступа, журналами событий и другими. Обеспечьте согласованность и целостность данных при их объединении и анализе.

3. Задача по разработке модели предсказания безопасности: Ваша задача - разработать модель предсказания безопасности на основе информационно-аналитической системы. Используя исторические данные о безопасности и методы машинного обучения, создайте модель, которая способна предсказывать потенциальные угрозы и события безопасности. Оцените эффективность модели и проведите ее дальнейшую настройку и улучшение.

4. Задача по разработке системы визуализации данных безопасности: Ваша задача - разработать систему визуализации данных безопасности, которая позволит наглядно представлять информацию об угрозах и событиях безопасности. Создайте дашборды, графики и отчеты, которые позволят пользователям системы легко понимать текущую ситуацию в области безопасности и принимать информированные решения.

5. Задача по разработке информационно-аналитической системы безопасности: Ваша задача - разработать информационно-аналитическую систему безопасности, которая будет отвечать требованиям и потребностям конкретной организации. Определите функциональные возможности системы, такие как сбор, анализ и визуализация данных о безопасности, обнаружение угроз и атак, мониторинг и реагирование на инциденты безопасности. Разработайте пользовательский интерфейс и систему отчетности.

6. Задача по интеграции информационно-аналитической системы безопасности с другими системами: Ваша задача - интегрировать информационно-аналитическую систему безопасности с другими системами, используемыми в организации. Обеспечьте совместимость и обмен данными между системами, такими как системы мониторинга безопасности, системы управления доступом и системы видеонаблюдения. Разработайте протоколы и механизмы интеграции.

7. Задача по анализу данных и обнаружению угроз в информационно-аналитической системе безопасности: Ваша задача - разработать алгоритмы и методы анализа данных в информационно-аналитической системе безопасности для обнаружения потенциальных угроз и атак. Исследуйте методы машинного обучения, статистического анализа и паттерн-распознавания для выявления аномалий в данных безопасности. Разработайте систему оповещений и реагирования на обнаруженные угрозы.

8. Задача по разработке системы визуализации и отчетности в информационно-аналитической системе безопасности: Ваша задача - разработать систему визуализации и отчетности в информационно-аналитической системе безопасности. Обеспечьте наглядную и понятную визуализацию данных о безопасности, такую как графики, диаграммы и карты. Разработайте отчеты и дашборды для представления ключевой информации о безопасности для руководства и сотрудников.

9. Задача по разработке информационно-аналитической системы безопасности: Ваша задача - разработать информационно-аналитическую систему безопасности, которая будет обрабатывать и анализировать данные из различных источников, связанных с безопасностью. Это может включать журналы событий, данные сенсоров и мониторов, информацию о доступе и другие источники. Разработайте систему для сбора, хранения, анализа и визуализации данных с целью обнаружения и предотвращения потенциальных угроз безопасности.

10. Задача по анализу данных для обнаружения аномалий: Ваша задача - разработать методики и алгоритмы для анализа данных в информационно-аналитической системе безопасности с целью обнаружения аномальных активностей или поведения. Исследуйте и примените методы машинного обучения, статистического анализа или другие подходы для выявления необычных паттернов или отклонений от нормы, которые могут указывать на потенциальные угрозы безопасности.

11. Задача по разработке системы предупреждения и реагирования на угрозы: Ваша задача - разработать систему предупреждения и реагирования на угрозы безопасности в информационно-аналитической системе. Это может включать разработку правил и политик оповещения о потенциальных угрозах, автоматическое выполнение действий в случае обнаружения угрозы, интеграцию с другими системами безопасности и т.д. Разработайте систему, которая будет своевременно и эффективно реагировать на угрозы и обеспечивать безопасность информационной инфраструктуры.

12. Задача по разработке информационно-аналитической системы безопасности: Ваша задача - разработать информационно-аналитическую систему безопасности для организации. Система должна быть способна собирать, анализировать и визуализировать информацию о безопасности, включая данные о событиях безопасности, угрозах, инцидентах и т.д. Разработайте платформу, которая позволит эффективно отслеживать и реагировать на потенциальные угрозы безопасности.

13. Задача по анализу безопасности данных в информационно-аналитической системе: Ваша задача - провести анализ безопасности данных в информационно-аналитической системе. Оцените уязвимости системы, потенциальные риски и угрозы, связанные с обработкой и хранением данных. Предложите меры для улучшения безопасности данных, такие как шифрование, контроль доступа, мониторинг и аудит.

14. Задача по обеспечению конфиденциальности и целостности данных в информационно-аналитической системе: Ваша задача - разработать механизмы и политики для обеспечения конфиденциальности и целостности данных в информационно-аналитической системе безопасности. Исследуйте методы шифрования данных, контроля доступа и проверки целостности,

чтобы гарантировать, что данные остаются надежными и защищенными от несанкционированного доступа и изменений.

15. Задача по обнаружению и предотвращению угроз безопасности в информационно-аналитической системе: Ваша задача - разработать механизмы обнаружения и предотвращения угроз безопасности в информационно-аналитической системе. Исследуйте современные методы машинного обучения и аналитики данных для выявления аномалий и поведения, связанного с безопасностью. Разработайте систему мониторинга и предупреждения для реагирования на потенциальные угрозы.

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.