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

Управление разработкой систем 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. Основные аспекты построения системы информационной безопасности.

1. Перечислите основные методы и средства защиты информации.
2. Дайте определения кодирования и декодирования.
3. Как осуществляется защита от несанкционированного доступа к данным?
4. Охарактеризуйте классы безопасности компьютерных систем.
5. Сформулируйте определение электронной цифровой подписи.
6. Какие ресурсы системы должны быть защищаемы и в какой степени?
7. Какова должна быть полная стоимость реализации защиты и затраты на эксплуатацию с учетом потенциальных угроз?
8. Какие угрозы должны быть устранены и в какой мере?
9. Что предполагает статическая целостность информации?
10. С помощью каких средств должна быть реализована защита?

Тема 2. Мероприятия по защите информации.

1. Какие механизмы обеспечения безопасности существуют?
2. Перечислите основные технологические мероприятия комплексной системы обеспечения информационной безопасности.
3. Какие проблемы информационной безопасности вы знаете?
4. Составляющие информационной безопасности.
5. Система формирования информационной безопасности.
6. Какие существуют модели защиты информации?
7. Что предполагает динамическая целостность информации?
8. Понятие конфиденциальности в информационной безопасности.
9. Перечислите основные мероприятия организации работ по обеспечению защиты информации.
10. Какие существуют уровни формирования информационной безопасности?

Тема 3. Требования к архитектуре ТКС для обеспечения безопасности ее функционирования.

1. Правильно построенная архитектура решает некоторые проблемы ИБ сетей?
2. Перечислите требования, предъявляемые к системам защиты информации.

3. Перечислите основные методы и средства обеспечения защиты информации.
4. Что включают в себя организационные средства обеспечения защиты информации?
5. Характеристика системы обнаружения вторжений (СОВ).
6. Основные методы защиты от атак на сетевую инфраструктуру.
7. Характеристика технических мер защиты от сетевых атак.
8. Что включают в себя программно-аппаратные средства защиты информации?
9. Руководящий документ «Классификация автоматизированных систем.
10. Что включают в себя инженерно-технические средства защиты информации?

Тема 4. Оценочные стандарты и технические спецификации.

1. Комплекс документов Банка России СТО БР ИББС, краткая характеристика, показатели ИБ. Способы оценивания показателей.
2. Понятие «стандарт», краткая характеристика «Оранжевой книги».
3. Что понимается под термином «политика безопасности»?
4. Характеристика стандарта ГОСТ Р ИСО/МЭК 15408
5. Что понимается под термином «уровень гарантированности»?
6. Перечислите методы и стандарты шифрования.
7. Опишите стандарты безопасности (WPA, WPA2). VPN.
8. Что понимается под термином «операционная гарантированность»?
9. Международные стандарты менеджмента ИБ серии ISO 27000. Модель PDCA, стандарты NIST.
10. Какие классы стандартов безопасности вы знаете?

Тема 5. Критерии оценки безопасности информационных технологий.

1. Опишите иерархию сущностей в "Критериях оценки безопасности информационных технологий".
2. Назовите основные термины, описанные в "Критериях оценки безопасности информационных технологий".
3. Опишите структуру класса «приватность».
4. Опишите структуру класса «использование ресурсов».
5. Что такое требования доверия безопасности и для чего они нужны?
6. Что такое уровни доверия?
7. Какие существуют механизмы обеспечения безопасности в распределённых системах?
8. Какие 3 составляющих информационной безопасности вы знаете?

9. Что является критерием безопасности?

10. Какие основные критерии и методологии используются для оценки безопасности информационных технологий?

Тема 6. Руководящие документы ФСТЭК России.

1. Какие руководящие документы ФСТЭК России существуют? Понятие "государственная тайна".
2. Что контролирует ФСТЭК?
3. Руководящий документ «Классификация по уровню контроля отсутствия недекларированных возможностей», характеристика, основные моменты.
4. Что такое сертификат ФСТЭК?
5. Кто руководит ФСТЭК?
6. Кто регулирует деятельность в области защиты информации?
7. Чем отличается ФСТЭК от фсб?
8. Кто выдает лицензию ФСТЭК?
9. Кому подчиняется ФСТЭК России?
10. Руководящий документ «СВТ. Показатели защищенности от НСД к информации», характеристика, основные моменты.

Критерии оценки:

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

3-8 баллов (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1-2 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие

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

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ К ПРАКТИЧЕСКИМ РАБОТАМ

Контрольные вопросы к практической работе №1

1. Какие функции выполняет СЗИ предприятия для решения задач защиты информации?
2. Как строится структура полномасштабной системы обеспечения безопасности и защиты информации предприятия?
3. Какие типовые организационные структуры входят в государственную систему защиты информации?
4. Что включает в себя система обеспечения информационной безопасности?
5. Какие органы отвечают за обеспечение ИБ в стране?
6. Какие 3 понятия характеризуют систему ИБ в компании?
7. О чем Доктрина информационной безопасности РФ?
8. Дайте характеристику Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»?
9. О чем Федеральный закон от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»?
10. Прокомментируйте выражение для определения прочности многозвенной защиты при противостоянии одному нарушителю.

Контрольные вопросы к практической работе №2

1. Какие существуют методы расчета прочности оболочки защиты?
2. Прокомментируйте выражение для определения прочности многозвенной защиты при противостоянии нескольким нарушителям.
3. Какие выводы можно сделать, если прочность слабейшего звена защиты удовлетворяет предъявленным требованиям оболочки защиты в целом?
4. Какие меры повышения прочности защиты можно порекомендовать, если звено защиты не удовлетворяет предъявленным требованиям?
5. Каким образом система будет способствовать целям бизнеса?
6. Требует ли разработка системы технологии, которая до этого не использовалась в организации?
7. Какие этапы оценки вы знаете?
8. Опишите рамки информационной безопасности NIST (NIST CSF).
9. В чем заключается сложность функционального построения системы защиты объекта информатизации? Приведите примеры.

10. Приведите формулу для вычисления величины Ротки), прокомментируйте ее.

11. Приведите примеры многозвенной системы защиты объекта информатизации.

Контрольные вопросы к практической работе №3

1. Что должен включать отчет по результатам оценки CASE-средств?
2. Сколько поколения CASE-средств существует? Опишите их.
3. Опишите виды классификации CASE-средств.
4. Охарактеризуйте критерии выбора CASE-средств.
5. Какие требования предъявляются к CASE-средствам?
6. Какие направления развития CASE-средств используются наиболее интенсивно?
7. По каким критериям оценивается CASE-средство для UML?
8. Как делятся CASE-средства по функциональному назначению?
9. Опишите архитектуру CASE-средств.
10. Какие текущие проблемы существуют в организации и как новая система поможет их решить?
11. Опишите этапы программы оценки соответствия ИБ.

Контрольные вопросы к практической работе №4

1. Перечислите отличия сертифицированных версий от версий общего пользования.
2. Как проводится сертификация средств защиты информации?
3. Проекты международных стандартов по облачным вычислениям.
4. Опишите стандарты и руководства США.
5. Общая картина введенных в действие и ожидаемых в ближайшее время стандартов и руководств в области облачных вычислений.
6. Российская стандартизация облачных вычислений и ее проблемы и пути решения.
7. Что показывают характеристики данного средства защиты?
8. Можно ли устанавливать на сертифицированную операционную систему несертифицированные продукты?
9. Какой регулятор контролирует данную область информационной безопасности?
10. Какая основная информация содержится в сертификате?

Критерии оценки:

4 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными

примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

1-2 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

1.3 ПРОИЗВОДСТВЕННЫЕ ЗАДАЧИ

1. Задача формирования команды разработки: Сформируйте команду разработчиков, специалистов по безопасности и других необходимых участников проекта. Определите роли и ответственности каждого члена команды, учитывая их навыки и экспертизу в области безопасности информационных систем.

2. Задача разработки плана проекта: Разработайте подробный план проекта разработки системы безопасности, который включает в себя определение этапов, задач, сроков выполнения и ресурсов. Установите ключевые моменты, на которых будет осуществляться контроль прогресса проекта.

3. Задача составления бюджета проекта: Составьте бюджет на разработку системы безопасности, учитывая затраты на оборудование, программное обеспечение, экспертные услуги и обучение. Определите необходимые ресурсы и распределите бюджет между различными этапами проекта.

4. Задача формирования команды разработки: Составьте команду специалистов по безопасности, включая системных администраторов, инженеров безопасности, разработчиков и тестировщиков. Определите роли

и обязанности каждого члена команды и обеспечьте их взаимодействие и сотрудничество.

5. Задача установки и настройки безопасностных инструментов: Выберите и установите необходимые инструменты для обеспечения безопасности, такие как брандмауэры, системы обнаружения вторжений и антивирусные программы. Настройте и интегрируйте эти инструменты с существующей инфраструктурой и системами компании.

6. Задача разработки политики безопасности: Разработайте политику безопасности, которая будет определять стандарты и правила обеспечения безопасности информационных систем компании. Определите требования к паролям, правам доступа, шифрованию данных и другим аспектам безопасности. Убедитесь, что политика соответствует законодательству и бест-практикам.

7. Задача управления рисками: Идентифицируйте потенциальные риски и уязвимости в информационных системах и разработайте стратегии управления рисками. Оцените вероятность и воздействие каждого риска и разработайте планы митигации. Убедитесь, что система безопасности способна предотвратить или минимизировать эти риски.

8. Задача тестирования и аудита системы безопасности: Проведите тестирование и аудит системы безопасности, чтобы проверить ее эффективность и соответствие требованиям. Используйте автоматизированные инструменты и методики тестирования, проведите пенетрационное тестирование и проверку на уязвимости.

9. Задача планирования проекта: Разработайте план проекта по созданию системы безопасности. Определите цели, задачи, ресурсы и сроки выполнения. Разбейте проект на этапы и определите зависимости между ними. Разработайте детальный график работ и распределите задачи между членами команды.

10. Задача составления команды разработки: Составьте команду разработчиков, специализирующихся на системах безопасности. Определите требуемые навыки и опыт, проведите набор персонала и сформируйте сильную команду, способную разрабатывать и внедрять системы безопасности.

Критерии оценки:

6-8 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными

примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

3-4 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1-2 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

1.4 КЕЙС-ЗАДАЧА

Компания XYZ решила разработать и внедрить новую систему безопасности для защиты своих информационных ресурсов. Ваша задача - управлять процессом разработки этой системы и обеспечить ее успешное внедрение. Вот описание кейса:

Компания XYZ является крупным провайдером интернет-услуг и хранит значительное количество конфиденциальной информации о своих клиентах. В связи с увеличением числа кибератак и угроз информационной безопасности, компания решила усилить свою систему защиты данных.

Ваша роль - управляющего проектом по разработке и внедрению новой системы безопасности. Вам предоставлены следующие задачи:

1. Определение требований безопасности: Проведите анализ уязвимостей и рисков, связанных с текущей системой безопасности компании. Составьте список требований, которые должна удовлетворять новая система, чтобы обеспечить надежную защиту данных и информационных ресурсов компании.
2. Выбор поставщика и технологий: Исследуйте рынок систем безопасности и выберите подходящих поставщиков и технологии. Оцените их опыт, репутацию, функциональность и соответствие требованиям компании. Составьте план закупки и сотрудничества с поставщиками.
3. Управление процессом разработки: Разработайте план процесса разработки новой системы безопасности. Определите этапы разработки,

ресурсы, сроки и задачи для каждого этапа. Управляйте командой разработчиков, обеспечивая их синхронную работу, контролируйте выполнение плана и решайте возникающие проблемы.

Критерии оценки:

6-8 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

3-4 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1-2 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Следующее структурное подразделение службы защиты информации отвечает за проведение работ по повышению квалификации персонала
   1) Группа режима
   2) Группа охраны и сопровождения
   3) Техническая группа
   4) Детективная группа

2. Следующее структурное подразделение службы защиты информации отвечает за организацию прохода персонала и посетителей в различные зоны безопасности
   1) Группа режима
   2) Группа охраны и сопровождения
   3) Техническая группа
   4) Детективная группа

3. Следующее структурное подразделение службы защиты информации отвечает за наблюдение за обстановкой вокруг объекта и на его территории
   1) Группа режима
   2) Группа охраны и сопровождения
   3) Техническая группа
   4) Детективная группа

4. Следующее структурное подразделение службы защиты информации отвечает за контроль работоспособности элементов системы защиты и их проверке
   1) Группа режима
   2) Группа охраны и сопровождения
   3) Техническая группа
   4) Детективная группа

5. Следующее структурное подразделение службы защиты информации отвечает за обеспечении безопасности деятельности объекта с помощью систем сигнализации, наблюдения, связи
   1) Группа режима

2) Техническая группа
3) Детективная группа

6. Следующее структурное подразделение службы защиты информации отвечает за планирование и проведение мероприятий по специальной защите объекта
1) Группа режима
2) Группа охраны и сопровождения
3) Техническая группа
4) Детективная группа

7. Следующее структурное подразделение службы защиты информации отвечает за приобретение и установку различных технических средств для службы безопасности
1) Группа режима
2) Группа охраны и сопровождения
3) Техническая группа
4) Детективная группа

8. Следующее структурное подразделение службы защиты информации отвечает за техническое обеспечение мероприятий детективной группы
1) Группа режима
2) Группа охраны и сопровождения
3) Техническая группа

9. Ограниченность анализа межсетевого экрана
1) Не может выполнять аутентификацию пользователя.
2) Не может анализировать зашифрованные прикладные данные.
3) Не может анализировать данные прикладного уровня.
4) Не может отбрасывать пакеты.

10. Межсетевые экраны прикладного уровня могут
1) Выполнять авторизацию пользователя.
2) Автоматически распознавать новые протоколы.
3) Выполнять аутентификацию пользователя.
4) Шифровать данные пользователя.

11. Прокси-шлюзы прикладного уровня (выберите самое точное определение, один ответ)
1) Имеют базу данных пользователей, которым разрешен доступ к защищаемому ресурсу.
2) Имеют прокси-агента, являющегося посредником между клиентом и сервером.

3) Имеют базу данных IP-адресов, с которых разрешен доступ к защищаемому ресурсу.
4) Не разрывают TCP-соединение.

12. Персональные межсетевые экраны для настольных компьютеров и ноутбуков устанавливаются
    1) На маршрутизаторах, которые указаны на хосте в качестве шлюза по умолчанию.
    2) На конечных точках VPN.
    3) На отдельных компьютерах.
    4) На хостах, которые они защищают.

13. Выделенные прокси-серверы предназначены для того, чтобы обрабатывать трафик
    1) Конкретного пользователя.
    2) Конкретного уровня модели OSI.
    3) Конкретного адреса отправителя.
    4) Конкретного прикладного протокола.

14. Технология UPnP, которая позволяет приложению, установленному на компьютере за межсетевым экраном, автоматически запрашивать у межсетевого экрана открытие определенных портов
    1) По умолчанию должна быть разрешена.
    2) Должна быть всегда установлена на компьютере, не должно быть возможности ее запретить.
    3) По умолчанию должна быть запрещена.
    4) Не должна использоваться ни в каком случае.

15. Входящий трафик, IP-адресом получателя в котором является сам межсетевой экран
    1) Должен блокироваться, если только межсетевой экран не предоставляет сервисы для входящего трафика, которые требуют прямого соединения.
    2) Должен всегда блокироваться.
    3) Должен всегда разрешаться.
    4) Должен разрешаться, если в локальной сети расположены сервера, доступ к которым необходим извне.
16. Определение экстранет
    1) Сеть, логически состоящая из трех частей: две интранет соединены между собой через интернет с использованием VPN.
    2) Сеть, логически состоящая из двух локальных сетей, между которыми установлен межсетевой экран.
    3) Сеть, логически состоящая из локальной сети, имеющей выход в интернет через межсетевой экран прикладного уровня.

4) Сеть, логически состоящая из локальной сети, имеющей выход в интернет через пакетный фильтр.

17. Примеры IP-адресов, которые не должны появляться в пакетах
    1) 192.168.254.0
    2) 0.0.0.0
    3) с 127.0.0.0 по 127.255.255.255
    4) 192.168.0.254

18. Использование GRE-туннеля для соединения двух локальных сетей через магистральную сеть
    1) Если необходимо доставить пакет из тупикового сегмента X в тупиковый сегмент Y, то маршрутизатор NAT для сегмента X инкапсулирует пакет в IP-заголовок с IP-адресом получателя, установленным в IP-адрес хоста в сегменте Y.
    2) Если необходимо доставить пакет из тупикового сегмента X в тупиковый сегмент Y, то маршрутизатор NAT для сегмента X никак не преобразует пакет.
    3) Если необходимо доставить пакет из тупикового сегмента X в тупиковый сегмент Y, то маршрутизатор NAT для сегмента X инкапсулирует пакет в IP-заголовок с IP-адресом получателя, установленным в глобальный IP-адрес устройства, выполняющего NAT для сегмента Y.
    4) Использование NAT вместе с GRE-туннелем невозможно.

19. Маршрутизатор NAT
    1) Расположен на границе между двумя областями адресов и преобразует адреса в IP-заголовках таким образом, что пакет корректно маршрутизируется при переходе из одной области в другую.
    2) Расположен на границе между двумя локальными сетями с разными требованиями к безопасности.
    3) Расположен на границе между локальной сетью и интернетом.
    4) Расположен на границе между двумя областями адресов, в одной из которых адреса принадлежат частной сети, а в другой – внешней.

20. Отличия двойного NAT от традиционного и двунаправленного NAT
    1) В двойном NAT IP-адреса не изменяются при пересечении дейтаграммой границы пространства адресов.
    2) В двойном NAT изменяются только адреса из внешней сети при пересечении дейтаграммой границы пространства адресов.
    3) В двойном NAT IP-адреса как источника, так и получателя модифицируются NAT при пересечении дейтаграммой границы пространства адресов.
    4) В двойном NAT изменяются только адреса из частной сети при пересечении дейтаграммой границы пространства адресов.

21.NAT используется

1) В IPv32.
2) В IPv64.
3) В IPv6.
4) В IPv4.

22. Следующее структурное подразделение службы защиты информации отвечает за проверку кандидатов для приема на работу на объекте

1) Группа режима
2) Группа охраны и сопровождения
3) Техническая группа
4) Детективная группа

23. Следующее структурное подразделение службы защиты информации отвечает за проведение специальных мероприятий в отношении фирм-конкурентов

1) Группа режима
2) Группа охраны и сопровождения
3) Техническая группа
4) Детективная группа

24. Следующее структурное подразделение службы защиты информации отвечает за контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта

1) Группа режима
2) Группа охраны и сопровождения
3) Техническая группа

25. Следующее структурное подразделение службы защиты информации отвечает за контакты с правоохранительными органами по всем вопросам обеспечения безопасности деятельности объекта

1) Группа режима
2) Группа охраны и сопровождения
3) Техническая группа
4) Детективная группа

26. В обязанности какого сотрудника входит разработка и поддержка эффективных мер защиты по обработке информации для обеспечения сохранное данных

1) Сотрудник группы безопасности
2) Администратор безопасности системы
3) Администратор безопасности данных
4) Руководитель группы

27. В обязанности какого сотрудника входит контроль за выполнением плана восстановления после инцидента информационной безопасности

1) Сотрудник группы безопасности
2) Администратор безопасности системы
3) Администратор безопасности данных
4) Руководитель группы

28. В обязанности какого сотрудника входит реализация и изменение средств защиты данных

1) Сотрудник группы безопасности
2) Администратор безопасности системы
3) Администратор безопасности данных
4) Руководитель группы

29. В обязанности какого сотрудника входит контроль состояния защиты наборов данных

1) Сотрудник группы безопасности
2) Администратор безопасности системы
3) Администратор безопасности данных
4) Руководитель группы

30. В обязанности какого сотрудника входит опубликование нововведений в области защиты

1) Сотрудник группы безопасности
2) Администратор безопасности системы
3) Администратор безопасности данных
4) Руководитель группы

31. В обязанности какого сотрудника входит хранение резервных копий данных

1) Сотрудник группы безопасности
2) Администратор безопасности системы
3) Администратор безопасности данных
4) Руководитель группы

32. В обязанности какого сотрудника входит контроль за выполнением планов непрерывной работы

1) Сотрудник группы безопасности
2) Администратор безопасности системы
3) Администратор безопасности данных
4) Руководитель группы

33. В обязанности какого сотрудника входит контроль защиты наборов данных и программ

1) Сотрудник группы безопасности
2) Администратор безопасности системы
3) Администратор безопасности данных
4) Руководитель группы

34. В обязанности какого сотрудника входит организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности

1) Сотрудник группы безопасности
2) Администратор безопасности системы
3) Администратор безопасности данных
4) Руководитель группы

35. Количественный состав службы безопасности зависит, прежде всего от

1) Типа циркулирующей в ней конфиденциальной информации
2) От возможностей фирмы
3) Нормативных документов регуляторов
4) Численности штата

36. К какому сотруднику предъявляются следующие требования: высшее профессиональное образование и стаж работы в области защиты информации не менее 5 лет, хорошее знание законодательных актов в этой области и принципов планирования защиты

1) Директор
2) Начальник службы защита информации
3) Сотрудник сектора охраны и режима
4) Аналитик
5) Сотрудник сектора технической защиты

37. Кто вырабатывает политику обеспечения защиты информации и обеспечивает ее реализацию?

1) Директор
2) Начальник службы защита информации
3) Аналитик
4) Руководитель группы
5) Юрист
6) Администратор безопасности системы

38. Кто руководит проведением служебных расследований?

1) Директор
2) Начальник службы защиты информации
3) Аналитик

4) Руководитель группы
5) Юрист
6) Администратор безопасности системы

39. Кто несёт персональную ответственность за выполнение службой защиты информации своих функций?
1) Начальник службы защиты информации
2) Сотрудник сектора обеспечения безопасности
3) Аналитик
4) Руководитель группы
5) Юрист

40. Кто разрабатывает руководящие документы и инструкции по вопросам безопасности?
1) Директор
2) Начальник службы защиты информации
3) Сотрудник группы безопасности
4) Аналитик
5) Юрист

41. Кто обеспечивает режим допуска и доступа?
1) Начальник службы защита информации
2) Сотрудник сектора охраны и режима
3) Сотрудник сектора обеспечения безопасности
4) Сотрудник группы безопасности
5) Руководитель группы

42. Какой из перечисленных методов оценки риска основан на расчетах и анализе статистических показателей?
1) Вероятностный метод
2) Метод сценариев
3) Учет рисков при расчете чистой приведенной стоимости
4) Анализ чувствительности

43. Какой из перечисленных методов оценки риска дает представление о наиболее критических факторах инвестиционного проекта?
1) Построение дерева решений
2) Метод сценариев
3) Учет рисков при расчете чистой приведенной стоимости
4) Анализ чувствительности

44. Какой из перечисленных методов оценки риска используется в ситуациях, когда принимаемые решения сильно зависят от принятых ранее и определяют сценарии дальнейшего развития событий?
1) Имитационное моделирование

2) Вероятностный метод
3) Учет рисков при расчете чистой приведенной стоимости
4) Построение дерева решений

45. Каким образом при расчете чистой приведенной стоимости можно учитывать риск?

1) В знаменателе формулы NPV посредством корректировки ставки дисконта
2) Комбинация формул NPV посредством корректировки чистых денежных потоков
3) В числителе формулы NPV посредством корректировки чистых денежных поток
4) Все варианты верны

46. Какой из перечисленных методов оценки риска используется в ситуациях, когда принимаемые решения сильно зависят от принятых ранее и определяют сценарии дальнейшего развития событий?

1) Имитационное моделирование
2) Вероятностный метод
3) Учет рисков при расчете чистой приведенной стоимости
4) Анализ чувствительности
5) Построение дерева решений

47. Что представляет собой стандарт ISO/IEC 27799?

1) Стандарт по защите персональных данных о здоровье .
2) Новая версия BS 17799C.
3) Определения для новой серии ISO 27000.
4) Новая версия NIST 800-60.

48. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

1) Список стандартов, процедур и политик для разработки программы безопасности.
2) Текущая версия ISO 17799.
3) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях.
4) Открытый стандарт, определяющий цели контроля.

49. Из каких четырех доменов состоит CobiT?

1) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
2) Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
3) Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка

4) Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

50. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
1) COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
2) COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
3) COSO учитывает корпоративную культуру и разработку политик
4) COSO – это система отказоустойчивости

51. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?
1) NIST и OCTAVE являются корпоративными
2) NIST и OCTAVE ориентирован на ИТ
3) AS/NZS ориентирован на ИТ
4) NIST и AS/NZS являются корпоративными

52. Как называют протокол IPX, переносящий данные в интрасеть филиалов предприятия?
1) Протокол-пассажир
2) Несущий протокол
3) Протокол туннелирования

53. Что, из перечисленного, понимается под термином частная виртуальная сеть?
1) Шифрованный туннель внутри обычной сети.
2) Локальная сеть в здании.
3) Программный комплекс для шифрования.

54. Одна из причин, по которой коммутаторы не должны использоваться для предоставления каких-либо возможностей межсетевого экрана
1) Коммутаторы не могут видеть передаваемый трафик.
2) Коммутаторы не могут предотвращать возможные DoS-атаки.
3) Коммутаторы не могут видеть порт, на который ушел пакет.
4) Коммутаторы не могут видеть порт, на который пришел пакет.

55. Основное свойство коммутаторов (выберите самое точное определение, один ответ)
1) Коммутаторы передают пакеты только нужному адресату.
2) Коммутаторы могут фильтровать трафик в зависимости от интерфейса, с которого ушел пакет.

3) Коммутаторы могут фильтровать трафик в зависимости от интерфейса, на который пришел пакет.
4) Коммутаторы могут фильтровать трафик в зависимости от типа трафика.

56. Политика безопасности – это (выберите самое точное определение, один ответ)
1) Совокупность административных мер, которые определяют порядок прохода в компьютерные классы.
2) Межсетевые экраны, используемые в организации.
3) Множество критериев для предоставления сервисов безопасности.
4) Совокупность как административных мер, так и множества критериев для предоставления сервисов безопасности.

57. Основные классы атак на передаваемые по сети данные
1) Удаленная и локальная.
2) Видимая и невидимая.
3) Активная и пассивная.
4) Внешняя и внутренняя.

58. Атака называется пассивной, если
1) Оппонент не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения.
2) Оппонент не предполагает проникновение в систему.
3) Оппонент не использует никаких инструментальных средств для выполнения атаки.
4) Оппонент не анализирует перехваченные сообщения.

59. Что не относится к replay-атаке
1) Изменение передаваемых данных.
2) Выполнение незаконного проникновения в систему.
3) Просмотр передаваемых данных.
4) Повторное использование нарушителем перехваченного ранее сообщения.

60. Невозможность получения сервиса законным пользователем называется
1) Атакой «man-in-the-middle».
2) Replay-атакой.
3) DoS-атакой.
4) Пассивной атакой.

61. При анализе производительности межсетевого экрана следует определить
1) Какое количество портов существует на выбранном экземпляре межсетевого экрана.

2) Возможна ли балансировка нагрузки и резервирование для гарантирования высокой отказоустойчивости.
3) Какую пропускную способность, максимальное количество одновременно открытых соединений, соединений в секунду может обеспечивать межсетевой экран.
4) Что является более предпочтительным – аппаратный или программный межсетевой экран.

62. Под безопасностью информационной системы понимается
1) Защита от неавторизованного доступа или модификации информации во время хранения, обработки или пересылки.
2) Отсутствие выхода в интернет.
3) Меры, необходимые для определения, документирования и учета угроз.
4) Защита от отказа в обслуживании законных пользователей.

63. Что не относится к понятию «оборона в глубину»
1) Использование нескольких взаимосвязанных между собой технологий.
2) Использование нескольких коммутаторов.
3) Использование нескольких межсетевых экранов.
4) Использование аппаратных средств разных производителей.

64. Риск — это
1) Вероятность того, что в системе остались неизвестные уязвимости.
2) Вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости.
3) Невозможность ликвидировать все уязвимости в информационной системе.
4) Невозможность исправить все ошибки в программном обеспечении.

65. Возможные стратегии управления рисками
1) Избежать риск.
2) Принять риск.
3) Уменьшить риск.
4) Передать риск.

66. Целостность – это
1) Невозможность несанкционированного доступа к информации.
2) Невозможность несанкционированного выполнения программ.
3) Невозможность несанкционированного изменения информации.

67. Невозможность несанкционированного просмотра информации.
Сервис, который обеспечивает невозможность несанкционированного изменения данных, называется
1) Конфиденциальностью.
2) Целостностью.
3) Аутентификацией.

4) Доступностью.

68. Многофакторная аутентификация означает
    1) Аутентификация не может выполняться с помощью пароля.
    2) Аутентификация должна выполняться с использованием смарт-карты.
    3) Аутентифицируемой стороне необходимо предоставить несколько параметров, чтобы установить требуемый уровень доверия.
    4) Аутентификация должна выполняться третьей доверенной стороной.

69. Гибкость технологии VLAN означает
    1) VLAN обеспечивает эффективный способ аутентификации пользователей.
    2) VLAN являются эффективным способом группирования пользователей и компьютеров в виртуальные рабочие группы, независимо от их физического расположения в сети.
    3) VLAN являются эффективным способом групповой аутентификации пользователей.
    4) VLAN обеспечивает эффективный способ шифрования трафика.

70. Если к маршрутизатору подключены коммутаторы или другие устройства (например, рабочие станции пользователей), не поддерживающие технологию VLAN
    1) На маршрутизаторе можно выполнить сегментацию на требуемое число виртуальных локальных сетей.
    2) На маршрутизаторе можно создать только две VLAN.
    3) На маршрутизаторе можно создать только одну VLAN.
    4) На маршрутизаторе нельзя выполнить сегментацию на виртуальные локальные сети.

71. VLAN-трафик называется
    1) Маркированным (tagged).
    2) Отброшенным (dropped).
    3) Туннелированным (tunneled).
    4) Отфильтрованным (filtered).

72. Технология VLAN описана в стандарте
    1) IEEE 802.3.
    2) IEEE 802.1Q.
    3) RFC 2401.
    4) ISO 9000.

73. Технология VLAN обладает следующими характеристиками
    1) Увеличение пропускной способности сети.
    2) Аутентификация на канальном уровне.
    3) Целостность на канальном уровне.
    4) Целостность некоторой последовательности дейтаграмм.

74. Широковещательные пакеты передаются
    1) Всем хостам в сети, определяемой маской подсети.
    2) Всем хостам сети, подключенным к lan-интерфейсам.
    3) Всем хостам сети, которые доступны со всех интерфейсов маршрутизатора.
    4) Всем хостам сети, подключенным ко всем интерфейсам маршрутизатора или коммутатора.

75. Технология VLAN обладает следующими характеристиками
    1) Гибкость, связанная с возможностью группирования пользователей в виртуальные рабочие группы.
    2) Шифрование трафика.
    3) Аутентификация на уровне пользователя.
    4) Повышение безопасности, связанное с уменьшением широковещательного домена.

76. Состояние TCP-соединения LISTEN
    1) Состояние сервера после отправления клиенту пакета с флагами SYN, ACK.
    2) Состояние сервера после получения от клиента пакета с установленными флагами SYN, ACK.
    3) Состояние сервера, в котором он ожидает запрос от клиента на создание соединения.
    4) Состояние сервера после получения от клиента пакета с установленным флагом SYN.

77. Анализ состояния в пакетном фильтре означает
    1) Отслеживание состояния соединения и оповещение администратора о наличии пакета, который не соответствует ожидаемому.
    2) Отслеживание состояния соединения и отбрасывание пакетов, которые не соответствуют ожидаемому.
    3) Отслеживание состояния соединения и запрещение всего трафика, если обнаружен пакет, который не соответствует ожидаемому.
    4) Отслеживание состояния соединения и вставка собственных пакетов, если обнаружен пакет, который не соответствует ожидаемому.

78. Прикладной уровень модели OSI
    1) Посылает и получает данные конкретных приложений.
    2) Выполняет фрагментацию/ дефрагментацию пакетов.
    3) Выполняет шифрование трафика.
    4) Обеспечивает маршрутизацию между локальными сетями.

79. Транспортный уровень модели OSI
    1) Некоторые протоколы данного уровня гарантируют надежность соединения.

2) Все протоколы данного уровня гарантируют надежность соединения.
3) Предоставляет сервисы, ориентированные на соединение.
4) Некоторые протоколы данного уровня обеспечивают целостность соединения.

80. Адреса канального уровня называются
1) MAC-адресами.
2) Веб-именами.
3) IP-адресами.
4) DNS-именами.

81. Пакетные фильтры с поддержкой состояния
1) Анализирует правильную последовательность пакетов на транспортном уровне.
2) Анализируют состояние защищаемой локальной сети.
3) Анализируют состояние межсетевого экрана.
4) Анализирует правильную последовательность пакетов на прикладном уровне.

82. Сокетом называется
1) Пара (MAC-адрес, IP-адрес).
2) Пара (IP-адрес, порт).
3) Пара (DNS-имя, IP-адрес).
4) Пара (DNS-имя, порт).

83. Инициализация TCP-соединения выполняется
1) Сервером.
2) Клиентом.
3) Третьей доверенной стороной.
4) Администратором.

84. При установлении TCP-соединения
1) Клиент посылает пакет ClientHello.
2) Клиент посылает пакет с установленными битами SYN, ACK.
3) Клиент посылает пакет с установленным битом Start.
4) Клиент посылает пакет с установленным битом SYN.

85. Межсетевые экраны для веб-приложений располагают
1) Перед защищаемым веб-сервером (трафик вначале передается межсетевому экрану, затем веб-серверу).
2) Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, но трафик между ними не запрещен.
3) После защищаемого веб-сервера (трафик вначале передается веб-серверу, затем межсетевому экрану).
4) Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, трафик между ними запрещен.

86. Отличия выделенного прокси-сервера от прикладных прокси-шлюзов
    1) Выделенные прокси-сервера обладают меньшей производительностью.
    2) Выделенные прокси-сервера не могут выполнять аутентификацию пользователей.
    3) Выделенные прокси-сервера не могут анализировать заголовки транспортного уровня.
    4) Выделенные прокси-сервера имеют более ограниченные возможности межсетевого экранирования.

87. Недостатки межсетевых экранов прикладного уровня
    1) Производительность межсетевого экрана прикладного уровня ниже, чем у пакетного фильтра.
    2) Межсетевой экран прикладного уровня не может анализировать заголовки транспортного и сетевого уровней.
    3) Межсетевой экран прикладного уровня обеспечивает меньший уровень безопасности, чем пакетный фильтр.
    4) Межсетевой экран прикладного уровня обязательно разрывает TCP-соединение.

88. Прокси-сервер не может быть
    1) Исходящим.
    2) Шифрующим.
    3) Входящим.
    4) Туннелирующим.

89. Персональные межсетевые экраны для настольных компьютеров и ноутбуков являются
    1) Исключительно программными.
    2) Аппаратно-программными средствами защиты.
    3) Не могут быть встроенными в ОС, которую они защищают; всегда реализованы внешними производителями.
    4) Всегда встроены в ОС, которую они защищают; не могут быть реализованы внешними производителями.

90. При использовании прокси-шлюзов прикладного уровня
    1) Прокси-шлюз является абсолютно прозрачным для клиента.
    2) Внешние IP-адреса не видны изнутри.
    3) Внутренние IP-адреса не видны вовне.
    4) Прокси-шлюз изменяет IP-адрес источника на свой IP-адрес.

91. Недостатки использования системы унифицированного управления угрозами
    1) Может существенно усложниться управление всеми устройствами.
    2) Может существенно ухудшиться производительность, если системе унифицированного управления угрозами не будет хватать ресурсов.

3) Может существенно возрасти нагрузка на рабочие станции пользователей.
4) Может существенно возрасти нагрузка на прикладные сервера.

Задания в открытой форме

1) … процессом называется процесс изготовления одного или нескольких изделий в соответствии с требованиями принятой для данных условий производства технологической документации.
2) … – лишь один из многих способов (пусть и самый важный) обеспечить корпоративную защиту. Необходим комплекс мер – технических и организационных.
3) Важная особенность DLP-систем – их …
4) … - самый ценный ресурс в компании, а в некоторых случаях является и производственным ресурсом, от сохранности которого зависят важные технологические процессы.
5) … – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.
6) … — это комплекс мероприятий, направленных на обеспечение информационной безопасности.
7) … уровень является важнейшим для обеспечения информационной безопасности.… система — взаимосвязанная совокупность средств, методов и персонала, которые используются для хранения, обработки, передачи и получения информации в интересах достижения поставленной цели.
8) … информации в ИС – это такое состояние всех компонент информационной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне.
9) Под … в ИС понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности.
10) Цель … – обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством их предотвращения и сведения последствий к минимуму.
11) … — это защита от несанкционированного доступа к информации
12) Под ... информации подразумевается, ее защищенность от разрушения и несанкционированного изменения.
13) … — это возможность за приемлемое время получить требуемую информационную услугу.
14) … автоматизированной информационной системы -- состояние защищённости автоматизированной системы, при котором

обеспечиваются конфиденциальность, доступность, целостность, подотчётность и подлинность её ресурсов.

15) … можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)).
16) … – действие, которое потенциально может привести к нарушению безопасности
17) … – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.
18) … — меры физической защиты, персонал и его специфика;
19) … аспект. Означает, что нужно тщательно контролировать работу с данными, чтобы устранить возможность их утечки, а также предотвратить несанкционированный доступ к ним со стороны неизвестных людей.
20) Под … понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре…. — документ, содержащий требования безопасности для конкретной разработки, выполнение которых обеспечивает достижение поставленных целей безопасности.

Задание на установление соответствия

1. Установить соответствие видов угроз:

1) Аппаратная	a) Когда возможен несанкционированный доступ к данным и их потеря.
2) Вероятность утечки	b) Когда существует вероятность нарушения работоспособности оборудования.
3) Нестабильность ПО	c) Когда есть вероятность некорректной работы программного обеспечения.

2. Установить соответствие оценки рисков в зависимости от факторов:

1) Высокий риск	a) Предполагается, что без снижения таких рисков обращение к информационной системе предприятия может оказать отрицательное влияние на бизнес;

2) Существенный риск	b) Здесь требуется эффективная стратегия управления рисками, которая позволит уменьшить или полностью исключить отрицательные последствия нападения;
3) Умеренный риск	c) Усилия по управлению рисками в данном случае не будут играть важной роли.
4) Незначительный риск	d) В отношении рисков, попавших в эту область, достаточно применить основные процедуры управления рисками;

3. Установить соответствие:

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

4. Установить соответствие:

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

5. Установить соответствие:

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

6. Установить соответствие:

1) Правовая защита	a) Это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, которая исключает или ослабляет нанесение каких-либо убытков предприятию;
2) Организационная защита	b) Это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, которые обеспечивают защиту информации на правовой основе;
3) Инженерно-техническая защита	c) Это использование разнообразных технических средств, которые препятствуют нанесению убытков предприятию.

7. Установить соответствие:

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

	компьютере, так и распределенного в сети.
4) MTS (Microsoft Transaction Server)	d) Технология создания программируемых приложений, обеспечивающая программируемый доступ к внутренним службам этих приложений

8. Установить соответствие средств информационной защиты:

1) SIEM-системы	a) Виртуально-частная сеть определяет использование собственной частной сети внутри общедоступной. Поэтому ваше приложение, работающее по VPN, будет надежно защищено.
2) CloudAV	b) Они собирают информацию о возможных угрозах из различных источников: файервол, антивирус, межсетевой экран и др., потом проводят анализ и могут среагировать на вероятность возникновения потенциальной угрозы, предупредив о ней заранее.
3) Брандмаузер и фаервол	c) Это специальная система шифрования вашей информации. Шифровка происходит таким образом, что для того, чтобы расшифровать нужную информацию, необходимо обладать специальным шифром.
4) Криптографическое преобразование	d) Это специализированные средства, которые контролируют выход во всемирную паутину, при необходимости фильтруют или блокируют сетевой трафик.

9. Установить соответствие средств информационной защиты:

1) Программы-антивирусы	a) Это специальные технологии, которые предотвращают потерю конфиденциальной информации. Как правило, данная технология

	используется большими предприятиями, так как требует больших финансовых и трудоресурсных затрат.
2) VPN	b) Борются с самыми распространенными вирусами, также способны восстанавливать поврежденные файлы.
3) DLP-решения	c) Это облачные решения для обеспечения антивирусной защиты вашего ресурса.

10. Установить соответствие:

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

11. Установить соответствие:

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

12. Установить соответствие:

1) Точность результатов	a) Возможность совместного функционирования с некоторым оборудованием
2) Защищенность	b) Возможность совместного функционирования с другим программным обеспечением
3) Программная совместимость	c) Обеспечение конфиденциальности инф ормации;
4) Аппаратная совместимость	d) Обеспечение погрешности результатов не выше заданной;

13. Установить соответствие:

1) Точность результатов	a) Возможность совместного функционирования с некоторым оборудованием
2) Защищенность	b) Возможность совместного функционирования с другим программным обеспечением
3) Программная совместимость	c) Обеспечение конфиденциальности инф ормации;
4) Аппаратная совместимость	d) Обеспечение погрешности результатов не выше заданной;

14. Установить соответствие каналов утечки:

1) Электрические	a) Электромагнитные излучения радиодиапазона
2) Оптические	b) Электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра
3) Акустические и виброакустическ ие	c) Звуковые колебания в любом звукопроводящем материале или среде
4) Радиоканалы	d) Напряжение и ток в различных токопроводящих коммуникациях

15. Установить соответствие каналов утечки:

1) Защита от утечек информации электромагнитных излучений	a) Используется установка источников бесперебойного питания (ups)
2) Защита от сбоев в электропитании	b) Используется организация надежной и эффективной системы резервного копирования и дублирования данных
3) Защита от сбоев устройств для хранения информации	c) Используется резервирование особо важных компьютерных подсистем
4) Защита от сбоев серверов, рабочих станций и локальных компьютеров	d) Используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений

16. Установить соответствие каналов утечки:

1) Несанкционированное копирование, уничтожение или подделка информации	a) Ошибки персонала и пользователей
2) Перебои электропитания	b) Из-за некорректной работы программ
3) Случайное уничтожение или изменение данных	c) Потери информации, связанная с несанкционированным доступом
4) Потеря или изменение данных при ошибках по	d) Сбои оборудования, при котором теряется информация

17. Установить соответствие:

1) Программно-аппаратные	a) Для обеспечения безопасности используются приемы

(технические) методы	«перестраховки», с помощью которых исключается возможность ошибочного или несанкционированного проникновения в информационную систему
2) Физическая защита	b) Для осуществления информационной защиты используются специальные компьютерные технологии. С их помощью можно скрыть важные данные, не допустить утечки во время пересылки через интернет
3) Морально-этические методы	c) Профилактические действия, в основном, воспитательного характера
4) Технологические приемы	d) Мероприятия направлены на снижение риска потери данных и выявление лиц, пытающихся проникнуть на охраняемую территорию или в информационную систему

18. Установить соответствие:

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

19. Установить соответствие степеней происхождения угрозы информационной безопасности:

1) Естественная	a) Данные угрозы, в свою очередь, делятся на 2 подкатегории: преднамеренная подкатегория — это действия хакеров, конкурентов, недобросовестных сотрудников и т. д., непреднамеренная — действия происходят из-за людей по их неосторожности.
2) Искусственная	b) Это те угрозы, которые не зависят от деятельности человека: землетрясения, ураганы, смерчи, дожди, молнии и т. д.
3) Внутренняя	c) Все угрозы, которые происходят вне системы.
4) Внешняя	d) Угроза исходит изнутри самой системы.

20. Установить соответствие средства обеспечения информационной безопасности:

1) Организационные	a) Сюда входит весь перечень программного обеспечения, который поможет обеспечить должную информационную безопасность ресурса
2) Программные	b) Сюда входят сами приборы и устройства, которые обеспечивают защиту информации.
3) Аппаратные	c) Сюда входят: обеспечение качественного помещения для размещения серверов, качественное оборудование, продуманная кабельная система, организация правового статуса ресурса или компании и др.

Задание на установление правильной последовательности

1. Установить этапы построения программы обеспечения безопасности:
   1) Формирование политики безопасности организации
   2) Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности

3) Регулярный контроль пошаговой реализации плана безопасности
4) Установление уровня безопасности
5) Определение ценности технологических и информационных активов организации

2. Установить иерархию последовательно:
   1) Компонент
   2) Семейства
   3) Элемент
   4) Компонент

3. Установить этапы системы управления:
   1) Планирование.
   2) Внедрение.
   3) Мониторинг и анализ.
   4) Совершенствование.

4. Установите этапы PDCA:
   1) Планирование
   2) Проверка
   3) Действие
   4) Выполнение

5. Установите этапы этапы создания СУИБ:
   1) Внедрение и функционирование системы управления информационной безопасности.
   2) Проведение мониторинга и анализа системы управления информационной безопасности.
   3) Разработка системы управления информационной безопасности.
   4) Поддержка и улучшение системы управления информационной безопасности.

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

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

8. Основные этапы разработки системы управления информационной безопасностью:
   1) Обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов);
   2) Контроль выполнения и эффективности выбранных мер.
   3) Оценка защищенности информационной системы;
   4) Оценка информационных рисков;
   5) Инвентаризация активов;
   6) Внедрение выбранных мер обработки рисков;
   7) Категорирование активов;

9. Установить предпочтительную последовательность этапов внедрения межсетевого экрана:
   1) Конфигурирование
   2) Планирование
   3) Тестирование
   4) Развертывание
   5) Управление

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

11. Установите фазы анализа OCTAVE:
   1) Разработка профиля угроз, связанных с активом.
   2) Идентификация инфраструктурных уязвимостей.
   3) Разработка стратегии и планов безопасности.

12. Установите этапы процесса управления рисками:
   1) Выбор анализируемых объектов и уровня детализации их рассмотрения.
   2) Инвентаризация активов.
   3) Анализ угроз и их последствий, выявление уязвимых мест в защите.
   4) Оценка рисков.
   5) Выбор методики оценки рисков.

13. Установите этапы процесса управления рисками:
   1) Реализация и проверка выбранных мер.
   2) Выбор защитных мер.
   3) Обработка рисков.

4) Оценка остаточного риска.

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

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

16. Выберите правильную последовательность этапов разработки профиля защиты.
    1) Анализ среды применения ИТ-продукта с точки зрения безопасности.
    2) Выбор профиля-прототипа.
    3) Синтез требований.

17. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:
    1) Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
    2) Реализация защитных мер по противодействию скрытых каналов
    3) Организация контроля за противодействием скрытых каналов.
    4) Выявление скрытых каналов и оценка их опасности для активов организации

18. Выберите правильную последовательность этапов процесса управления рисками:
    1) Идентификация активов и ценности ресурсов, нуждающихся в защите;
    2) Анализ угроз и их последствий, определение слабостей в защите;
    3) Классификация рисков, выбор методологии оценки рисков и проведение оценки;
    4) Выбор, реализация и проверка защитных мер;
    5) Оценка остаточного риска;
    6) Выбор анализируемых объектов и степени детальности их рассмотрения;

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

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

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

2.2КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1. Задача планирования процесса разработки системы безопасности: Вам поручено управлять процессом разработки системы безопасности для нового проекта. Ваша задача - разработать детальный план, включающий определение целей системы безопасности, этапы разработки, ресурсы, сроки и оценку затрат. Учтите различные аспекты, такие как угрозы, требования безопасности и бюджет.

2. Задача определения требований безопасности: Сотрудники различных отделов компании имеют доступ к различным системам и данным. Ваша задача - провести обзор бизнес-процессов и определить требования безопасности для каждого отдела. Учтите различные аспекты, такие как конфиденциальность данных, контроль доступа и аудит безопасности.

3. Задача выбора технологий и инструментов: Определите подходящие технологии и инструменты для разработки системы безопасности. Исследуйте различные решения, проведите оценку их функциональности, соответствия требованиям безопасности и бюджету проекта. Разработайте рекомендации по выбору и внедрению этих технологий и инструментов.

4. Задача управления рисками: Разработайте стратегию управления рисками в процессе разработки системы безопасности. Определите потенциальные угрозы и уязвимости, проведите анализ рисков и разработайте планы по их снижению или устранению. Включите меры по контролю и мониторингу рисков на протяжении всего процесса разработки.

5. Задача оценки качества системы безопасности: Разработайте методику оценки качества системы безопасности. Определите ключевые показатели эффективности и стандарты безопасности, которые должны быть достигнуты. Разработайте процедуры тестирования и аудита системы безопасности, чтобы убедиться в ее соответствии требованиям и эффективности.

6. Задача определения требований безопасности: Ваша компания решила разработать новую информационную систему, и вам поручено определить требования безопасности для этой системы. Исследуйте бизнес-потребности компании, проведите анализ рисков и угроз, и разработайте набор требований безопасности, которые должны быть учтены в процессе разработки системы.

7. Задача управления жизненным циклом системы безопасности: Ваша компания уже имеет системы безопасности, и ваша задача - управлять их жизненным циклом. Создайте планы обновления и модернизации систем, определите процедуры тестирования и внедрения изменений, и обеспечьте своевременное внедрение новых технологий и методов безопасности.

8. Задача разработки политики безопасности: Вам поручено разработать политику безопасности для вашей компании. Проведите анализ рисков, определите правила доступа и использования информации, разработайте процедуры управления учетными записями и обработки конфиденциальных данных, и создайте понятную и эффективную политику безопасности, которая будет соответствовать бизнес-потребностям компании.

9. Задача выбора и внедрения систем безопасности: Вам необходимо выбрать и внедрить системы безопасности в вашей компании. Исследуйте рынок, оцените различные системы безопасности, проведите анализ их функциональности и соответствия требованиям компании. После выбора системы разработайте план внедрения, определите этапы и ресурсы, необходимые для успешного внедрения и настройки системы безопасности.

10. Задача координации команды разработки безопасности: Ваша задача - координировать работу команды разработки безопасности. Управляйте распределением задач, обеспечьте коммуникацию и сотрудничество между членами команды, отслеживайте прогресс разработки и обеспечьте своевременное выполнение поставленных целей и задач.

11. Задача определения требований безопасности: Вам поручено управлять процессом разработки новой информационной системы с учетом аспектов безопасности. Ваша задача - провести анализ рисков и уязвимостей, определить требования безопасности, которые должны быть учтены при разработке, и создать список необходимых мер безопасности.

12. Задача выбора архитектуры безопасности: Вам необходимо выбрать подходящую архитектуру безопасности для новой информационной системы. Исследуйте различные модели и методы защиты, оцените их применимость и выберите наиболее эффективную архитектуру безопасности, которая будет соответствовать требованиям системы.

13. Задача разработки плана обеспечения безопасности: Разработайте план обеспечения безопасности для проекта разработки новой системы. Определите этапы и мероприятия, которые необходимо выполнить для обеспечения безопасности на различных уровнях: физическом, логическом и операционном. Включите в план тестирование, аудит и обучение персонала.

14. Задача координации команды разработки: Управляйте командой разработки, которая работает над созданием системы безопасности. Распределите задачи между участниками команды, обеспечьте коммуникацию и сотрудничество, следите за прогрессом и качеством работы. Управляйте ресурсами и сроками проекта, чтобы обеспечить успешное выполнение задачи.

15. Задача тестирования и оценки эффективности системы безопасности: Разработайте план тестирования системы безопасности и

проведите соответствующие тесты и оценки. Используйте инструменты и методики тестирования, чтобы проверить эффективность реализованных мер безопасности, выявить слабые места и рекомендовать улучшения.

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.