

СОГЛАСОВАН

решением Ученого совета
АНО ВО «МБИ
имени Анатолия Собчака»
(протокол от «25» декабря 2021 г. № 6)

АКТУАЛИЗИРОВАН

решением Ученого совета
АНО ВО «МБИ
имени Анатолия Собчака»
(протокол от «25» декабря 2025 г. № 7)

УТВЕРЖДЕН

приказом ректора
АНО ВО «МБИ
имени Анатолия Собчака»
от «27» декабря 2021 г. № 65

УТВЕРЖДЕНА

актуализированная версия
приказом ректора
АНО ВО «МБИ
имени Анатолия Собчака»
от «30» декабря 2025 г. № 59

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ по дисциплине **Управление информационной безопасностью**

специальность

38.05.01 Экономическая безопасность

специализация

Экономико-правовое обеспечение экономической безопасности

уровень образования

высшее образование - специалитет

форма обучения

очно-заочная

год набора

2022

Санкт-Петербург
2021

СОДЕРЖАНИЕ

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ И ЭТАПЫ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ	3
2. СТРУКТУРА ФОС ПО ДИСЦИПЛИНЕ.....	3
3. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНКИ КОМПЕТЕНЦИЙ	5
4. ШКАЛА ОЦЕНИВАНИЯ РЕЗУЛЬТАТА.....	6
5. ПЕРЕЧЕНЬ ЗАДАНИЙ ПО ДИСЦИПЛИНЕ	6
5.1. ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ:.....	6
5.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ТЕКУЩЕЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ.....	7
5.3 ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ.....	17
6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ...	24
7. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ.....	25
7.1. ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ.....	27
7.2. ЗАДАНИЯ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ.....	28

1. ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ И ЭТАПЫ ИХ ФОРМИРОВАНИЯ В ПРОЦЕССЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1. Фонд оценочных средств предназначен для оценки результатов обучения по учебной дисциплине.

Рабочей программой дисциплины (модуля) предусмотрено формирование следующих компетенций:

Код и наименование компетенции выпускника	Код и наименование индикатора достижения компетенций	Планируемые результаты обучения по дисциплине
ПК-3 Способен осуществлять информационно-аналитическое обеспечение защиты экономических интересов хозяйствующих субъектов, выявлять скрытые угрозы и прогнозировать риски на основе анализа больших данных и открытых источников	ПК-3.2 Использует методы предотвращения утечек информации и защиты конфиденциальных данных компании при проведении аналитических исследований, защищает информацию и информационную инфраструктуру организации от негативных воздействий	<i>Знать:</i> международные и отечественные стандарты, лучшие практики и фреймворки по управлению информационной безопасностью ресурсов ИТ; методы и средства обеспечения безопасности ИТ, критерии оценки безопасности ИТ; методы контроля безопасности ИТ; методы непрерывного улучшения управления информационной безопасностью; <i>Уметь:</i> формировать и декомпозировать цели управления информационной безопасностью ресурсов ИТ; использовать методы и средства обеспечения безопасности ИТ, соответствующие критериям оценки безопасности ИТ; формировать команду и организовывать персонал и стейкхолдеров для управления информационной безопасностью; осуществлять мониторинг и контроль управления информационной безопасностью; организовывать деятельность по непрерывному улучшению УИБ ресурсов ИТ; <i>Владеть:</i> навыками решения профессиональных задач посредством частных инструментов по управлению ИБ

1.2. Входной уровень знаний, умений, опыта деятельности, требуемых для формирования компетенции

– на уровне знаний: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах

– на уровне умений: разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем; анализировать и оценивать угрозы информационной безопасности объекта

– на уровне навыков: навыками анализа и синтеза структурных и функциональных схем защищенных автоматизированных информационных систем; навыками анализа основных характеристик и возможностей теле-коммуникационных систем по передаче информации

2. СТРУКТУРА ФОС ПО ДИСЦИПЛИНЕ

Оценка проводится методом сопоставления параметров продемонстрированной обучающимся продукта деятельности с заданными эталонами и стандартами по критериям.

Таблица – 1.1. Объекты оценивания и наименование оценочных средств

Номер и наименование	Формы текущего	Объекты оценивания	Вид занятия /	Форма проведения
----------------------	----------------	--------------------	---------------	------------------

е разделов/тем	контроля успеваемости / промежуточной аттестации		Наименование оценочных средств	оценки Устная/ письменная
Тема 1 Базовые вопросы управления ИБ	Текущий контроль	Стандартизация в области управления ИБ. Важность и актуальность дисциплины. - Ее взаимосвязь с другими дисциплинами специальности. Содержание дисциплины. Виды контроля знаний. Сущность и функции управления. Наука управления. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Стандартизация в области построения систем управления.	ДП доклад презентации, Т – тест	устная/ письменная
Тема 2 Системы управления ИБ	Текущий контроль	Процессный подход. Понятие процесса. Методы формализации процессов. Область деятельности СУИБ. Понятие области деятельности СУИБ. Механизм выбора области деятельности. Ролевая структура СУИБ. Понятие роли. Использование ролевого принципа в рамках СУИБ. Политика СУИБ. Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ. Источники информации для разработки Политики СУИБ.	Доклад презентации Тест Задания Реферат коллоквиум	Устная письменная
Тема 3 Основы управления рисками ИБ	Текущий контроль	Рискология ИБ. Основные определения и положения рискологии. Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Анализ рисков ИБ. Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов.	Доклад презентации Тест Задания Реферат коллоквиум	Письменная Устная
Тема 4 Процессы управления ИБ.	Текущий контроль	Основные процессы СУИБ. Обязательная документация СУИБ. Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».	Доклад презентации Тест Лабораторная Задания Реферат коллоквиум	Устная письменная
Тема 5 Внедрение разработанных процессов	Текущий контроль	Документ «Положение о применимости». Этапы внедрения процессов и их последовательность. Обучение сотрудников, как один из этапов внедрения. Сложности, возникающие при внедрении процессов управления ИБ и способы их решения. Контроль над внедрением процессов. Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа. Внедрение мер (контрольных процедур) по обеспечению ИБ Категории контрольных процедур. Перечень контрольных процедур по обеспечению ИБ в соответствии с лучшими международными практиками.	Доклад презентации Тест Лабораторная Задания Реферат коллоквиум	Устная письменная

		Содержание контрольных процедур по обеспечению ИБ в интерпретации лучших практик.		
Тема 6. Процесс «Управление инцидентами ИБ»	Текущий контроль	Процесс «Управление инцидентами ИБ». Цели и задачи процесса «Управления инцидентами ИБ, важность процесса с точки зрения управления ИБ. Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ. Процесс «Обеспечение непрерывности ведения бизнеса». Цели и задачи процесса «Обеспечение непрерывности ведения бизнеса». Входные/выходные данные процесса. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.	Доклад с презентацией Тест Лабораторная Задания Реферат коллоквиум	Письменная устная
Тема 7. Эксплуатация и независимый аудит СУИБ	Текущий контроль	Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены)	Доклад с презентацией Тест Лабораторная Задания Реферат коллоквиум	Письменная Устная
Все темы и разделы:	Промежуточная аттестация	Обобщенные результаты обучения по овладению теоретическими знаниями и практическими навыками	Т – тест (1-30)	Письменная

3. ПОКАЗАТЕЛИ И КРИТЕРИИ ОЦЕНКИ КОМПЕТЕНЦИЙ

Оценка знаний, умений, владений выражается в пятибалльной системе.

Таблица 3.1 – Текущий контроль

№ п/п	Виды работ	Критерии оценивания			
		Неудовлетворительно (2 балла)	Удовлетворительно (3 балла)	Хорошо (4 балла)	Отлично (5 баллов)
1	Работа на лекциях	Отсутствие участия студента в работе на занятии	Единичное высказывание	Высказывание суждений, активное участие в работе на занятии	Высказывание неординарных суждений, активное участие в работе на занятии
2	Работа на практических занятиях, решение общих практических задач	Отсутствие участия в обсуждении, решении, неправильное решение	Единичное высказывание, решение с ошибками	Высказывание суждений, активное участие в ходе решения, правильное решение с отдельными замечаниями	Высказывание неординарных суждений, активное участие в ходе решения, правильное решение без ошибок
3	Работа на практических занятиях, решение индивидуальных практических задач	Отсутствие участия в обсуждении, решении, неправильное решение	Единичное высказывание, решение с ошибками	Высказывание суждений, активное участие в ходе решения, правильное решение с отдельными замечаниями	Высказывание неординарных суждений, активное участие в ходе решения, правильное решение без ошибок

Критерии оценивания формулируются для каждой компетенции и отражают деятельность обучающегося, поддающуюся измерению.

Таблица 3.2 – Обобщенные критерии оценивания освоения компетенции

Неудовлетворительно (2 балла)	Удовлетворительно (3 балла)	Хорошо (4 балла)	Отлично (5 баллов)
Компетенция не освоена. Обучающийся не показывает знания, входящие в состав компетенции, не понимает их необходимость и/или не может их применять	Компетенция освоена. Обучающийся показывает общие знания, входящие в состав компетенции, имеет представление об их применении, умение извлекать и использовать основную (важную) информацию из полученных знаний	Компетенция освоена. Обучающийся показывает полноту знаний, демонстрирует умения и навыки решения типовых задач	Компетенция освоена. Обучающийся показывает глубокие знания, демонстрирует умения и навыки решения сложных задач, умение принимать решения, создавать и применять документы, связанные с профессиональной деятельностью; способен самостоятельно решать проблему/задачу на основе изученных методов, приемов и технологий.

4. ШКАЛА ОЦЕНИВАНИЯ РЕЗУЛЬТАТА

Таблица 4.1 – Шкала критериев оценивания компетенций

Оценка	Содержание
Неудовлетворительно (2 балла)	Демонстрирует непонимание проблемы, не восприятие материала. Работа незакончена и/или это плагиат
Удовлетворительно (3 балла)	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены. Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер
Хорошо (4 балла)	Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены. Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения
Отлично (5 баллов)	Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены. Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостный характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход

Шкалы оценивания и процедуры оценивания результатов обучения по дисциплине регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования.

5. ПЕРЕЧЕНЬ ЗАДАНИЙ ПО ДИСЦИПЛИНЕ

5.1. ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ:

Таблица - 5.1 Перечень заданий текущего контроля и их наименование

Наименование оценочных средств	Содержание задания
Доклад презентацией	Наиболее распространенные угрозы доступности.. Программные угрозы доступности. Основные угрозы целостности. Статическая и динамическая целостность.. Основные угрозы конфиденциальности. Таксономия угроз безопасности. Что такое уязвимость защиты? Таксономия угроз безопасности. Ошибки в системах защиты. Что такое антивирусная программа? Вирусная сигнатура. Виды антивирусных программ. Основополагающие принципы решения задачи закрытия каналов несанкционированного доступа. Понятие политики и модели безопасности. Структура монитора обращений.
коллоквиум	Методы идентификации и аутентификации. Способы аутентификации – пользователь «знает», пользователь «имеет» и пользователь «есть». Базовые представления моделей безопасности. Субъекты, объекты и доступ. Произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа. Модель Харрисона-Руззо-Ульмана.. Мандатная модель Белла-Лападулы. Свойство простой безопасности. Свойства ограничения. Свойство самостоятельной защиты. Правила перехода. Какая главная задача стандартов информационной безопасности? «Оранжевая книга» США. Базовые требования

	безопасности. Четыре группы критериев безопасности. Европейские критерии безопасности информационных технологий. Адекватность средств защиты. Уровни безопасности системы.
реферат	1. Основные руководящие документы Гостехкомиссии по вопросам защиты от несанкционированного доступа к информации. Классы защищенности. 2. ГОСТ Р ИСО МЭК 15048-2002 «Общие критерии оценки безопасности информационных технологий». Профиль защиты. функции безопасности. Предложения безопасности. 3. Основные функции организационно-правовой базы защиты информации. Виды информационных ресурсов. Какую информацию относят к защищаемой? 4. Признаки защищаемой информации. Владельцы защищаемой информации. Понятие «государственная тайна». 5. Криптографические механизмы и примитивы. Базовые методы преобразования информации используемые в криптографии. Основные группы методов защитных преобразований. Методы перестановки, подстановки, аддитивные и комбинированные. 6. Криптография с симметричными ключами. Алгоритм DES, ГОСТ 28147-80., IDEA. Преимущества и недостатки криптографии с симметричными ключами. 7. Ассиметричные алгоритмы шифрования. Криптосистема с открытым ключом RSA. ХЭШ-функция. Понятие односторонней функции. Коллизия хэш-функции. 8. Иерархический метод разработки защищенных систем. Понятие доверенной вычислительной среды (trusted computing base - TCB)
Лабораторная	Лабораторная работа 1. Сбор исходных данных для аудита информационной Безопасности объекта Лабораторная работа 2. Выявление уязвимостей информационной системы Лабораторная работа 3. Идентификация защитных механизмов Лабораторная работа 4. Идентификация нарушителей
задания	1. Международные стандарты в сфере управления информационной безопасностью. 2. Программные и программно-аппаратные средства защиты информации. 3. Программные средства автоматизации процедур проведения аудита информационной безопасности и анализа политики информационной безопасности. 4. Программные средства поддержки процессов управления информационной безопасностью
Тест	Темы тестовых заданий: Тема 1 Базовые вопросы управления ИБ Тема 2. Системы управления ИБ Тема 3. Основы управления рисками ИБ Тема 4. Процессы управления ИБ. Тема 5. Внедрение разработанных процессов Тема 6. Процесс «Управление инцидентами ИБ» Тема 7. Эксплуатация и независимый аудит СУИБ

5.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ТЕКУЩЕЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

Первая контрольная точка - в форме доклада (письменная).

Темы докладов: Темы докладов с презентацией

1. Бизнес-ориентированное управление ИТ на современном предприятии.
2. Виды программ технического обслуживания (стандартные программы).
3. Значение технического обслуживания.
4. Как обслуживаются высококритичные системы.
5. Концепция управления ИТ-подразделением — IT Service Management.
6. Функциональные требования. Вопросы гарантий и эффективности в европейском стандарте ITSEC
7. Гарантии безопасности компьютерных систем в системе общих критериев
8. Классификация защищенности компьютерной системы по требованиям безопасности информации в системе общих критериев
9. Основные угрозы безопасности информации в компьютерных системах
10. Государственная политика в области безопасности компьютерных систем
11. Порядок сертификации средств защиты информации для разработчика СЗИ.
12. Порядок сертификации защищенных информационных систем
13. Порядок лицензирования в области создания средств защиты информации и защищенных информационных систем
14. Разработка политик безопасности для защищенных компьютерных систем
15. Порядок аттестации защищенных компьютерных систем

16. Критерии эффективности работы ИС.
17. Оперативные мероприятия.
18. Организация технического обслуживания ИТ.
19. Плановые мероприятия.
20. Понятие гарантии.
21. Порядок внедрения SLM-системы.
22. Порядок осуществления гарантии.
23. Преимущества внедрения ITSM.
24. Причины отказа в гарантийном обслуживании.
25. Программы технического обслуживания.
26. Разовые мероприятия.
27. Расширенные программы технического обслуживания.
28. Регламентные мероприятия.
29. Содержание модели ITSM HP. Процессы взаимодействия и ИТ-служб.
30. Содержание модели ITSM HP. Процессы проектирования и управления услугами.
31. Содержание модели ITSM HP. Процессы разработки услуг.
32. Содержание модели ITSM HP. Процессы эксплуатации.
33. Схемы технического обслуживания.
34. Эталонная модель Hewlett-Packard управления ИТ-услугами.

Методические рекомендации:

Обучающийся может подготовить не более пяти докладов с презентацией. Критерии оценки одного доклада с презентацией: 5 баллов выставляется обучающемуся, если он перечисляет все существенные характеристики обозначенного в вопросе предмета и возможные варианты дальнейшего развития решения проблемы, если это возможно; 4 балла, если студент раскрыл только часть основных положений вопроса, продемонстрировал неточность в представлениях о предмете вопроса; 3 балла, если студент обозначил общую траекторию ответа, но не смог конкретизировать основные компоненты; 2 балла, если студент не продемонстрировал знаний основных понятий, представлений об изучаемом предмете.

Методические указания по написанию доклада с презентацией. Требования, предъявляемые к докладу с презентацией:

1. Объем доклад не должен превышать 5-8 страниц. Печать производится через 1,5 интервала, размер шрифта 14, с выравниванием по ширине. Левое поле листа 30 мм, правое – 10 мм, верхнее – 20 мм, нижнее 20 мм. Текст должен оформляться абзацами с отступом 1,25 см.
2. Эссе должно восприниматься как единое целое, идея должна быть ясной и понятной.
3. Необходимо писать коротко и ясно. Эссе не должно содержать ничего лишнего, должно включать только ту информацию, которая необходима для раскрытия вашей позиции, идеи.
4. Доклад должно иметь грамотное композиционное построение, быть логичным, четким по структуре.
5. Каждый абзац доклад должен содержать только одну основную мысль.
6. Доклад должен показывать, что его автор знает и осмысленно использует теоретические понятия, термины, обобщения, мировоззренческие идеи.
7. Доклад должен содержать убедительную аргументацию заявленной по проблеме позиции.

контрольная точка - в форме теста (письменная).

Тесты

1. Что такое домен безопасности?
 - а) собрание участников безопасности, имеющих единый центр, использующий единую базу, единую групповую и локальную политики, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров
 - б) виртуальная частная сеть с единым центром управления
 - с) локальная сеть, не имеющая выхода в сети общего пользования

d) сетевая операционная система

2. Какое из требований необязательно для операционных систем, сертифицированных по 5 классу РД СВТ?

a) Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ

b) ОС должна содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа

c) Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов)

d) В ОС должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа

3. Присутствуют ли в ОС семейства Windows механизмы, осуществляющие криптографические преобразования?

a) нет

b) присутствуют механизмы ЭЦП и хеширования

c) присутствуют механизмы обмена ключами

d) присутствуют механизмы для симметричного шифрования данных

4. Что такое РАМ?

a) набор библиотек подключаемых модулей шифрования

b) набор открытых библиотек подключаемых модулей аутентификации

c) набор открытых библиотек подключаемых модулей резервного восстановления

d) набор открытых библиотек подключаемых модулей доверенной загрузки

5. Открытой распределенной информационной системой (open distributed information system) называется система:

a. располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики

b. располагающая службами, пользование которыми возможно при использовании специальных синтаксиса и семантики

c. располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики

d. не располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики

Угроза это:

a) совокупность сообщений, направленных на запугивание

b) совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу.

c) совокупность сообщений, направленных на причинение вреда

d) любое действие, направленное на причинение ущерба

7. Классами защищенности автоматизированных систем от несанкционированного доступа являются:

a) 1Е

b) 2А

c) 2В

d) 3Б

8. Определите класс автоматизированной системы по следующим классификационным признакам:

АС, в которых работает один пользователь, допущенный ко всей информации

АС, размещенной на носителях одного уровня конфиденциальности, обрабатывается

“Коммерческая тайна”.

a) 2Б

b) 1Г

c) 1Д

d) 3Б

9. Определите класс автоматизированной системы по следующим классификационным признакам: многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. И все пользователи имеют равные права доступа ко всей информации АС, обрабатывается “Служебная тайна” и общедоступная информация:

a) 2Б

b) 2А

c) 1Г

d) 1Д

10. Методы и средства защиты информации бывают:

a) Технические (аппаратные)

b) Программные

c) Прикладные

d) Организационные

11. Информация по категории доступа классифицируется как:

a) Конфиденциальная

b) Общедоступная

c) Особо конфиденциальная

d) Ограниченного доступа

12. Уязвимость это:

a) Совокупность действий, направленная на преодоление системы защиты

b) Злонамеренное внедрение специального ПО

c) Слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

d) Результат действия вируса

13. Прерывание это:

a) временное прекращение процесса

b) остановка процесса

c) временное прекращение процесса, вызванное событием, внешним по отношению к этому процессу, и совершенное таким образом, что процесс может быть продолжен

d) событие, при котором меняется нормальная последовательность команд, выполняемых процессором

14. Что такое тупиковая ситуация для процесса?

a) невозможность выделения процессу требуемого ресурса

b) ситуация когда процесс ожидает некоторого события, которое никогда не произойдет

c) прерывание процесса операционной системой

d) критическая системная ошибка во время выполнения процесса

15. В каком порядке задаются права доступа в ОС Linux?

a) группа-владелец-остальные

b) владелец-группа-остальные

c) остальные-владелец-группа

d) остальные-группа-владелец

16. Что такое ACL?

a) средство для хранения паролей

b) сценарий входа в систему

c) список управления доступом

d) инструмент мандатного управления доступом в ОС

17. Что из перечисленного не содержится в маркере доступа пользователя?

a) идентификатор пользователя

b) привилегии пользователя

c) идентификатор сеанса работы пользователя, к которому относится маркер доступа

d) уровень доступа пользователя в системе

18. Какова должна быть минимальная длина пароля в случае смены ежеквартально?

- a) 13 символов
- b) 12 символов
- c) 8 символов
- d) 6 символов

19. Что из перечисленного не является требованием к подсистеме регистрации и учета:

- a) использование идентификационного и аутентификационного механизма
- b) запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.)
- c) обеспечение доверенной загрузки ОС
- d) действия по изменению ПРД

Инструкция по выполнению. Выбрать один правильный ответ

Критерии оценивания: • 5 баллов выставляется, если обучающийся ответил правильно на 100-85% заданий теста; • 4 балла выставляется, если обучающийся ответил на 84-69 % заданий; • 3 балла выставляется, если обучающийся ответил на 68-50% заданий; 2 балла выставляется, если обучающийся ответил менее, чем на 50 % заданий.

Контрольная точка в форме заданий (устная, письменная).

Компетентностно-ориентированные задания

1. Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8бит.
2. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 200 узлов.
3. Определить максимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 8бит.
4. Определить минимальную длину кодового слова с возможностью исправления 1-х кратных ошибок при кодировании информации длиной 16бит.
5. Определить минимальную длину кодового слова с возможностью исправления 3-х кратных ошибок при кодировании информации длиной 32бит.
6. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 8 Мбит/с и состоит из 120 узлов.
7. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 50 узлов.
8. С какой максимальной скоростью могут обмениваться данными два узла в сети, если сеть построена на разделяемой среде с пропускной способностью 10 Мбит/с и состоит из 80 узлов.
9. В действующей сети между узлами А и В существует три потока и три альтернативных маршрута. Можно ли направить каждый поток по отдельному маршруту?

Практическая работа №1. Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение.

1. Какие части документа относятся к вопросам защиты информации?
2. Что такое CISQ?
3. Что показывают комментарии к данному документу?
4. Как менялся текст нормативного акта с момента его создания по настоящее время?

5. Анализ методик и технологий управления рисками.
6. Раскройте качественные методики управления рисками.
7. Какие количественные методики управления рисками вы знаете?
8. Опишите метод CRAMM.
9. Раскройте важность и сложность проблемы информационной безопасности.
10. Задачи комитета технической безопасности ETSI.

Практическая работа №2. Определение показателей защищенности информации при несанкционированном доступе.

1. В чем заключается сложность функционального построения системы защиты объекта информатизации? Приведите примеры.
2. Приведите формулу для вычисления величины Ротки), прокомментируйте ее.
3. Приведите примеры многозвенной системы защиты объекта информатизации.
4. Прокомментируйте выражение для определения прочности многозвенной защиты при противостоянии одному нарушителю.
5. Прокомментируйте выражение для определения прочности многозвенной защиты при противостоянии нескольким нарушителю.
6. Какие выводы можно сделать, если прочность слабейшего звена защиты удовлетворяет предъявленным требованиям оболочки защиты в целом?
7. Какие меры повышения прочности защиты можно порекомендовать, если звено защиты не удовлетворяет предъявленным требованиям?
8. Каким образом система будет способствовать целям бизнеса?
9. Требуется ли разработка системы технологии, которая до этого не использовалась в организации?

10. Что должен включать отчет по результатам оценки CASE-средств?
 11. Какие этапы оценки вы знаете?
 12. Опишите рамки информационной безопасности NIST (NIST CSF).
- Практическая работа №3. Критерии оценки и выбора CASE-средств.
1. Сколько поколений CASE-средств существует? Опишите их.
 2. Какие требования предъявляются к CASE-средствам?
 3. Какие направления развития CASE-средств используются наиболее интенсивно?

4. По каким критериям оценивается CASE-средство для UML?
5. Как делятся CASE-средства по функциональному назначению?
6. Опишите архитектуру CASE-средств.
7. Опишите виды классификации CASE-средств.
8. Охарактеризуйте критерии выбора CASE-средств.
9. Какие текущие проблемы существуют в организации и как новая система поможет их решить?
10. Опишите этапы программы оценки соответствия ИБ.

Практическая работа №4. Составление обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Проекты международных стандартов по облачным вычислениям.
5. Опишите стандарты и руководства США.
6. Общая картина введенных в действие и ожидаемых в ближайшее

время стандартов и руководств в области облачных вычислений.

7. Российская стандартизация облачных вычислений и ее проблемы и пути решения.

8. Что произойдет с организацией, если система не будет введена в эксплуатацию?

9. Какая основная информация содержится в сертификате?

Критерии оценивания. «отлично» – студент правильно выполнил задание. Показал отличные владения навыками применения полученных знаний и умений при решении задач в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы; «хорошо» – студент выполнил задание с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов; «удовлетворительно» – студент выполнил задание с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей; «неудовлетворительно» – при выполнении задания студент продемонстрировал недостаточный уровень владения умениями и навыками при решении задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено множество неточностей

Контрольная точка в форме коллоквиума (устная).

Вопросы для коллоквиума

1. Из каких элементов состоит трёхуровневая модель оценки защищенности информационной системы?

2. Какими путями осуществляется стандартизация подходов к обеспечению информационной безопасности и какие международные стандарты для этого применяются?

3. Какие уровни реализуются в технологической модели подсистемы информационной безопасности ИС?

4. С какой целью производится шифрование данных и информации и на каком уровне работы с информацией это применяется?

5. Что такое «единое информационное пространство»? Каковы его составляющие?

6. В каком случае возникает несовместимость вычислительных, информационных и телекоммуникационных устройств?

7. Как можно определить понятие «открытая информационная или программная система»?

8. Какими свойствами обладает открытая система?

9. Что такое итология и какие методы лежат в основе итологии?

10. Какие организации образуют структуру международной стандартизации в области информационных технологий?

11. Какие международные организации занимаются вопросами стандартизации в среде Web-сервисов?

12. Что составляет методологическую основу базиса открытых систем?

13. Какие прикладные программы работают в функциональной среде открытых систем?

14. В чём состоит суть эталонной модели взаимосвязи открытых систем (Open Systems Interconnection)?

15. Сколько уровней взаимодействия содержит модель ВОС? Какие это уровни?

16. Каким образом определяют понятие «профиль открытой системы»?

17. Что является базовой основой профиля?

18. С какой целью была разработана таксономия профилей?

19. Что включает в себя международный стандартизированный профиль ISP?

20. Для чего разработан профиль переносимости приложений APP и какое

отношение он имеет к профилю GOSIP?

21. Какие четыре основных типа интерфейсов OSE вводит классификация интерфейсов открытых систем?

22. Что является основными целями разработки OSE и OSI профилей?

23. Каким образом и с помощью каких профилей связаны архитектурный и функциональный уровни открытой информационной системы?

24. Что включает в себя процесс проектирования профиля открытой системы?

25. Какие основные функциональные профили выбираются, компонуются и применяются на стадиях реализации жизненного цикла информационной системы?

26. Какие два основных значения имеет термин Internet?

27. Какие информационные услуги реализуют Internet-службы?

28. Что такое пространство Intranet и чем оно отличается от пространства Internet?

29. Перечислите основные архитектуры компьютерных сетей.

30. Приведите классификацию компьютерных сетей по различным классификационным признакам.

31. Какие топологии локальных компьютерных сетей существуют? Определите преимущества и недостатки каждой топологии.

32. Назовите основные физические архитектуры локальных компьютерных сетей.

33. Что является содержанием понятия «экономическая безопасность предприятия»?

34. Как можно охарактеризовать понятие «информационная безопасность» и что оно в себя включает (основные составляющие)?

35. О каких основных аспектах следует говорить при построении систем корпоративной информационной безопасности?

36. Для чего необходимо формировать политику информационной безопасности и из каких основных разделов она состоит?

37. Кто разрабатывает политику информационной безопасности предприятия? Какие менеджеры и специалисты входят в рабочую группу?

38. Какие вопросы информационной безопасности являются ключевыми?

39. Из чего складывается инфраструктура информационной безопасности?

40. Какие существуют виды угроз ИБ и каким образом оцениваются соответствующие риски?

41. На какие виды подразделяется защищаемая информация?

42. Что включает в себя модель информационной безопасности?

43. В каких аспектах рассматриваются мероприятия по защите информации?

44. Каким образом оценивается соотношение эффективности и рентабельности систем информационной безопасности?

45. В каком случае информационная система считается защищенной?

46. Каким образом архитектура информационной системы может способствовать общей информационной безопасности и почему?

47. Чем отличается схема симметричной криптосистемы с закрытым ключом от схемы асимметричной криптосистемы с открытым ключом?

48. Что такое VPN и для каких целей используются эти технологии?

49. Какие типы вирусов выделены в настоящее время?

50. Какие существуют общие правила для пользователей для обеспечения антивирусной безопасности?

51. Каким общим требованиям должен удовлетворять качественный антивирусный программный продукт?

Методические рекомендации:

Обучающийся может подготовить не более двух ответов на вопросы к коллоквиуму. Критерии оценивания одного ответа: 5 баллов выставляется обучающемуся, если он перечисляет все существенные характеристики обозначенного в вопросе предмета и возможные варианты дальнейшего развития решения проблемы, если это возможно; 4 балла, если студент раскрыл только

часть основных положений вопроса, продемонстрировал неточность в представлениях о предмете вопроса; 3 балла, если студент обозначил общую траекторию ответа, но не смог конкретизировать основные компоненты; 2 балла, если студент не продемонстрировал знаний основных понятий, представлений об изучаемом предмете

Контрольная точка - в форме лабораторных работ (письменная).

ЛАБОРАТОРНАЯ РАБОТА 1. Сбор исходных данных для аудита информационной безопасности объекта

- Дайте определение «аудит информационной безопасности объекта»
- Перечислите виды аудита безопасности?
- Как происходит сбор исходных данных?
- Какие существуют методы для сбора исходных данных?

ЛАБОРАТОРНАЯ РАБОТА 2. Выявление уязвимостей информационной системы

- Что понимается под уязвимостью информационной системы?
- Идентификация уязвимостей на стадии проектирования ИС, на этапе реализации, на этапе эксплуатации
- Каким образом осуществляется представление рисков в виде дерева уязвимостей, угроз и контрмер.

ЛАБОРАТОРНАЯ РАБОТА 3. Идентификация защитных механизмов

- Что понимается под понятием «защитный механизм»?
- Перечислите первичные защитные механизмы
- Перечислите вторичные защитные механизмы
- Как происходит идентификация защитных механизмов?

ЛАБОРАТОРНАЯ РАБОТА 4. Идентификация нарушителей

- Дайте определение понятию «идентификация»
- Кто называется нарушителем?
- Опишите механизм идентификации нарушителей

Критерии оценивания. «отлично» – студент правильно выполнил задание. Показал отличные владения навыками применения полученных знаний и умений при решении задач в рамках усвоенного учебного материала. Ответил на все дополнительные вопросы; «хорошо» – студент выполнил задание с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении задач в рамках усвоенного учебного материала. Ответил на большинство дополнительных вопросов; «удовлетворительно» – студент выполнил задание с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено много неточностей; «неудовлетворительно» – при выполнении задания студент продемонстрировал недостаточный уровень владения умениями и навыками при решении задач в рамках усвоенного учебного материала. При ответах на дополнительные вопросы было допущено множество неточностей

ПРИМЕРНАЯ ТЕМАТИКА РЕФЕРАТОВ

Примерный список тем рефератов:

1. Задачи аналитической работы в сфере защиты информации;
2. Источники, угрозы, каналы распространения и утраты конфиденциальной информации;
3. Задачи аналитической работы по выявлению угроз и каналов утраты конфиденциальной информации;
4. Критерии целесообразности защиты информации;
5. Направления использования результатов аналитической работы для формирования системы защиты информации.
6. Направления классификации информационных ресурсов в предпринимательской сфере;
7. Критерии ценности, полезности и конфиденциальности информации;

8. Содержание процедуры разработки перечня ценных и конфиденциальных сведений;
9. Содержание процедуры ведения перечня ценных и конфиденциальных сведений;
10. Назначение и содержание перечня конфиденциальных документов фирмы

Методические рекомендации по написанию реферата, требования к оформлению

Реферат (от лат. *refero* – сообщаю) – краткое изложение в письменном виде научно-исследовательской работы студента, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. Содержание реферата должно быть логичным, а изложение материала должно носить проблемно-тематический характер.

Каждая работа, носящая реферативный характер, должна быть оформлена в соответствии с Государственным Образовательным Стандартом (ГОСТ).

Структура работы:

- титульный лист;
- оглавление;
- введение (указывается актуальность, цель, задачи);
- не менее 3х глав;
- выводы (личное мнение);
- приложения (если есть);
- список используемой литературы.

Каждый новый раздел начинается с новой страницы.

Во введении обязательно должны быть указаны следующие параметры: тема реферата; предмет и объект исследования; цель; задачи; актуальность; методы исследования.

В основной части формулируются ключевые понятия и положения, вытекающие из анализа теоретических источников (точек зрения, моделей, концепций), документальных источников и материалов практики, экспертных оценок по вопросам исследуемой проблемы, а также результатов эмпирических исследований. Реферат носит исследовательский характер, содержит результаты творческого поиска автора.

В заключении (1-2 страницы) подводятся главные итоги авторского исследования в соответствии с целью и задачами реферата делаются выводы или даются практические рекомендации по разрешению исследуемой проблемы.

Требования к оформлению работы:

- объём 15-20 страниц;
 - поля – по 2 см сверху и снизу, 3 см – слева, 1,5 см – справа;
 - выравнивание текста по ширине;
 - номера страниц – внизу страницы, справа; номер на первой странице не указывается;
 - шрифт – «Times New Roman»;
 - основной текст – 14 кегль, междустрочный интервал – 1,5 (основной текст, между абзацами);
 - абзацный отступ – 1,25;
 - расстановка переносов не применяется;
 - все лишние пробелы убираются, между словами должен быть только один пробел;
- знаки препинания (за исключением тире) ставятся сразу же за предваряющим его словом без пробела;
- ссылки – затекстовые (вынесенные за текст реферата и оформленные как список использованной литературы в алфавитном порядке), использование автоматических постраничных ссылок не допускается;
 - не менее 5 источников;
 - ссылки оформляются в соответствии с ГОСТ Р 7.0.100-2018 (приложение 2);
 - для связи с текстом порядковый номер библиографической записи из списка литературы указывают в отсылке, которую приводят в квадратных скобках в строку с текстом. Если ссылку приводят на конкретный фрагмент текста, в отсылке указывают порядковый номер и страницы, на которых помещен объект ссылки. Сведения разделяют запятой. Если отсылка содержит сведения о нескольких затекстовых ссылках, группы сведений разделяют знаком точка с

запятой.

Критерии оценки реферата. При оценке реферата преподаватель руководствуется следующими критериями: – соответствие содержания текста выбранной теме; – наличие четкой и логичной структуры; – качество аналитической работы, проделанной при написании реферата; 12 – использование адекватных выбранной теме литературных источников; – самостоятельность, невторичность текста; – обоснованность сделанных автором реферата выводов, соответствие их поставленной цели; – отсутствие орфографических, пунктуационных, стилистических, а также фактических ошибок; – соответствие оформления работы предъявляемым требованиям; – сдачи реферата в установленный срок.

5.3 ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы **5 семестр**

Итоговый тест (с ответами) для проверки сформированности компетенций

ПК-3 Способен осуществлять информационно-аналитическое обеспечение защиты экономических интересов хозяйствующих субъектов, выявлять скрытые угрозы и прогнозировать риски на основе анализа больших данных и открытых источников

1. Прочитайте текст и выберите один правильный ответ. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

- а) Чтобы убедиться, что проводится справедливая оценка.
- б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ.
- в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа.
- г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку.

Правильный ответ: в)

2. Прочитайте текст и запишите правильный ответ.

Прочитайте текст и выберите два правильных ответа. Какие устройства НЕ находятся в системном блоке?

- а) принтер;
- б) процессор;
- в) сканер;
- г) жёсткий диск;
- д) сетевая карта.

Правильный ответ: а), в)

3. Прочитайте текст и выберите один правильный ответ. С помощью каких прикладных программных пакетов можно обработать статистические данные:

- А) Microsoft Word, Microsoft Excel
- Б) Excel, Lotus 1-2-3, QuattroPro, Mathcad
- В) Corel Draw, Adobe Photoshop
- Г) 1С: Предприятие, Microsoft Project

Правильный ответ: б)

4. Прочитайте текст и выберите один правильный ответ Режим защиты информации не устанавливается в отношении сведений, относящихся к ...

- б) государственной тайне
- в) конфиденциальной информации
- г) персональным данным
- д) деятельности государственных деятелей

Правильный ответ: г).

5. Прочитайте текст и выберите один правильный ответ Прочитайте текст, выберите два правильных ответа. Основные объекты обеспечения информационной безопасности России:

- а) квалифицированные кадры в области информационных технологий
- б) информационные продукты
- в) информационные ресурсы, содержащие сведения, которые относятся к государственной тайне и конфиденциальной информации
- г) помещения, предназначенные для ведения закрытых переговоров

Правильный ответ: в), г)

6. Закончите фразу. Ответ следует записать с маленькой буквы, в именительном падеже Свойство информации, заключающееся в достаточности данных для принятия решения, называется ...

Правильный ответ: полнота

7. Закончите фразу. Ответ следует записать с маленькой буквы, в именительном падеже Какое устройство не является периферийным?

Правильный ответ: жесткий диск

8. Закончите фразу. Ответ следует записать с маленькой буквы, в именительном падеже _____ банковское обслуживание – оказание банковских услуг на расстоянии, без посещения клиентами офиса банка, без непосредственного контакта с сотрудниками банка.

Правильный ответ: Дистанционное

9. Закончите фразу. Ответ следует записать с маленькой буквы, в именительном падеже Способ предоставления информационных ресурсов, таких как вычислительные мощности, хранилища данных и приложения, через интернет, называется _____

Правильный ответ: облачные технологии

10. Закончите фразу. Ответ следует записать с маленькой буквы, в именительном падеже Система охраняемых силой государства социальных норм и отношений, возникающих в информационной сфере — сфере производства, преобразования и потребления информации при осуществлении информационных процессов – это ...

Правильный ответ: информационное право

11. Установите правильное соответствие между типом компьютерной сети в зависимости от применяемых технологий и ее описанием:

- 1. Кабельные
- 2. Оптоволоконные
- 3. WiFi, Bluetooth
- 4. Спутниковые технологии

Варианты ответов:

а) сигнал передается посредством спутника, от которого доходит до конечного пользователя; обратная связь осуществляется с использованием стандартных технологий

(ADSL, оптоволокно).

б) передача сигнала происходит при прохождении лазерного луча через прозрачное волокно, обладающее специфическими свойствами, при этом свет не может покинуть пределы волокна и проходит расстояние в несколько километров, затем усиливается и передается дальше

в) сигнал передается без проводов с использованием радиоволн на специально отведенной для этого частоте (2,4 гигагерц); таким образом можно передать сигнал в локальной сети на несколько десятков метров

г) для передачи данных используются металлические провода.

Правильный ответ: 1)-г, 2)-б, 3)-в, 4)-а.

12. Установите правильное соответствие

1 В системном подходе к исследованию основным является

А) наличие
необходимой
информации

2 В понятие «поведенческого подхода» при исследовании системы управления входит:

- Б) определение целостности и связи явлений
- В) ориентация на человека и его потребности

Правильный ответ (1Б, 2В)

13. Установите правильное соответствие:

- 1. Принцип, относящийся к диалектическому подходу
- 2. Принцип, не относящийся к диалектическому подходу

- А) краткость
- Б) объективность
- В) оптимальность

Правильный ответ: (1Б, 2В)

14. Установите правильное соответствие

- 1 Предметом исследования физиократов явилась сфера
- 2 Предметом исследования меркантилистов явилась сфера

- А) производства
- Б) обращения
- В) потребления

Правильный ответ: (1А, 2Б)

15. Установите правильное соответствие

- 1. Сведения об окружающем мире, которые уменьшают имеющуюся степень неопределенности, неполноты знаний, отчужденные от их создателя и ставшие сообщения
- 2. Процесс насыщения производства и всех сфер жизни и деятельности человека информацией

- А) факты
- Б) информация
- В) информатизация

Правильный ответ: (1Б, 2В)

1

- 6 вокруг объекта и элементов защиты замкнутую среду вокруг объекта и элементов защиты

- П а) организационно-административные
- р б) технические
- о в) методологические
- ч г) программные

Правильный ответ: б)

1

- а) идентификации
- й б) ратификации
- т в) аутентификации
- н г) верификации

Правильный ответ: в)

1

- а) распознавание информации
- к б) полное игнорирование информации
- с в) присвоение какому-либо объекту или субъекту уникального имени или образа
- н г) последовательность действий, приводящих к пониманию информации

Правильный ответ: в)

1

- а) защита данных от несанкционированного копирования
- н б) удостоверение подлинности сведений
- ы в) выявление закономерностей построения производственных процессов
- и г) ограничение доступа к информационным массивам
- й д) защита программ от нелегального использования

Правильный ответ: б)

Организационно-административные средства защиты

- а) регистрация пользователей компьютерных средств в журналах
- б) разграничение доступа к информации в соответствии с функциональными обязанностями должностных лиц
- в) использование автономных средств защиты аппаратуры
- г) создание контрольно-пропускного режима на территории расположения средств обработки информации

Правильный ответ: б), г)

21. Закончите фразу. Ответ следует записать с маленькой буквы, в именительном падеже. Как называется профессионал, способный взломать системы электронной защиты, найти в них бреши и уязвимости?

Правильный ответ: хакер

22. Закончите фразу. Ответ следует записать с маленькой буквы, в именительном падеже. Защита данных методом их шифрования _____

Правильный ответ: криптография

23. Закончите фразу. Ответ следует записать с маленькой буквы, в именительном падеже. Установление подлинности объекту или субъекту _____

Правильный ответ: аутентификация

24. Закончите фразу. Ответ следует записать с маленькой буквы, в именительном падеже. Присвоение какому-либо объекту или субъекту уникального имени или образа _____

Правильный ответ: идентификация

25. Закончите фразу. Ответ следует записать с маленькой буквы, в именительном падеже. Пользователь, который имеет полный набор прав доступа для всего компьютера и неограниченный доступ ко всем файлам и ключам системного реестра называется _____

Правильный ответ: администратор

26. Установите соответствие

- 1) идентификация уникального имени или образа
- 2) аутентификация
- 3) система защиты информации
- а) присвоение какому-либо объекту или субъекту
- б) установление подлинности
- в) совокупность организационных и технологических мер, технических средств, правовых норм, направленных на противодействие угрозам нарушителей

Правильный ответ: 1) – а) 2) – б) 3) – в)

27. Установите правильную последовательность этапов в формировании представлений о мерах по защите информации:

- а) появление технических средств обработки информации и передачи сообщений с помощью электрических сигналов и электромагнитных полей;
- б) начало создания осмысленных и самостоятельных средств и методов защиты информации;
- в) внедрением автоматизированных систем обработки, передачи и хранения информации.

Правильный ответ: б), а), в)

28. Укажите правильное соответствие между базовыми принципами защиты информации и их сущностью:

- 1. Конфиденциальность.
- 2. Целостность.
- 3. Доступность.

Варианты ответов:

- а) обеспечение защищённости информационных данных от изменений и нарушений их структуры в процессе их сбора, обработки, передачи и хранения;

б) информация доступна для пользователей по мере возникновения у них необходимости в ней;

в) взаимодействовать с информацией могут только лица, которые без неё не могут осуществлять свою рабочую деятельность и выполнять свои должностные обязанности.

Правильный ответ: 1)-в, 2)-а, 3)-б.

29. Установите соответствие.

1) Угроза

2) Безопасность информации

3) Уязвимость системы

а) событие, которое потенциально может нанести вред организации путем раскрытия, модификации или разрушения информации

б) способность системы обеспечить защиту информации от негативных явлений

в) характеристика, которая делает возможным возникновение угрозы

Правильный ответ: 1) – а) 2) – б) 3) – в)

30. Установите правильную последовательность. Установите этапы становления информационного права в хронологической последовательности:

а) Изучение и исследование понятия «информация», возникновение новой науки -кибернетики.

б) Признание существования информационных отношений, требующих правового регулирования

в) Исследование информационно-общественных отношений в рамках новой науки - информатики. Появились первые правила и нормы, не закреплённые законодательно

г) Официальное признание термина «информационное право» и изучение правовой природы этого понятия.

Правильный ответ: а); в); б); г)

Инструкция по выполнению. При ответе на вопросы:

Выбрать один правильный ответ. Дополнить фразу, сопоставить, установить последовательность

Вопросы для самостоятельной подготовки к зачету с оценкой

1. Что понимается под адекватной безопасностью?

2. Что такое компрометация в информационной безопасности?

3. Что понимается под нарушением информационной безопасности?

4. Что понимается под уровнем (степенью) критичности ИС?

5. Определите окружение (среду) ИС .

6. Охарактеризуйте процесс воздействия на производственную деятельность.

7. Дайте определение понятию «риск».

8. В чем особенности рисков, связанных с информационными технологиями.

9. Что такое остаточный риск?

10. Что такое совокупный (суммарный, полный) риск.

11. Определите понятие «Анализ рисков».

12. В чем состоит управление рисками в информационной безопасности?

13. Что такое нейтрализация (уменьшение, ослабление) рисков?

14. Что такое терпимость по отношению к риску?

15. Определите основные категории безопасности.

16. Что понимают под уровнем защищенности.

17. Дайте определение угроз конфиденциальной информации.

18. Что такое атака?

19. Что такое окно опасности?

20. Какие события происходят во время существования окна опасности?

21. Что такое угрозы воздействия на источник информации?

22. Что такое угрозы утечки информации?

23. Какие угрозы называются преднамеренными?

24. Какие угрозы называются случайными?

25. Что такое канал несанкционированного доступа?
 26. Что такое утечка информации?
 27. Что такое перехват в теории информационной безопасности?
 28. Что такое канал утечки информации?
 29. Что такое технический канал утечки информации?
 30. Охарактеризуйте случайный и организованный канал утечки информации.
 31. Что такое источник угроз безопасности информации?
 32. Назовите основные источники преднамеренных угроз.
 33. Назовите основные источники случайных угроз.
 34. Прокомментируйте наиболее распространенные угрозы доступности.
 35. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
 36. Что такое отказ пользователей?
 37. Прокомментируйте внутренний отказ ИС в качестве угрозы.
 38. Прокомментируйте отказ поддерживающей инфраструктуры в качестве угрозы.
 39. Каким образом происходит повреждение или даже разрушение оборудования?
 40. Что такое вредоносное программное обеспечение?
 41. Какие негативные последствия в функционировании ИС вызывает вредоносное ПО?
 42. Охарактеризуйте основные угрозы целостности конфиденциальной информации.
 43. Перечислите основные угрозы конфиденциальности информации
 44. Что понимают под перехватом данных и в чем заключается угроза конфиденциальности?
 45. Охарактеризуйте этап выбора эффективных и экономичных защитных средств (нейтрализация рисков).
 46. В чем заключается суть мероприятий по управлению рисками?
 47. Какие возможны действия по отношению к выявленным рискам?
 48. Какие этапы управления рисками относятся к вспомогательным и почему?
 49. Почему карта информационной системы способствует управлению рисками?
 50. Какие этапы управления рисками относятся к основным и почему?
 51. Почему важен процесс интегрирования управления рисками в жизненный цикл ИС?
- Перечень вопросов для текущего контроля:
1. Каким образом производится выбор анализируемых объектов
 2. Почему важен уровень детализации при рассмотрении анализируемых объектов?
 3. Что такое инфологическая модель ИС?
 4. Приведите основные объекты инфологической модели объекта
 5. Как сформировать карту информационной системы организации?
 6. Что такое идентификация активов в управлении рисками информационной безопасности?
 7. Какие средства автоматизации идентификация активов ИС организации Вы знаете?
 8. Приведите перечень наиболее распространенных угроз.
 9. Что такое модель угроз организации?
 10. Приведите основные компоненты модели угроз организации.
 11. Охарактеризуйте процедуры идентификации угроз.
 12. Приведите основные источники возникновения угроз.
 13. Что включает в себя понятие «модель (облик) нарушителя»?
 14. Приведите возможную классификацию нарушителей.
 15. Прокомментируйте возможности конкурентов, клиентов, посетителей и хакеров в качестве потенциальных злоумышленников
 16. Определите цели администраторов, программистов, операторов, руководителей, технического персонала, сотрудников, уволенных с работы в качестве потенциальных нарушителей ИБ
 17. Что такое матрица нарушений ИБ? Приведите ее возможную структуру.
 18. Зачем необходим сценарий нарушения ИБ?
 19. Приведите модели оценки вероятности осуществления угрозы.
 20. Охарактеризуйте основные метрики, используемые для оценки вероятности

осуществления угрозы.

21. Дайте определение способа защиты информации.
22. Охарактеризуйте способ предупреждения возможных угроз.
23. Прокомментируйте основные действия способа выявления угроз
24. Охарактеризуйте способ обнаружения угроз.
25. Охарактеризуйте способ пресечения или локализации угроз.
26. Прокомментируйте основные действия способа ликвидации последствий.
27. Перечислите основные защитные действия при реализации способов ЗИ,
28. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
29. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
30. Назовите три группы мероприятий по технической защите информации.
31. Прокомментируйте основные организационные мероприятия по технической защите информации.
32. В каких ограничительных мерах выражаются организационные мероприятия по ЗИ.
33. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
34. Прокомментируйте основные технические мероприятия по технической защите информации.
35. Как оценить стоимости защитных мер.
36. В чем заключается проблема совместимости нового средства защитных мер со сложившейся организационной и аппаратно-программной структурой, с традициями организации?
37. Планирование реализации и проверки новых регуляторов безопасности.
38. План тестирования (автономного и комплексного) программно-технических механизмов защиты.

Перечень вопросов для текущего контроля:

1. Почему управление рисками рассматривается на административном уровне ИБ?
2. Охарактеризуйте роль руководителя организации в процессе управления рисками информационной безопасности.
3. Охарактеризуйте роль начальника управления (отдела) информатизации в процессе управления рисками информационной безопасности.
4. Охарактеризуйте роль владельцев систем и информации в процессе управления рисками информационной безопасности.
5. Охарактеризуйте роль руководителей производственных отделов и отдела закупок в процессе управления рисками информационной безопасности.
6. Охарактеризуйте роль начальника отдела (управления) информационной безопасности в процессе управления рисками информационной безопасности.
7. Охарактеризуйте роль администраторов безопасности в процессе управления рисками информационной безопасности.
8. Охарактеризуйте роль специалистов по обучению персонала в процессе управления рисками информационной безопасности.
9. Почему управление рисками рассматривается на административном уровне ИБ?
10. Охарактеризуйте роль руководителя организации в процессе управления рисками информационной безопасности.
11. Охарактеризуйте роль начальника управления (отдела) информатизации в процессе управления рисками информационной безопасности.
12. Охарактеризуйте роль владельцев систем и информации в процессе управления рисками информационной безопасности.
13. Охарактеризуйте роль руководителей производственных отделов и отдела закупок в процессе управления рисками информационной безопасности.
14. Охарактеризуйте роль начальника отдела (управления) информационной безопасности в процессе управления рисками информационной безопасности.

15. Охарактеризуйте роль администраторов безопасности в процессе управления рисками информационной безопасности.
16. Охарактеризуйте роль специалистов по обучению персонала в процессе управления рисками информационной безопасности.
17. Назовите и охарактеризуйте этапы процесса управления рисками.
18. Какие этапы управления рисками относятся к вспомогательным и почему?
19. Опишите этап выбора анализируемых объектов и уровня детализации их рассмотрения процесса управления рисками.
20. Какие этапы управления рисками относятся к основным и почему?
21. Охарактеризуйте основные шаги анализа угроз в процедуре управления рисками.
22. Охарактеризуйте этап оценки рисков в процедуре управления рисками.
23. Охарактеризуйте этап выбора защитных мер в процедуре управления рисками.
24. Охарактеризуйте этап реализации и проверки выбранных мер защиты в процедуре управления рисками.
25. Что такое оценка остаточного риска?
26. Определение приоритетов, оценка и реализация контрмер, уменьшающих риски и рекомендованных по результатам оценки рисков.
27. Назовите различные возможности в процессе принятия риска
28. Назовите различные возможности в процессе уклонения от риска
29. Назовите различные возможности в процессе ограничения (нейтрализации) риска
30. Назовите различные возможности в процессе переадресации риска.
31. В чем состоит оценка экономической эффективности.
32. Приведите возможный формат отчета об оценке рисков.
33. Приведите возможный формат плана реализации контрмер.
34. Приведите возможные трактовки и способы вычисления рисков.
35. Каким образом осуществляется представление рисков в виде дерева уязвимостей, угроз и контрмер.

6. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ

Комплект оценочных средств хранится на кафедре, подлежит обновлению по мере необходимости. Для промежуточной аттестации в виде экзамена каждое ОС по дисциплине обновляется и утверждается за 14 дней до начала сессионного периода и хранится в недоступном месте от несанкционированного доступа. Ответственность несет кафедра.

Порядок проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по ОПОП регламентируются Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам высшего образования.

Текущий контроль успеваемости является формой контроля качества знаний обучающихся, осуществляемого в межсессионный период обучения с целью определения качества освоения ОПОП.

Текущий контроль успеваемости осуществляется: на лекциях, практических (семинарских) занятиях, в рамках контроля самостоятельной работы.

Обучающиеся заранее информируются о критериях и процедуре текущего контроля успеваемости преподавателями по соответствующей учебной дисциплине (модуля).

Успеваемость при текущем контроле характеризует объем и качество выполненной обучающимся работы по дисциплине (модулю).

Педагогические виды и формы, используемые в процессе текущего контроля успеваемости обучающихся, определяются методической комиссией кафедры. Выбираемый вид текущего контроля обеспечивает наиболее полный и объективный контроль (измерение и фиксирование) уровня освоения результатов обучения по дисциплине.

Преподаватели предоставляют сведения о текущей успеваемости обучающихся в рамках проведения текущей аттестации в семестре в деканаты/ учебный отдел института в сроки, определенные внутренними распорядительными документами института.

В целях обеспечения текущего контроля успеваемости преподаватель проводит

консультации.

Преподаватель, ведущий занятия семинарского типа, проводит аттестацию обучающихся за прошедший период. Аттестация проводится, если проведено не менее 3 практических (семинарских) или лабораторных занятий, в установленные деканатом сроки, не реже 1 раза за учебный семестр. Обучающиеся аттестуются путем выставления в соответствующую групповую ведомость записей по системе: «аттестован» или «не аттестован».

Преподаватель, проставляя итоги текущей аттестации, доводит результаты аттестации до сведения студенческой группы и объясняет причины отрицательной аттестации по запросу обучающегося.

При аттестации обучающихся учитываются следующие факторы:

- результаты работы на занятиях, показанные при этом знания по дисциплине (модулю), усвоение навыков практического применения теоретических знаний, степень активности на практических (семинарских) занятиях;
- результаты и активность участия в семинарах и коллоквиумах;
- результаты выполнения контрольных работ;
- результаты и объем выполненных заданий в рамках самостоятельной работы обучающихся;
- результаты личных бесед со студентами по материалу учебной дисциплины (модуля);
- посещение студентами, семинарских и практических занятий, лабораторных работ;
- своевременная ликвидация задолженностей по пройденному материалу, возникших вследствие пропуска занятий либо неудовлетворительных оценок по результатам работы на занятиях.
- результаты прохождения контрольных точек по дисциплине.

Промежуточная аттестация обучающихся института является формой контроля результатов обучения по дисциплине с целью комплексного определения соответствия уровня и качества знаний, умений и навыков обучающихся требованиям, установленным образовательной программой.

Формирование оценки текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины осуществляется с использованием пятибалльной системы оценки знаний обучающихся.

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций. Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 5 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации. Промежуточная аттестация проводится в форме экзамена. Экзамен проводится по расписанию экзаменационной сессии в письменном виде. Количество вопросов в экзаменационном задании – 30. Проверка ответов и объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

7. ОСОБЕННОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

Адаптированные оценочные материалы содержатся в адаптированной ОПОП. Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся (обучающегося).

Самостоятельная работа обучающихся с ограниченными возможностями здоровья и инвалидов позволяет своевременно выявить затруднения и отставание и внести коррективы в

учебную деятельность. Конкретные формы и виды самостоятельной работы обучающихся лиц с ограниченными возможностями здоровья и инвалидов устанавливаются преподавателем. Выбор форм и видов самостоятельной работы, обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется с учетом их способностей, особенностей восприятия и готовности к освоению учебного материала. Формы самостоятельной работы устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге или на компьютере, в форме тестирования, электронных тренажеров и т.п.).

Основные формы представления оценочных средств – в печатной форме или в форме электронного документа. Для обучающихся с нарушениями зрения предусматривается возможность проведения текущего и промежуточного контроля в устной форме. Для обучающихся с нарушениями слуха предусматривается возможность проведения текущего и промежуточного контроля в письменной форме.

Таблица 7.1. Категории обучающихся с ОВЗ, способы восприятия ими информации и методы их обучения.

Категории обучающихся по нозологиям		Методы обучения
с нарушениями и зрения	Слепые. Способ восприятия информации: осязательно-слуховой	Аудиально-кинестетические, предусматривающие поступление учебной информации посредством слуха и осязания. Могут использоваться при условии, что визуальная информация будет адаптирована для лиц с нарушениями зрения: визуально-кинестетические, предполагающие передачу и восприятие учебной информации при помощи зрения и осязания;
	Слабовидящие. Способ восприятия информации: зрительно-осязательно-слуховой	аудио-визуальные, основанные на представлении учебной информации, при которых задействовано зрительное и слуховое восприятие; аудио-визуально-кинестетические, базирующиеся на представлении информации, которая поступает по зрительному, слуховому и осязательному каналам восприятие.
с нарушениями и слуха	Глухие. Способ восприятия информации: зрительно-осязательный	визуально-кинестетические, предполагающие передачу и восприятие учебной информации при помощи зрения и осязания. Могут использоваться при условии, что аудиальная информация будет адаптирована для лиц с нарушениями слуха: аудио-визуальные, основанные на представлении учебной информации, при которых задействовано зрительное и слуховое восприятие;
	Слабослышащие. Способ восприятия информации: Зрительно-осязательно-слуховой	аудиально-кинестетические, предусматривающие поступление учебной информации посредством слуха и осязания; аудио-визуально-кинестетические, базирующиеся на представлении информации, которая поступает по зрительному, слуховому и осязательному каналам восприятие.
с нарушениями и опорно-двигательного аппарата	Способ восприятия информации: зрительно-осязательно-слуховой	— визуально-кинестетические; — аудио-визуальные; — аудио-кинестетические; — аудио-визуально-кинестетические.

Таблица 7.2. – Способы адаптации образовательных ресурсов.

Условные обозначения:

«+» —образовательный ресурс, не требующий адаптации;

«АФ» — адаптированный формат к особенностям приема-передачи информации обучающихся инвалидов и лиц с ОВЗ формат образовательного ресурса, в том числе с использованием специальных технических средств;

«АЭ»— альтернативный эквивалент используемого ресурса

Категории обучающихся по нозологиям		Образовательные ресурсы				
		Электронные				Печатные
		мультимедиа	графические	аудио	текстовые, электронные аналоги печатных изданий	
С нарушениями зрения	Слепые	АФ	АЭ (например, создание материальной модели графического объекта (3Dмодели)	+	АЭ (например, аудио описание)	АЭ (например, печатный материал, выполненный рельефно-точечным шрифтом Л. Брайля)
	Слабовидящие	АФ	АФ	+	АФ	АФ
С нарушениями слуха	Глухие	АФ	+	АЭ (например, текстовое описание, гиперссылки)	+	+
	Слабослышащие	АФ	+	АФ	+	+
С нарушениями опорно-двигательного аппарата		+	+	+	+	+

Таблица 7.3. - Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ

Категории обучающихся по нозологиям	Форма контроля и оценки результатов обучения
С нарушениями зрения	– устная проверка: дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; – с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, дистанционные формы, если позволяет острота зрения - графические работы и др.
С нарушениями слуха	– письменная проверка: контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; – с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы и др.
С нарушениями опорно-двигательного аппарата	– письменная проверка, с использованием специальных технических средств (альтернативных средства ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; – устная проверка, с использованием специальных технических средств (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; – с использованием компьютера и специального ПО (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, Графические работы, дистанционные формы - предпочтительнее обучающимся, ограниченным в передвижении и др.

7.1. ЗАДАНИЯ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ДЛЯ ИНВАЛИДОВ И ЛИЦ

С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

Текущий контроль и промежуточная аттестация обучающихся инвалидов и лиц с ОВЗ осуществляется с использованием оценочных средств, адаптированных к ограничениям их здоровья и восприятия информации, в том числе с использованием специальных технических средств.

Текущий контроль успеваемости для обучающихся инвалидов и лиц с ОВЗ направлен на своевременное выявление затруднений и отставания в обучении и внесения коррективов в учебную деятельность. Возможно осуществление входного контроля для определения его способностей, особенностей восприятия и готовности к освоению учебного материала.

7.2. ЗАДАНИЯ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

Форма промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа. Промежуточная аттестация, при необходимости, может проводиться в несколько этапов. Для этого рекомендуется использовать рубежный контроль, который является контрольной точкой по завершению изучения раздела или темы дисциплины, междисциплинарного курса, практик и ее разделов с целью оценивания уровня освоения программного материала. Формы и срок проведения рубежного контроля определяются