Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Кузнецова Эмилия Васильевна
Должность: Исполнительный директор
Дата подписания: 23.11.2025 16:18:17
Уникальный программный ключ:
01e176f1d70ae109e92d86b7d8f33ec82fbb87d6

ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЕГИОНАЛЬНЫЙ ИНСТИТУТ БИЗНЕСА И УПРАВЛЕНИЯ»

Рассмотрено и одобрено на заседании Учебно-Методического совета
Протокол № 1 от 23 августа 2024 г.

УТВЕРЖДЕНО
Проректор по учебной работе
_____ Ю.И. Паничкин
Личная подпись инициалы, фамилия
«23» августа 2024 года

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

к рабочей программе дисциплины

«Информационная безопасность»

Направление подготовки	**09.03.03 Прикладная информатика**
Направленность подготовки (профиль)	**Прикладная информатика**
Уровень программы	**бакалавриат**
Форма обучения	**очно-заочная**

Рязань 2024 г.

Фонд оценочных средств текущей и промежуточной аттестации по дисциплине «Информационная безопасность»

Фонд оценочных средств является неотъемлемой частью рабочей программы дисциплины и основной образовательной программы.

Фонд оценочных средств представляет собой комплекс учебных заданий, предназначенных для измерения уровня достижений обучающимся установленных результатов обучения, и используется при проведении текущей и промежуточной аттестации (в период зачетно-экзаменационной сессии).

Цель ФОС – установление соответствия уровня подготовки обучающихся на данном этапе обучения требованиям рабочей программы дисциплины.

Основными задачами ФОС по учебной дисциплине являются:

- контроль достижений целей реализации ОП – формирование компетенций;
- контроль процесса приобретения обучающимся необходимых знаний, умений, навыков(владения/опыта деятельности) и уровня сформированности компетенций;
- оценка достижений обучающегося;
- обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование методов обучения в образовательном процессе.

1. Планируемые результаты обучения по дисциплине в рамках планируемых результатов освоения основной образовательной программы. Перечень компетенций в процессе освоения образовательной программы.

Дисциплина «Информационная безопасность» обеспечивает освоение следующих компетенций с учетом этапа освоения:

Код компетенции	Наименование компетенции
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
ПК-7	Способен проводить описание прикладных процессов и информационного обеспечения решения прикладных задач

Раздел/тема	**Краткое тематическое содержание** /этапы формирования компетенции	**Методы текущего контроля успеваемости**	**Компетенции**
Введение в информационную безопасность (ИБ)	Основные понятия. Анализ угроз. Проблемы безопасности компьютерных сетей. Политика безопасности. Основные составляющие политики безопасности. Нормативно-правовое обеспечение ИБ. Стандарты ИБ. Принципы защиты информационных систем (ИС).	О, Т	ОПК-3, ПК-7
Технологии защиты данных.	Принципы криптозащиты. Криптографические алгоритмы. Симметричные и асимметричные системы шифрования. Технологии аутентификации. Биометрическая аутентификация.	О, Т	ОПК-3, ПК-7

Технологии защиты вычислительны х систем	Обеспечение безопасности операционных систем (ОС). Межсетевые экраны. Защита в виртуальных сетях VPN. Защита на уровнях модели OSI.	О, Т	ОПК-3, ПК-7
Технологии обнаружения вторжений	Анализ защищенности. Обнаружение атак. Программные средства обнаружения вторжение. Защита удаленного доступа. Защита от вирусов и спама.	О, Т	ОПК-3, ПК-7
Управление безопасностью	Задачи управления ИБ в информационных системах (ИС). Архитектура и функционирование систем управления ИБ в (ИС). Аудит и мониторинг безопасности (ИС). Обзор систем управления безопасностью.	О, Т	ОПК-3, ПК-7

2.Соответствие уровня освоения компетенции планируемым результатам обучения и критериям их оценивания

Код компетенции	Наименование компетенции
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Показатель оценивания/индикаторы	**Критерии оценивания**			
	2	3	4	5
Знает	Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины	Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении	Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач	Показывает глубокое знание и понимание материала, способен применить изученный материал на практике

Показатель оценивания/ индикаторы	**Критерии оценивания**			
	2	3	4	5
Умеет	Не умеет воспроизвести хотя бы 50 % основного материала курса, однако испытывает затруднения при решении практических задач	Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач	Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач	Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки
Владеет	Не владеет навыками теоретического и экспериментального исследования объектов профессионально й деятельности, усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания основных разделов дисциплины.	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания основных разделов дисциплины.	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, способен самостоятельно выделять главные положения в изученном материале. Испытывает незначительные затруднения в решении задач.	Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала

Код компетенции	Наименование компетенции
ПК-7	Способен проводить описание прикладных процессов и информационного обеспечения решения прикладных задач

Показатель оценивания/инди каторы	**Критерии оценивания**			
	2	3	4	5

Показатель оценивания/индикаторы	**Критерии оценивания**			
	2	3	4	5
Знает	Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины	Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении	Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач	Показывает глубокое знание и понимание материала, способен применить изученный материал на практике
Умеет	Не умеет воспроизвести хотя бы 50 % основного материала курса, однако испытывает затруднения при решении практических задач	Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач	Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач	Умеет решать стандартные профессиональные задачи с применением полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки

Показатель оценивания/индикаторы	Критерии оценивания			
	2	3	4	5
Владеет	Не владеет навыками теоретического и экспериментального исследования объектов профессионально й деятельности, усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания основных разделов дисциплины.	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания основных разделов дисциплины.	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, способен самостоятельно выделять главные положения в изученном материале. Испытывает незначительные затруднения в решении задач.	Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала

3. **Фонд оценочных средств и материалы текущего контроля успеваемости обучающихся и промежуточной аттестации по дисциплине**

3.1. В ходе реализации дисциплины «Информационная безопасность» используются следующие формы текущего контроля успеваемости обучающихся:

опрос, тестирование и т.д.

3.2. Преподаватель при текущем контроле успеваемости, оценивает уровень подготовленности обучающихся к занятию по следующим показателям:

- устные (письменные)ответы на вопросы преподавателя по теме занятия;
- количество правильных ответов при тестировании;
- по сформированности собственных суждений основанных на значимых фактах и практических результатах отраженных в реферате, эссе;
- аргументированности, актуальности, новизне содержания доклада;
- по точному выполнению целей и задач контрольной работы.

Детализация баллов и критерии оценки текущего контроля успеваемости утверждается на заседании кафедры.

- **.2.1. Вопросы для подготовки к опросу по всем изучаемым тема дисциплины:**

Задания в форме устного опроса

Семестр 3

1. Введение в информационную безопасность (ИБ)
2. Основные понятия ИБ.
3. Анализ угроз.
4. Проблемы безопасности компьютерных сетей.
5. Политика безопасности.
6. Основные составляющие политики безопасности.
7. Нормативно-правовое обеспечение ИБ.
8. Стандарты ИБ.
9. Международные стандарты в сфере ИБ.
10. Принципы защиты информационных систем (ИС).
11. Технологии защиты данных.
12. Принципы криптозащиты.
13. Криптографические алгоритмы.
14. Криптоанализ.
15. Симметричные и асимметричные системы шифрования.
16. Технологии электронно-цифровой подписи.
17. Функции хэширования.
18. Технологии аутентификации.
19. Биометрическая аутентификация.

Семестр 4

1. Технологии защиты вычислительных систем.
2. Обеспечение безопасности операционных систем (ОС).
3. Межсетевые экраны.
4. Сертификация и стандартизация.
5. Защита в виртуальных сетях VPN.
6. Защита на уровнях модели OSI.
7. Технологии обнаружения вторжений.
8. Средство анализа сетевого трафика Wireshark.
9. Сканирование сети.
10. Анализ защищенности.
11. Обнаружение атак.
12. Программные средства обнаружения вторжения.
13. Защита удаленного доступа.
14. Защита от вирусов и спама.
15. Управление безопасностью.
16. Задачи управления ИБ в информационных системах (ИС).
17. Архитектура и функционирование систем управления ИБ в (ИС).
18. Аудит и мониторинг безопасности (ИС).
19. Обзор систем управления безопасностью.

Контролируемые компетенции: ОПК-3, ПК-7.

Устный (письменный) опрос проводится в течение установленного времени преподавателем. Опрашиваются все обучающиеся группы. За опрос выставляется оценка до 10 баллов. Набранные баллы являются рейтинг-баллами.

Рейтинг-баллы	**Аттестационная оценка обучающегося по дисциплине учебного плана в национальной системе**
	оценивания

8-10	отлично
6-7	хорошо
4-5	удовлетворительно
0-3	неудовлетворительно

При оценивании учитывается:

1. Целостность, правильность и полнота ответов
2. В ответе приводятся примеры из практики, даты, Ф.И.О. авторов
3. Применяются профессиональные термины и определения

Процедура оценки опроса:

1. Если ответ удовлетворяет 3-м условиям – 8-10 баллов.
2. Если ответ удовлетворяет 2-м условиям – 6-7 баллов.
3. Если ответ удовлетворяет 1-муусловию – 4-5 баллов.
4. Если ответ не удовлетворяет ни одному условию – 0-3

5. 2.2.Темы рефератов и эссе:

Эссе – это творческая работа, в которой должна быть выражена позиция автора по избранной теме. Сформулировать предмет анализа в эссе или исходные тезисы в соответствии с установленными компетенциями. Правильно подобрать и эффективно использовать необходимые источники (посредством ЭИОС ММА). Критически проанализировать различные факты и оценить их интерпретацию. Сформулировать собственные суждения и оценки, основанные на значимых фактах и практических результатах, процессах трансформации.

Реферат – форма научно-исследовательской деятельности, направленная на развитие научного мышления, на формирование познавательной деятельности по дисциплине через комплекс взаимосвязанных методов исследования, на самообразование и творческую деятельность. Используя ЭИОС ММА, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, базы данных, ЭБС, выделять значимые и актуальные положения, противоположные мнения с обоснованием собственной точки зрения.

Не предусмотрены

Критерии оценки:

1. Выполнение задания в срок. Сформулированы предмет анализа или исходные тезисы.
2. Отражены суждения и оценки, основанные на значимых фактах и практических результатах.
3. Использованы электронные информационные ресурсы, базы данных, ЭБС

Процедура оценки реферата, эссе:

1. Если ответ удовлетворяет 3-м условиям – 18-20 баллов.
2. Если ответ удовлетворяет 2-м условиям – 15-17 баллов.
3. Если ответ удовлетворяет 1-му условию – 10-14 баллов.
4. Если ответ не удовлетворяет ни одному условию – 1-9

Рейтинг- баллы	**Аттестационная оценка обучающегося по дисциплине учебного плана в национальной системе оценивания**
18-20	Отлично

15-17	Хорошо
10-14	Удовлетворительно
1-9	Неудовлетворительно

3.2.3 Тестовые задания для проведения тестирования:
Семестр 3

1. Кто является основным ответственным за определение уровня классификации информации?
Руководитель среднего звена Высшее руководство Владелец
Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
Сотрудники Хакеры Атакующие
Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
Улучшить контроль за безопасностью этой информации Снизить уровень классификации этой информации

4. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
Поддержка высшего руководства
Эффективные защитные меры и методы их внедрения Актуальные и адекватные политики и процедуры безопасности Проведение тренингов по безопасности для всех сотрудников

5. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Когда риски не могут быть приняты во внимание по политическим соображениям
Когда необходимые защитные меры слишком сложны
Когда стоимость контрмер превышает ценность актива и

потенциальные потери

6. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
Только военные имеют настоящую безопасность
Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
Военным требуется больший уровень безопасности, т.к. их риски существенно выше
Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

7. Защита информации от утечки – это деятельность по предотвращению: получения защищаемой информации заинтересованным субъектом с

нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;
воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

8. Защита информации это:
процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

9. Естественные угрозы безопасности информации вызваны: деятельностью человека;
ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
корыстными устремлениями злоумышленников; ошибками при действиях персонала.

10. Искусственные угрозы безопасности информации вызваны: деятельностью человека;
ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;
воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;
корыстными устремлениями злоумышленников; ошибками при действиях персонала.

11. К основным непреднамеренным искусственным угрозам АСОИ относится:
физическое разрушение системы путем взрыва, поджога и т.п.; перехват побочных

электромагнитных, акустических и других
излучений устройств и линий связи;
изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;
чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

12. К посторонним лицам нарушителям информационной безопасности относится:
представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;
персонал, обслуживающий технические средства; технический персонал, обслуживающий здание; пользователи;
сотрудники службы безопасности; представители конкурирующих организаций. лица,

нарушившие пропускной режим;

13. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:
черный пиар; фишинг; нигерийские письма; источник слухов; пустые письма.

14. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
черный пиар; фишинг; нигерийские письма; источник слухов; пустые письма.

15. Активный перехват информации - это перехват, который:
заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
неправомерно использует технологические отходы информационного

процесса;
16. осуществляется путем использования оптической техники; осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

17. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
активный перехват; пассивный перехват;аудиоперехват; видеоперехват; просмотр мусора.

18. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
активный перехват; пассивный перехват;аудиоперехват; видеоперехват; просмотр мусора.

19. Перехват, который осуществляется путем использования оптической техники называется:
активный перехват;
пассивный перехват;аудиоперехват; видеоперехват; просмотр мусора.

20. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это
уязвимость информации надежность информации защищенность информации безопасность информации

21. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это аудит аутентификацияавторизация идентификация

22. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется актуальностью информациидоступностью качеством информациицелостностью

23. Первым этапом разработки системы защиты ИС является анализ потенциально возможных угроз информациииизучение информационных потоков стандартизация программного обеспеченияоценка возможных потерь

24. Надежность системы защиты информации определяется усредненным показателем
самым слабым звеном количеством отраженных атаксамым сильным звеном

25. Политика информационной безопасности — этопрофиль защиты
итоговый документ анализа рисковстандарт безопасности совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации

26. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это аутентификацияидентификация аудит авторизация
27. Какой тип воздействия осуществляет программная закладка, которая внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всюили выбранную информацию в скрытой области памяти: компрометацияперехват наблюдение уборка мусора

28. Содержанием параметра угрозы безопасности информации

«конфиденциальность» является
несанкционированная модификацияискажение
несанкционированное получениеуничтожение

29. Требования к техническому обеспечению системы защиты: аппаратурные и физические
управленческие и документарные процедурные и раздельные административные и аппаратурные

30. Цель процесса внедрения и тестирования средств защиты — определить
уровень расходов на систему защиты выявить нарушителя
гарантировать правильность реализации средств защитывыбор мер и средств защиты

31. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство
восстанавливаемостьдетермированность целостность доступность

32. Трояские программы — это
программы-вирусы, которые распространяются самостоятельновсе программы, содержащие ошибки
часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба
текстовые файлы, распространяемые по сети

33. Наиболее надежным механизмом для защиты содержания сообщенийявляется
специальный аппаратный модуль специальный режим передачи сообщениядополнительный хост
криптография

34. Основной целью системы брандмауэра является управление доступом к архивам
внутри защищаемой сети
к секретной информациик защищаемой сети

35. Процесс имитации хакером дружественного адреса называется
«крэком» проникновениемвзломом
«спуфингом»

36. Предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы — это
идентификация аудит аутентификацияавторизация

37. Проверка подлинности пользователя по предъявленному им идентификатору — это
авторизация аутентификацияаудит идентификация

38. Свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов — это детерминированностьдостоверность целостность конфиденциальность

39. Система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую, называется
брандмауэром браузером маршрутизаторомфильтром

40. Компьютерным вирусом называется:

любая программа, созданная на языках низкого уровня
небольшая программа, способная к самокопированию, которая может приписывать себя к другим программам
файл, содержащий макросынет правильного ответа

41. +то из нижеперечисленного является одним из способов защитыинформации на компьютере?
защита паролем данных дефрагментация жесткого диска полное отключение системного блокапереустановка операционной системынет правильного ответа
все ответы правильные

42. +то такое руткит?
вредоносная программа, отслеживающая, какие сайты посещает пользователь
программа, блокирующая доступ к компьютеру и требующая деньги за разблокировку
программа для скрытого взятия под контроль взломанной системы нет правильного ответа все ответы верны

43. Под фишингом понимают
рассылки от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.
перераспределение файлов и логической структуры диска преобразование информации в целях скрытия от неавторизованных лиц
нет правильного ответавсе ответы верны

44. Как называется информация, круг лиц, имеющих доступ к которойограничен?
открытая конфиденциальнаязашифрованная

45. Шифрование информации это - ...
преобразование информации, при котором содержание становится непонятным для не обладающих соответствующими полномочиями субъектов
преобразование информации в двоичный код
процесс сжатия информации, с целью уменьшения занимаемого ей объема на диске
все ответы верны
нет правильного ответа

46. +то называют защитой информации?
предотвращение утечки информации предотвращение несанкционированных действий предотвращение непреднамеренных воздействий на защищаемую информацию
все ответы верны

47. +то понимают под утечкой информации?
бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.
преднамеренная порча или уничтожение информации преднамеренное овладение конфиденциальной информацией лицом,
не имеющим права доступа к данным.

Семестр 4

1. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
Анализ рисков
Анализ затрат / выгодыРезультаты ALE
Выявление уязвимостей и угроз, являющихся причиной риска

2. +то лучше всего описывает цель расчета ALE? Количественно оценить уровень безопасности среды Оценить возможные потери для каждой контрмеры Количественно оценить затраты / выгоды
Оценить потенциальные потери от угрозы в год

3. Тактическое планирование – это:
Среднесрочное планирование Долгосрочное планирование Ежедневное планирование Планирование на 6 месяцев

4. +то является определением воздействия (exposure) на безопасность? Нечто, приводящее к ущербу от угрозы
Любая потенциальная опасность для информации или систем Любой недостаток или отсутствие информационной безопасностиПотенциальные потери от угрозы

5. Как рассчитать остаточный риск?
Угрозы х Риски х Ценность актива
(Угрозы х Ценность актива х Уязвимости) х Риски SLE х +астоту = ALE
(Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

6. +то из перечисленного не является целью проведения анализа рисков? Делегирование полномочий
Количественная оценка воздействия потенциальных угрозВыявление рисков
Определение баланса между воздействием риска и стоимостью необходимыхконтрмер

7. +то из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
Поддержка
Выполнение анализа рисковОпределение цели и границ Делегирование полномочий

8. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
+тобы убедиться, что проводится справедливая оценка
Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

9. +то является наилучшим описанием количественного анализа рисков?
Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков Метод, основанный на суждениях и интуиции

достижим и используется
Он присваивает уровни критичности. Их сложно перевести в денежный вид. Это связано с точностью количественных элементов
Количественные измерения должны применяться к качественным элементам

10. Почему количественный анализ рисков в чистом виде не достижим? Он

11. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
Много информации нужно собрать и ввести в программу Руководство должно одобрить создание группы
Анализ рисков не может быть автоматизирован, что связано с самой природойоценки Множество людей должно одобрить данные

12. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?
Стандарты
Должный процесс (Due process)Должная забота (Due care) Снижение обязательств

13. +то такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
Список стандартов, процедур и политик для разработки программы безопасности Текущая версия ISO 17799
Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
Открытый стандарт, определяющий цели контроля

14. Из каких четырех доменов состоит CobiT?
Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг иОценка

15. +то представляет собой стандарт ISO/IEC 27799? Стандарт по защите персональных данных о здоровьеНовая версия BS 17799
Определения для новой серии ISO 27000Новая версия NIST 800-60

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

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

всего произойдет сбой?
Анализ связующего дерева AS/NZS NIST
Анализ сбоев и дефектов

20. +то было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
Безопасная OECD ISO\IEC
OECD CPTED

18. Какой из следующих методов анализа рисков пытается определить, гдевероятнее

21. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:
гаммирования;подстановки; кодирования; перестановки; аналитических преобразований.

22. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод: гаммирования;подстановки;
кодирования; перестановки;
аналитических преобразований.

23. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод: гаммирования;подстановки;
кодирования; перестановки;
аналитических преобразований.

24. Пространство ключей k – это… набор возможных значений ключа длина ключа
нет правильного ответа

25. Криптосистемы разделяются на:симметричные
ассиметричные с открытым ключом не полностью симметричные

26. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования 1
2
3

27. Сколько ключей используется в системах с открытым ключом 2
3 1

28. Как связаны ключи друг с другом в системе с открытым ключоммматематически
логически алгоритмически

29. Электронной подписью называется…
присоединяемое к тексту его криптографическое преобразованиетекст зашифрованный текст

30. Криптостойкость – это…
характеристика шрифта, определяющая его стойкость к дешифрованию без

знания ключа

свойство гаммы все ответы верны

31. Показатели криптостойкости: количество всех возможных ключей
среднее время, необходимое для криптоанализаколичество символов в ключе

32. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
знание алгоритма шифрования не должно влиять на надежность защиты структурные элементы алгоритма шифрования должны быть неизменными не должно быть простых и легко устанавливаемых зависимостью между
ключами последовательно используемыми в процессе шифрования
длина шифрованного текста должна быть равной лине исходного текста зашифрованное сообщение должно поддаваться чтению только при
наличии ключа
нет правильного ответа

33. Основные современные методы шифрования:алгоритма гаммирования алгоритмы сложных математических преобразованийалгоритм перестановки

34. Символы исходного текста складываются с символами некой случайной последовательности – это…
алгоритм гаммированияалгоритм перестановки
алгоритм аналитических преобразований

35. Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это…
алгоритм перестановкиалгоритм подстановки алгоритм гаммрования

36. Самой простой разновидность подстановки являетсяпростая замена перестановка
простая перестановка

37. Из скольки последовательностей состоит расшифровка текста по таблице Вижинера
3
4
5

38. Какие таблицы Вижинера можно использовать для повышения стойкости шифрования
во всех (кроме первой) строках таблицы буквы располагаются впроизвольном порядке
в качестве ключа используется случайность последовательных чиселнет правильного ответа

39. В чем суть метода перестановки
символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов
замена алфавитавсе правильные

40. Сколько существует способов гаммирования 2
5

3

41. +ем определяется стойкость шифрования методом гаммирования свойством гаммы длина ключа
нет правильного ответа

42. +то может использоваться в качестве гаммы любая последовательность случайных символовчисло все ответы верны

43. Какой метод используется при шифровании с помощью аналитических преобразований
алгебры матрицматрица факториал

44. +то используется в качестве ключа при шифровании с помощью аналитических преобразований
матрица Авектор
обратная матрица

45. Как осуществляется дешифрование текста при аналитических преобразованиях умножение матрицы на вектор
деление матрицы на векторперемножение матриц

46. Комбинации комбинированного метода шифрования: подстановка+гаммирование гаммирование+гаммирование подстановка+перестановка

47. Для чего использовался DES-алгоритм из-за небольшого размер ключа закрытия

коммерческой информации
шифрования секретной информациинет правильного ответа

48. Основные области применения DES-алгоритма хранение данных на компьютере электронная система платежей аутентификация сообщений

49. Достоинства ГОСТа 28147-89высокая стойкость
цена
гибкость

50. +ем отличается блок-схема алгоритма ГОСТ от блок-схемы DES-алгоритма отсутствием начальной перестановки и числом циклов шифрования длиной ключа методом шифрования

51. Ключ алгоритма ГОСТ – это…
массив, состоящий из 32-мерных векторовпоследовательность чисел алфавит

52. Какой ключ используется в шифре ГОСТ
256-битовый
246-битовый 356-битовый

53. Примеры программных шифраторов: PGP
BestCrypt 6.04PTR

54. Плюсы программных шифраторов: цена
гибкость быстродействие

55. УКЗД – это…
устройство криптографической защиты данных устройство криптографической заданности данныхнет правильного ответа

56. Блок управления – это…
основной модуль шифратора, который «заведует» работой всех остальных устройство криптографической заданности данных
проходной шифратор

57. Вычислитель – это…

набор регистров, сумматоров, блоков подстановки, связанных собой шинами передачи данных файлы, использующие различные методы кэшированияязык описания данных

58. Блок управления – это…
аппаратно реализованная программа, управляющая вычислителемязык описания данных процесс определения отвечает на текущее состояние разработкитребованиям данного этапа 59. Какой шифратор можно использовать для защиты передаваемой в Сеть информации
обычный шифратор проходной шифратортабличный шифратор

60. Из каких структурных единиц состоит шифропроцессорвычислитель
блок управления буфер ввода-вывода

61. Криптографические действия выполняет…вычислитель
буфер ввода-выводаблок управления

62. Наиболее известные разновидности полиалфавита: одноконтурные многоконтурныеполиконтурные

63. Устройство, дающее статически случайный шум – это… генератор случайных чисел

контроль ввода на компьютерУКЗД

64. Какие дополнительные порты ввода-вывода содержит УКЗД: COM USBFGR

65. Сколько существует перестановок в стандарте DES3
4
2

66. Какие перестановки существуют в стандарте DES простые расширенныесокращенные

Контролируемые компетенции: ОПК-3, ПК-7.

По результатам теста выставляется оценка до 20 баллов. Набранные баллы являются рейтинг-баллами.

Параметры оценивания:
0-2 ошибки: «отлично» (18-20 баллов);
3-4 ошибки: «хорошо» (15-17 баллов);
5-6 ошибки: «удовлетворительно» (10-14 баллов)
7. и более ошибок: «неудовлетворительно» (1-9 баллов

Рейтинг-баллы	**Аттестационная оценка обучающегося по дисциплине учебного плана в национальной системе оценивания**
18-20	Отлично
15-17	Хорошо
10-14	Удовлетворительно
1-9	Неудовлетворительно

8. 2.4. Тематика контрольных работ (не предусмотрено)

Контрольная работа предполагает выработку умений обучающимся показать глубокое знание теории предмета; на основе материала, установить и проанализировать следственно-логические связи и продемонстрировать навыки практического применения теоретической информации изучаемой дисциплины. Написание контрольной работы требует формулирование цели и задачи всей работы, заключение или выводы следуют из поставленных целей и задач.

Критерии оценки контрольной работы:

1. Выполнение задания в срок. Соответствие содержания заявленной теме;
2. Самостоятельность в выполнении работы, точность и полнота изложенного материала.
3. Логическое изложение материала. Соблюдение требований к оформлению работы.

Процедура оценки контрольной работы:

1. Если ответ удовлетворяет 3-м условиям – 18-20 баллов.
2. Если ответ удовлетворяет 2-м условиям – 15-17 баллов.
3. Если ответ удовлетворяет 1-му условию – 10-14 баллов.
4. Если ответ не удовлетворяет ни одному условию – 1-9

Рейтинг-баллы	**Аттестационная оценка студента по дисциплине учебного плана в национальной системе оценивания**

18-20	Отлично
15-17	Хорошо
10-14	Удовлетворительно
1-9	Неудовлетворительно

4. **Форма и средства (методы) проведения промежуточной аттестации**

4.1. Промежуточный контроль: зачет, экзамен (рейтинговая система)

Зачет и экзамен проводится в устной форме. Время, отведенное на подготовку вопросов зачета и экзамена, составляет 15 мин. По рейтинговой системе оценки, формы контроля оцениваются отдельно. Зачёт и экзамен составляет от 0 до 20 баллов. Допуск к зачету и экзамену составляет 45 баллов.

Типовые оценочные средства.

Вопросы к зачетуСеместр 3

1. Основные понятия защиты информации и информационной безопасности
2. Анализ угроз информационной безопасности
3. Проблемы безопасности IP-сетей
4. Угрозы и уязвимости проводных корпоративных сетей
5. Угрозы и уязвимости беспроводных сетей
6. Способы обеспечения информационной безопасности
7. Основные понятия политики безопасности
8. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности
9. Роль стандартов информационной безопасности 10. Стандарты ISO/IEC 17799:2002 (BS 7799:2000)
11. Стандарт BSI
12. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»
13. Стандарты для беспроводных сетей
14. Стандарты информационной безопасности в Интернете
15. Отечественные стандарты безопасности информационных технологий
16. Основные понятия криптографической защиты информации
17. Симметричные криптосистемы шифрования
18. Асимметричные криптосистемы шифрования
19. Комбинированная криптосистема шифрования
20. Электронная цифровая подпись и функция хэширования
21. Управление криптоключами
22. Классификация криптографических алгоритмов
23. Симметричные алгоритмы шифрования. Блочные алгоритмы шифрования данных
24. Асимметричные криптоалгоритмы. Алгоритм шифрования RSA. Алгоритмы цифровой подписи
25. Аутентификация, авторизация и администрирование действий пользователей
26. Методы аутентификации, использующие пароли и PIN-коды
27. Строгая аутентификация
28. Биометрическая аутентификация пользователя
29. Угрозы безопасности ОС
30. Понятие защищенной ОС
31. Основные функции подсистемы защиты ОС
32. Идентификация, аутентификация и авторизация субъектов доступа
33. Разграничение доступа к объектам ОС
34. Аудит безопасности в ОС.

Вопросы к экзаменуСеместр 4

1. Основные понятия защиты информации и информационной безопасности

2. Анализ угроз информационной безопасности
3. Анализ угроз сетевой безопасности.
4. Способы обеспечения информационной безопасности
5. Основные понятия политики безопасности.
6. Структура политики безопасности организации. Процедуры безопасности
7. Разработка политики безопасности.
8. Стандарты информационной безопасности
9. Основные понятия криптографической защиты информации
10. Симметричные криптосистемы шифрования
11. Асимметричные криптосистемы шифрования
12. Комбинированная криптосистема шифрования
13. Электронная цифровая подпись и функция хэширования
14. Управление криптоключами
15. Аутентификация, авторизация и администрирование действий пользователей
16. Безопасность КИС.
17. Безопасность облачных вычислений.
18. Обеспечение безопасности ОС.
19. Функции межсетевых экранов
20. Особенности функционирования
21. Схемы сетевой защиты на базе МЭ
22. Концепция построения виртуальных защищенных сетей VPN
23. VPN-решения для построения защищенных сетей
24. Протоколы формирования защищенных каналов на канальном уровне
25. Протоколы формирования защищенных каналов на сеансовом уровне
26. Защита беспроводных сетей
27. Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP
28. Протокол управления криптоключами IKE
29. Основные схемы применения IPSec. Преимущества средств безопасности IPSec
30. Управление идентификацией и доступом
31. Организация защищенного удаленного доступа.
32. Централизованный
33. контроль удаленного доступа
34. Управление доступом по схеме однократного входа с авторизацией Single Sign-On (SSO)
35. Протокол Kerberos
36. Инфраструктура управления открытыми ключами PKI
37. Технология анализа защищенности
38. Технологии обнаружения атак
39. Компьютерные вирусы и проблемы антивирусной защиты.
40. Концепция адаптивного управления безопасностью.

Контролируемые компетенции: ОПК-3, ПК-7

Градация перевода рейтинговых баллов обучающихся в пятибалльную систему аттестационных оценок и систему аттестационных оценок ECTS.

Академический рейтинг обучающегося	Аттестационная оценка обучающегося по дисциплине учебного плана в национальной системе оценивания	Аттестационная оценка обучающегося по дисциплине учебного плана в системе ECTS
95-100	Отлично	+ A (excellent)
80-94		A (excellent)
75-79	Хорошо	+B (good)
70-74		B (good)

55-69	Удовлетворительно	C (satisfactory)
50-54		D (satisfactory)
45-49	Неудовлетворительно	E (satisfactory failed)
1-44		F (not rated)
0		N/A (not rated)

5. **Практическая работа (практическая подготовка):** проверка выполнения заданий по практической подготовке в профессиональной деятельности и самостоятельной работы на практических занятиях.

Практическое задание – это частично регламентированное задание по практической подготовке в профессиональной деятельности, имеющее алгоритмическое или нестандартное решение, позволяющее диагностировать умения, интегрировать знания различных научных областей в практическую подготовку связанную с профессиональной деятельности. Может выполняться в индивидуальном порядке или группой обучающихся.

Работа во время проведения практического занятия состоит из следующих элементов:

- консультирование обучающихся преподавателем с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем практических заданий и задач;
- самостоятельное выполнение практических заданий согласно обозначенной учебной программой тематики;
- ознакомление с инструктивными материалами с целью осознания задач практического занятия, техники безопасности при работе в аудитории.

Обработка, обобщение полученных результатов практической подготовки проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач).

6. **Примерные темы к курсовым работам(проектам)**

Курсовая работа/проект– предусмотрена/не предусмотрена

7. **Оценка компетенций (в целом)**

Оценка компетенций (в целом) осуществляется по итогам суммирования текущих результатов обучающегося и промежуточной аттестации.

8. оценке освоения компетенций (в целом) учитывают: полноту знания учебного материала по теме, степень активности обучающегося на занятиях в семестре; логичность изложения материала; аргументированность ответа; уровень самостоятельного мышления,

практической подготовки; умение связывать теоретические положения с практикой, в том числе и с будущей профессиональной деятельностью с промежуточной аттестации.