федеральное государственное бюджетное образовательное учреждение высшего образования "Приволжский исследовательский медицинский университет" Министерства здравоохранения Российской Федерации

УТВЕРЖДАЮ
Проректор по учебной работе
_____ Богомолова Е.С.
«__» мая 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине **Информационная безопасность предприятия**

направление подготовки **09.04.02 Информационные системы и технологии**

профиль **Информационные системы и технологии в здравоохранении**

Квалификация выпускника:
Магистр

Форма обучения:
очно-заочная

Нижний Новгород
2021

Фонд оценочных средств по дисциплине «Информационная безопасность предприятия» предназначен для контроля знаний по программе магистратуры по направлению подготовки 09.04.02 «Информационные системы и технологии», профилю «Информационные системы и технологии в здравоохранении».

1. Паспорт фонда оценочных средств по дисциплине «Информационная безопасность предприятия»

Компетенция	*Результаты обучения*	*Виды занятий*	*Оценочные средства*
ПК-1	способен осуществлять интеллектуальный анализ данных и управление знаниями по тематике проекта		
	Знать: ИД-7$_{ПК-1.7}$ основные типы угроз информационной безопасности и способы обнаружения и защиты от угроз информационной безопасности; современные направления развития систем информационной безопасности. **Уметь**: ИД-15$_{ПК-1.15}$ идентифицировать и проводить анализ угроз информационной безопасности предприятия. **Владеть**: ИД-23$_{ПК-1.23}$ приемами идентификации и анализа угроз информационной безопасности предприятия.	**лекции, самостоятельная работа, семинары**	Реферат Собеседование
ПК-2	способен разрабатывать и управлять проектной и программной документацией в области информационных систем		
	Знать: ИД-8$_{ПК-2.8}$ нормативно-правовые основы организации информационной безопасности; стандарты и руководящие документы по защите информационных систем. **Уметь**: ИД-16$_{ПК-2.16}$ практическими навыками разработки пользовательских, функциональных и не функциональных требований к МИС. **Владеть**: ИД-24$_{ПК-2.24}$ прикладными и инструментальными средствами создания систем информационной безопасности.	**лекции, самостоятельная работа, семинары**	Реферат Собеседование

Текущий контроль по дисциплине «Информационная безопасность предприятия» осуществляется в течение всего срока освоения данной дисциплины. Выбор оценочного средства для проведения текущего контроля на усмотрение преподавателя.

Промежуточная аттестация обучающихся по дисциплине «Информационная безопасность предприятия» проводится по итогам обучения и является обязательной.

2. Критерии и шкала оценивания

Индикаторы компетенции	*Критерии оценивания*	
	Не зачтено	*Зачтено*
Полнота знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Могут быть допущены несущественные ошибки
Наличие умений	Не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Выполнены все задания. Могут быть допущены несущественные ошибки.
Наличие навыков (владение опытом)	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Продемонстрированы базовые навыки при решении стандартных задач. Могут быть допущены несущественные ошибки.
Мотивация (личностное отношение)	Учебная активность и мотивация слабо выражены, готовность решать поставленные задачи качественно отсутствуют	Проявляется учебная активность и мотивация, демонстрируется готовность выполнять поставленные задачи.
Характеристика сформированности компетенции	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение	Сформированность компетенции соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения практических (профессиональных) задач.
Уровень сформированности компетенций	Низкий	Средний/высокий

3. Оценочные средства

3.1. Текущий контроль

3.1.1. Контролируемый раздел дисциплины «Понятие информации в современном научном мире, информационные концепции. Информационные революции. Основные свойства информации, делающей ее уязвимой для злоумышленников»

Темы рефератов:

1). Определение термина информация в современном его понимании.
2). Антропоцентрическая (социоориентированная), атрибутивная и функциональная концепции понятия информация, их достоинства и недостатки.
3). Пять информационных революций в сфере коммуникаций и их влияние на развитие цивилизации.
4). Основные свойства и особенности информации, материальные носители информации.

3.1.2. Контролируемый раздел дисциплины «Понятие опасности и безопасности. Современная терминология в сфере защиты информации. Понятия персональных данных

коммерческой и государственной тайны»

Темы рефератов:

1). Угрозы информации, адекватность методов зашиты уровню опасности.

2). Открытая и закрытая информация, конфиденциальная информация, секретная информация, персональные данные граждан

3.1.3. Контролируемый раздел дисциплины «Уязвимость информации. Угрозы информационной безопасности закрытых автоматизированных систем обработки информации»

Темы рефератов:

1). Источники угроз информационной безопасности.

2). Основные принципы организации работы автоматизированных систем обработки закрытой информации.

3.1.4. Контролируемый раздел дисциплины «Математические методы защиты конфиденциальности и целостности информации. Основы современной абстрактной алгебры»

Темы рефератов:

1). Общие методы обеспечения защиты целостности, конфиденциальности и доступности информации

2). Основы современной абстрактной алгебры. Конечные группы, кольца, поля, векторные пространства. Структура конечного поля.

3.1.5. Контролируемый раздел дисциплины «Основы методов и средств помехоустойчивого кодирования, криптографии и стеганографии»

Темы рефератов:

1). Основы компьютерной вирусологии.

2). Основные положения теории помехоустойчивого кодирования, линейные блоковые коды, циклические коды, сверхточные коды.

3). Современные симметричные и несимметричные методы шифрования.

4). Современные подходы к стеганографии

3.1.6. Контролируемый раздел дисциплины «Реализация современных средств обеспечения доступности информации в автоматизированных системах обработки информации»

Темы рефератов:

1). Автоматизация методов работы с документами ограниченного доступа

2). Методы и средства идентификации, аутентификации и аудита.

3.1.7. Контролируемый раздел дисциплины «Концепция совершенствования правового обеспечения информационной безопасности Российской Федерации»

Темы рефератов:

1). Состояние правового обеспечения информационной безопасности Российской Федерации.

2). Цели и принципы правового обеспечения информационной безопасности Российской

3). Федерации.

4). Основные направления совершенствования правового обеспечения информационной безопасности Российской Федерации.

5). Реализация Концепции совершенствования правового обеспечения информационной безопасности Российской Федерации.

3.2. **Промежуточный контроль**

Вопросы для зачёта:

1. Место информационной безопасности в обеспечении системы общественной безопасности.
2. Определение информационной безопасности.
3. Основные направления и задачи обеспечения информационной безопасности общества.
4. Основные компоненты информационной безопасности автоматизированных информационных систем.
5. Уровни реализации информационной безопасности.
6. Определение и классификация информационных ресурсов.
7. Основные виды угроз информационным ресурсам.
8. Особенности угроз конфиденциальной информации.
9. Причины возникновения каналов несанкционированного доступа к информации.
10. Классификация видов каналов несанкционированного доступа к информации.
11. Технические каналы несанкционированного доступа к информации.
12. Легальные и нелегальные методы обеспечения действия каналов утечки информации.
13. Особенности угроз автоматизированным информационным системам.
14. Классификация удаленных атак.
15. Основные направления правовой защиты информации.
16. Нормативные акты, защищающих право граждан на своевременное получение достоверной информации.
17. Объекты защиты авторских прав.
18. Сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
19. Определение коммерческой тайны и сведения, которые не могут быть ее объектом.
20. Принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.
21. Основные положения концепции информационной безопасности предприятия.
22. Регламент обеспечения информационной безопасности предприятия.
23. Основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.
24. Схема каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.
25. Способы и элементы программно-технической защиты информационных ресурсов.
26. Классификация компьютерных вирусов.
27. Основные антивирусные программы.
28. Основные способы криптографического преобразования данных.
29. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
30. Виды угроз информационной безопасности Российской Федерации.
31. Роль и место информационной безопасности в общей системе национальной безопасности Российской Федерации.
32. Состояние информационной безопасности Российской Федерации.
33. Основные цели и задачи обеспечения информационной безопасности Российской

Федерации.

34. Объекты информационной безопасности Российской Федерации.
35. Основные факторы, влияющие на состояние информационной безопасности Российской Федерации.
36. Оценка состояния и ключевые проблемы обеспечения информационной безопасности Российской Федерации.
37. Источники угроз информационной безопасности Российской федерации.
38. Способы воздействия угроз на объекты информационной безопасности Российской Федерации.
39. Возможные последствия воздействия угроз информационной безопасности Российской Федерации.
40. Общие методы обеспечения информационной безопасности.
41. Базовые методы предотвращения, парирования и нейтрализации угроз информационной безопасности.
42. Особенности обеспечения информационной безопасности в различных сферах деятельности.
43. Особенности обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах.
44. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности.
45. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации.
46. Основные положения государственной политики обеспечения информационной безопасности субъектов Российской Федерации.
47. Правовое обеспечение информационной безопасности Российской Федерации.
48. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации.
49. Основные функции системы обеспечения информационной безопасности Российской Федерации.
50. Организационная структура системы информационной безопасности Российской Федерации.
51. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации.
52. Состояние правового обеспечения информационной безопасности Российской Федерации.
53. Цели и принципы правового обеспечения информационной безопасности Российской Федерации.
54. Основные направления совершенствования правового обеспечения информационной безопасности Российской Федерации.
55. Реализация Концепции совершенствования правового обеспечения информационной безопасности Российской Федерации.

Тестовые вопросы

Тестовые вопросы и варианты ответов	*Компетенция,*

	формируемая тестовым вопросом
1. СИСТЕМА ЗАЩИТЫ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ 1) 1 основывается на Уголовном Кодексе РФ 2) 2 регулируется секретными нормативными документами 3) 3 определена Законом РФ "О государственной тайне" 4) 4 осуществляется в соответствии со всеми перечисленными пунктами	ПК-1
2. ДЕЙСТВИЕ ЗАКОНА "О ГОСУДАРСТВЕННОЙ ТАЙНЕ" РАСПРОСТРАНЯЕТСЯ 1) 1 на всех граждан и должностных лиц РФ 2) 2 только на должностных лиц 3) 3 на граждан, которые взяли на себя обязательство выполнять требования законодательства о государственной тайне 4) 4 на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения	ПК-1
3. К ГОСУДАРСТВЕННОЙ ТАЙНЕ ОТНОСИТСЯ... 1) 1 информация в военной области 2) 2 информация о внешнеполитической и внешнеэкономической деятельности государства 3) 3 информация в области экономики, науки и техники и сведения в области разведывательной и оперативнорозыскной деятельности 4) 4 все перечисленное	ПК-1
4. ПОРЯДОК ЗАСЕКРЕЧИВАНИЯ СОСТОИТ В УСТАНОВЛЕНИИ СЛЕДУЮЩИХ ПРИНЦИПОВ: 1) 1 целесообразности и объективности 2) 2 необходимости и обязательности 3) 3 законности, обоснованности и своевременности 4) 4 всех перечисленных	ПК-1
5. ПРЕДЕЛЬНЫЙ СРОК ПЕРЕСМОТРА РАНЕЕ УСТАНОВЛЕННЫХ ГРИФОВ СЕКРЕТНОСТИ СОСТАВЛЯЕТ 1) 1 5 лет 2) 2 1 год 3) 3 10 лет 4) 4 15 лет	ПК-2
6. СРОК ЗАСЕКРЕЧИВАНИЯ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ 1) 1 составляет 10 лет 2) 2 ограничен 30 годами 3) 3 устанавливается Указом Президента РФ	ПК-1

4) 4 ничем не ограничен	
7. ЗА НАРУШЕНИЯ ЗАКОНОДАТЕЛЬСТВА РФ О ГОСУДАРСТВЕННОЙ ТАЙНЕ ПРЕДУСМАТРИВАЕТСЯ СЛЕДУЮЩАЯ ОТВЕТСТВЕННОСТЬ ЛИЦА: 1) уголовная и административная 2) гражданско-правовая 3) дисциплинарная 4) все перечисленные виды ответственности	ПК-2
8. КАК РЕАЛИЗУЕТСЯ МАНДАТНЫЙ КОНТРОЛЬ? 1) подсистемой защиты на аппаратном уровне 2) подсистемой защиты на уровне операционной системы 3) подсистемой защиты на программном уровне 4) подсистемой защиты на самом низком аппаратно-программном уровне	ПК-2
9. КАКОЙ ПРИЗНАК ПРИСУЩ АКТИВНОЙ АТАКЕ, ПРИ ИСПОЛЬЗОВАНИИ САМОСИНХРОНИЗИРУЮЩИХСЯ ШИФРОВ? 1) изменение знака шифротекста при активной атаке не вызывает ошибок при расшифровании других знаков шифротекста 2) искажение значений ключевого потока 3) изменение знака шифротекста при активной атаке не вызывает ошибок при расшифровании других знаков шифротекста 4) любое изменение знаков шифротекста активным противником приведет к тому, что несколько знаков шифротекста расшифруются неправильно и это с большей (по сравнению с синхронными шифрами) вероятностью будет замечено со стороны получателя, расшифровывающего сообщение	ПК-2
10. ЧТО ПОНИМАЕТСЯ ПОД ТЕРМИНОМ «ИЕРАРХИЯ ДОВЕРИЯ»? 1) система проверки цифровых сертификатов 2) система проверки цифровых подписей 3) система аннулирования сертификатов 4) доверенный центр	ПК-2
11. В ЧЕМ ЗАКЛЮЧАЕТСЯ КОНТРОЛЬ ИСХОДНОГО СОСТОЯНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ? 1) в регулярной проверке правильности результатов, получаемых при работе программного обеспечения 2) в проверке избыточности файлов программного обеспечения 3) в проверке полноты программного обеспечения	ПК-2

4) в фиксации исходного состояния программного обеспечения и сравнении полученных результатов с приведенными в документации	
12. КАКИЕ ЛИЦА РАССМАТРИВАЮТСЯ В КАЧЕСТВЕ ВОЗМОЖНЫХ НАРУШИТЕЛЕЙ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ? 1) поставщики программного обеспечения автоматизированных систем 2) разработчики программного обеспечения автоматизированных систем 3) хакеры 4) лица, имеющие доступ к работе со штатными средствами автоматизированных систем	ПК-1
13. ЧТО ИСПОЛЬЗУЕТ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ SECRET DISK ДЛЯ ХРАНЕНИЯ ПАРОЛЕЙ? 1) оперативную память компьютера 2) жесткий диск компьютера 3) электронные ключи	ПК-2
14. ЧТО ПРЕДСТАВЛЯЕТ СОБОЙ КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ, СОСТАВЛЯЮЩУЮ КОММЕРЧЕСКУЮ ТАЙНУ? 1) совокупность аппаратных средств для защиты информации 2) совокупность программных средств для защиты информации 3) действующие в единой совокупности законодательные, организационные, технические и другие способы и средства, обеспечивающие защиту информации, составляющей коммерческую тайну предприятия, по всем выявленным возможным каналам утечки	ПК-1
15. КАКИЕ ВИДЫ АЛГОРИТМОВ ИСПОЛЬЗУЕТ ОДИН И ТОТ ЖЕ КЛЮЧ ДЛЯ ШИФРОВАНИЯ И ДЕШИФРОВКИ? 1) асимметричный 2) симметричный 3) правильного ответа нет 4) ассиметричный и симметричный	ПК-2
16. УСЛОВИЕ, ПРИ КОТОРОМ В РАСПОРЯЖЕНИИ АНАЛИТИКА НАХОДИТЬСЯ ВОЗМОЖНОСТЬ ПОЛУЧИТЬ РЕЗУЛЬТАТ ЗАШИФРОВКИ ДЛЯ ПРОИЗВОЛЬНО ВЫБРАННОГО ИМ ЗАШИФРОВАННОГО СООБЩЕНИЯ РАЗМЕРА N ИСПОЛЬЗУЕТСЯ В АНАЛИЗЕ:	ПК-2

1) на основе произвольно выбранного шифротекста 2) на основе произвольно выбранного открытого текста 3) на основе только шифротекста	
17. ВЫБЕРИТЕ НАИБОЛЕЕ ВАЖНЫЙ МОМЕНТ ПРИ РЕАЛИЗАЦИИ ЗАЩИТНЫХ МЕР ПОЛИТИКИ БЕЗОПАСНОСТИ: 1) аудит, анализ затрат на проведение защитных мер 2) аудит, анализ безопасности 3) аудит, анализ уязвимостей, риск-ситуаций	ПК-2
18. СИСТЕМА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ: 1) BFox Pro 2) CAudit Pro 3) Крипто Про 4) TimeViewer	ПК-2
19. ПОЛИТИКА БЕЗОПАСНОСТИ В СИСТЕМЕ (СЕТИ) – ЭТО КОМПЛЕКС: 1) руководств, требований обеспечения необходимого уровня безопасности 2) инструкций, алгоритмов поведения пользователя в сети 3) нормы информационного права, соблюдаемые в сети 4) нормы, соблюдаемые пользователем на рабочем месте	ПК-1
20. ВИРУСЫ, КОТОРЫЕ АКТИВИЗИРУЮТСЯ В САМОМ НАЧАЛЕ РАБОТЫ С ОПЕРАЦИОННОЙ СИСТЕМОЙ: 1) загрузочные вирусы 2) троянцы 3) черви 4) нет правильного варианта ответа 5) все варианты правильные	ПК-2
21. ИНФОРМАЦИОННАЯ СИСТЕМА – ЭТО: 1) взаимосвязанная совокупность средств, методов и персонала, участвующих в обработке информации 2) взаимосвязанная совокупность средств, методов и персонала, участвующих в обработке информации и объединенная общей территорией 3) взаимосвязанная совокупность средств, методов и персонала, участвующих в обработке информации, работающих в сети Интернет 4) взаимосвязанная совокупность средств, методов и персонала, работающих в одной организации	ПК-1

22. ВЫБЕРИТЕ, ЧТО САМОЕ ГЛАВНОЕ ДОЛЖНО ПРОДУМАТЬ РУКОВОДСТВО ПРИ КЛАССИФИКАЦИИ ДАННЫХ: 1) управление доступом, которое должно защищать данные 2) оценить уровень риска и отменить контрмеры 3) необходимый уровень доступности, целостности и конфиденциальности	ПК-2
23. КОНФИДЕНЦИАЛЬНОСТЬ – ЭТО…: 1) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов 2) описание процедур 3) защита от несанкционированного доступа к информации	ПК-1
24. ЧТО ТАКОЕ УГРОЗА ИНФОРМАЦИОННОЙ СИСТЕМЕ (КОМПЬЮТЕРНОЙ СЕТИ)? 1) Вероятное событие 2) Детерминированное (всегда определенное) событие 3) Событие, происходящее периодически	ПК-2
25. КАКИЕ ТРУДНОСТИ ВОЗНИКАЮТ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПРИ КОНФИДЕНЦИАЛЬНОСТИ? 1) сведения о технических каналах утечки информации являются закрытыми 2) на пути пользовательской криптографии стоят многочисленные технические проблемы 3) все ответы правильные	ПК-1
26. УГРОЗА – ЭТО…: 1) потенциальная возможность определенным образом нарушить информационную безопасность 2) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных 3) процесс определения отвечает на текущее состояние разработки требованиям данного этапа	ПК-1
27. ОКНО ОПАСНОСТИ – ЭТО…: 1) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется. 2) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области	ПК-2

3) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере	
28. ПО АКТИВНОСТИ РЕАГИРОВАНИЯ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ДЕЛЯТ: 1) пассивные 2) активные 3) полупассивные 4) все варианты правильные	ПК-2
29. КАКИЕ СРЕДСТВА ПРИМЕНЯЮТСЯ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ: 1) аппаратные 2) криптографические 3) физические 4) нет правильного варианта ответа	ПК-2
30. ПРОГРАММНЫЕ СРЕДСТВА – ЭТО…: 1) специальные программы и системы защиты информации в информационных системах различного назначения 2) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла 3) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними 4) нет правильного варианта ответа	ПК-2

Эталоны ответов

Номер тестового задания	*Номер эталона ответа*
1	3
2	4
3	4
4	4
5	1
6	2
7	1
8	4

9	4
10	1
11	4
12	4
13	2
14	3
15	2
16	1
17	3
18	3
19	1
20	1
21	1
22	3
23	3
24	1
25	3
26	1
27	1
28	12
29	123
30	1