МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан ФРТЭ_____ Небольсин В.А.
«16» декабря 2022 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Защита информации в медицинских системах»

Направление подготовки 12.03.04 Биотехнические системы и технологии

Профиль Биотехнические и медицинские аппараты и системы

Квалификация выпускника бакалавр

Нормативный период обучения 4 года / 4 года 11 месяцев

Форма обучения очная / заочная

Год начала подготовки 2023

Автор программы _____ /Львович И.Я./

Заведующий кафедрой Системного анализа и управления в медицинских системах _____ /Коровин Е.Н./

Руководитель ОПОП _____ / Новикова Е.И./

Воронеж 2022

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах

1.2. Задачи освоения дисциплины получение представлений об общей проблеме информационной безопасности медицинских систем, об объектах защиты и основных угрозах безопасности информации в медицинских системах; ознакомление с моделями потенциальных нарушителей и способами мошенничества в информационных системах; с принципами организации систем обеспечения безопасности данных и требованиями, предъявляемыми к ним; получение знаний об основных методах защиты данных; ознакомление с физическими и аппаратными средствами защиты медицинских информационных систем; изучение криптографических методов и средств защиты данных, получение практических навыков их использования; ознакомление с методами идентификации и установления подлинности объекта, имеющего доступ к информационным ресурсам; получение знаний о методах защиты информации в локальных вычислительных сетях и в глобальной компьютерной сети Internet; изучение технологии проектирования систем защиты информации в автоматизированных системах обработки данных; ознакомление с международными стандартами защиты информации и методологией оценки уровня безопасности информации; с программой информационной безопасности России и путях ее реализации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Защита информации в медицинских системах» относится к дисциплинам части, формируемой участниками образовательных отношений (дисциплина по выбору) блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Защита информации в медицинских системах» направлен на формирование следующих компетенций:

ПК-4 - готовностью к проведению консультаций и обучения персонала учреждений здравоохранения навыкам работы с современными информационными системами

ПК-5 - способностью разрабатывать инструкции для персонала по эксплуатации технического оборудования и программного обеспечения биомедицинских и экологических лабораторий

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-4	Знать методики обучения персонала навыкам работы с современными информационными системами.
	Уметь проводить консультации и обучение персонала

	медицинских организаций навыкам работы с современными информационными системами.
	Владеть методиками и технологиями обучения персонала медицинских организаций навыкам работы с современными информационными системами.
ПК-5	Знать стандарты, методы и алгоритмы составления инструкций для персонала по эксплуатации технического оборудования и программного обеспечения биомедицинских и экологических лабораторий.
	Уметь использовать современные технологии для разработки инструкций для персонала по эксплуатации технического оборудования и программного обеспечения биомедицинских и экологических лабораторий.
	Владеть методами и технологиями разработки инструкций для персонала по эксплуатации технического оборудования и программного обеспечения биомедицинских и экологических лабораторий.

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Защита информации в медицинских системах» составляет 3 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		7
Аудиторные занятия (всего)	54	54
В том числе:		
Лекции	18	18
Лабораторные работы (ЛР)	36	36
Самостоятельная работа	54	54
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

заочная форма обучения

Виды учебной работы	Всего часов	Семестры
		9
Аудиторные занятия (всего)	8	8
В том числе:		
Лекции	4	4

Лабораторные работы (ЛР)	4	4
Самостоятельная работа	96	96
Часы на контроль	4	4
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Информация как предмет защиты	Информационная безопасность в здравоохранении Основные угрозы безопасности информации. Основные понятия. Классификация угроз безопасности данных. Модель потенциального нарушителя. Способы мошенничества в информационных системах. Цель и задачи защиты информации.Принципы организации систем обеспечения безопасности данных. Основные понятия. Принципы организации систем обеспечения безопасности данных и требования к ним.	4	4	8	16
2	Методы и средства защиты данных	Основные методы защиты данных. Классификация средств защиты данных. Формальные средства защиты. Физические средства защиты. Аппаратные средства защиты. Криптографические методы и средства защиты данных. Симметричные криптоалгоритмы. Скремблеры. Блочные шифры. Общие сведения о конкурсе AES. Симметричные криптосистемы. Асимметричные криптоалгоритмы. Общие сведения об асимметричных криптоалгоритмах. Алгоритм RSA. Технологии цифровых подписей. Механизм распространения открытых ключей. Обмен ключами по алгоритму Диффи-Хеллмана. Аутентификация пользователя. Защита исходных текстов и двоичного кода. Противодействие изучению исходных текстов. Противодействие анализу двоичного кода.	4	8	8	20
3	Сетевая безопасность	Основные понятия компьютерной безопасности. Особенности безопасности компьютерных сетей. Удаленные атаки на распределенные вычислительные системы (ВС). Характеристика и механизмы реализации типовых удаленных атак. Анализ сетевого трафика. Подмена доверенного объекта или субъекта распределенной ВС. Ложный объект распределенной ВС. Технологии обнаружения сетевых атак. Этапы реализации атак. Средства обнаружения компьютерных атак. Брандмауэр	4	4	8	16
4	Корпоративная безопасность	Защита информационных ресурсов предприятия. Модель построения системы защиты информации. Модель реализации угроз информационной безопасности. Комплексная система безопасности. Классификации объектов и систем в аспектах информационной безопасности. Требования по работе с конфиденциальной информацией. Политика ролей. Разработка документированной политики безопасности.	2	8	10	20

5	Защищенность и отказоустойчивость операционных систем	Основные понятия безопасности. Классификация угроз. Базовые технологии безопасности. Аутентификация, авторизация, аудит. Отказоустойчивость файловых и дисковых систем. Восстанавливаемость файловых систем. Избыточные дисковые подсистемы RAID	2	8	10	20
6	Стандарты и спецификации в области информационной безопасности	Основные понятия. Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Гармонизированные критерии Европейских стран	2	4	10	16
		Итого	**18**	**36**	**54**	**108**

заочная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Информация как предмет защиты	Информационная безопасность в здравоохранении Основные угрозы безопасности информации. Основные понятия. Классификация угроз безопасности данных. Модель потенциального нарушителя. Способы мошенничества в информационных системах. Цель и задачи защиты информации.Принципы организации систем обеспечения безопасности данных. Основные понятия. Принципы организации систем обеспечения безопасности данных и требования к ним.	1	0	16	17
2	Методы и средства защиты данных	Основные методы защиты данных. Классификация средств защиты данных. Формальные средства защиты. Физические средства защиты. Аппаратные средства защиты. Криптографические методы и средства защиты данных. Симметричные криптоалгоритмы. Скремблеры. Блочные шифры. Общие сведения о конкурсе AES. Симметричные криптосистемы. Асимметричные криптоалгоритмы. Общие сведения об асимметричных криптоалгоритмах. Алгоритм RSA. Технологии цифровых подписей. Механизм распространения открытых ключей. Обмен ключами по алгоритму Диффи-Хеллмана. Аутентификация пользователя. Защита исходных текстов и двоичного кода. Противодействие изучению исходных текстов. Противодействие анализу двоичного кода.	1	0	16	17
3	Сетевая безопасность	Основные понятия компьютерной безопасности. Особенности безопасности компьютерных сетей. Удаленные атаки на распределенные вычислительные системы (ВС). Характеристика и механизмы реализации типовых удаленных атак. Анализ сетевого трафика. Подмена доверенного объекта или субъекта распределенной ВС. Ложный объект распределенной ВС. Технологии обнаружения сетевых атак. Этапы реализации атак. Средства обнаружения компьютерных атак. Брандмауэр	1	0	16	21
4	Корпоративная безопасность	Защита информационных ресурсов предприятия. Модель построения системы защиты информации. Модель реализации угроз информационной безопасности. Комплексная система безопасности. Классификации объектов и систем в аспектах информационной безопасности. Требования по работе с конфиденциальной информацией. Политика ролей. Разработка документированной политики безопасности.	0	4	17	17
5	Защищенность и отказоустойчивость операционных систем	Основные понятия безопасности. Классификация угроз. Базовые технологии безопасности. Аутентификация, авторизация, аудит. Отказоустойчивость файловых и дисковых систем.	0,5	0	16,5	17

		Восстанавливаемость файловых систем. Избыточные дисковые подсистемы RAID				
6	Стандарты и спецификации в области информационной безопасности	Основные понятия. Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Гармонизированные критерии Европейских стран	0,5	0	14,5	15
		Итого	**4**	**4**	**96**	**104**

5.2 Перечень лабораторных работ

Очная форма обучения

№ п/п	Наименование лабораторной работы	Содержание лабораторной работы
1	Количественная оценка стойкости парольной защиты	Реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому
2	Реализация генератора паролей с заданными требованиями	Реализация простейшего генератора паролей, обладающего основными требованиями к парольным генераторам
3	Реализация дискреционной модели политики безопасности	Познакомиться с проблемами реализации политик безопасности в компьютерных системах на примере разработанной самостоятельно дискреционной модели безопасности
4	Реализация мандатной модели политики безопасности	Познакомиться с проблемами реализации политик безопасности в компьютерных системах на примере разработанной самостоятельно мандатной модели безопасности
5	Шифрование методами замены, перестановки и битовых манипуляций	Изучить основные методы криптографической защиты данных, типы шифров. Программно реализовать один из описанных алгоритмов шифрации методами перестановки и замены, а также битовых манипуляций
6	Работа со специализированными программами защиты данных	Реализовать на программно-аппаратном уровне положения документированной политик безопасности. Ознакомиться и получить практические навыки настройки и эксплуатации антивирусного программного обеспечения, межсетевых экранов, систем ЭЦП

Заочная форма обучения

№ п/п	Наименование лабораторной работы	Содержание лабораторной работы
1	Количественная оценка стойкости парольной защиты	Реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому
2	Реализация генератора паролей с заданными требованиями	Реализация простейшего генератора паролей, обладающего основными требованиями к парольным генераторам
3	Реализация дискреционной модели политики безопасности	Познакомиться с проблемами реализации политик безопасности в компьютерных системах на примере разработанной самостоятельно дискреционной модели безопасности
4	Реализация мандатной модели политики безопасности	Познакомиться с проблемами реализации политик безопасности в компьютерных системах на примере разработанной самостоятельно мандатной модели безопасности

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-4	Знать методики обучения персонала навыкам работы с современными информационными системами.	Выполнение лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь проводить консультации и обучение персонала медицинских организаций навыкам работы с современными информационными системами.	Выполнение лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть методиками и технологиями обучения персонала медицинских организаций навыкам работы с современными информационными системами.	Выполнение лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	Знать стандарты, методы и алгоритмы составления инструкций для персонала по эксплуатации технического оборудования и программного обеспечения биомедицинских и экологических лабораторий.	Выполнение лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь использовать современные технологии для	Выполнение лабораторных работ	Выполнение работ в срок, предусмотренный в	Невыполнение работ в срок, предусмотренный

	разработки инструкций для персонала по эксплуатации технического оборудования и программного обеспечения биомедицинских и экологических лабораторий.		рабочих программах	в рабочих программах
	Владеть методами и технологиями разработки инструкций для персонала по эксплуатации технического оборудования и программного обеспечения биомедицинских и экологических лабораторий.	Выполнение лабораторных работ	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 7 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-4	Знать методики обучения персонала навыкам работы с современными информационными системами.	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	Уметь проводить консультации и обучение персонала медицинских организаций навыкам работы с современными информационными системами.	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть методиками и технологиями обучения персонала медицинских организаций навыкам работы с современными информационными системами.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-5	Знать стандарты, методы и алгоритмы составления инструкций для	Тест	Выполнение теста на 70-100%	Выполнение менее 70%

	персонала по эксплуатации технического оборудования и программного обеспечения биомедицинских и экологических лабораторий.			
	Уметь использовать современные технологии для разработки инструкций для персонала по эксплуатации технического оборудования и программного обеспечения биомедицинских и экологических лабораторий.	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	Владеть методами и технологиями разработки инструкций для персонала по эксплуатации технического оборудования и программного обеспечения биомедицинских и экологических лабораторий.	Решение прикладных задач в конкретной предметной области	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Активный перехват информации это – перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

2. Пассивный перехват информации это – перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;

4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

3. Аудиоперехват перехват информации это – перехват, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

4. Просмотр мусора это – перехват информации, который:

1. заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;
2. основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;
3. неправомерно использует технологические отходы информационного процесса;
4. осуществляется путем использования оптической техники;
5. осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

5. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации, называется:

1. активный перехват;
2. пассивный перехват;
1. аудиоперехват;
2. видеоперехват;
3. просмотр мусора.

6. Перехват, который осуществляется путем использования оптической техники, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

7. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

8. Перехват, который осуществляется с помощью подключения к

телекоммуникационному оборудованию компьютера, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

9. Перехват, который неправомерно использует технологические отходы информационного процесса, называется:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

10. Как называется способ несанкционированного доступа к информации, который заключается в несанкционированном доступе в компьютер или компьютерную сеть без права на то?

1. «За дураком»;
2. «Брешь»;
1. «Компьютерный абордаж»;
2. «За хвост»;
3. «Неспешный выбор».

7.2.2 Примерный перечень заданий для решения стандартных задач

Защита информации – это:

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

Информационные процессы – это:

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

Доступ к информации – это:

1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее.

Защита информации от утечки – это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

2. 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;

3. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

4. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

Защита информации от несанкционированного воздействия – это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

2. воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также

1. утрате, уничтожению или сбою функционирования носителя информации;

1. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

2. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

3. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от непреднамеренного воздействия – это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

1. 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;

2. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

3. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

4. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от разглашения – это деятельность по предотвращению:

1. получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

1. 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;

1. воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

2. неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

3. несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Носитель информации – это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;

3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

4. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;

5. участник правоотношений в информационных процессах.

Собственник информации – это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;

3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

1. субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;

2. участник правоотношений в информационных процессах.

Владелец информации – это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов,

технических решений и процессов;

2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;

3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

4. субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;

5. участник правоотношений в информационных процессах.

Пользователь (потребитель) информации – это:

1. физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

2. субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;

3. субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

4. субъект, в полном объеме реализующий полномочия, пользования, распоряжения информацией в соответствии с законодательными актами;

Естественные угрозы безопасности информации вызваны:

1. деятельностью человека;

2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

3. воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека;

4. корыстными устремлениями злоумышленников;

5. ошибками при действиях персонала.

7.2.3 Примерный перечень заданий для решения прикладных задач

Метод защиты информации ограничение доступа заключается:

1. в контроле доступа к внутреннему монтажу, линиям связи и технологическим органам управления;

2. в создании физической замкнутой преграды с организацией доступа лиц, связанных с объектом функциональными обязанностями;

3. в разделении информации на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями;

4. в том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы;

5. в проверке, является ли проверяемый объект (субъект) тем, за кого себя выдает.

Шифрование методом подстановки:

1. символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста;

2. символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности;

3. шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор;

4. символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов;

5. замена слов и предложений исходной информации шифрованными.

По среде обитания классические вирусы разделяются:

1. на ссылки;
2. на компаньоны;
3. на скриптовые;
4. на паразитические;
5. на перезаписывающие.

Атака, которая позволяет воздействовать на перехваченную информацию (модифицировать информацию):

1. подмена доверенного объекта или субъекта распределенной вычислительной сети;
2. ложный объект распределенной вычислительной сети;
3. анализ сетевого трафика;
4. отказ в обслуживании;
5. удаленный контроль над станцией в сети.

К посторонним нарушителям информационной безопасности относятся:

1. пользователи;
2. персонал, обслуживающий технические средства;
3. клиенты;
4. технический персонал, обслуживающий здание;
5. сотрудники службы безопасности.

7.2.4 Примерный перечень вопросов для подготовки к зачету

1. Актуальность информационной безопасности.
2. Понятие защищаемой информации. Уровни важности информации
3. Объекты защиты
4. Национальные интересы РФ в информационной сфере и их обеспечение.
5. Классификация компьютерных преступлений.
6. Способы совершения компьютерных преступлений.
7. Пользователи и злоумышленники в Интернете.
8. Причины уязвимости сети Интернет.
9. Виды угроз информационной безопасности РФ.
10. Источники угроз информационной безопасности РФ.
11. Угрозы информационной безопасности для АСОИ.
12. Основные методы защиты данных
13. Средства защиты данных
14. Физические средства защиты
15. Аппаратные средства защиты
16. Удаленные атаки на интрасети
17. Условия существования вредоносных программ.
18. Классические компьютерные вирусы.
19. Сетевые черви.

20. Троянские программы.
21. Спам.
22. Хакерские утилиты и прочие вредоносные программы.
23. Кто и почему создает вредоносные программы.
24. Признаки заражения компьютера.
25. Источники компьютерных вирусов.
26. Основные правила защиты.
27. Антивирусные программы.
28. Классификация методов криптографического закрытия информации.
29. Шифрование.
30. Основные требования к методам защитного преобразования информации
31. Методы шифрования. Методы замены
32. Методы шифрования. Методы перестановки
33. Методы шифрования. Методы аналитических преобразований
34. Методы шифрования. Комбинированные методы
35. Шифрование с открытым ключом
36. Кодирование.
37. Стеганография.
38. Электронная цифровая подпись.
39. Законодательство в области лицензирования и сертификации.
40. Правила функционирования системы лицензирования.

7.2.5 Примерный перечень заданий для решения прикладных задач

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачет проводится по билетам, каждый из которых содержит 2 вопроса.

1. «Не зачтено», т.е. оценка «Неудовлетворительно» ставится в случае, если студент при ответе на вопросы не овладел основными знаниями и умениями в соответствии с требованиями программы и допустил больше ошибок и недочетов, чем необходимо для зачета или не может ответить ни на один из поставленных вопросов..

2. «Зачтено» ставится в случае, если студент обнаруживший всестороннее, систематическое и глубокое знание учебного и нормативного материала, умеющий свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Информация как предмет защиты	ПК-4, ПК-5	Тест, защита лабораторных работ
2	Методы и средства защиты данных	ПК-4, ПК-5	Тест, защита лабораторных работ
3	Сетевая безопасность	ПК-4, ПК-5	Тест, защита лабораторных работ

4	Корпоративная безопасность	ПК-4, ПК-5	Тест, защита лабораторных работ
5	Защищенность и отказоустойчивость операционных систем	ПК-4, ПК-5	Тест, защита лабораторных работ
6	Стандарты и спецификации в области информационной безопасности	ПК-4, ПК-5	Тест, защита лабораторных работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

1. Краковский Ю.М. Защита информации [Электронный ресурс] : учебное пособие / Ю.М. Краковский. — Электрон. текстовые данные. — Ростов-на-Дону: Феникс, 2016. — 349 c. — 978-5-222-26911-4. — Режим доступа: http://www.iprbookshop.ru/59350.html.

2. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 702 c. — 978-5-4488-0070-2. — Режим доступа: http://www.iprbookshop.ru/63594.html

3. Казанцев С.Я., Згадзай О.Э., Оболенский Р.М. и др. Правовое обеспечение информационной безопасности: Учебное пособие для студентов вузов/Под ред. С.Я. Казанцева – М:Академия, 2005

4. Мельников В.П. Информационная безопасность и защита информации: Учебное пособие для вузов – М:Академия, 2006

5. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учебное пособие –

М:Финансы и статистика, 2004

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Dr.Web, Microsoft Visual Studio, Lazarus, Embarcadero RAD Studio

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Компьютерный класс, оснащенный персональными компьютерами с установленными на них программным обеспечением (Microsoft Office), а также с выходом в Интернет

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Защита информации в медицинских системах» читаются лекции, проводятся лабораторные работы.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Лабораторные работы выполняются на лабораторном оборудовании в соответствии с методиками, приведенными в указаниях к выполнению работ.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторная работа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает

	следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.