МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КЕМЕРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Кузбасский гуманитарно-педагогический институт
Факультет физической культуры, естествознания и природопользования

«УТВЕРЖДАЮ»
Декан
В. А. Рябов
«23» января 2025 г.

.

Рабочая программа дисциплины

К.М.09.05 Защита информации

Специальность
30.05.03 Медицинская кибернетика

Направленность (профиль)
«Медицинские информационные системы»

Программа специалитета

Квалификация выпускника
Врач-кибернетик

Форма обучения
Очная

Год набора 2026

Новокузнецк 2025

Лист внесения изменений
в РПД

Сведения об утверждении:
РПД утверждена Учёным советом факультета физической культуры, естествознания и природопользования
протокол Учёного совета факультета № 7 от 23.01.2025 г.

Одобрена на заседании методической комиссии факультета физической культуры, естествознания и природопользования
протокол методической комиссии факультета № 4 от 23.01.2025г.

Рассмотрена на заседании обеспечивающей кафедры математики, физики и математического моделирования
протокол №5 от 18.12.2024 г. Зав. кафедрой Решетникова Е.В.

Оглавление

1 Цель дисциплины.

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы специалитета (далее - ОПОП): ОПК-6, ОПК-9.

1.1 Формируемые компетенции, индикаторы достижения компетенций, знания, умения, навыки

Таблица 1 – Индикаторы достижения компетенций, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
ОПК-6 Способен понимать принципы работы информационных технологий, обеспечивать информационно-технологическую поддержку в области здравоохранения; применять средства информационно-коммуникационных технологий и ресурсы биоинформатики в профессиональной деятельности; выполнять требования информационной безопасности	ОПК 6.1 Понимает принципы работы информационных технологий и умеет их применять в профессиональной деятельности. ОПК 6.2 Обеспечивает информационно-технологическую поддержку в области здравоохранения ОПК 6.3 Знает и умеет применять средства информационно-коммуникационных технологий и ресурсы биоинформатики в профессиональной деятельности ОПК 6.4 Выполняет требования информационной безопасности	**Знать:** – основное содержание, средства и методы, используемые при защите медицинских информационных систем и информационных систем персональных данных; – современные информационно-коммуникационные технологии. **Уметь**: – применять методы и средства защиты информации при решении задач профессиональной деятельности; – участвовать в подготовке и корректировке организационно-распорядительной документации по защите персональных данных в рамках медицинской информационной системы; **Владеть**: – навыками обеспечения защиты информации в процессе решения задач профессиональной деятельности; – навыками разработки эксплуатационной и организационно-распорядительной документации по защите персональных данных
ОПК-9 Способен соблюдать принципы врачебной этики и деонтологии в работе с пациентами (их родственниками/законными представителями), коллегами	ОПК-9.1 Соблюдает правовые основы профессиональной деятельности	**Знать:** – законодательные акты в сфере защиты врачебной тайны. **Уметь**: – определять, допустимо ли предоставление сведений, составляющих врачебную тайну, при решении задач профессиональной деятельности. **Владеть**: – навыками обеспечения защиты врачебной тайны в процессе решения задач профессиональной деятельности.

1.2 Место дисциплины

Дисциплина включена в модуль «Информационные технологии и системы в профессиональной деятельности» ОПОП ВО, обязательная часть. Дисциплина осваивается на 2 курсе в 4 семестре.

2 Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации.

Таблица 2 – Объем и трудоемкость дисциплины по видам учебных занятий

Общая трудоемкость и виды учебной работы по дисциплине, проводимые в разных формах	Объём часов по формам обучения
	ОФО
1 Общая трудоемкость дисциплины	108
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	64
Аудиторная работа (всего):	64

в том числе:	
лекции	28
лабораторные работы	36
в интерактивной форме	
3 Самостоятельная работа обучающихся (всего)	44
4 Промежуточная аттестация обучающегося – зачет с оценкой (4 семестр)	

3. Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 3 - Учебно-тематический план очной формы обучения

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)			Формы текущего контроля и промежуточной аттестации успеваемости
			ОФО			
			Аудиторн. занятия		СРС	
			лекц.	пр.		
	1. Основы информационной безопасности	**32**	**10**	**10**	**12**	
1	1.1 Информация. Свойства информации. Каналы передачи информации	8	2	2	4	Устный опрос
2	1.2 Понятие информационной безопасности. Составляющие информационной безопасности	12	4	4	4	Устный опрос
3	1.3 Угрозы информационной безопасности	12	4	4	4	Устный опрос. Тест
	2. Информация с ограниченным доступом	**24**	**6**	**8**	**10**	
4	2.1 Государственная тайна	6	2	2	2	Устный опрос
5	2.2 Служебная и коммерческая тайна	6	2	2	2	Устный опрос
6	2.3 Профессиональная тайна	12	2	4	6	Доклад. Тест
	3. Защита информации	**34**	**8**	**12**	**14**	
7	3.1 Уровни защиты информации. Законодательный уровень защиты информации	6	2	2	2	Устный опрос
8	3.2 Административный уровень защиты информации. Процедурный уровень защиты информации	12	2	4	6	Устный опрос. Индивидуальное задание
9	3.3 Программно-технический уровень защиты информации	6	2	2	2	Устный опрос. Доклад
10	3.4 Вредоносное программное обеспечение	10	2	4	4	Доклад. Тест
	4. Информационно-психологическая безопасность	**18**	**4**	**6**	**8**	
11	4.1. Социальная инженерия. Источники информационно-психологического воздействия.	12	2	4	6	Индивидуальное задание. Тест
12	4.2. Информационная культура и сетевой этикет. Девиантное поведение в информационно-коммуникационной среде	6	2	2	2	Устный опрос
	Промежуточная аттестация					зачет с оценкой
	Всего:	**108**	**28**	**36**	**44**	

4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации.

Для получения положительной оценки по результатам освоения дисциплины обучающемуся необходимо выполнить все установленные виды учебной работы. Оценка результатов работы обучающегося в баллах (по видам) приведена в таблице 4.

Таблица 4 - Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС)

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы
Текущая	**100**	Лекционные занятия	1 б. - посещение и конспект 1	1-14

учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий)		(14 занятий)	лекционного занятия	
		Практические занятия (18 занятий)	1 б. – посещение 1 занятия и выполнение работы на 51–65% 2 б. – посещение 1 занятия и выполнение работы на 66-100%	18 – 36
		Тесты (2 работы)	1 тест 6 –7 б. (выполнено 51 - 65% заданий) 8 – 9 б. (выполнено 66 - 85% заданий) 10 – 12 б. (выполнено 86 - 100% заданий)	12– 24
		Индивидуальное задание (2 работы)	1 работа 10 – 11 б. (выполнено 51 - 85% заданий) 12 – 13 б. (выполнено 86 - 100% заданий)	20 -26
Итого по текущей работе в семестре				51 – 100
Промежуточная аттестация (зачет с оценкой)	20	Тест.	6 баллов (пороговое значение) 10 баллов (максимальное значение)	6 - 10
		Ответ на вопрос.	2 балла (пороговое значение) 4 балла (максимальное значение)	2 - 4
		Решение задачи.	2 балла (пороговое значение) 6 баллов (максимальное значение)	2 - 6
Итого по промежуточной аттестации (зачету с оценкой)				10 – 20 б.
Суммарная оценка по дисциплине: Сумма баллов текущей и промежуточной аттестации 51 – 100 б.				

Если к моменту проведения зачета/ экзамена студент набирает 51 балл и более баллов, оценка может быть выставлена ему в ведомость и в зачетную книжку без процедуры принятия зачета/ экзамена. Выставление оценок производится на последней неделе теоретического обучения по данной дисциплине.

В промежуточной аттестации оценка выставляется в ведомость в 100-балльной шкале и в буквенном эквиваленте (таблица 5)

Таблица 5 – Соотнесение 100-балльной шкалы и буквенного эквивалента оценки

Сумма набранных баллов	Уровни освоения дисциплины и компетенций	*Экзамен*		*Зачет*
		Оценка	*Буквенный эквивалент*	*Буквенный эквивалент*
86 - 100	Продвинутый	5	отлично	Зачтено
66 - 85	Повышенный	4	хорошо	
51 - 65	Пороговый	3	удовлетворительно	
0 - 50	Первый	2	неудовлетворительно	Не зачтено

5 Материально-техническое, программное и учебно-методическое обеспечение дисциплины.

5.1 Учебная литература

Основная учебная литература

1. Башлы, П. Н. Информационная безопасность и защита информации : учебник / П. Н. Башлы, А.В. Бабаш, Е.К. Баранова. – Москва : РИОР, 2013. – 222 с. – ISBN 978-5-369-001178-2. – URL: http://znanium.com/bookread2.php?book=405000 . – Доступ из локальной сети КГПИ КемГУ свободный, с домашних ПК – авторизованный

2. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2024. — 170 с. — (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544965 . – Доступ из локальной сети КГПИ КемГУ свободный, с домашних ПК – авторизованный

Дополнительная учебная литература

1. Войниканис, Е. А. Правовое регулирование информационных отношений в

сфере защиты информации с ограниченным доступом : учебное пособие для вузов / Е. А. Войниканис ; под редакцией М. А. Федотова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 54 с. — (Высшее образование). — ISBN 978-5-534-21161-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/559476 . – Доступ из локальной сети КГПИ КемГУ свободный, с домашних ПК – авторизованный

2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2023. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511998 . – Доступ из локальной сети КГПИ КемГУ свободный, с домашних ПК – авторизованный

5.2 Материально-техническое и программное обеспечение дисциплины.

Учебные занятия по дисциплине проводятся в учебных аудиториях КГПИ КемГУ:

Наименование аудитории, оборудование	адрес
410 аудитория. Специализированная многофункциональная учебная аудитория для проведения учебных занятий лекционного типа, семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, в том числе для организации практической подготовки обучающихся с перечнем основного оборудования: *Специализированная (учебная) мебель:* доска меловая, кафедра, моноблоки аудиторные. *Оборудование для презентации учебного материала*: компьютер с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза, экран, проектор, акустическая система.	Учебный корпус №4. 654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19
508 аудитория. Компьютерный класс. Специализированная многофункциональная учебная аудитория для проведения учебных занятий лекционного типа, семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, в том числе для организации практической подготовки обучающихся с перечнем основного оборудования: *Специализированная (учебная) мебель*: доска меловая, кафедра, столы, стулья. *Оборудование для презентации учебного материала*: компьютер преподавателя с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза, проектор, экран. *Лабораторное оборудование*: компьютеры для обучающихся с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза.	Учебный корпус №4. 654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19
502 аудитория. Помещение для самостоятельной работы обучающихся с перечнем основного оборудования: *Специализированная (учебная) мебель:* доска меловая, кафедра, столы, стулья. *Оборудование для презентации учебного материала*: компьютер с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза, проектор, экран. *Лабораторное оборудование*: компьютеры для обучающихся с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду вуза	Учебный корпус №4. 654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19

5.3 Современные профессиональные базы данных и информационные справочные системы.

Электронные библиотечные ресурсы:

1. Электронная полнотекстовая база данных периодических изданий по общественным и гуманитарным наукам ООО «ИВИС», https://eivis.ru/basic/details Договор № 427 – П от 13.01.2025 г период подписки с 01.01.2025 г. по 31.12.2025 г., – Доступ из

локальной сети КГПИ КемГУ свободный, с домашних ПК – авторизованный.

2. Научная электронная библиотека – http://elibrary.ru. Доступ к отдельным периодическим изданиям. Доступ к отдельным периодическим изданиям. Договор № № SU-365/2025 от 20.12.2024 г. период подписки с 01.01.2025 г. по 31.12.2025 г. – Доступ из локальной сети КГПИ КемГУ свободный, с домашних ПК – авторизованный.

3. Межвузовская электронная библиотека (МЭБ) - https://icdlib.nspu.ru КГПИ КемГУ является участником и пользователем МЭБ. Договор № 34 от 30.09.2020 г. (договор бессрочный). – Доступ из локальной сети КГПИ КемГУ свободный, с домашних ПК – авторизованный.

4. Электронная библиотека КГПИ КемГУ – https://elib.nbikemsu.ru/MegaPro/Web – Доступ из локальной сети КГПИ КемГУ свободный, с домашних ПК – авторизованный.

Информационные справочные системы

1. Math-Net.Ru Информационная система «Общероссийский математический портал», режим доступа свободный: http://www.mathnet.ru/

2. Информационная система «Экспонента» - центр инженерных технологий и моделирования, режим доступа свободный: https://exponenta.ru/

3. База данных Science Direct (более 1500 журналов издательства Elsevier, среди них издания по математике и информатике), режим доступа свободный : https://www.sciencedirect.com/

6 Иные сведения и (или) материалы.

6.1.Примерные темы письменных учебных работ

6.1.1 Примерные задания для тестов

Тест по теме 1.3 Угрозы информационной безопасности

1. Что такое угроза информационной безопасности?
   a) Условие, при котором информация становится недоступной
   b) Возможность реализации атаки на информационные системы
   c) Процесс защиты информации от несанкционированного доступа
   d) Метод шифрования данных
2. Какой из следующих видов угроз относится к внутренним?
   a) Вирусные атаки
   b) Фишинг
   c) Утечка данных сотрудником
   d) Атака DDoS
3. К техническим средствам добывания информации относятся средства
   a) подслушивания, подглядывания, перехвата и физико-химического анализа;
   b) подслушивания, наблюдения, перехвата и физико-химического анализа;
   c) подслушивания, наблюдения, перехвата и компьютерные;
   d) подслушивания, подглядывания, перехвата и программные.
4. Конфиденциальность, целостность, доступность - это основные составляющие
   a) информационной безопасности;
   b) политики безопасности;
   c) программы безопасности;
   d) Доктрины информационной безопасности.
5. Верно ли, что при оценке достоверности информации можно использовать такой критерий как "разборчивость речи"?
   a) верно;
   b) неверно.
6. Какой из перечисленных факторов не является угрозой информационной безопасности?
   a) Утечка данных
   b) Неправильная конфигурация системы
   c) Обновление программного обеспечения

d) Атака с использованием вредоносного ПО

7. Какое из следующих действий помогает предотвратить атаки типа DDoS?

a) Использование антивируса

b) Настройка брандмауэра и систем обнаружения вторжений

c) Регулярное резервное копирование данных

d) Шифрование данных

Тест по теме 2.3 Профессиональная тайна

1. Что такое профессиональная тайна?

a) Информация, доступная только для специалистов в определенной области

b) Конфиденциальная информация, полученная в процессе профессиональной деятельности

c) Любая информация, касающаяся работы компании

d) Секреты, связанные с личной жизнью сотрудников

2. Кто несет ответственность за соблюдение профессиональной тайны?

a) Только руководитель организации

b) Все сотрудники, имеющие доступ к конфиденциальной информации

c) Только юридический отдел

d) Клиенты и партнеры

3. Какой из следующих примеров является нарушением профессиональной тайны?

a) Обсуждение рабочих вопросов на корпоративном собрании

b) Передача конфиденциальной информации третьим лицам без разрешения

c) Использование информации для внутреннего анализа

d) Хранение документов в защищенном месте

4. Какой из следующих факторов может привести к утечке профессиональной тайны?

a) Наличие системы защиты данных

b) Неправильное обращение с конфиденциальной информацией

c) Регулярные тренинги по безопасности

d) Подписание соглашений о неразглашении

5. Что такое соглашение о неразглашении (NDA)?

a) Документ, подтверждающий право на доступ к информации

b) Соглашение, запрещающее разглашение конфиденциальной информации

c) Политика компании по защите данных

d) Программа обучения сотрудников

6. Какой из следующих аспектов не относится к профессиональной тайне?

a) Личные данные клиентов

b) Финансовая информация компании

c) Общественная информация о компании

d) Результаты исследований и разработок

7. Каковы возможные последствия нарушения профессиональной тайны?

a) Увеличение доверия со стороны клиентов

b) Уголовная ответственность и штрафы

c) Повышение карьерного роста

d) Устранение конкуренции

Тест по теме 3.4 Вредоносное программное обеспечение

1. Какой тип вредоносного ПО обычно использует уязвимости программного обеспечения для распространения?

a) Троян

b) Шпионское ПО

c) Вирус

d) Червь

2. Какой из следующих типов вредоносного ПО предназначен для шифрования

данных и требования выкупа?

a) Троян

b) Вирус

c) Шифровальщик (Ransomware)

d) Червь

3. Какой метод распространения вредоносного ПО наиболее распространен?

a) Установка антивируса

b) Загрузка программ с официальных сайтов

c) Открытие вложений в электронных письмах от незнакомых отправителей

d) Использование облачных сервисов

4. Какой из следующих типов вредоносного ПО может самостоятельно размножаться и распространяться по сети?

a) Вирус

b) Червь

c) Троян

d) Шпионское ПО

5. Что такое шпионское ПО (Spyware)?

a) Программа, предназначенная для защиты данных

b) Программа, собирающая информацию о пользователе без его ведома

c) Программа, которая удаляет вирусы

d) Программа для создания резервных копий

6. Какое действие не является признаком заражения компьютера вредоносным ПО?

a) Замедление работы системы

b) Появление неожиданных рекламных окон

c) Увеличение объема свободного места на диске

d) Частые сбои и перезагрузки системы

7. Что такое "ботнет"?

a) Сеть компьютеров, зараженных вредоносным ПО и управляемых злоумышленником

b) Система защиты от вирусов

c) Программа для создания резервных копий данных

d) Облачный сервис для хранения информации

Тест по теме 4.1. Социальная инженерия. Источники информационно-психологического воздействия.

1. Что такое фишинг?

a) Метод защиты информации

b) Попытка получения конфиденциальной информации под ложным предлогом

c) Вредоносное программное обеспечение

d) Способ шифрования данных

2. Какой из следующих методов является наиболее эффективным для защиты от угроз социальной инженерии?

a) Антивирусные программы

b) Обучение сотрудников основам безопасности

c) Регулярные обновления программного обеспечения

d) Брандмауэр

3. Какое из следующих утверждений является верным в отношении социальной инженерии?

a) Она всегда требует технических навыков

b) Она основана на доверии и манипуляции с эмоциями людей

c) Она не может быть использована для получения финансовой выгоды

d) Она не связана с киберпреступностью

4. Что такое "предварительная разведка" в контексте социальной инженерии?

a) Сбор информации о цели перед атакой

b) Процесс восстановления данных после атаки

c) Обновление антивирусного ПО

d) Разработка программного обеспечения

5. Какой из следующих примеров является классическим методом социальной инженерии?

a) Установка антивируса на компьютер

b) Фишинговое письмо, содержащее ссылку на поддельный сайт банка

c) Использование сложных паролей

d) Регулярные обновления операционной системы

6. Какую информацию злоумышленники часто пытаются получить через социальную инженерию?

a) Номер телефона пользователя

b) Конфиденциальные данные, такие как пароли и номера кредитных карт

c) Информацию о погоде

d) Данные о местоположении пользователя

7. Какой из следующих способов может помочь защититься от атак социальной инженерии?

a) Никогда не проверять информацию перед ее передачей

b) Обучение сотрудников распознаванию признаков мошенничества и манипуляций

c) Игнорирование звонков от незнакомцев

d) Открытие всех вложений в электронных письмах

8. Какую роль играют эмоции в социальной инженерии?

a) Эмоции не имеют значения в процессе манипуляции

b) Эмоции используются для создания доверия и давления на жертву

c) Эмоции помогают защитить пользователей от атак

d) Эмоции мешают злоумышленникам достигать своих целей

6.1.2 Образец заданий для индивидуального задания

Индивидуальное задание по теме 3.2. Административный уровень защиты информации. Процедурный уровень защиты информации

1. Разработайте краткую политику безопасности информации для больницы. Включите в документ следующие элементы:

– Цели и задачи политики.

– Основные принципы защиты информации.

– Ответственность сотрудников за соблюдение политики.

2. Проведите оценку рисков для больницы. Определите три основных риска, связанных с защитой информации, и предложите меры по их минимизации.

– Описание риска.

– Вероятность его возникновения (высокая, средняя, низкая).

– Меры по снижению риска.

Индивидуальное задание по теме 4.1. Социальная инженерия. Источники информационно-психологического воздействия.

1. Дайте определения терминам и проиллюстрируйте их применение в реальной жизни:

– Фишинг.

– Вишинг.

– Смишинг.

2. Исследуйте три различных источника информационно-психологического воздействия, которые могут использоваться в социальной инженерии (например, СМИ, социальные сети, личные взаимодействия). Для каждого источника ответьте на следующие вопросы:

– Как этот источник может быть использован для манипуляции людьми?

– Какие психологические механизмы задействуются при воздействии через этот источник?

– Приведите примеры успешного использования этого источника в контексте социальной инженерии.

6.1.3 Примерные темы докладов

Доклад по теме 2.3 Профессиональная тайна

1. История и развитие врачебной тайны: как формировались нормы врачебной тайны в разных культурах и правовых системах.
2. Законодательные аспекты врачебной тайны: анализ ключевых законов и нормативных актов, регулирующих врачебную тайну в различных странах.
3. Этические принципы врачебной тайны: как соблюдение врачебной тайны влияет на доверие между пациентом и врачом.
4. Исключения из врачебной тайны: обзор случаев, когда раскрытие информации может быть законным или необходимым (например, угроза жизни).
5. Современные вызовы для врачебной тайны: влияние технологий (телемедицина, электронные медицинские записи) на соблюдение врачебной тайны.

Доклад по теме 3.3 Программно-технический уровень защиты информации

1. Основы криптографии: принципы шифрования данных и их применение для защиты информации.
2. Системы управления доступом: как программное обеспечение управляет правами доступа к информации и какие методы используются для их защиты.

3. Безопасность облачных технологий: риски и методы защиты данных в облачных хранилищах.
4. Аудит безопасности информационных систем: как проводить аудит и оценивать уровень защиты информации в организации.

Доклад по теме 3.4 Вредоносное программное обеспечение

1. Типы вредоносного ПО: обзор различных видов вредоносного программного обеспечения (вирусы, трояны, шпионские программы и т.д.) и их особенности.
2. Методы распространения вредоносного ПО: как злоумышленники используют социальную инженерию и другие техники для распространения вредоносных программ.
3. Влияние вредоносного ПО на бизнес: как атаки с использованием вредоносного ПО могут повлиять на финансовое состояние и репутацию компаний.
4. Современные тенденции в развитии вредоносного ПО: какие новые угрозы появляются и как они эволюционируют с течением времени.
5. Методы защиты от вредоносного ПО: эффективные стратегии и инструменты для предотвращения заражения и минимизации ущерба от вредоносного ПО.

6.2. Примерные вопросы и задания / задачи для промежуточной аттестации

Таблица 6 - Примерные теоретические вопросы и практические задания / задачи к зачету с оценкой

Разделы и темы	Примерные теоретические вопросы	Примерные практические задания / задачи
1. Основы информационной безопасности		
1.1 Информация. Свойства информации. Каналы передачи информации	1. Информация. Свойства информации. 2. Виды информации. 3. Каналы передачи информации. 4. Персональные данные. 5. Оператор персональных данных. 6. Телемедицина.	1. Перечислите каналы передачи информации в медицинском учреждении и приведите пример информации, которая по ним передается. 2. Какие законодательные акты нарушает управляющая компания, размещающая на двери подъезда списки должников за ремонт и содержание жилья, где указаны фамилии, имена, отчества, сумма задолженности, №

	Информационно-коммуникационные технологии для телемедицины.	квартиры? 3. Если к администратору гостиницы обратится некто с просьбой сообщить данные одного из постояльцев, то в каком случае эти данные придется сообщить и почему?
1.2 Понятие информационной безопасности. Составляющие информационной безопасности	7. Основные понятия информационной безопасности. 8. Проблема информационной безопасности общества. 9. Структура понятия «информационная безопасность».	4. Опишите риски для небольшой клиники, выявив основные угрозы и уязвимости в области информационной безопасности. 5. Опишите персональные риски, выявив основные угрозы и уязвимости в области информационной безопасности. 6. Оцените безопасность своего аккаунта в сети Интернет. Аргументируйте свою точку зрения.
1.3 Угрозы информационной безопасности	10.Информационные угрозы, их виды и причины возникновения. 11.Классы несанкционированного доступа к информации. 12.Информационные угрозы для государства.	7. Определить угрозы информационной безопасности больницы. 8. Определить угрозы информационной безопасности стоматологии.
2. Информация с ограниченным доступом		
2.1 Государственная тайна	13.Государственная тайна. Сведения, которые относятся к государственной тайне. 14.Государственная тайна. Механизмы защиты государственной тайны.	9. Составьте учебный сценарий для тренинга по работе с государственной тайной для сотрудников государственного органа, включая практические примеры. 10. Опишите сходства и различия подходов к защите государственной тайны в разных странах, выделив лучшие практики и возможные улучшения. 11. Проведите анализ инцидента, связанного с утечкой государственной тайны. Сформулируйте рекомендации по улучшению систем защиты.
2.2 Служебная и коммерческая тайна	15. Служебная тайна. Сведения, которые относятся к служебной тайне. 16.Коммерческая тайна. Сведения, которые относятся к коммерческой тайне. 17. Сведения, которые не могут быть коммерческой тайной.	12. На заводе с химическим опасным производством произошла авария, погиб человек. Один из работников выложил видео аварии на своей странице в социальной сети «Вконтакте». Является ли данный поступок разглашением коммерческой тайны? Аргументируйте свою точку зрения. 13. Администрация города хочет запросить документы о деятельности компании «Элита», юридический адрес которой находится в этом городе. Должна ли будет организация предоставить все необходимые документы, или она может сослаться на защиту коммерческой тайны? Аргументируйте свою точку зрения.
2.3 Профессиональная тайна	18. Профессиональная тайна. Сведения, которые относятся к профессиональной тайне. 19. Врачебная тайна. Механизмы защиты врачебной тайны. 20. Случаи, в которых можно сообщить третьему лицу	14. Почему после смерти пациента врач отказывается выдать его супруге медицинские документы пациента? Аргументируйте свою точку зрения. 15. Приведите примеры случаев утечки врачебной тайны в медицинских учреждениях. Сформулируйте причины утечки. Предложите рекомендации по предотвращению подобных

	сведения, относящиеся к врачебной тайне.	утечек в будущем. 16. Сформулируйте рекомендации для медицинского персонала по соблюдению врачебной тайны, включающие примеры правильного и неправильного обращения с данными пациентов.
3. Защита информации		
3.1 Уровни защиты информации. Законодательный уровень защиты информации	21.Уровни защиты информации. 22.Законодательный уровень защиты информации	17. Сформулируйте рекомендации для медицинского персонала по соблюдению законодательства о защите персональных данных (ПД пациентов). 18. Приведите примеры нарушения законодательства в сфере защиты информации. Предложите рекомендации по предотвращению подобных нарушений в будущем.
3.2 Административный уровень защиты информации. Процедурный уровень защиты информации	23.Административный уровень защиты информации. 24.Политика безопасности. 25.Процедурный уровень защиты информации.	19. Опишите процедуру реагирования на инциденты безопасности информации, включая этапы выявления, анализа, устранения и отчетности. 20. Напишите инструкцию для сотрудников по безопасному обращению с конфиденциальной информацией, включая примеры ситуаций и рекомендации по действиям.
3.3 Программно-технический уровень защиты информации	26.Авторизация и аутентификация. 27.Биометрия. 28.Двухфакторная аутентификация. 29.Аутентификация с помощью физического устройства.	21. Опишите процедуру аутентификации на рабочем ПК работника регистратуры (администратора) небольшого медицинского центра. 22. Опишите процедуру аутентификации на рабочем ПК врача стоматологической клиники. 23. Опишите технические средства защиты, которые можно применить для защиты информации небольшой клиники.
3.4 Вредоносное программное обеспечение	30. Вредоносные программы: понятие, классификация. 31. Защита от вредоносного ПО.	24. Опишите процесс восстановления пораженных компьютерными вирусами объектов. 25. Опишите антивирусное ПО и другие средства, которые могут быть применены для защиты ПК небольшого медицинского центра от вирусов.
4. Информационно-психологическая безопасность		
4.1. Социальная инженерия. Источники информационно-психологического воздействия.	32.Социальная инженерия в различных отраслях. 33.Известные социальные инженеры. 34.Информационные угрозы для личности (физического лица). 35.Применение методов социальной инженерии для похищения персональных данных.	26. Составить концепцию фишингового письма для персонажа, пользуясь методами социальной инженерии. 27. Определите наиболее популярные методы социальной инженерии в здравоохранении.
4.2. Информационная культура и сетевой этикет. Девиантное	36.Сетевой этикет. 37.Девиантное поведение в информационно-коммуникационной среде.	28. Опишите процесс формирования зависимости от Интернета. 29. Опишите проблему киберхулиганства. Приведите примеры.

поведение в информационно-коммуникационной среде		
Компетенции		
ОПК-6 Способен понимать принципы работы информационных технологий, обеспечивать информационно-технологическую поддержку в области здравоохранения; применять средства информационно-коммуникационных технологий и ресурсы биоинформатики в профессиональной деятельности; выполнять требования информационной безопасности		
Задание 1 Ситуация: вы работаете в частной клинике "Здоровье+" и отвечаете за управление медицинскими записями пациентов. Ваша клиника активно использует электронные медицинские записи (ЭМЗ) для хранения информации о пациентах. Недавно в клинике произошел инцидент, связанный с утечкой данных. Описание инцидента: один из сотрудников, не имеющий доступа к ЭМЗ, случайно получил доступ к конфиденциальной информации о пациенте, включая его диагноз, историю болезни и контактные данные. Информация была случайно отправлена на общую электронную почту клиники. В результате этого инцидента один из пациентов выразил недовольство и потребовал разъяснений о том, как его данные могли быть раскрыты. Задание: 1. Провести анализ ситуации: – определить возможные причины утечки данных; – указать, какие меры безопасности были нарушены; – оценить потенциальные последствия утечки информации для клиники и пациента. 2. Разработать план действий для устранения последствий инцидента. Включить в него следующие пункты: – шаги по уведомлению пациента о произошедшем инциденте. – меры по предотвращению повторных утечек данных. – предложить структуру семинара для обучения сотрудников по вопросам защиты врачебной тайны.	Оценивание результата (0-10 баллов): 1. Анализ ситуации (0-5 баллов) • 1 балл: Не выявлены причины утечки данных; отсутствует анализ. • 2 балла: Выявлены некоторые причины, но анализ неполный или поверхностный. • 3 балла: Основные причины утечки определены, но недостаточно подробностей о мерах безопасности. • 4 балла: Полный анализ причин утечки и нарушенных мер безопасности; рассмотрены потенциальные последствия. • 5 баллов: Глубокий и всесторонний анализ ситуации с ясным пониманием всех последствий для клиники и пациента. 2. План действий (0-5 баллов) • 1 балл: Отсутствует план действий или он совершенно неадекватен. • 2 балла: План действий недостаточно проработан; не все ключевые аспекты охвачены. • 3 балла: План включает основные шаги, но требует дополнительной детализации и конкретики. • 4 балла: Четкий и логичный план действий с описанием всех необходимых шагов. • 5 баллов: Полный и детализированный план действий с учетом всех аспектов, включая предотвращение будущих инцидентов.	
ОПК-9 Способен соблюдать принципы врачебной этики и деонтологии в работе с пациентами (их родственниками/законными представителями), коллегами		
Задание 2 Ситуация: вы работаете в частной клинике "Здоровье+" и отвечаете за управление медицинскими записями пациентов. Адвокат подсудимого в уголовном деле обращается к вам с целью получения медицинских данных своего клиента, который находится под следствием. Адвокат утверждает, что эти данные необходимы для защиты клиента, так как они могут подтвердить его психическое состояние на момент совершения преступления. Однако медицинские данные содержат конфиденциальную информацию, и необходимо оценить, можно ли предоставить эти данные без нарушения врачебной тайны. Задание: 1. Провести анализ ситуации: – рассмотреть ситуацию с юридической точки зрения; – рассмотреть ситуацию с этической точки зрения; – рассмотреть ситуацию с медицинской точки зрения. 2. Сформулируйте заключение о том, следует ли	Оценивание результата (0-10 баллов): 1. Анализ юридических аспектов (0-5 баллов) • 1 балл: Юридические аспекты не рассмотрены или полностью игнорируются. • 2 балла: Поверхностный анализ юридических норм; не указаны ключевые законы или прецеденты. • 3 балла: Основные юридические аспекты рассмотрены, но не все нюансы учтены. • 4 балла: Полный анализ юридических норм с указанием соответствующих законов и прецедентов. • 5 баллов: Глубокий и всесторонний анализ юридических аспектов с учетом всех возможных последствий. 2. Этические соображения (0-5 баллов) • 1 балл: Этические аспекты не обсуждаются или полностью игнорируются. • 2 балла: Этические соображения упомянуты, но анализ поверхностный и недостаточный.	

удовлетворить просьбу адвоката.	• 3 балла: Основные этические вопросы рассмотрены, но не достаточно глубоко. • 4 балла: Хороший анализ этических аспектов, включая возможные конфликты интересов. • 5 баллов: Глубокое понимание этических вопросов с четкими рекомендациями по их разрешению.

Составитель (и): Гаврилова Ю. С., старший преподаватель кафедры МФММ

(*фамилия, инициалы и должность преподавателя (ей)*)