ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА Е.А. ВАГНЕРА» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФГБОУ ВО ПГМУ им. академика. Е.А. Вагнера Минздрава России)

УТВЕРЖДАЮ
Проректор по образовательной деятельности
ФГБОУ ВО ПГМУ им. академика Е.А. Вагнера
Минздрава России
_____ Н.В. Минаева
«22» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.02. **Информационно-коммуникационные технологии и информационная безопасность (ИКТ и ИБ)**

для ординаторов

Направление подготовки: 31.00.00 Клиническая медицина
Направление подготовки: 32.00.00 Науки о здоровье и профилактическая медицина

Форма обучения: очная

Трудоемкость: 1 ЗЕТ / 36 часов

Документ подписан электронной подписью
Минаева Наталия Витальевна
00EE54182069D3F55B4CE8DF1C14C3B0DD
Срок действия с 29.03.2024 до 22.06.2025

Пермь, 2024

Разработчики:

Зав. кафедрой медицинской информатики и управления медицинскими системами, к.т.н.	Байдаров А.А.

1. Цель и задачи изучения дисциплины.

Целью изучения дисциплины «Информационно-коммуникационные технологии и информационная безопасность» является формирование компетентности в области деятельности в сфере информационных технологий при оказания медицинской помощи населению.

2. Место дисциплины в структуре основной образовательной программы ординатуры

2.1. Дисциплина относится к *обязательной* части образовательной программы, реализуется в первом семестре обучения.

2.3. Изучение дисциплины направлено на обеспечение задач профессиональной деятельности следующих типов:

- научно-исследовательский
- организационно-управленческий.

3. Требования к результатам освоения дисциплины.

3.1. Компетенции ординатора, формируемые в результате освоения дисциплины

Изучение данного модуля способствует формированию общепрофессиональной компетенции ОПК-1

3.2. Технологическая карта формирования целевых компетенций в процессе изучения дисциплины (модуля)

ОПК-1. Способен использовать информационно-коммуникационные технологии в профессиональной деятельности и соблюдать правила информационной безопасности

Код и наименование компетенции, индикатора достижения компетенции	Компоненты компетенции	Планируемые результаты обучения по дисциплине (модулю)	Технологии формирования	Средства и технологии оценки
ОПК-1.1 Выбирает источники информации, включая национальные и международные базы данных, электронные библиотечные системы, специализированные пакеты прикладных программ для решения профессиональных задач	знать	– Основные направления использования современных информационных технологий в работе врача; – Организацию работы медицинских информационных систем медицинских организаций, включая возможности использования систем поддержки принятия врачебных и управленческих решений, телемедицинские технологии; – Основные понятия и методы доказательной медицины; – Современные технологии семантического анализа информации	Лекционные, практические/ семинарские занятия, самостоятельная работа	Тесты, опрос, задания для самостоятельной работы
	уметь	– Использовать современные средства сети Интернет для поиска	Практические/ семинарские	Задания для самостоятельн

		профессиональной информации по отдельным разделам медицинских знаний в своей практической работе, а также при самостоятельном обучении, повышении квалификации; – Структурировать и формализовать медицинскую информацию.	занятия, самостоятельная работа	ой работы
	владеть	– Навыками поиска необходимой медицинской информации с применением средств сети Интернет; – Навыками работы с различными медицинскими системами; использования систем поддержки принятия клинических решений; – Навыками анализа содержания медицинских публикаций с позиций доказательной медицины; – Навыками использования программных средств для алгоритмизации лечебно-диагностического процесса	Практические занятия, самостоятельная работа	Задания для самостоятельной работы
ОПК-1.2 Создает, поддерживает, сохраняет информационную базу исследований и нормативнометодическую базу по выбранной теме и соблюдает правила информационной безопасности	знать	– Основные требования информационной безопасности, предъявляемы к организации электронного документооборота в здравоохранении и способы их реализации	Лекционные, практические/ семинарские занятия, самостоятельная работа	Тесты, задания для самостоятельной работы
	уметь	– Использовать современные подходы, обеспечивающие информационную безопасность, в практической работе врача	практические/ семинарские занятия, самостоятельная работа	задания для самостоятельной работы
	владеть	– Навыками «безопасной» работы в информационной среде медицинской организации, в практической работе врач	Практические занятия, самостоятельная работа	Задания для самостоятельной работы

4. Объем, виды учебной работы, форма аттестации

Трудоемкость дисциплины составляет 1 ЗЕ / 36 часов

Виды учебной работы	Всего акад. часов
Аудиторные занятия, всего часов в том числе:	36
лекции, час	6
практические занятия, семинары, час	20
Самостоятельная работа	8
Контроль	2

Форма аттестации: зачет

5. Содержание дисциплины (модуля)

5.1. Виды учебной работы по модулям

№	Разделы программы	Количество часов по видам занятий			
		Лекции	Практ./семин.. занятия	Самост. работа	Всего
1.	**Тема 1**. Сетевые технологии	2	8	2	14
2.	**Тема 2**. Основы информационной безопасности	2	6	4	10
3.	**Тема 3**. Информационная безопасность при взаимодействии с информационными медицинскими системами	2	6	2	10
4.	Зачет				2
	Итого	**6**	**20**	**8**	**36**

Итоговый контроль знаний: зачет

5.2. Тематический план дисциплины

5.2.1. Тематический план лекций

№	Наименование раздела. Тема лекции	Кол-во часов
1.	**Тема 1. Информационно-коммуникационные технологии**	**2**
1.1	Современные технологии в здравоохранении	1
1.2	Информационно-коммуникационные технологии	1
2.	**Тема 2. Основы информационной безопасности**	**2**
2.1	Нормативно-правовые акты в сфере информационной безопасности	1
2.2	Основы информационной безопасности	1
3.	**Тема 3. Информационная безопасность при взаимодействии с информационными медицинскими системами**	**2**
3.1	Подключение к информационным медицинским системам с применением сертификата электронной подписи	1
3.2	Защищенное рабочее место для взаимодействия с информационными медицинскими системами	1
	ИТОГО	**6**

5.2.2. Тематический план практических занятий

№	Тема занятия	Кол-во часов
		Аудит.
1	**Тема 1. Информационно-коммуникационные технологии**	**8**

1.1	Архитектура сетей и протоколы передачи информации	4
1.2	Сетевые угрозы, атаки и механизмы защиты от них	4
2.	**Тема 2. Основы информационной безопасности**	**6**
2.1	Врачебная тайна, персональные данные	3
2.2	Общая безопасность АРМ-врача	3
3.	**Тема 3. Информационная безопасность при взаимодействии с информационными медицинскими системами**	**6**
3.1	Применение электронной подписи в медицинских информационных системах	3
3.2	Средства защиты рабочего места	3
	ИТОГО	**20**

5.2.3. План самостоятельной работы

№	Наименование раздела дисциплины	Содержание самостоятельной работы	Часы
1.	**Тема 1. Сетевые технологии**	Самостоятельное изучение рекомендованной литературы и информационных источников.	2
2.	**Тема 2. Основы информационной безопасности в профессиональной деятельности**	Самостоятельное изучение нормативных актов. Выполнение индивидуальных заданий по написанию эссе.	4
3.	**Тема 3. Информационная безопасность при взаимодействии с информационными медицинскими системами**	Самостоятельное изучение рекомендованной литературы и информационных источников.	2
	ИТОГО часов:		**8**

6. Учебно-методическое обеспечение дисциплины

Учебно-методическое обеспечение образовательного процесса по дисциплине включает:

- методические рекомендации для обучающихся (Приложение 1)
- методические рекомендации для преподавателей (Приложение 2)
- фонд оценочных средств для входного (фонового) контроля (Приложение 3)
- фонд оценочных средств для итогового контроля и промежуточной (полугодовой) аттестации (Приложение 4)

7. Информационное обеспечение дисциплины

7.1. Перечень литературы, необходимой для освоения дисциплины

Основная:

1	Брюхомицкий, Ю. А. Безопасность информационных технологий. В 2 ч. Ч. 1 : учебное пособие / Ю. А. Брюхомицкий. - Ростов н/Д : ЮФУ, 2020. - 171 с. - ISBN 978-5-9275-3571-2. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785927535712.html (дата обращения: 22.09.2024). - Режим доступа : по подписке.	Удаленный доступ
2	Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие / В. Я. Ищейнов. - Москва ; Берлин : Директ-Медиа, 2020. - 270 с. - ISBN 978-5-4499-0496-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785449904966.html (дата обращения: 22.09.2024). - Режим доступа : по подписке.	Удаленный доступ
3	Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. - 4-е изд. , стер. - Москва : ФЛИНТА, 2022. - 184 с. - ISBN 978-5-9765-1904-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785976519046.html (дата обращения: 22.09.2024). - Режим доступа : по подписке.	Удаленный доступ
4	Ерохин, В. В. Безопасность информационных систем : учеб. пособие / Ерохин В. В. , Погонышева Д. А. , Степченко И. Г. - 3-е изд. , стер. - Москва : ФЛИНТА, 2016. - 184 с. - ISBN 978-5-9765-1904-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN97859765190461.html (дата обращения: 22.09.2024). - Режим доступа : по подписке.	Удаленный доступ
5	Бахаров, Л. Е. Информационная безопасность и защита информации : сб. тестов / Л. Е. Бахаров. - Москва : МИСиС, 2015. - 43 с. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/Misis_294.html (дата обращения: 22.09.2024). - Режим доступа : по подписке.	Удаленный доступ
6	Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. - Москва : Инфра-Инженерия, 2022. - 104 с. - ISBN 978-5-9729-0864-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785972908646.html (дата обращения: 22.09.2024). - Режим доступа : по подписке.	Удаленный доступ
7	Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. - Москва : Инфра-Инженерия, 2022. - 104 с. - ISBN 978-5-9729-0864-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. -	Удаленный доступ

	URL : https://www.studentlibrary.ru/book/ISBN9785972908646.html (дата обращения: 22.09.2024). - Режим доступа : по подписке.	

Дополнительная:

1. Нестеров С. А. Основы информационной безопасности: Учебное пособие. — 3-е изд. стер. — СПб, 2017. — 324 с. — (Учебники для вузов. Специальная литература).

2. Олифер В. Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб, 2010. — 943 с.

7.2. Нормативные документы

1. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 31.07.2023) "Об информации, информационных технологиях и о защите информации";
2. Федеральный закон от 21.11.2011 N 323-ФЗ (ред. от 24.07.2023) "Об основах охраны здоровья граждан в Российской Федерации", статья 13 (соблюдение врачебной тайны);
3. Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) "Об утверждении Перечня сведений конфиденциального характера".

Перечень электронных ресурсов

1. КонсультантПлюс — справочная правовая система https://www.consultant.ru/;
2. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) — федеральный орган исполнительной власти, осуществляющий реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам обеспечения безопасности информационной инфраструктуры России https://fstec.ru/;
3. РТ Медицинские информационные системы (РТ МИС) – крупнейшая IT-команда в отрасли цифровизации здравоохранения России, разработчик инновационных решений для врача и пациента. https://rtmis.ru/;
4. Официальный сайт Роскомнадзора - федеральный орган исполнительной власти, в задачи которого входят надзор в сфере связи, информационных технологий и СМИ, а также надзор по защите персональных данных и регулирование радиочастотной службы.https://rkn.gov.ru/.

8. Условия реализации дисциплины

Занятия проходят в учебных аудиториях для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Для проведения занятий лекционного имеются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам.

Занятия проходят по адресу: ул. Крупской, 44, кафедра «Медицинская информатика и управление в медицинских системах».

Приложение 1

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ

Для получения зачета ординатору необходимо:

1. Посетить все лекционные занятия. По окончанию лекций у каждого ординатора в виде конспекта должна быть зафиксирована основная информация из лекции;
2. Посетить все практические занятия. На семинарских занятиях участвовать в дискуссиях по теме занятия, отвечать на вопросы преподавателя, принимать активное участие в ходе занятия. Выполнить все практические задания.
3. По окончанию дисциплины сдать написанную самостоятельно реферативную работу по требуемой теме.
4. Выполнить тестовые задания для итоговой оценки знаний на оценку «удовлетворительно» и выше.

Приложение 4

ФОНД ТЕСТОВЫХ ЗАДАНИЙ

Условия применения, критерии оценивания. Тестовые задания – вопросы закрытого типа с одним правильным ответом из четырех предложенных вариантов.

Проверка выполненных заданий: за каждый верный ответ – 1 балл, за неверный – 0 баллов.

Оценка за тестирование определяется по доле правильных ответов:

- «удовлетворительно» - при 70-79% правильных ответов;
- «хорошо» - при 80-89% правильных ответов;
- «отлично» - при 90-100% правильных ответов.

Инструкция: выберите один правильный ответ:

Тестовые задания для итоговой оценки знаний:

1. **Сведения (сообщения, данные) независимо от формы их представления:**

a) Информация;
b) Информационные технологии;
c) Информационная система;
d) Информационно-телекоммуникационная сеть.

2. **Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов:**

a) Информационные технологии
b) Информация
c) Информационная система
d) Информационно-телекоммуникационная сеть

3. **Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации:**

a) Обладатель информации
b) Источник информации
c) Потребитель информации
d) Носитель информации

4. Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники это:

a) Информационно-телекоммуникационная сеть
b) Медицинская информационная система
c) База данных
d) Информационная система

5. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя это:

a) Конфиденциальность информации
b) Распространение информации
c) Предоставление информации
d) Доступ к информации

6. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц это:

a) Распространение информации
b) Предоставление информации
c) Конфиденциальность информации
d) Доступ к информации

7. Возможность получения информации и ее использования это:

a) Доступ к информации
b) Сохранение информации
c) Распространение информации
d) Предоставление информации

8. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети:

a) Электронное сообщение
b) Информационное сообщение
c) Текстовое сообщение
d) SMS-сообщение

9. Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные это:

a) Информационная система персональных данных
b) База данных
c) Централизованное хранилище данных
d) Сервер

10. Отношения, связанные с обработкой персональных данных, регулируются законом…

a) Федеральным законом «О персональных данных»
b) «Об информации, информационных технологиях»
c) «О защите информации»
d) Федеральным законом «О конфиденциальной информации»

11. Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т. д это:

a) «Обработка персональных данных»
b) «Работа с персональными данными»
c) «Преобразование персональных данных»
d) «Изменение персональных данных»

12. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:

a) Идентификация
b) Авторизация
c) Аутентификация
d) Обезличивание

13. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:

a) Аутентификация
b) Авторизация
c) Обезличивание
d) Идентификация

14. Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом

a) Авторизация
b) Идентификация
c) Аутентификация
d) Обезличивание

15. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:

a) Login
b) Password
c) Пароль
d) Смарт-карта

16. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:

a) Шифрование
b) Идентификация
c) Аутентификация
d) Авторизация

17. Несанкционированный доступ к информации это:

a) Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
b) Работа на чужом компьютере без разрешения его владельца
c) Вход на компьютер с использованием данных другого пользователя
d) Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей

18. «Персональные данные» это:

a) Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
b) Фамилия, имя, отчество физического лица
c) Год, месяц, дата и место рождения, адрес физического лица
d) Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

19. В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности:

a) В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности
b) Выход в Интернет без разрешения администратора
c) В случаях установки нелицензионного ПО
d) В случае не выхода из информационной системы

20. Наиболее опасным источником угроз информационной безопасности предприятия являются:

a) Рядовые сотрудники предприятия
b) Другие предприятия (конкуренты)
c) Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
d) Хакеры

21. Для того чтобы снизить вероятность утраты информации необходимо:

a) Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)
b) Регулярно производить антивирусную проверку компьютера
c) Защитить вход на компьютер к данным паролем
d) Проводить периодическое обслуживание ПК

22. Пароль пользователя должен

a) Содержать цифры и буквы, знаки препинания и быть сложным для угадывания
b) Содержать только цифры или только буквы
c) Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
d) Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

23. Информационная безопасность обеспечивает…

a) Сохранность информации

b) Блокирование информации
c) Искажение информации
d) Недоступность информации

24. Основной закон в сфере информационной безопасности:

a) Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
b) "Конституция Российской Федерации"
c) Гражданский кодекс Российской Федерации (ГК РФ)
d) ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

25. К правовым методам, обеспечивающим информационную безопасность, относятся:

a) Разработка и конкретизация правовых нормативных актов обеспечения безопасности
b) Разработка аппаратных средств обеспечения правовых данных
c) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
d) Разработка правил работы с программными и аппаратными средствами

26. Виды информационной безопасности:

a) Персональная, корпоративная, государственная
b) Клиентская, серверная, сетевая
c) Локальная, глобальная, смешанная
d) Индивидуальная, общая

27. Цели информационной безопасности – своевременное обнаружение, предупреждение:

a) несанкционированного доступа, воздействия в сети
b) инсайдерства в организации
c) чрезвычайных ситуаций
d) сбоев работы в компьютерных сетях

28. Основными рисками информационной безопасности являются:

a) Потеря, искажение, утечка информации
b) Искажение, уменьшение объема, перекодировка информации
c) Техническое вмешательство, выведение из строя оборудования сети
d) Недополучение ожидаемой прибыли

29. ЭЦП – это:

a) Электронно-цифровая подпись
b) Электронно-цифровой преобразователь
c) Электронно-цифровой процессор
d) Электрическая цифровая подпись

30. Когда получен спам по e-mail с приложенным файлом, следует:

a) Удалить письмо с приложением, не раскрывая (не читая) его
b) Прочитать приложение, если оно не содержит ничего ценного – удалить
c) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
d) Игнорировать письмо с приложением

31. Угроза информационной системы (компьютерной сети) – это:

a) Вероятное событие
b) Детерминированное (всегда определенное) событие
c) Событие, происходящее периодически
d) Ожидаемой событие

32. Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

a) Защищаемой
b) Регламентированной
c) Правовой
d) Скрытой

33. Федеральный закон «об информации, информатизации и защите информации» направлен на:

a) Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ
b) Регулирование взаимоотношений в гражданском обществе РФ
c) Регулирование требований к работникам служб, работающих с информаций
d) Формирование необходимых норм и правил работы с информацией

34. Хищение информации – это…

a) Несанкционированное копирование информации
b) Утрата информации
c) Блокирование информации
d) Искажение информации
e) Продажа информации

35. Доступ к информации – это:

a) Возможность получения информации и ее использования
b) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
c) Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
d) Информация, переданная или полученная пользователем информационно-телекоммуникационной сети

Эталоны ответов;

Тестовые задания для итоговой оценки знаний:

1.	a	11. a	21. a	31. a
2.	a	12. a	22. a	32. a
3.	a	13. a	23. a	33. a
4.	a	14. a	24. a	34. a
5.	a	15. a	25. a	35. a
6.	a	16. a	26. a	
7.	a	17.a	27. a	
8.	a	18. a	28. a	
9.	a	19. a	29. a	
10.	a	20. a	30. a	