ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

«УТВЕРЖДАЮ»
Декан медицинского факультета
_____/А.В. Добрин/

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.01.01 Безопасность информационных систем

Направление подготовки: 09.04.01 Информатика и вычислительная техника
Направленность (профиль): Управление цифровой трансформацией медицинских организаций
Квалификация (степень): магистр
Форма обучения: *очная*

Факультет: Медицинский
Кафедра: Медицинской информатики и кибернетики

	очная форма	**очно-заочная форма**	**заочная форма**
Курс	**2**		
Семестр/триместр	**4**		

Лекции	**14**		
Лабораторные занятия	**28**		
Практические (семинарские) занятия			
в т.ч. практическая подготовка	**2**		
Консультации			
Форма(ы) промежуточной аттестации	**Экзамен – 0,3**		
Контроль	**9**		
Иные формы работы			
Самостоятельная работа	**92,7**		

Всего часов:144
Трудоемкость: 4 зачетные единицы.

Разработчик(и) рабочей программы:
кандидат физико-математических наук, доцент _____ *Гладких О.Б.*

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины: научная и практическая подготовка магистров по направлениям применения методов научного познания, формирование представления о современном состоянии и проблемах методологии и методах научного исследования.

Задачи изучения дисциплины:

Задачами изучения дисциплины «Безопасность информационных систем» являются:

- дать общее представление о процессе научного исследования;
- знать основные области и задачи применения методов научного исследования;
- научить магистров использовать в своей практической деятельности методы научных исследований;
- привить магистрам умение ориентироваться в методах научного исследования.

Место дисциплины в структуре ОПОП: реализуется в рамках части, формируемой участниками образовательных отношений блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ПКС-1	**Знать:** – международные и отечественные стандарты, лучшие практики и фреймворки по разработке и реализации стратегии развития ИТ.	**Знает:** – основные законы РФ нормативы и стандарты, обеспечивающие правовую защиту информациив информационных системах.
	Уметь: – формировать и согласовывать стратегические цели развития ИТ; – организовывать деятельность по разработке и выполнению стратегии развития ИТ.	**Умеет:** – организовать мероприятия, парирующие внутренние и внешние угрозы безопасности информации в информационных системах.
	Владеть: – методами организации разработки и реализации стратегии развития ИТ.	**Владеет:** – методами и приёмами защиты информации в информационных системах от несанкционированного доступа, хищения и разрушения.

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№ п/п	Наименование разделов и тем	Всего	Аудиторные занятия			Сам. раб.
			ЛК	ПЗ	ЛБ	
	Раздел 1. Общие вопросы информационной безопасности	**28**	**2**	**6**		**20**
1	Тема 1. Основные понятия и определения. Международные стандарты информационного обмена.	15	1	4		10
2	Тема 2. Комплексность системы защиты информации.	13	1	2		10

	Раздел 2. Государственная система информационной безопасности	**30**	**4**	**6**		**20**
3	Тема 3. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	16	2	4		10
4	Тема 4. Лицензирование и сертификация в области защиты информации. Концепция информационной безопасности.	24	2	2		20
	Раздел 3. Теоретические основы методов защиты информационных систем	**32**	**4**	**8**		**20**
5	Тема 5. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Методы криптографии. Алгоритмы электронно-цифровой подписи.	32	4	8		20
	Раздел 4. Алгоритмы безопасности в компьютерных сетях	**44,7**	**4**	**8**		**32,7**
6	Тема 6. Межсетевые экраны.	26	2	4		20
7	Тема 7. Атаки на сервера.	18,7	2	4		12,7
8	*Экзамен*	0,3				
9	*Контроль:*	9				
10	*Итого за 4 семестр*	144	14	28		92,7
11	в т.ч. практическая подготовка	2				
	ИТОГО:	**144**	**14**	**28**		**92,7**

Очно-заочная форма обучения

(не реализуется)

Заочная форма обучения

(не реализуется)

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме контрольной работы в виде теста, реферата.

Типовой вариант контрольной работы

Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. **конфиденциальная информация**

Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это…

1. **комплексное обеспечение ИБ**
2. безопасность АС
3. угроза ИБ
4. атака на АС
5. политика безопасности

Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….

1. идентификатор пользователя
2. **пароль пользователя**
3. учетная запись пользователя
4. парольная система

Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

1. Защита информации
2. **Компьютерная безопасность**
3. Защищенность информации
4. Безопасность данных

Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной сети от заданного множества угроз безопасности:

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. атака на автоматизированную систему
5. **политика безопасности**

К функциям информационной безопасности относятся:

1. **совершенствование законодательства РФ в сфере обеспечения информационной безопасности**
2. **выявление источников внутренних и внешних угроз**
3. **Страхование информационных ресурсов**
4. **защита государственных информационных ресурсов**
5. **подготовка специалистов по обеспечению информационной безопасности**

К типам угроз безопасности парольных систем относятся

1. словарная атака
2. тотальный перебор
3. атака на основе психологии
4. разглашение параметров учетной записи
5. **все варианты ответа верны**

К достоинствам технических средств защиты относятся:

1. регулярный контроль
2. **создание комплексных систем защиты**
3. степень сложности устройства
4. Все варианты верны

Информационная безопасность это:

1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
2. **Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз**
3. Состояние, когда не угрожает опасность информационным системам
4. Политика национальной безопасности России

Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:

1. **конфиденциальность**
2. доступность
3. аутентичность
4. целостность

Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:

1. защита информации от непреднамеренного воздействия
2. защита информации от несанкционированного воздействия
3. защита информации от несанкционированного доступа
4. **защита от утечки информации**

Исследование возможности расшифрования информации без знания ключей:

1. криптология
2. **криптоанализ**
3. взлом
4. несанкционированный доступ

Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости компьютерной сети.

1. Комплексное обеспечение информационной безопасности
2. Безопасность компьютерной сети
3. Угроза информационной безопасности
4. **Атака на компьютерную сеть**
5. Политика безопасности

К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан ...»

1. **Информация без ограничения права доступа**
2. Информация с ограниченным доступом
3. Информация, распространение которой наносит вред интересам общества
4. Объект интеллектуальной собственности
5. Иная общедоступная информация

Примерная тематика рефератов

1. Основные нормативные акты РФ, связанные с правовой защитойинформации.
2. Виды компьютерных преступлений.
3. Способы и механизмы совершения информационных компьютерныхпреступлений.
4. Основные параметры и черты информационной компьютернойпреступности в России.
5. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
6. Виды защищаемой информации.
7. Государственная тайна как особый вид защищаемой информации.
8. Конфиденциальная информация.
9. Система защиты государственной тайны.Правовой режим защиты государственной тайны.
10. Защита интеллектуальной собственности средствами патентного иавторского права.
11. Международное законодательство в области защиты информации.
12. Программно-аппаратные средства обеспечения информационной безопасности в информационных системах.

Промежуточная аттестация обучающихся осуществляется в форме экзамена с использованием следующих оценочных материалов: перечень вопросов к экзамену.

Вопросы к экзамену
(4 семестр, очная форма обучения)

1. Понятия информация, информатизация, информационная система, информационная безопасность.
2. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.
3. Защита информации, тайна, средства защиты информации.
4. Международные стандарты информационного обмена.
5. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.
6. Требования к защите информации.
7. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
8. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
9. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
10. Доктрина информационной безопасности Российской Федерации.
11. Структура государственной системы информационной безопасности.
12. Структура законодательной базы по вопросам информационной безопасности.
13. Лицензирование и сертификация в области защиты информации.
14. Концепция информационной безопасности.
15. Понятие угрозы.
16. Виды противников или «нарушителей».
17. Классификация угроз информационной безопасности.
18. Виды угроз.
19. Основные нарушения.
20. Характер происхождения угроз (умышленные и естественные факторы).
21. Источники угроз.
22. Предпосылки появления угроз.
23. Классы каналов несанкционированного получения информации.
24. Причины нарушения целостности информации.
25. Основные положения теории информационной безопасности информационных систем.
26. Формальные модели безопасности.
27. Дискреционная модель Харрисона-Руззо-Ульмана.
28. Типизированная матрица доступа.
29. Модель распространения прав доступа Take-Grant.
30. Мандатная модель Белла-ЛаПадулы.
31. Ролевая политика безопасности.
32. Ограничения на области применения формальных моделей.
33. Методы криптографии.
34. Симметричное и асимметричное шифрование.
35. Электронно-цифровая подпись.
36. Алгоритмы электронно-цифровой подписи.
37. Хеширование.
38. Имитовставки.
39. Криптографические генераторы случайных чисел.
40. Способы распространения ключей.

41. Обеспечиваемая шифром степень защиты.
42. Криптоанализ и атаки на криптосистемы.
43. Сжатие информации.
44. Межсетевые экраны.
45. Проектирование МЭ.
46. Атаки на сервера.
47. Атаки на рабочие станции.
48. Атака типа «отказ в обслуживании».
49. Протоколирование.
50. Сетевые защищенные протоколы.

IV.ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 01.06.2022). – Библиогр.: с. 196-205. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988. – Текст : электронный.
2. Основы администрирования информационных систем : учебное пособие : [16+] / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 202 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 01.06.2022). – Библиогр. в кн. – ISBN 978-5-4499-1674-7. – DOI 10.23681/598955. – Текст : электронный.

4.2. Дополнительная литература

1. Кияев, В. Безопасность информационных систем: курс : учебное пособие : [16+] / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429032 (дата обращения: 01.06.2022). – Текст : электронный.
2. Мансуров, Г. З. Право цифровой безопасности : учебник : [16+] / Г. З. Мансуров. – Москва :Директ-Медиа, 2022. – 148 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=687364 (дата обращения: 01.06.2022). – Библиогр. в кн. – ISBN 978-5-4499-3061-3. – Текст : электронный.

V.ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	http://edu.ru/	**Российское образование: Федеральный портал. Включает**	Свободный доступ

		ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	

VI.СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- LibreOffice и др.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных классах, оснащенных автоматизированными рабочими местами с компьютерами.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.