ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

«УТВЕРЖДАЮ»
Директор института математики, естествознания и техники
_____/Н.В.Черноусова/

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.08 Основы информационной безопасности

Направление подготовки: *10.03.01 Информационная безопасность*
Направленность (профиль): *Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)*
Квалификация (степень): *бакалавр*
Форма обучения: *очная*

Институт: *математики, естествознания и техники*
Кафедра: *математического моделирования, компьютерных технологий и информационной безопасности*

	очная форма	**очно-заочная форма**	**заочная форма**
Курс	**2**		
Семестр	**3,4**		

Лекции	**36**		
Лабораторные занятия	**72**		
Практические (семинарские) занятия	**36**		
в т. ч. практическая подготовка			
Форма(ы) промежуточной аттестации	**Зачет** **Экзамен - 0,6**		
Контроль	**18**		
Иные формы работы			
Самостоятельная работа	**125,4**		

Всего часов: 288
Трудоемкость: 8 зачетных единицы.
Разработчик(и) рабочей программы:
кандидат физико-математических наук, доцент С.А. Рощупкин

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

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

Задачи изучения дисциплины:

- развитие творческих подходов при решении сложных научно технических задач, связанных с обеспечением информационной безопасности государства и его информационной инфраструктуры;
- развитие профессиональной культуры, формирование научного мировоззрения и развитие системного мышления;
- привитие стремления к поиску оптимальных, простых и надежных решений;
- расширение кругозора.

Место дисциплины в структуре ОПОП: реализуется в рамках базовой части блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-10	**Знать**: - принципы реализации, развития и совершенствования систем обеспечения информационной безопасности предприятия в рамках комплексного подхода; - структуру политики информационной безопасности; - основные технические методы и принципы управления информационной безопасностью предприятий отрасли.	**Знает:** - основные термины, цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; - методологию создания систем защиты информации; - перспективные направления развития средств и методов защиты информации; - роль и место информационной безопасности в системе национальной безопасности страны; - угрозы информационной безопасности государства.
	Уметь: - определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем; - разрабатывать политику информационной безопасности объекта защиты; - применять на практике основные механизмы управления информационной безопасностью на объекте защиты.	**Умеет:** - выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации.

	Владеть: - навыками планирования и организации системы защиты информации; - навыками реализации элементов политики информационной безопасности; - методами организации и управления деятельностью служб защиты информации на предприятии.	**Владеет:** - навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.
ОПК-12	**Знать**: - перечень необходимых исходных данных для проектирования подсистем и средств обеспечения защиты информации, основные возможные проектные решения автоматизированных систем и подсистем, средства их защиты; - правила выполнения технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности.	**Знает:** - современные подходы к построению систем защиты информации; - компьютерную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности; - особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.
	Уметь: - проводить анализ исходных данных для проектирования подсистем передачи информации и средств обеспечения информационной безопасности; - проводить технико-экономический анализ и обоснование проектных решений, связанных с обеспечением информационной безопасности.	**Умеет:** - пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; - применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований.
	Владеть: - навыками обеспечения информационной безопасности исходных данных для проектирования подсистем и средств; - навыками выполнения технико-экономического анализа и обоснования проектных решений, связанных с обеспечением информационной безопасности.	**Владеет:** - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты.

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

№	Наименование разделов и тем	Всего часов	Аудиторные занятия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
3 семестр						
Раздел 1. «Информационная безопасность в системе национальной безопасности»		**62**	**8**	**8**	**16**	**30**
1	Тема 1. Понятийный аппарат и основы терминологии информационной и национальной безопасности. Виды национальной безопасности и их краткая характеристика. Системные связи информационной безопасности с другими видами национальной безопасности	30	4	4	8	14
2	Тема 2. Системные связи информационной безопасности с другими видами национальной безопасности	32	4	4	8	16
Раздел 2. «Информационные уязвимости объектов»		**62**	**8**	**8**	**16**	**30**
3	Тема 3. Антропогенные информационные уязвимости. Техногенные информационные уязвимости.	30	4	4	8	14
4	Тема 4. Организационно-правовые и комбинированные информационные уязвимости	32	4	4	8	16
Раздел 3. «Угрозы информационной безопасности и их источники»		**20,7**	**2**	**2**	**4**	**12,7**
5	Тема 5. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация. Угрозы конфиденциальности, целостности и доступности информации. Системная классификация угроз. Информационная война как высшая форма угрозы информационной безопасности	20,7	2	2	4	12,7
	Форма отчетности	*экзамен*				
	Контроль	**9**				
	Экзамен	**0,3**				
	Зачет					
	Итого за 3 семестр	***144***	***18***	***18***	***36***	***62,7***
	в т.ч. практическая подготовка					
4 семестр						
Раздел 4. «Средства обеспечения информационной безопасности»		**26**	**4**	**4**	**8**	**10**
6	Тема 6. Организационно-правовые средства обеспечения информационной безопасности, категорирование информации, допуск и доступ к информационным ресурсам. Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности. Пассивные и активные средства	26	4	4	8	10

	противодействия техническим разведкам. Защита информации от утечки по техническим каналам.					
Раздел 5. «Государственная политика в области информационной безопасности»		**32,7**	**6**	**6**	**8**	**12,7**
7	Тема 7. Национальные интересы личности, общества и государства в информационной сфере. Государственные органы обеспечения информационной безопасности. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного противоборства.	32,7	6	6	8	12,7
Раздел 6. «Риски информационной безопасности и проблема построения комплексной системы защиты информации.»		**76**	**8**	**8**	**20**	**40**
8	Тема 8. Стратегия и концепция защиты информации. Формирование политики обеспечения информационной безопасности. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения.	38	4	4	10	20
9	Тема 9. Построение комплексной оптимальной системы защиты. Оценка рисков и организация управления процессом защиты информации.	38	4	4	10	20
	Форма отчетности	*экзамен*				
	Контроль	**9**				
	Экзамен	**0,3**				
	Зачет					
	Итого за 4 семестр	***144***	***18***	***18***	***36***	***62,7***
	в т.ч. практическая подготовка					
	ИТОГО	**252**	**38**	**28**	**38**	**138,7**

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.

Типовой вариант контрольной работы

1. Информационная безопасность в системе национальной безопасности
2. Понятийный аппарат и основы терминологии информационной и национальной безопасности.
3. Виды национальной безопасности и их краткая характеристика.

4. Системные связи информационной безопасности с другими видами национальной безопасности.
5. Информационные уязвимости объектов.
6. Антропогенные информационные уязвимости.
7. Техногенные информационные уязвимости.
8. Организационно-правовые информационные уязвимости.
9. Комбинированные информационные уязвимости
10. Угрозы информационной безопасности и их источники.
11. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.
12. Эндогенные и экзогенные, угрозы информационной безопасности, их классификация.
13. Антропогенные и техногенные угрозы информационной безопасности, их классификация.
14. Системная классификация угроз информационной безопасности.
15. Угрозы конфиденциальности, целостности и доступности информации.
16. Информационная война как высшая форма угрозы информационной безопасности.
17. Категорирование информации.
18. Допуск к информационным ресурсам.
19. Основные принципы защиты информации от несанкционированного доступа.
20. Средства обеспечения информационной безопасности.
21. Аппаратные средства обеспечения информационной безопасности.
22. Программные средства обеспечения информационной безопасности.
23. Криптографические средства обеспечения информационной безопасности.
24. Стеганографические средства обеспечения информационной безопасности.
25. Организационно-правовые средства обеспечения информационной безопасности,
26. Государственная политика в области информационной безопасности.
27. Государственные органы обеспечения информационной безопасности.
28. Приоритетные направления обеспечения информационной безопасности в условиях информационного общества.
29. Приоритетные проблемы обеспечения информационной безопасности в условиях информационного общества.
30. Технические каналы утечки конфиденциальной информации. Основные методы защиты.
31. Пассивные средства противодействия техническим разведкам.
32. Активные средства противодействия техническим разведкам.
33. Базовые стратегии организации защиты информации.
34. Полное множество функций защиты информации.
35. Задачи защиты информации. Репрезентативное множество задач защиты.
36. Формирование политики обеспечения информационной безопасности объекта.
37. Проектирование оптимальных систем защиты информации.
38. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения.
39. Риски информационной безопасности
40. Статистика инцидентов информационной безопасности.
41. Основные макропроцессы управления функционированием комплексной системы защиты информации

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

Вопросы к экзамену
(3 семестр, очная форма обучения)

1. Понятийный аппарат и основы терминологии информационной и национальной безопасности.
2. Методики составления обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности;
3. Виды национальной безопасности и их краткая характеристика.
4. Проблема социальной значимости профессии, высокой мотивации к выполнению профессиональной деятельности в области обеспечения информационной безопасности.
5. Системные связи информационной безопасности с другими видами национальной безопасности.
6. Определение места и роли информационной безопасности в системе национальной безопасности России.
7. Антропогенные информационные уязвимости.
8. Методика изучения и обобщения опыта работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации.
9. Техногенные информационные уязвимости.
10. Проблема технических каналов утечки информации, возможности
технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.
11. Организационно-правовые и комбинированные информационные уязвимости.
12. Проблема использования естественнонаучных законов и применения математического аппарата в профессиональной деятельности при выявлении сущности проблем, возникающих в задачах обеспечения информационной безопасности.
13. Эндогенные и экзогенные, антропогенные и техногенные угрозы информационной безопасности, их классификация.
14. Проблема определения видов и форм информации, подверженной угрозам, видов, возможных методов и путей реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.
15. Угрозы, целостности, доступности и конфиденциальности информации.
16. Классификация правонарушений в сфере компьютерной информации.
17. Роль информации в развитии современного общества, применение достижений информатики и вычислительной техники в задачах переработки больших объемов информации и проведения целенаправленного поиска в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных сетях,
18. Противодействия нарушениям конфиденциальности, целостности и доступности информации и киберпреступности.

Вопросы к экзамену
(4 семестр, очная форма обучения)

1. Информационная война как высшая форма угрозы информационной безопасности.
2. Проблема применения методов и средств выявления угроз безопасности автоматизированным системам.
3. Организационно-правовые средства обеспечения информационной
безопасности, категорирование информации, допуск и доступ к информационным ресурсам.
4. Проблема применения методик проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности.
5. Программно-аппаратные, криптографические и стеганографические средства обеспечения информационной безопасности.
6. Проблема разработки методик проведения совместного анализа функционального процесса объекта защиты и применяемых информационных технологий и технических средств с целью определения возможных источников информационных угроз, их вероятных целей и тактики.
7. Пассивные и активные средства противодействия техническим разведкам, информационное противоборство.
8. Применение принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
9. Статистика инцидентов информационной безопасности.
10. Проблема применения принципов и методов анализа и оценки угроз информационной безопасности объекта.
11. Проблема применения методов формирования требований по защите информации по критерию цена-качество.
12. Проблема равнопрочного распределения ограниченных средств обеспечения информационной безопасности по информационным уязвимостям, методы и критерии ее решения.
13. Проблемам разработки методик применения комплексного подхода к обеспечению информационной безопасности в различных сферах деятельности.
14. Проблема применения принципов и методов анализа и оценки угроз информационной безопасности.
15. Государственные органы обеспечения информационной безопасности.
16. Применение основных нормативных правовых актов в области информационной безопасности и защиты информации, а также нормативных методических документов ФСБ России, ФСТЭК России в данной области.
17. Приоритетные направления и проблемы обеспечения информационной безопасности в условиях информационного общества.
18. Проблема стимулирования готовности и способности к активной состязательной деятельности при решении задач обеспечения информационной безопасности в условиях информационного противоборства.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Гультяева, Т.А. Основы информационной безопасности : учебное пособие : / Т.А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574729 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-7782-3640-0. – Текст : электронный.

4.2. Дополнительная литература

1. Горбенко, А.О. Основы информационной безопасности (введение в профессию) : учебное пособие / А.О. Горбенко. – Санкт-Петербург : ИЦ "Интермедия", 2017. – 336 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=482788 (дата обращения: 01.09.2021). – ISBN 978-5-4383-0136-3. – Текст : электронный.
2. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 105 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=362895 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-4475-3947-4. – DOI 10.23681/362895. – 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** ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	Свободный доступ

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 индивиду-

			альный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	www.consultant.ru	Российская компьютерная справочно-правовая система	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;
- Libre Office 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 компьютерных классах. Перечень основного оборудования: автоматизированные рабочие места с компьютерами, программное обеспечение общего и профессионального назначения.

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

Предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.