ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.12 Основы управления информационной безопасностью

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	**3,4**		
Семестр	**6,7**		

Лекции	**38**		
Лабораторные занятия	**38**		
Практические (семинарские) занятия	**28**		
в т. ч. практическая подготовка			
Форма(ы) промежуточной аттестации	**Зачет Экзамен - 0,3**		
Контроль	**9**		
Иные формы работы			
Самостоятельная работа	**138,7**		

Всего часов: 252
Трудоемкость: 7 зачетных единицы.
Разработчик(и) рабочей программы:
кандидат физико-математических наук, доцент С.А. Рощупкин

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

получение необходимых знаний о принципах и методах, инструментальных средств, нормативных документах регуляторах, позволяющих успешно управлять информационной безопасностью организации в условиях активного использования информационных технологий.

Задачи изучения дисциплины:

- ознакомление студентов с терминологией управления информационной безопасностью;
- изучение методов и средств обеспечения информационной безопасности;
- освоение навыков формирования требований к системе управления ИБ конкретного объекта.

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
УК-6	**Знать:** - свои ресурсы и их пределы (личностные, психофизиологические, ситуативные, временные и т.д.) для успешного выполнения порученной работы.	**Знает:** - критерии оценки систем и отдельных методов и средств защиты информации, пользоваться современной научно-технической информацией по исследуемым проблемам и задачам, а также в ходе научных исследований, выявлять угрозы и каналы утечки информации.
	Уметь: - планировать перспективные цели деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда; - критически оценивать эффективность использования времени и других ресурсов при решении поставленных задач, а также относительно полученного результата.	**Умеет:** - принимать управленческие решения в сфере защиты информации
	Владеть: - навыками реализации намеченной цели деятельности с учетом условий, средств, личностных возможностей, этапов карьерного роста, временной перспективы развития деятельности и требований рынка труда; - навыками использования предоставляемых возможностей для приобретения новых знаний и навыков.	**Владеет:** - навыками использования предоставляемых возможностей для управления информационной безопасностью.
ОПК-10	**Знать**:	**Знает:**

	- 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.	- методы и средства управления информационной безопасностью, а также основные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта;
	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:** - мотивированно выполнять профессиональную деятельность в области обеспечения информационной безопасности.
	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:** - правилами, методами, средствами, процедурами управления информационной безопасностью объекта.
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:** - терминологию, основные руководящие и регламентирующие документы в области управления информационной безопасности.
	Уметь: - проводить анализ исходных данных для проектирования подсистем передачи информации и	**Умеет:** - контролировать эффективность мер защиты, создавать необходимые

	средств обеспечения информационной безопасности; - проводить технико-экономический анализ и обоснование проектных решений, связанных с обеспечением информационной безопасности.	условия для использования программно-аппаратных средств обеспечения информационной безопасности современных информационных технологий,
	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:** - навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.

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	
6 семестр						
Раздел 1. «Теоретические основы информационной безопасности»		**108**	**18**	**18**	**18**	**54**
1	Тема 1. Базовые понятия. Общая схема процесса обеспечения безопасности. Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом	38	6	6	6	20
2	Тема 2. Защита от несанкционированного доступа. Модели безопасности. Модель Харрисона–Рузо–Ульмана Модель Белла–ЛаПадула	38	6	6	6	20
3	Тема 3. Ролевая модель безопасности Процесс построения и оценки системы обеспечения безопасности	38	6	6	6	14
	Форма отчетности	зачет				
	Зачет					
	Итого за 6 семестр	***108***	***18***	***18***	***18***	***54***
	в т.ч. практическая подготовка					
7 семестр						
Раздел 2. «Основы криптографии. Защита информации в сетях»		**66**	**10**	**6**	**10**	**40**

4	Тема 4. Основные понятия. Классификация шифров. Симметричные шифры. Схема Фейстеля.	16	2	2	2	10
5	Тема 5. Шифр DES. Шифр ГОСТ 28147-89. Шифр Blowfish. Управление криптографическими ключами для симметричных шифров	17	4	1	2	10
6	Тема 6. Асимметричные шифры. Основные понятия. Распределение ключей по схеме Диффи–Хеллмана. Криптографическая система RSA Криптографическая система Эль–Гамаля. Совместное использование симметричных и асимметричных шифров	17	2	1	4	10
7	Тема 7. Хэш-функции. Хэш-функции без ключа. Алгоритм SHA-14. Хэш-функции с ключом. Инфраструктура открытых ключей. Цифровые сертификаты. Протоколы защиты	16	2	2	2	10
Раздел 3. «Анализ и управление рисками в сфере информационной безопасности»		**68,7**	**10**	**4**	**10**	**44,7**
8	Тема 8. Введение в проблему. Управление рисками. Модель безопасности с полным перекрытием	21	2	1	2	16
9	Тема 9. Методики построения систем защиты информации. Методики и программные продукты для оценки рисков	25	4	1	4	16
10	Тема 10. Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель».	22,7	4	2	4	12,7
	Форма отчетности	*экзамен*				
	Контроль	**9**				
	Экзамен	**0,3**				
	Итого за 7 семестр	***144***	***20***	***10***	***20***	***84,7***
	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. Разработка модели угроз конкретного объекта.
2. Разработка модели нарушителя ИБ конкретного объекта.
3. Оценка рисков ИБ.

4. Разработка корпоративной методики анализа рисков.
5. Типовые процессы управления ИБ.
6. Разработка политики безопасности ИБ конкретного объекта.
7. Разработка плана проведения аудита ИБ конкретного объекта.
8. Аудит состояний информационной безопасности.
9. Управление информационной безопасностью на государственном уровне: Общие принципы и российская практика.
10. Построение системы управления информационной безопасностью (СУИБ).
11. Разработка документации СУИБ.
12. Внедрение и сопровождение комплексных систем СУИБ.
13. Поддержка разработанной СУИБ или отдельных процессов.

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

Вопросы к зачету
(6 семестр, очная форма обучения)

1. Понятие информационной безопасности. Объект защиты информации.
2. Основные составляющие информационной безопасности.
3. Управление информационной безопасностью.
4. Важность и сложность проблемы информационной безопасности.
5. Основные определения и критерии классификации угроз. Основные угрозы доступности.
6. Основные угрозы целостности. Основные угрозы конфиденциальности.
7. Вредительские программы.
8. Общая схема процесса обеспечения безопасности.
9. Идентификация, аутентификация, управление доступом.
10. Защита от несанкционированного доступа.
11. Модели безопасности.
12. Модель Харрисона–Рузо–Ульмана.
13. Модель Белла–ЛаПадула.
14. Ролевая модель безопасности.
15. Процесс построения и оценки системы обеспечения безопасности.
16. Стандарт ISO/IEC 15408.

Вопросы к зачету
(7 семестр, очная форма обучения)

1. Основные понятия. Классификация шифров.
2. Симметричные шифры.
3. Схема Фейстеля.
4. Шифр DES.
5. Шифр ГОСТ 28147-89.
6. Шифр Blowfish.
7. Управление криптографическими ключами для симметричных шифров.
8. Асимметричные шифры.
9. Основные понятия.
10. Распределение ключей по схеме Диффи–Хеллмана.
11. Криптографическая система RSA.

12. Криптографическая система Эль–Гамаля.
13. Совместное использование симметричных и асимметричных шифров.
14. Хэш-функции.
15. Хэш-функции без ключа.
16. Алгоритм SHA-14.
17. Хэш-функции с ключом.
18. Инфраструктура открытых ключей. Цифровые сертификаты.
19. Протокол защиты электронной почты S/MIME.
20. Протоколы SSL и TLS.
21. Протоколы IPSec и распределение ключей.
22. Межсетевые экраны.
23. Управление рисками. Модель безопасности с полным перекрытием.
24. Управление информационной безопасностью. Стандарты ISO/IEC 17799/27002 и 27001.
25. ГОСТ Р ИСО/МЭК 17799:2005 «Информационная технология. Практические правила управления информационной безопасностью».
26. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».
27. Методики построения систем защиты информации.
28. Методики и программные продукты для оценки рисков.
29. Модель Lifecycle Security.
30. Модель многоуровневой защиты.
31. Методика управления рисками, предлагаемая.
32. Майкрософт.
33. Методика CRAMM.
34. Методика FRAP.
35. Методика OCTAVE.
36. Методика RiskWatch.
37. Проведение оценки рисков в соответствии с методикой Майкрософт.
38. Анализ существующих подходов.
39. Выбор проекта системы обеспечения информационной безопасности.
40. Игровая модель конфликта «защитник-нарушитель».

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Шилов, А.К. Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ, Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=500065 (дата обращения: 01.09.2021). – Библиогр.: с. 81-82. – ISBN 978-5-9275-2742-7. – Текст : электронный.

4.2. Дополнительная литература

2. Абденов, А. Современные системы управления информационной безопасностью : учебное пособие : [16+] / А. Абденов, Г. Дронова, В. Трушин ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2017. – 48 с. : ил. – Режим доступа: по подписке. –

URL: https://biblioclub.ru/index.php?page=book&id=574594 (дата обращения: 01.09.2021). – Библиогр.: с.43-44. – ISBN 978-5-7782-3236-5. – Текст : электронный.

3. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Санкт-Петербургский государственный политехнический университет. – Санкт-Петербург : Издательство Политехнического университета, 2014. – 322 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=363040 (дата обращения: 01.09.2021). – ISBN 978-5-7422-4331-1. – 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 индивидуальный 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.