

# ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА



## **Б1.О.04.12 Основы управления информационной безопасностью**

**Направление подготовки:** 10.03.01 Информационная безопасность

**Направленность (профиль):** Безопасность компьютерных систем (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	28		
Лабораторные занятия	56		
Практические (семинарские) занятия	28		
в т. ч. практическая подготовка			
Форма(ы) промежуточной аттестации	Зачет (6 семестр) Экзамен - 0,3 (7 семестр)		
Контроль	9		
Иные формы работы			
Самостоятельная работа	238,7		

**Всего часов:** 360

**Трудоемкость:** 10 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 обязательной части блока Б1. Дисциплины (модули).

### Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-6	<b>Знать:</b> <ul style="list-style-type: none"><li>- основные нормативные правовые акты, технические стандарты и спецификации, нормативные методические документы ФСБ РФ и ФСТЭК РФ в сфере информационной безопасности;</li><li>- стандарты по лицензированию деятельности в области обеспечения технической защиты информации конфиденциального характера, по аттестации объектов информатизации и сертификации средств защиты информации.</li></ul>	<b>Знает:</b> <ul style="list-style-type: none"><li>- законодательные акты Российской Федерации, регулирующих вопросы защиты информации, требования к защите государственной тайны, инструкции и регламенты, изданные ФСБ и ФСТЭК;</li><li>- требований к получению лицензии на деятельность, связанную с защитой информации, процедуры аттестации информационных систем и сертификационных процессов для средств защиты информации согласно установленным стандартам.</li></ul>
	<b>Уметь:</b> <ul style="list-style-type: none"><li>- использовать нормативно-правовые документы, технические стандарты и спецификации, нормативные методические документы ФСБ РФ и ФСТЭК РФ в сфере информационной безопасности на конкретных объектах защиты;</li><li>- обоснованно выбирать и применять соответствующие конкретной ситуации стандарты по лицензированию деятельности в области обеспечения технической защиты информации конфиденциального характера, по аттестации автоматизированных систем.</li></ul>	<b>Умеет:</b> <ul style="list-style-type: none"><li>- применять нормы законодательства и рекомендации регуляторов для обеспечения соответствия информационных систем требованиям безопасности, правильно интерпретировать положения нормативных документов и адаптировать их под конкретные условия эксплуатации информационных систем;</li><li>- оценивать необходимость получения лицензии на выполнение работ по защите информации, проводить аттестацию систем обработки конфиденциальной информации, осуществлять выбор подходящих стандартов и</li></ul>

		методик для сертификации средств защиты информации.
	<b>Владеть:</b> - навыками проведения анализа информационной безопасности объектов и систем на соответствие требованиям нормативно-правовой базе, стандартам и спецификациям, нормативным методическим документам ФСБ РФ и ФСТЭК РФ в сфере информационной безопасности; - методами теоретического и экспериментального исследования при решении различных профессиональных задач с учетом основополагающих документов по лицензированию, стандартизации, сертификации.	<b>Владеет:</b> - навыками проведения аудитов и проверок информационных систем на предмет соблюдения установленных норм и стандартов, выявление нарушений и разработка предложений по устранению недостатков; - аналитическими подходами и экспериментальными методами для изучения проблем управления информационной безопасностью, оценивать соответствие систем и средств защиты предъявляемым требованиям.
ОПК-10	<b>Знать:</b> - 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.	<b>Знает:</b> - методы и средства управления информационной безопасностью, а также основные подходы к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта;
	<b>Уметь:</b> - 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.	<b>Умеет:</b> - мотивированно выполнять профессиональную деятельность в области обеспечения информационной безопасности.
	<b>Владеть:</b> - навыками планирования и организации системы защиты информации; - навыками реализации элементов политики информационной безопасности;	<b>Владеет:</b> - правилами, методами, средствами, процедурами управления информационной безопасностью объекта.

	- методами организации и управления деятельностью служб защиты информации на предприятии.	
ОПК-12	<b>Знать:</b> - 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.	<b>Знает:</b> - терминологию, основные руководящие и регламентирующие документы в области управления информационной безопасности.
	<b>Уметь:</b> - 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.	<b>Умеет:</b> - контролировать эффективность мер защиты, создавать необходимые условия для использования программно-аппаратных средств обеспечения информационной безопасности современных информационных технологий,
	<b>Владеть:</b> - 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.	<b>Владеет:</b> - навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем.
ОПК-1.1	<b>Знать:</b> - процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах.	<b>Знает:</b> - процесс разработки политики доступа, включающей идентификацию пользователей, аутентификацию, авторизацию и контроль прав доступа к ресурсам. Также необходимо знать механизмы реализации этих процедур в рамках корпоративных ИТ-систем.
	<b>Уметь:</b> - проводить процедуру формирования и выполнения комплекса мер по обеспечению управления доступом в компьютерных системах.	<b>Умеет:</b> - разрабатывать политику управления доступом, настраивать средства контроля доступа, осуществлять мониторинг и аудит действий пользователей, а также корректно реагировать

		на инциденты, связанные с нарушением правил доступа.
	<b>Владеть:</b> - практическим опытом планирования и применения комплекса мер по обеспечению управления доступом в компьютерных системах.	<b>Владеет:</b> - опытом внедрения и поддержки систем управления доступом, настройкой ролей и привилегий пользователей, применения технологий многофакторной аутентификации, а также управление жизненным циклом учетных записей сотрудников и внешних контрагентов.
ОПК-1.2	<b>Знать:</b> - принципы настройки и администрирования средств обеспечения информационной безопасности в компьютерных системах и сетях.	<b>Знает:</b> - архитектуру и функциональные возможности различных средств защиты информации, а также особенности их интеграции в инфраструктуру предприятия.
	<b>Уметь:</b> - выбирать алгоритмы работы средств обеспечения информационной безопасности в компьютерных системах и сетях.	<b>Умеет:</b> - оценивать различные сценарии угроз и подбирать оптимальные методы защиты, соответствующие специфике конкретной среды, включая выбор параметров и настроек средств защиты, обеспечивающих необходимый уровень безопасности.
	<b>Владеть:</b> - практическим опытом настройки и администрирования средств обеспечения информационной безопасности различных по своему характеру объектов защиты в компьютерных системах и сетях.	<b>Владеет:</b> - навыками конфигурирования и мониторинга средств защиты для разных типов объектов (серверы, рабочие станции, сетевое оборудование) с учётом особенностей каждого объекта, умение устранять возникающие проблемы и обеспечивать бесперебойную работу защитных механизмов.
ОПК-1.4	<b>Знать:</b> - процедуру анализа информационной безопасности компьютерных систем и сетей на соответствие требованиям стандартов.	<b>Знает:</b> - процедуру анализа информационной безопасности компьютерных систем и сетей на соответствие требованиям стандартов, методологии проведения аудита ИБ, а также принципов оценки рисков и уязвимостей.
	<b>Уметь:</b> - проводить процедуру анализа информационной безопасности компьютерных систем и сетей на соответствие требованиям стандартов.	<b>Умеет:</b> - планировать и организовывать аудит, собирать данные о текущем состоянии системы защиты информации, анализировать результаты проверок, выявлять несоответствия стандартам и предлагать меры для их устранения.

	<p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>- практическим опытом применения методов анализа информационной безопасности компьютерных систем и сетей на соответствие требованиям стандартов.</li> </ul>	<p><b>Владеет:</b></p> <ul style="list-style-type: none"> <li>- навыками использования специализированных инструментов для тестирования безопасности, документирования результатов проверки, подготовки отчетов и рекомендаций по улучшению уровня защищенности информационных ресурсов организации.</li> </ul>
--	---	---

## 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 ча- сов	Аудиторные заня- тия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
6 семестр						
Раздел 1. «Теоретические основы информационной безопасности»		216	18	18	36	54
1	Тема 1. Базовые понятия. Общая схема процесса обеспечения безопасности. Общая схема процесса обеспечения безопасности. Идентификация, аутентификация, управление доступом	72	6	6	12	48
2	Тема 2. Защита от несанкционированного доступа. Модели безопасности. Модель Харрисона–Рузо–Ульмана Модель Белла–ЛаПадула	72	6	6	12	48
3	Тема 3. Ролевая модель безопасности Процесс построения и оценки системы обеспечения безопасности	72	6	6	12	48
	Форма отчетности	зачет				
	Зачет					
	Итого за 6 семестр	216	18	18	36	144
	в т.ч. практическая подготовка					
7 семестр						
Раздел 2. «Основы криптографии. Защита информации в сетях»		61	5	6	10	40
4	Тема 4. Основные понятия. Классификация шифров. Симметричные шифры. Схема Фейстеля.	15	1	2	2	10
5	Тема 5. Шифр DES. Шифр ГОСТ 28147-89. Шифр Blowfish. Управление криптографическими ключами для симметричных шифров	14	1	1	2	10
6	Тема 6. Асимметричные шифры. Основные понятия. Распределение ключей по схеме Диффи–Хеллмана. Криптографическая система RSA	16	1	1	4	10

	Криптографическая система Эль–Гамала. Совместное использование симметричных и асимметричных шифров					
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
<b>Раздел 3. «Анализ и управление рисками в сфере информационной безопасности»</b>		<b>73,7</b>	<b>5</b>	<b>4</b>	<b>10</b>	<b>54,7</b>
8	Тема 8. Введение в проблему. Управление рисками. Модель безопасности с полным перекрытием	25	1	1	2	21
9	Тема 9. Методики построения систем защиты информации. Методики и программные продукты для оценки рисков	28	2	1	4	21
10	Тема 10. Выбор проекта системы обеспечения информационной безопасности. Игровая модель конфликта «защитник-нарушитель».	20,7	2	2	4	12,7
	<i>Форма отчетности</i>	<i>экзамен</i>				
	<i>Контроль</i>	<b>9</b>				
	<i>Экзамен</i>	<b>0,3</b>				
	<b>Итого за 7 семестр</b>	<b>144</b>	<b>10</b>	<b>10</b>	<b>20</b>	<b>94,7</b>
	в т.ч. практическая подготовка					
	<b>ИТОГО</b>	<b>360</b>	<b>28</b>	<b>28</b>	<b>56</b>	<b>238,7</b>

**Очно-заочная форма обучения не реализуется**

**Заочная форма обучения не реализуется**

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

Оценка освоения обучающимися содержания дисциплины (модуля) включает текущий контроль успеваемости и промежуточную аттестацию обучающихся.

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплин (модулей) и осуществляется с помощью следующих оценочных средств: контрольная работа.

#### **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 экзамену (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–Гамала.
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. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544029> (дата обращения: 18.04.2024).
2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/544290> (дата обращения: 18.04.2024).

### **4.2. Дополнительная 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: 18.04.2024). — Библиогр.: с. 81-82. — ISBN 978-5-9275-2742-7. — Текст : электронный.
2. Абденов, А. Современные системы управления информационной безопасностью : учебное пособие : / 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: 18.04.2024). – Библиогр.: с.43-44. – ISBN 978-5-7782-3236-5. – 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.	<a href="http://edu.ru/">http://edu.ru/</a>	<b>Российское образование: Федеральный портал. Включает</b> ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
2.	<a href="http://citforum.ru/database/osbd/contents.shtml">http://citforum.ru/database/osbd/contents.shtml</a>	Информационно-аналитические материалы	Свободный доступ

## VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	<a href="http://www.biblioclub.ru">http://www.biblioclub.ru</a>	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.	<a href="http://www.garant.ru">www.garant.ru</a>	Информационно-правовой портал	Свободный доступ
3.	<a href="http://www.elibrary.ru">www.elibrary.ru</a>	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	<a href="http://www.consultant.ru">www.consultant.ru</a>	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.