ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

«УТВЕРЖДАЮ»
Директор института цифровых технологий и математики
_____ С.А. Рощупкин

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.06 Технология построения защищенных автоматизированных систем

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: цифровых технологий и математики
Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	**очно-заочная форма**	**заочная форма**
Курс	**3**		
Семестр/триместр	**5,6**		

Лекции	**36**		
Лабораторные занятия	**54**		
Практические (семинарские) занятия	**54**		
в т.ч. практическая подготовка	**12**		
Форма(ы) промежуточной аттестации	**зачет, экзамен-0,3 КП-0,5**		
Контроль	**9**		
Иные формы работы	**1**		
Самостоятельная работа	**97,2**		

Всего часов: 252
Трудоемкость: 7 зачетных единиц.
Разработчик рабочей программы: к.п.н., доцент Щучка Т.А.

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

- формирование у студентов знаний основ технологии построения, проектирования и создания защищенных автоматизированных систем, а также навыков и умения в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач защиты информации с учетом требований системного подхода.

Задачи изучения дисциплины:

- концепции обеспечения информационной безопасности автоматизированных систем;
- технологии функционирования защищенной автоматизированной системы;
- методологии оценки защищенности автоматизированных систем;
- принципов построения защищенных информационных систем;
- методов и средств проектирования, создания и сопровождения защищенных автоматизированных систем;
- технологического цикла реализации защищенной системы обработки и хранения информации.

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:** - сущность и понятие информационной безопасности, характеристику ее составляющих, источники угроз и меры по их предотвращению; - методы и средства управления информационной безопасностью, а также основные подходы к разработке, реализации, эксплуатации, диагностике, анализу, сопровождению и совершенствованию систем защиты информации.	**Знает:** - сущность и определение информационной безопасности, характеристику её компонентов, источники угроз и способы их предотвращения; - методы и инструменты управления информационной безопасностью, включая ключевые подходы к созданию, внедрению, эксплуатации, диагностике, анализу, поддержке и улучшению систем защиты информации.
	Уметь: - оценивать защищенность, классифицировать основные угрозы, обеспечивать информационную безопасность компьютерных систем, применяя необходимые программно-аппаратные средства и системы защиты информации; - принимать управленческие и административные решения в сфере защиты информации.	**Умеет:** - обеспечивать информационную безопасность компьютерных систем посредством использования соответствующих программно-аппаратных средств и систем защиты информации; - принимать управленческие решения в области защиты информации.
	Владеть:	**Владеет:**

	- категориальным аппаратом в области обеспечения комплекса мер по администрированию и диагностике систем защиты информации; - правилами, методами, средствами, процедурами управления и администрирования информационной безопасностью объекта.	- категориальной базой для разработки и применения комплекса мер по управлению и диагностике систем защиты информации; - правилами, методами, инструментами, процессами управления и администрирования информационной безопасностью объекта.

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. Угрозы информационной безопасности в АС	**64**	**10**	**10**	**10**	**34**
1.	Тема 1. Особенности современных АС как объектов защиты; уязвимость основных структурно-функциональных узлов, распределенных АС	18	2	2	2	12
2.	Тема 2. Угрозы безопасности информации, АС и субъектов информационных отношений; источники угроз безопасности	24	4	4	4	12
3.	Тема 3. Классификация угроз безопасности; преднамеренные и непреднамеренные классификация каналов проникновения в систему и утечки информации; неформальная модель нарушителя, модель угроз по методике ФСТЭК.	22	4	4	4	10
	Раздел 2. Виды мер и основные принципы обеспечения информационной безопасности	**44**	**8**	**8**	**8**	**20**
4.	Тема 4. Морально-этические, технологические, организационные, меры физической защиты, технические; достоинства и недостатки мер защиты	22	4	4	4	10
5.	Тема 5. Основные принципы построения защиты ресурсов	22	4	4	4	10
	Зачет					
	Итого за 5 семестр	*108*	*18*	*18*	*18*	*54*
	в т.ч. практическая подготовка	6				
	Раздел 3. Организационная структура системы обеспечения информационной безопасности	**48**	**6**	**12**	**12**	**18**

6.	Тема 6. Понятие технологии обеспечения информационной безопасности. Цели создания системы обеспечения информационной безопасности; регламентация действий пользователей и обслуживающего персонала АС	16	2	4	4	6
7.	Тема 7. Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты; разовые мероприятия; мероприятия, проводимые по необходимости; служба безопасности	16	2	4	4	6
8.	Тема 8. Система организационно-распорядительных документов по организации комплексной системы защиты информации	16	2	4	4	6
	Раздел 4. Обязанности конечных пользователей и ответственных за ОИБ в подразделениях	**85,2**	**12**	**24**	**24**	**25,2**
9.	Тема 9. Обязанности ответственного за обеспечение безопасности информации в подразделении; администратор ИБ	14	2	4	4	4
10.	Тема 10. Порядок работы с носителями ключевой информации; обязанности исполнителя; действия при компрометации ключей; ответственность за нарушение	14	2	4	4	4
11.	Раздел 11. Документы, регламентирующие порядок изменения конфигурации аппаратно-программных средств АС	14	2	4	4	4
12.	Тема 12. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратных ресурсов АС	16	2	4	4	6
13.	Тема 13. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов АС	27,2	4	8	8	7,2
	Экзамен	*0,3*				
	Курсовой проект	*0,5*				
	Иные формы работы	*1*				
	Контроль	*9*				
	Итого за 6 семестр	*144*	*18*	*36*	*36*	*43,2*
	в т.ч. практическая подготовка	6				
	ИТОГО:	252	36	54	54	97,2

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, реферата.

Типовой вариант контрольной работы

1 Из каких элементов состоит трёхуровневая модель оценки защищенности автоматизированной системы системы?

2. Какими путями осуществляется стандартизация подходов к обеспечению информационной безопасности и какие международные стандарты для этого применяются?

3. Какие уровни реализуются в технологической модели подсистемы информационной безопасности АС?

4. С какой целью производится шифрование данных и информации и на каком уровне работы с информацией это применяется?

5. Что такое «единое информационное пространство»? Каковы его составляющие?

6. В каком случае возникает несовместимость вычислительных, информационных и телекоммуникационных устройств?

7. Как можно определить понятие «открытая информационная или программная система»?

Примерная тематика рефератов

1. Методы и алгоритмы шифрования данных;
2. Защита информации в автоматизированных системах;
3. Использование VPN для обеспечения безопасности сетей;
4. Антивирусные программы и их роль в защите автоматизированных систем;
5. Двухфакторная аутентификация: преимущества и недостатки;
6. Межсетевые экраны (фаерволы) в обеспечении безопасности автоматизированных систем;
7. Криптографические методы защиты информации;
8. Безопасность операционных систем и приложений;
9. Атаки на автоматизированные системы и методы их предотвращения;
10. Современные тенденции в области защиты автоматизированных систем.

Промежуточная аттестация обучающихся осуществляется в форме зачета, экзамена с использованием следующих оценочных материалов: вопросы к зачету, вопросов к экзамену.

Вопросы к зачету
(5 семестр, очная форма обучения)

1. Актуальность проблемы обеспечение безопасности автоматизированных информационных систем;
2. Особенности современных АС как объектов защиты;
3. Уязвимость основных структурно-функциональных узлов, распределенных АС; угрозы безопасности информации, АС и субъектов информационных отношений; источники угроз безопасности;
4. Классификация угроз безопасности;
5. Преднамеренные и непреднамеренные угрозы;
6. Классификация каналов проникновения в систему и утечки информации;
7. Неформальная модель нарушителя, модель угроз по методике ФСТЭК;
8. Морально-этические меры защиты информации;
9. Технологические меры защиты информации;
10. Организационные меры защиты информации;
11. Меры физической защиты;
12. Технические меры защиты информации;
13. Достоинства и недостатки мер защиты;
14. Основные принципы построения защиты ресурсов.

Вопросы к экзамену
(6 семестр, очная форма обучения)

1. Понятие технологии обеспечения информационной безопасности;
2. Цели создания системы обеспечения информационной безопасности;
3. Регламентация действий пользователей и обслуживающего персонала АС;
4. Основные организационные и организационно-технические мероприятия по созданию и обеспечению функционирования комплексной системы защиты;
5. Разовые мероприятия; мероприятия, проводимые по необходимости;
6. Служба безопасности;
7. Система организационно-распорядительных документов по организации комплексной системы защиты информации;
8. Обязанности ответственного за обеспечение безопасности информации в подразделении; администратор ИБ;
9. Порядок работы с носителями ключевой информации;
10. Обязанности исполнителя; действия при компрометации ключей;
11. Ответственность за нарушение;
12. Документы, регламентирующие порядок изменения конфигурации аппаратно-программных средств АС;
13. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратных ресурсов АС;
14. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов АС;

15. Идентификация и аутентификация пользователей;
16. Разграничение доступа зарегистрированных пользователей к ресурсам АС; списки полномочий субъектов; списки управления доступом к объекту; атрибутные схемы; регистрация и оперативное оповещение о событиях безопасности;
17. Криптографические методы защиты информации;
18. Криптографическое сокрытие хранимых и передаваемых по каналам связи данных;
19. Контроль целостности и аутентичности передаваемых данных;
20. Контроль целостности программных и информационных ресурсов.

Примерные темы курсового проекта
(6 семестр, очная форма обучения)

1. Разработка автоматизированной системы проверки почтовых сообщений;
2. Разработка защищенной системы хранения и конвертации документов в различные форматы;
3. Разработка интернет-ресурса профессиональных видеоинструкций;
4. Разработка автоматизированной системы формирования профилей абонентов для интернет-провайдеров;
5. Разработка защищенного облачного хранилища заданий студентов;
6. Разработка автоматизированной системы планирования бюджета;
7. Разработка автоматизированной системы контроля за пассажирским автотранспортом;
8. Разработка защищенной автоматизированной системы персональных контактов;
9. Разработка автоматизированной системы мониторинга состава транспортных средств;
10. Разработки системы продвижения сайтов на основе статистики поисковых запросов;
11. Разработка автоматизированной системы онлайн тестирование.

IV.ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — 2-е изд. — Москва : Издательство Юрайт, 2024. — 366 с. — (Высшее образование). — ISBN 978-5-534-15951-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/510320 (дата обращения: 18.04.2025).

4.2. Дополнительная литература

1. Проектирование информационных систем : учебник и практикум для вузов / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 273 с. — (Высшее образование). — ISBN 978-5-534-20361-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560485 (дата обращения: 18.04.2025).
2. Лаврищева, Е. М. Программная инженерия и технологии программирования сложных систем : учебник для вузов / Е. М. Лаврищева. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 432 с. — (Высшее образование). — ISBN 978-5-534-07604-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561885 (дата обращения: 18.04.2025).

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

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;
- 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 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.