ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.02.ДВ.01.02 Безопасность автоматизированных систем

Направление подготовки: *44.03.05 Педагогическое образование (с двумя профилями подготовки)*
Направленность (профиль): *Математика и информатика, Экономика*
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**		
Семестр/триместр	**6**		

Лекции	**16**		
Лабораторные занятия	**16**		
Практические (семинарские) занятия			
в т.ч. практическая подготовка	**2**		
Консультации			
Форма(ы) промежуточной аттестации	**зачет**		
Контроль			
Иные формы работы			
Самостоятельная работа	**40**		

Всего часов: 72

Трудоемкость: 2 **зачетных единиц.**

Разработчик(и) рабочей программы:
к.ф.-м. наук, доцент кафедры ММКТиИБ С.А. Рощупкин

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины: овладение знаниями и навыками комплексного подхода к обеспечению информационной безопасности автоматизированных систем, проблемами защиты информации и подходами к их решению.

Задачи изучения дисциплины:

• сформировать и обучить использовать теоретические и правовые вопросы защиты информации и обеспечения безопасности автоматизированных систем (АС);

• изучить принципы построения комплексных систем защиты АС;

• освоить основные направления деятельности служб технической защиты информации (подразделений обеспечения безопасности АС);

• сформировать навыки использования современных технологий обеспечения безопасности АС, предусматривающие рациональное распределение функций и организацию эффективного взаимодействия по вопросам защиты информации сотрудников всех подразделений, которые используют АС в процессе работы и гарантируют ее функционирование;

• изучить вопросы разработки нормативно-методических и организационно-распорядительных документов, необходимых для реализации технологии обеспечения безопасности АС;

• научиться разрабатывать защищенные АС.

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

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
УК-1	**Знать**: - методы поиска информации и работы с ней; - сущность системного подхода.	**Знает:** - основные методы поиска угроз безопасности информации и модели нарушителя в АС.
	Уметь: - анализировать задачу, выделять этапы ее решения, осуществлять действия по решению; - находить различные варианты решения задачи, оценивать их преимущества и риски.	**Умеет:** - анализировать и оценивать риски информационной безопасности.
	Владеть: - навыками оценивания практических последствий возможных вариантов решения задачи; - навыками грамотного, логичного, аргументированного формулирования собственных суждений и оценок.	**Владеет:** - навыками разработки системы организационно-распорядительных и нормативно методических документов по защите информации.
ПКС-2	**Знать:** - закономерности, принципы и уровни формирования и реализации содержания образования по дисциплинам Математика, Информатика, Экономика; - структуру, состав и дидактические	**Знает:** - АС как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;

	единицы содержания школьного предмета по дисциплинам Математика, Информатика, Экономика.	- содержание и порядок деятельности персонала по эксплуатации защищенных АС;
	Уметь: - осуществлять отбор учебного содержания для реализации в различных формах обучения дисциплин Математика, Информатика, Экономика в соответствии с дидактическими целями, возрастными особенностями обучающихся и требованиями ФГОС общего образования.	**Умеет:** - разрабатывать модели угроз и нарушителей в АС.
	Владеть: - предметным содержанием дисциплин Математика, Информатика, Экономика; - умениями отбора вариативного содержания с учетом взаимосвязи урочной и внеурочной форм обучения дисциплинам Математика, Информатика, Экономика.	**Владеет:** - профессиональной терминологией использования основных защитных механизмов подсистем безопасности АС.

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. Основы безопасности автоматизированных систем	**22**	**6**		**6**	**10**
1.	Тема 1. Актуальность проблемы обеспечения безопасности автоматизированных систем	4	1		1	2
2.	Тема 2. Основные понятия в области безопасности автоматизированных систем	4	1		1	2
3.	Тема 3. Угрозы безопасности автоматизированных систем	4	1		1	2
4.	Тема 4. Меры и основные принципы обеспечения безопасности автоматизированных систем	4	1		1	2
5.	Тема 5. Правовые основы обеспечения безопасности автоматизированных систем	3	1		1	1
6.	Тема 6. Государственная система защиты информации	3	1		1	1
	Раздел 2. Обеспечение безопасности автоматизированных систем	**18**	**4**		**4**	**10**
7.	Тема 7. Организационная структура системы обеспечения безопасности автоматизированных систем	3	0,5		0,5	2
8.	Тема 8. Обязанности пользователей и ответственных за	3	0,5		0,5	2

	обеспечение информационной безопасности в подразделениях					
9.	Тема 9. Регламентация работ по обеспечению безопасности автоматизированных систем	4	1		1	2
10.	Тема 10. Категорирование и документирование защищаемых ресурсов	4	1		1	2
11.	Тема 11. Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем автоматизированной системы	4	1		1	2
	Раздел 3. Средства защиты информации от несанкционированного доступа	**14**	**2**		**2**	**10**
12.	Тема 12. Назначение и возможности средств защиты информации от несанкционированного доступа	5	0,5		0,5	4
13.	Тема 13. Аппаратно-программные средства защиты информации от несанкционированного доступа	4	1		1	2
14.	Тема 14. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа	5	0,5		0,5	4
	Раздел 4. Обеспечение безопасности компьютерных сетей	**18**	**4**		**4**	**10**
15.	Тема 15. Проблемы обеспечения безопасности в компьютерных сетях	4	1		1	2
16.	Тема 16. Защита периметра корпоративной сети	4	1		1	2
17.	Тема 17. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности	5	1		1	3
18.	Тема 18. Мониторинг событий безопасности	5	1		1	3
	Контроль					
	Зачет					
	Итого за 6 семестр	*72*	*16*		*16*	*40*
	в т.ч. практическая подготовка	*2*			*2*	
	Итого:	**72**	**16**		**16**	**40**

Очно-заочная форма обучения *(не реализуется)*

Заочная форма обучения *(не реализуется)*

III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Текущая аттестация проводится в форме контрольной работы.

Типовые вопросы для контрольных работ

1. Охарактеризуйте место и роль автоматизированных систем в управлении бизнес-процессами.
2. Какие факторы определяют актуальность проблемы защиты АС в современных условиях?
3. Перечислите особенности современных автоматизированных систем как объектов защиты.

4. Назовите причины обострения проблемы обеспечения информационной безопасности.

5. Почему проблема обеспечения безопасности АС относится к числу трудноразрешимых?

6. Что понимается под риском информационной безопасности? Каковы составляющие риска?

7. В чем заключается анализ рисков и управление ими? Перечислите этапы анализа и управления.

8. Каковы требования к методам оценки целесообразности затрат на обеспечение безопасности АС?

9. Назовите категории затрат, связанных с безопасностью АС; кратко охарактеризуйте каждую категорию и перечислите статьи расходов для каждой из них.

10. Что понимается под безопасностью вообще и безопасностью АС в частности?

11. Дайте определение АС и безопасности АС.

12. Приведите определения информации и информационных ресурсов.

13. Перечислите категории субъектов информационных отношений.

14. Охарактеризуйте три свойства информации — конфиденциальность, целостность и доступность.

15. Сформулируйте цели защиты АС и циркулирующей в ней информации.

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

Вопросы к зачету
(6 семестр, очная форма обучения)

1. Дайте определение понятий «угроза», «уязвимость» и «атака».

2. Какие классификационные схемы угроз ИБ вам известны?

3. Перечислите источники угроз ИБ.

4. Назовите каналы проникновения в автоматизированную систему и утечки информации.

5. Какие факторы лежат в основе формирования модели нарушителя?

6. Каковы цели разработки моделей угроз и нарушителей?

7. В чем разница между нарушителем и злоумышленником?

8. Перечислите основные виды мер противодействия угрозам безопасности АС (контрмер).

9. Охарактеризуйте каждую меру противодействия.

10. Какая мера противодействия является, на ваш взгляд, наиболее важной, а какая — второстепенной?

11. Перечислите достоинства и недостатки различных мер защиты.

12. Возможно ли создание идеально надежной системы защиты?

13. Перечислите основные принципы построения систем защиты информации. Какие из них, по вашему мнению, являются важнейшими? Кратко охарактеризуйте каждый принцип.

14. Приведите классификацию информации по доступности с точки зрения Федерального закона «Об информации, информационных технологиях и о защите информации».

15. Дайте определения обладателя информации и оператора информационной системы.

16. Перечислите права и обязанности обладателя информации.

17. Дайте определение понятия «коммерческая тайна» в соответствии с Федеральным законом «О коммерческой тайне».

18. Какая информация не может быть отнесена к коммерческой тайне?

19. Каким нормативным актом утвержден Перечень сведений конфиденциального характера?

20. В каком кодексе предусмотрена ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)?

21. В каком кодексе предусмотрена ответственность за «незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»?

22. Какие статьи Уголовного кодекса РФ определяют ответственность за преступления в сфере компьютерной информации?

23. С какого возраста предусмотрена уголовная ответственность за преступления в сфере компьютерной информации?

24. В какой статье Уголовного кодекса РФ определяется ответственность за создание, использование и распространение вредоносных программ для ЭВМ ?

25. Что такое лицензирование?

26. Какие виды лицензирования вам известны?

27. Для кого аттестация АИС по требованиям безопасности информации ФСТЭК России является обязательной?

28. Когда проводится аттестация АИС по требованиям безопасности информации ФСТЭК России?

29. Перечислите классы защищенности СВТ в соответствии с руководящими документами ФСТЭК России.

30. Перечислите классы защищенности АС в соответствии с руководящими документами ФСТЭК России.

31. Какие подсистемы включает в себя комплекс программно-технических средств защиты информации от НСД в АС?

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие : / В. В. Бондарев. – 2-е изд. – Москва : МГТУ им. Н.Э. Баумана, 2018. – 252 с. : схем., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571750 – Библиогр.: с. 237-238. – ISBN 978-5-7038-4899-9. – Текст : электронный.

2. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум : практикум : / авт.-сост. М. А. Лапина, Д. М. Марков, Т. А. Гиш, М. В. Песков и др. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016. – 242 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=458012. – Библиогр. в кн. – Текст : электронный.

4.2. Дополнительная литература

1. Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации : учебное пособие / С. И. Козьминых ; Финансовый университет при Правительстве Российской Федерации. – Москва : Юнити, 2020. – 544 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=615695 – Библиогр. в кн. – ISBN 978-5-238-03200-9. – Текст : электронный.

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

№ п/п	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

№ п/п	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем индивидуальный неограниченный 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
3.	www.iprbookshop.ru	Электронно-библиотечная система (ЭБС)	Доступ возможен с любого компьютера сети ЕГУ или с домашних компьютеров после однократной саморегистрации с любого компьютера университета.

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.