

ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.02.ДВ.01.01 Методы и средства защиты компьютерной информации

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		
Форма(ы) промежуточной аттестации	зачет		
Контроль	-		
Иные формы работы	-		
Самостоятельная работа	40		

Всего часов: 72

Трудоемкость: 2 зачетных единицы

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

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

- формирование базовых знаний о современной структуре сетей и систем передачи информации, о задачах, методах и современных средствах проектирования, создания и эксплуатации сетевого аппаратного и программного обеспечения;
- обучение студентов приемам защиты информации в компьютерных системах и сетях;
- выработка навыков, необходимых для решения научных и практических задач, включая этапы постановки и решения задачи, а также выбора необходимых технических средств для создания сетей различного назначения и конфигурации.

Задачи изучения дисциплины:

- изучение научно-технической информации, отечественного и зарубежного опыта по компьютерным системам и сетям;
- изучение базовых правовых норм в области защиты информации;
- изучение угроз информационной безопасности (ИБ), изучение мер по противодействию угрозам ИБ.
- проведение измерений и наблюдений, составление описания проводимых исследований, подготовка данных для составления обзоров, отчетов и научных публикаций;
- составление отчета по выполненному заданию, участие во внедрении результатов исследований и разработок.

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
УК-1	Знать: - методы поиска информации и работы с ней; - сущность системного подхода.	Знает: - методы и средства поиска для защиты компьютерной информации.
	Уметь: - анализировать задачу, выделять этапы ее решения, осуществлять действия по решению; - находить различные варианты решения задачи, оценивать их преимущества и риски.	Умеет: -находить различные средства защиты компьютерной информации.
	Владеть: - навыками оценивания практических последствий возможных вариантов решения задачи; - навыками грамотного, логичного, аргументированного формулирования собственных суждений и оценок.	Владеет: - навыками защиты компьютерной информации
ПКС-2	Знать: - закономерности, принципы и уровни формирования и реализации содержания образования по дисциплинам Математика, Информатика, Экономика; - структуру, состав и дидактические единицы содержания школьного предмета по дисциплинам Математика, Информатика, Экономика.	Знает: - задачи, методы и современные средства проектирования, создания и эксплуатации сетевого аппаратного и программного обеспечения.

	<p>Уметь:</p> <ul style="list-style-type: none"> - 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. 	<p>Умеет:</p> <ul style="list-style-type: none"> - использовать приемы защиты информации в компьютерных системах и сетях.
	<p>Владеть:</p> <ul style="list-style-type: none"> - предметным содержанием дисциплин Математика, Информатика, Экономика; - умениями отбора вариативного содержания с учетом взаимосвязи урочной и внеурочной форм обучения дисциплинам Математика, Информатика, Экономика. 	<p>Владеет:</p> <ul style="list-style-type: none"> - навыками, необходимыми для решения научных и практических задач, включая этапы постановки и решения задачи, а также выбора необходимых технических средств для создания сетей различного назначения и конфигурации.

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. Право в области ИБ. Утечка информации.						
1	Тема 1. Понятие интеллектуальной собственности. Предпринимательская деятельность в условиях рыночной экономики.	4	1		1	2
2	Тема 2. Необходимость защиты информации в современном мире.	4	1		1	2
3	Тема 3. Авторское право. Охрана авторского права государством.	4	1		1	2
4	Тема 4. Законодательство, регулирующее защиту информации.	4	1		1	2
5	Тема 5. Принципы политики безопасности. Виды политики безопасности. Уровни политики безопасности. Стратегии безопасности.	4	1		1	2
6	Тема 6. Роли и обязанности должностных лиц по разработке и внедрению политики безопасности.	4	1		1	2
7	Тема 7. Каналы утечки информации.	4	1		1	2
8	Тема 8. Защита информационных систем системами криптографии данных.	4	1		1	2
Раздел 2. Средства защиты информации						
9	Тема 9. Программные средства защиты. Объекты и назначение программной защиты.	4	1		1	2
10	Тема 10. Подходы к выбору средств защиты.	4	1		1	2
11	Тема 11. Программные средства защиты и борьбы с	4	1		1	2

	пиратством.					
12	Тема 12. Ограничение доступа к компьютеру и операционной системе.	4	1		1	2
13	Тема 13. Технические средства борьбы с промышленным шпионажем.	4	1		1	2
14	Тема 14. Программная защита интеллектуальной собственности. Ролевое управление доступом в коммерческом банке.	4	1		1	2
15	Тема 15. Применение программных продуктов для защиты интеллектуальной собственности. Примеры программных продуктов.	4	1		1	2
16	Тема 16. Хакерские атаки и методы защиты от них.	12	1		1	10
	<i>Зачет</i>					
	в т. ч. практическая подготовка				2	
	ИТОГО:	72	16		16	40

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

Вариант 1. Разработать план-отчет по организационным мерам обеспечения информационной безопасности в сети учебного заведения.

Вариант 2. Разработать приблизительный план-отчет по реализации технических мер защиты информации в конструкторском бюро промышленного предприятия с учетом наличия коммерческой тайны.

Вариант 3. Описать на примерах наиболее распространенные атаки, связанные с социальным инжинирингом.

Примерная тематика рефератов

1. Интеллектуальная собственность в условиях рыночной экономики.
2. Предпринимательская деятельность в условиях рыночной экономики.
3. Маркетинг инновационных разработок.
4. Вложение средств в исследования для завоевания рынков сбыта.
5. Теория и практика рыночной экономики.
6. Теория и практика сетевой экономики.
7. Теория и практика охраны авторского права законами государства.
8. Обеспечение информационной безопасности на предприятии.
9. Каналы утечки информации на предприятии.
10. Современный промышленный шпионаж.
11. Средства борьбы с промышленным шпионажем.
12. Организация программной защиты.
13. Программная организация доступа.
14. Ролевое управление доступом.

15. Системы криптографии данных.

Промежуточная аттестация обучающихся осуществляется в форме зачета с использованием следующих оценочных материалов: перечень вопросов.

Вопросы к зачету

1. Нормативно-правовая база функционирования систем защиты информации.
2. Компьютерные преступления и особенности их расследования.
3. Промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.
4. Криптографические модели.
5. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации.
6. Режим простой замены.
7. Режим гаммирования.
8. Режим гаммирования с обратной связью.
9. Режим выработки имитовставки.
10. Блочные и поточные шифры.
11. Методы генерации псевдослучайных последовательностей чисел.
12. Стандартные алгоритмы шифрования.
13. Основные понятия и определения.
14. Шифры перестановки.
15. Шифрующие таблицы.
16. Применение магических квадратов.
17. Концепция криптосистемы с открытым ключом.
18. Криптосистема шифрования данных RSA.
19. Безопасность и быстродействие криптосистемы RSA.
20. Изучение американского стандарта шифрования данных DES.
21. Основные режимы работы алгоритма DES.
22. Отечественный стандарт шифрования данных.
23. Классификация способов защиты информации в компьютерных сетях.
24. Понятие разрушающего программного воздействия.
25. Модели взаимодействия прикладной программы и программной закладки.
26. Методы перехвата и навязывания информации.
27. Методы внедрения программных закладок.
28. Компьютерные вирусы как особый класс разрушающих программных воздействий.
29. Защита от разрушающих программных воздействий.
30. Антивирусная защита в сетях.
31. Понятие изолированной программной среды.
32. Рекомендации по защите информации в Internet.
33. Программная защита при передаче данных.
34. Программная защита интеллектуальной собственности.
35. Современные программные продукты для поддержки предпринимательской деятельности.
36. Сетевые программные продукты для мониторинга предпринимательской деятельности.
37. Сетевой мониторинг инновационных проектов на федеральном уровне.
38. Электронная подпись.
39. Обнаружение хакерских атак.
40. Использование защит для отражения хакерских атак.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. *Зенков, А.В.* Информационная безопасность и защита информации: учебное пособие для вузов / А.В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/477968> (дата обращения: 01.09.2022).
2. *Запечников, С.В.* Криптографические методы защиты информации: учебник для вузов / С.В. Запечников, О.В. Казарин, А.А. Тарасов. — Москва : Издательство Юрайт, 2021. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/468902> (дата обращения: 01.09.2022).

4.2. Дополнительная литература

1. *Белов, Е.Б.* Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва : Горячая линия — Телеком, 2006.
2. *Кабанов, А.С.* Основы информационной безопасности / А. С. Кабанов, А. Б. Лось, В. И. Тунцев. — Москва : РИО МИЭМ, 2012.
3. Основы организационного обеспечения информационной безопасности объектов информатизации : учебное пособие / С. Н. Сёмкин, Э. В. Беяков, С. В. Гребнев, В. И. Козачок. — Москва : Гелиос АРВ, 2005.
4. *Ярочкин, В.И.* Информационная безопасность : учебник для вузов / В. И. Ярочкин. — 4-е изд. — Москва : Академический проект, 2008.

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

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	https://infourok.ru/	Инфоурок: образовательный интернет-проект России. Включает: конспекты уроков, презентации, тесты, видеоуроки и другие материалы по предметам школьной программы.	Свободный доступ
2.	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.	
3.	https://docs.microsoft.com/ru-ru/learn/	Виртуальная академия Microsoft	
4.	https://cisco.com/	Портал CISCO	
5.	http://www.ict.edu.ru	Федеральный образовательный портал "Информационно-коммуникационные технологии в образовании"	

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	https://urait.ru/	Образовательная платформа Юрайт — образовательный ресурс, электронная библиотека и интернет-магазин, где читают и покупают электронные и печатные учебники авторов — преподавателей ведущих университетов для всех уровней профессионального образования, а также пользуются видео- и аудиоматериалами, тестированием и сервисами для преподавателей, доступными 24 часа 7 дней в неделю.	
3	www.garant.ru	Информационно-правовой портал	Свободный доступ
4	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	
5	www.consultant.ru	Российская компьютерная справочно-правовая система	

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- LibreOffice;
- Google Chrome / Mozilla Firefox
- VurtualBox
- IPython 6.0 / JupyterLab.

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.