ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.04.08 Защита информации в компьютерных системах и сетях

Направление подготовки: 01.03.02 Прикладная математика и информатика
Направленность (профиль): Моделирование и цифровизация социально-экономических систем
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	**1**		
Семестр/триместр	**1,2**		

Лекции	**54**		
Лабораторные занятия	**72**		
Практические (семинарские) занятия	**72**		
в т. ч. практическая подготовка	**-**		
Форма(ы) промежуточной аттестации	**Экзамен-0,3 Экзамен – 0.3**		
Контроль	**18**		
Иные формы работы			
Самостоятельная работа	**143,4**		

Всего часов: 360
Трудоемкость: 10 зачетных единиц.

Разработчик(и) рабочей программы:
Петров А.А., к.т.н., доцент кафедры ММКТиИБ

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 угорозам 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 обязательной части блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-4	Знать: – принципы работы современных информационных технологий и способы их использования для решения задач профессиональной деятельности;	**Знает:** - меры для защиты информации, контроля их эффективности; - современное ПО для контроля безопасности и формирования корпоративной политики в области защиты внутренних данных.
	Уметь: – обоснованно выбирать современные информационные технологии и использовать их для решения задач профессиональной деятельности;	**Умеет:** - производить тестирование периметра для качественной оценки степени защиты информации в корпоративных системах; - использовать бесплатное и проприетарное ПО для защиты

		информации; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.
	Владеть: – обоснованно выбирать современные информационные технологии и использовать их для решения задач профессиональной деятельности.	**Владеет:** - способами оценки защищенности помещений от утечки информации, навыками разработки мероприятий по защите информации от утечки.

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.	**170,7**	**36**	**36**	**36**	**62,7**
1	Тема 1. Понятие интеллектуальной собственности. Предпринимательская деятельность в условиях рыночной экономики.	20	4	4	4	8
2	Тема 2. Необходимость защиты информации в современном мире.	20	4	4	4	8
3	Тема 3. Авторское право. Охрана авторского права государством.	20	4	4	4	8
4	Тема 4. Законодательство, регулирующее защиту информации.	20	4	4	4	8
5	Тема 5. Принципы политики безопасности. (Виды политики безопасности. Уровни политики безопасности. Стратегии безопасности).	20	4	4	4	8
6	Тема 6. Роли и обязанности должностных лиц по	20	4	4	4	8

	разработке и внедрению политики безопасности.					
7	Тема 7. Каналы утечки информации.	26	6	6	6	8
8	Тема 8. Защита информационных систем системами криптографии данных.	26,7	6	6	6	6,7
	Экзамен	*0,3*				
	Контроль	*9*				
	Итого за 1 семестр	*180*	*36*	*36*	*36*	*62,7*
	Раздел 2. Средства защиты информации	**80**	**18**	**36**	**36**	**80,7**
9	Тема 9. Программные средства защиты. Объекты и назначение программной защиты.	20	2	4	4	10
10	Тема 10. Подходы к выбору средств защиты.	20	2	4	4	10
11	Тема 11. Программные средства защиты и борьбы с пиратством.	20	2	4	4	10
12	Тема 12. Ограничение доступа к компьютеру и операционной системе.	20	2	4	4	10
13	Тема 13. Технические средства борьбы с промышленным шпионажем.	20	2	4	4	10
14	Тема 14. Программная защита интеллектуальной собственности. Ролевое управление доступом в коммерческом банке.	20	2	4	4	10
15	Тема 15. Применение программных продуктов для защиты интеллектуальной собственности. Примеры программных продуктов.	21	3	6	6	10
16	Тема 16. Хакерские атаки и методы защиты от них.	21,7	3	6	6	10,7
	Экзамен	*0,3*				
	Контроль	*9*				
	Итого за 2 семестр	*180*	*18*	*36*	*36*	*80,7*
	в т. ч. практическая подготовка	-				
	ИТОГО:	**360**	**54**	**72**	**72**	**143,4**

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 экзаменов с использованием следующих оценочных материалов: перечень вопросов к экзамену.

Вопросы к зачету экзамену
(1 семестр, очная форма обучения)

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.

Вопросы к экзамену
(2 семестр, очная форма обучения)

1. Классификация способов защиты информации в компьютерных сетях.
2. Понятие разрушающего программного воздействия.
3. Модели взаимодействия прикладной программы и программной закладки.
4. Методы перехвата и навязывания информации.
5. Методы внедрения программных закладок.
6. Компьютерные вирусы как особый класс разрушающих программных воздействий.
7. Защита от разрушающих программных воздействий.
8. Антивирусная защита в сетях.
9. Понятие изолированной программной среды.
10. Рекомендации по защите информации в Internet.
11. Программная защита при передаче данных.
12. Программная защита интеллектуальной собственности.
13. Современные программные продукты для поддержки предпринимательской деятельности.

14. Сетевые программные продукты для мониторинга предпринимательской деятельности.
15. Сетевой мониторинг инновационных проектов на федеральном уровне.
16. Электронная подпись.
17. Обнаружение хакерских атак.
18. 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: 01.09.2021).

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: 01.09.2021).

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. Беляков, 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,	Свободный доступ

		видеоуроки и другие материалы по предметам школьной программы.	
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.	Свободный доступ
3.	https://docs.microsoft.com/ru-ru/learn/	Виртуальная академия Microsoft	Свободный доступ
4.	https://cisco.com/	Портал CISCO	Свободный доступ
5.	http://www.ict.edu.ru	Федеральный образовательный портал "Информационно-коммуникационные технологии в образовании"	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.	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.	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет

3	www.garant.ru	Информационно-правовой портал	Свободный доступ
4	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
5	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;
- Oracle VirtualBox;
- 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.