ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.04.08 Информационная безопасность и защита информации

Направление подготовки: 09.03.02 Информационные системы и технологии
Направленность (профиль): Информационные технологии в технических системах
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	**5,6**		

Лекции	**36**		
Лабораторные занятия	**36**		
Практические (семинарские) занятия	**18**		
в т. ч. практическая подготовка	**-**		
Консультации	**-**		
Форма(ы) промежуточной аттестации	**Зачет** **Экзамен -0,3**		
Контроль	**9**		
Иные формы работы	**-**		
Самостоятельная работа	**188,7**		

Всего часов: 288
Трудоемкость: 8 зачетных единиц.

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

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины: предоставление обучаемым знаний основных типов и способов защиты информации; приобретение студентами умения проектировать системы защиты информации; овладение современными программными и аппаратными средствами защиты информации.

Задачи изучения дисциплины:

- обеспечение информационной безопасности в современных условиях и основные факторы, влияющие на ее защиту;
- определение взаимосвязи национальных интересов и национальной безопасности;
- проведение анализа форм и методов ведения информационной войны;
- определение геополитической стратегии Российской Федерации в сфере информационной безопасности.

Место дисциплины в структуре ОПОП: реализуется в рамках базовой (обязательной) части блока Б1. Дисциплины (модули)

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-3	**Знать:** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	**Знает:** методы и средства обеспечения информационной безопасности в современных условиях и основные факторы, влияющие на ее защиту.
	Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	**Умеет:** применять методы и средства обеспечения целостности данных.
	Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	**Владеет:** анализом возможностей реализации требований к программному обеспечению; навыками осуществления защиты информации.

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	
5 семестр						
	Раздел 1. «История вопроса и состояние проблемы»	**28**	**2**		**2**	**24**
1.	Тема 1. «История вопроса»	14	1		1	12
2.	Тема 2. «Состояние проблемы»	14	1		1	12
	Раздел 2. «Основы информационной безопасности»	**116**	**16**		**16**	**84**
3.	Тема 1. «Сущностные основы теории информационной безопасности»	36	4		4	28
4.	Тема 2. «Типология информационной безопасности»	36	4		4	28
5.	Тема 3. «Принципы, законы, право и психология информационной безопасности»	44	8		8	28
	Зачет					
	Итого за 5 семестр	*144*	*18*		*18*	*108*
	в т.ч. практическая подготовка					
6 семестр						
	Раздел 3. «Теория информационной безопасности и национальной стратегии России»	**84,7**	**12**	**12**	**12**	**48,7**
6.	Тема 1. «О национальной стратегии информационной безопасности России»	23	2	2	2	17
7.	Тема 2. «Основы национальной стратеги России»	35	6	6	6	17
8.	Тема 3. «Государство, информационная безопасность и информационные технологии: основные тенденции»	26,7	4	4	4	14,7
	Раздел 4. «Государство и геополитическая стратегия»	**50**	**6**	**6**	**6**	**32**
9.	Тема 1. «Информационная безопасность и общество»	22	2	2	2	16
10.	Тема 2. «Геополитическая стратегия России в сфере информационной безопасности»	28	4	4	4	16
	Экзамен	*0,3*				
	Контроль	*9*				
	Итого за 6 семестр	*144*	*18*	*18*	*18*	*80,7*
	в т.ч. практическая подготовка					
	ИТОГО:	**288**	**36**	**18**	**36**	**188,7**

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 теста.

Перечень заданий для проведения тестирования

Информация, не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. **конфиденциальная информация**

Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это…

1. **комплексное обеспечение ИБ**
2. безопасность АС
3. угроза ИБ
4. атака на АС
5. политика безопасности

Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:

1. компаньон - вирусами
2. **черви**
3. паразитические
4. студенческие
5. призраки
6. стелс - вирусы
7. макровирусы

Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ….

1. идентификатор пользователя
2. **пароль пользователя**
3. учетная запись пользователя
4. парольная система

К принципам информационной безопасности относятся

1. скрытость
2. масштабность
3. **системность**
4. **законность**
5. **открытости алгоритмов**

Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

1. Защита информации
2. **Компьютерная безопасность**
3. Защищенность информации
4. Безопасность данных

Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:
1. конфиденциальность
2. **целостность**
3. доступность
4. аутентичность
5. аппелеруемость

Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной сети от заданного множества угроз безопасности:
1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. атака на автоматизированную систему
5. **политика безопасности**

К функциям информационной безопасности относятся:
1. **совершенствование законодательства РФ в сфере обеспечения информационной безопасности**
2. **выявление источников внутренних и внешних угроз**
3. **Страхование информационных ресурсов**
4. **защита государственных информационных ресурсов**
5. **подготовка специалистов по обеспечению информационной безопасности**

К типам угроз безопасности парольных систем относятся
1. словарная атака
2. тотальный перебор
3. атака на основе психологии
4. разглашение параметров учетной записи
5. **все варианты ответа верны**

Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти, и поиске в них известных и новых вирусов называется:
1. ревизором
2. иммунизатором
3. **сканером**
4. доктора и фаги

В соответствии с особенностями алгоритма вирусы можно разделить на два класса:
1. вирусы, изменяющие среду обитания, но не распространяющиеся
2. **вирусы, изменяющие среду обитания при распространении**
3. **вирусы, не изменяющие среду обитания при распространении**
4. вирусы, не изменяющие среду обитания и не способные к распространению в дальнейшем

К достоинствам технических средств защиты относятся:
1. регулярный контроль

2. **создание комплексных систем защиты**
3. степень сложности устройства
4. Все варианты верны

Информационная безопасность это:

1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
2. **Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз**
3. Состояние, когда не угрожает опасность информационным системам
4. Политика национальной безопасности России

Наиболее распространенные угрозы информационной безопасности:

1. **угрозы целостности**
2. угрозы защищенности
3. угрозы безопасности
4. **угрозы доступности**
5. **угрозы конфиденциальности**

Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:

1. **конфиденциальность**
2. доступность
3. аутентичность
4. целостность

Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:

1. защита информации от непреднамеренного воздействия
2. защита информации от несанкционированного воздействия
3. защита информации от несанкционированного доступа
4. **защита от утечки информации**

Идентификатор субъекта доступа, который является его секретом:

1. **пароль**
2. ключ
3. электронно-цифровая подпись
4. сертификат ключа подписи

Исследование возможности расшифрования информации без знания ключей:

1. криптология
2. **криптоанализ**
3. взлом
4. несанкционированный доступ

Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:

1. **Информационная безопасность**
2. Безопасность
3. Национальная безопасность

4. Защита информации

Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости компьютерной сети.

1. Комплексное обеспечение информационной безопасности
2. Безопасность компьютерной сети
3. Угроза информационной безопасности
4. **Атака на компьютерную сеть**
5. Политика безопасности

К какому уровню доступа информации относится следующая информация: «Информация, содержащая сведения об обстоятельствах и фактах, предоставляющих угрозу жизни, здоровью граждан …»

1. **Информация без ограничения права доступа**
2. Информация с ограниченным доступом
3. Информация, распространение которой наносит вред интересам общества
4. Объект интеллектуальной собственности
5. Иная общедоступная информация

Свойство данных быть доступными для санкционированного пользования в произвольный момент времени, когда в обращении к ним возникает необходимость:

1. Конфиденциальность
2. Целостность
3. **Доступность**
4. Аутентичность
5. Аппелируемость

Гарантия неразглашения банковского счета, операций по счету и сведений о клиенте:

1. Государственная тайна
2. Коммерческая тайна
3. **Банковская тайна**
4. Конфиденциальная информация

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

Вопросы к зачету
(5 семестр, очная форма обучения)

1. Понятия информация, информатизация, информационная система, информационная безопасность.
2. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.
3. Защита информации, тайна, средства защиты информации.
4. Международные стандарты информационного обмена.
5. Показатели информации: важность, полнота, адекватность, релевантность, толерантность.
6. Требования к защите информации.
7. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
8. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

9. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
10. Доктрина информационной безопасности Российской Федерации.
11. Структура государственной системы информационной безопасности.
12. Структура законодательной базы по вопросам информационной безопасности.
13. Лицензирование и сертификация в области защиты информации.
14. Место информационной безопасности экономических систем в национальной безопасности страны.
15. Концепция информационной безопасности.
16. Понятие угрозы.
17. Виды противников или «нарушителей».
18. Классификация угроз информационной безопасности.
19. Виды угроз.
20. Основные нарушения.
21. Характер происхождения угроз (умышленные и естественные факторы).
22. Источники угроз.
23. Предпосылки появления угроз. Классы каналов несанкционированного получения информации.
24. Причины нарушения целостности информации.
25. Основные положения теории информационной безопасности информационных систем

Вопросы к экзамену
(6 семестр, очная форма обучения)

1. Формальные модели безопасности.
2. Дискреционная модель Харрисона-Руззо-Ульмана.
3. Типизированная матрица доступа.
4. Модель распространения прав доступа Take-Grant.
5. Мандатная модель Белла-ЛаПадулы.
6. Ролевая политика безопасности.
7. Ограничения на области применения формальных моделей.
8. Методы криптографии.
9. Симметричное и асимметричное шифрование.
10. Электронно-цифровая подпись.
11. Алгоритмы электронно-цифровой подписи.
12. Хеширование.
13. Имитовставки.
14. Криптографические генераторы случайных чисел.
15. Способы распространения ключей.
16. Обеспечиваемая шифром степень защиты.
17. Криптоанализ и атаки на криптосистемы.
18. Сжатие информации.
19. Межсетевые экраны.
20. Проектирование МЭ.
21. Снифферы.
22. Эксплоиты.
23. Атаки на сервера.
24. Атаки на рабочие станции.
25. Атака типа «отказ в обслуживании».
26. Протоколирование.
27. Сетевые защищенные протоколы.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1 Основная литература

1. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485. – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.

4.2 Дополнительная литература

1. Ковалев, Д.В. Информационная безопасность: учебное пособие / Д.В. Ковалев, Е.А. Богданова; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону: Издательство Южного федерального университета, 2016. - 74 с.: схем., табл., ил. - Библиогр. в кн. - ISBN 978-5-9275-2364-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493175.

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;
- LibreOffice 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.

Предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.