ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.01.01 ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

Направление подготовки: *10.03.01 Информационная безопасность*
Направленность (профиль): *Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)*
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**		

Лекции	**36**		
Лабораторные занятия	**36**		
Практические (семинарские) занятия	**36**		
в т. ч. практическая подготовка	**4**		
Консультации	**-**		
Форма(ы) промежуточной аттестации	**Экзамен - 0,3**		
Контроль	**9**		
Иные формы работы	**-**		
Самостоятельная работа	**98,7**		

Всего часов: 216
Трудоемкость: 6 зачетные единицы.
Разработчик(и) рабочей программы:
кандидат физико-математических наук, доцент *С.А. Рощупкин*

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

- формирование у обучаемых знаний в области теоретических основ информационной безопасности;
- формирование навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

Задачи изучения дисциплины:

- освоение технологий диагностики опасностей и угроз для информационных систем и методов работы с моделями безопасности;
- изучение основных типов угроз и способы парирования таких угроз: каналы утечки информации, компьютерные вирусы, закладки, атаки на информационные системы, имеющие доступ к глобальным телекоммуникациям (несанкционированный доступ с применением сетевых технологий)
- разъяснение значения закрытия информации, как важного средства сохранения ее целостности и недоступности для несанкционированного доступа к ней, применения брандмауэров и выявления слабых мест информационных систем с целью их устранения

Место дисциплины в структуре ОПОП: реализуется в рамках вариативной части 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: – основы информационной безопасности и защиты информации; основные понятия, связанные с хранением и обработкой данных; типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа
	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: – проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем
	Владеть: - категориальным аппаратом в области обеспечения комплекса мер по админи-	Владеет: – правилами, методами и средствами по обеспечению на пред-

	стрированию и диагностике систем защиты информации; - правилами, методами, средствами, процедурами управления и администрирования информационной безопасностью объекта.	приятии (в организации) деятельности в области защиты информации
ПКС-2	Знать: - основные виды и классификацию информационных ресурсов организации (предприятия); - сущность профессиональной деятельности по обеспечению защиты информации в процессе эксплуатации автоматизированных систем.	Знает: – о социальной значимости своей будущей профессии при выполнении профессиональной деятельности в области обеспечения информационной безопасности, законодательство РФ о государственной гражданской службе
	Уметь: - выделять из общих информационных ресурсов предприятия информацию, подлежащую защите; - строить модели защиты информации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем.	Умеет: – ориентироваться в законодательстве РФ о государственной гражданской службе, нормативных-правовых актах в области информационной безопасности
	Владеть: - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем: - навыками реализации моделей защиты информации на основе анализа структуры и содержания информационных процессов и особенностей эксплуатации автоматизированных систем.	Владеет: – навыками анализа эффективности профессиональной деятельности в области обеспечения информационной безопасности

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. Введение в информационную безопасность	**96**	**18**	**18**	**18**	**42**
1	Тема 1. Угрозы информационной безопасности и их классификация.	32	6	6	6	14
2	Тема 2. Законодательный уровень обеспечения информационной безопасности	32	6	6	6	14
3	Тема 3. Стандарты и технические спецификации в	32	6	6	6	14

	области информационной безопасности					
	Раздел 2. Административный уровень обеспечения ИБ	**110,7**	**18**	**18**	**18**	**58,7**
4	Тема 4. Процедурный и Программно-технический уровни обеспечения ИБ.	38	6	6	6	20
5	Тема 5. Сеть Фейстеля. Криптоанализ.	36	6	6	6	18
6	Тема 6. Вредоносное ПО и защита от него	36,7	6	6	6	18,7
	Экзамен	0,3				
	Контроль	9				
	Итого за 1 семестр	216	36	36	36	98,7
	в т.ч. практическая подготовка	4		2	2	
	ИТОГО:	**216**	**36**	**36**	**36**	**98,7**

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 в виде теста, реферата.

Типовая контрольная работа

Вопрос № 1
Как расшифровывается аббревиатура ФСТЭК России?

Федеральная служба по экспортному и техническому контролю
Федеральная специальная техническая комиссия экспертов
Федеральный совет технических экспертов криминалистов
Федеральная служба технико-экологического контроля

Вопрос № 2
В каком случае ФСТЭК России не осуществляет функциональное регулирование деятельности по обеспечению защиты информации?

В случае если применяются криптографические методы защиты информации
В случае если не применяются криптографические методы защиты информации
В любом случае
Никогда не является

Вопрос № 3
Какой орган исполнительной власти осуществляет экспортный контроль?

ФСТЭК России
ФСБ России

МВД России
МИД России

Вопрос № 4
В задачи какого органа исполнительной власти входит осуществление государственной научно-технической политики в области защиты информации?

ФНС России
МВД России
Прокуратура РФ
ФСТЭК России

Вопрос № 5
Что не является задачей ФСТЭК России?

Реализация государственной политики и организация межведомственного взаимодействия в области экспортного контроля?
Прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации
Организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а так же руководство указанной государственной системой
Разработка алгоритмов шифрования

Вопрос № 6
ФСТЭК России в целях реализации своих полномочий имеет право:

осуществлять радиоконтроль
издавать в пределах своей компетенции нормативные правовые акты, методические документы и индивидуальные правовые акты
утверждать квалификационные требования к специалистам, работающим в области агентурной разведки
приостанавливать или отменять действия выданных сертификатов

Вопрос № 7
При каком органе исполнительной власти действует Академия криптографии России?

ФСБ России
МинФине России
ФСТЭК России
МО России

Вопрос № 8
В задачи какого органа исполнительной власти входит осуществление государственной научно-технической политики в области обеспечения информационной безопасности?

ФСБ России
ФСТЭК России
МО России
ФНС России

Вопрос № 9
Что не является функцией ФСБ России?

участие в разработке и реализации мер по обеспечению информационной безопасности страны и защите сведений, составляющих государственную тайну?
осуществляет и организует в соответствии с федеральным законодательством лицензирование отдельных видов деятельности
занимается сертификацией средств защиты информации от несанкционированного доступа
организует работу комиссий по аттестации автоматизированных систем по требования безопасности

Вопрос № 10
Какие два основных документа содержат совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации?

Доктрина информационной безопасности Российской Федерации
Концепция национальной безопасности Российской Федерации
Конвенция о защите информации Российской Федерации
Трактат о защите информации Российской Федерации

Вопрос № 11
К принципам построения системы защиты относятся:

Принцип системности
Принцип компетентности
Принцип разумной достаточности
Принцип неуправляемости

Вопрос № 12
Как называется программа (некоторая совокупность выполняемого кода/инструкций), которая способна создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты/ресурсы компьютерных систем, сетей и т.д. без ведома пользователя (при этом копии сохраняют способность дальнейшего распространения)?

Компьютерный вирус
Прикладное ПО
Компьютерный помощник
Плохая программка

Вопрос № 13
Какие два способа заражения среды обитания используют компьютерные вирусы?

Резидентный
Нерезидентный
Полурезидентный
Сетевой

Вопрос № 14
По особенностям алгоритма вирусы делятся на:

компаньон-вирусы (companion)
вирусы-“черви” (worm)
“полиморфик”-вирусы
касперский

Вопрос № 15
Как называются вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов?

паразитические
студенческие
“стелс”-вирусы
макро-вирусы

Вопрос № 16
Как называются вирусы которые проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии?

вирусы-“черви” (worm)
“стелс”-вирусы
безвредные
оранжевые

Вопрос № 17
Как называются вирусы не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода?

“полиморфик”-вирусы
“макро-вирусы”
“паразитические”
компаньон-вирусы (companion)

Вопрос № 18
Как называются действия третьей стороны, цель которых - подтвердить то, что изделие или услуга соответствует определенным стандартам или другим нормативным документам?

Сертификация
Лицензирование
Аттестация
Пробы

Вопрос № 19
Какие вирусы могут гарантированно обнаружить антивирусные программы-сканеры?

уже известные КВ
неизвестные КВ
все КВ
никаких КВ

Вопрос № 20

Какой метод позволяет обнаруживать ранее неизвестные КВ, даже если они не пытаются изменять сектора и файлы?

Эвристический анализ
Резидентный сторож
Метод вакцинирования
Метод обнаружения изменений

Вопрос № 21
Какой метод поиска КВ предполагает, что антивирусные программы должны постоянно находиться в оперативной памяти компьютера и отслеживать все подозрительные действия, выполняемые другими программами?

Метод резидентных сторожей
Метод эвристического анализа
Вакцинирование
Метод обнаружения изменений

Вопрос № 22
Какой из методов поиска КВ заключается в том, что антивирусная программа предварительно запоминает характеристики всех областей диска, которые могут подвергаться нападению КВ, а затем периодически проверяет их?

Метод обнаружения изменений
Метод сканирования
Метод эвристического анализа
Вакцинирование

Вопрос № 23
В какой стране разработан персональный идентификатор eToken?

Израиль
США
Германия
Россия

Вопрос № 24
Какие цели преследует защита программного обеспечения?

ограничение несанкционированного доступа к программам или их преднамеренное разрушение и хищение
исключение несанкционированного копирования (тиражирования) программ
обеспечение физической охраны средств вычислительной техники
обучении персонала новым методам работы

Вопрос № 25
Какие две категории из перечисленных относятся к категориям авторского права?

экономические права, дающие их обладателям право на получение экономических вы-

год от продажи или использования программных продуктов и баз данных
моральные права, обеспечивающие защиту личности автора в его произведении
человеческие права, дающие право человеку чувствовать гордость за созданный им программный продукт
дружеские права, дающие возможность друзьям автора распространять и использовать его программные продукты и базы данных

Вопрос № 26
Как выглядит знак авторсого права?

©
®
TM
WWW

Вопрос № 27
Какой вид лицензии предполагает продажу всех имущественных прав на программный продукт или базу данных, покупателю лицензии предоставляется исключительное право на их использование, а автор или владелец патента отказывается от самостоятельного их применения или предоставления другим лицам?

Исключительная лицензия
Простая лицензия
Этикеточная лицензия
Коробочная лицензия

Вопрос № 28
Какой вид лицензии распространяетя на одну копию программного продукта или базы данных?

Одиночная лиценция
Исключительная лицензия
Простая лицензия
Этикеточная лицензия

Вопрос № 29
Какая лицензия предоставляет право лицензиату использовать программный продукт или базу данных, оставляя за собой право применять их и предоставлять на аналогичных условиях неограниченному числу лиц (лицензиат при этом не может сам выдавать сублицензии, может лишь продать копии приобретенного программного продукта или базы данных)?

Простая лицензия
Этикеточная лицензия
Исключительная лицензия
Неполная лицензия

Вопрос № 30
Какой вид лицензии приобретают дилер (торговец) либо фирмы-производители, использующие купленные лицензии как сопутствующий товар к основному виду деятельности?

Простая лицензия

Дополнительная лицензия
Суперлицензия
Магазинная лицензия

Вопрос № 31
Основными функции электронного архива являются:

Регистрация документов в системе (заполнение регистрационной карточки), присоединение к карточке любого количества файлов произвольного формата
Поиск документов по любому из полей регистрационной карточки и по тексту присоединенных к карточке файлов с учетом морфологии русского языка
Предупреждение персонала о приходе начальника
Пожарная сигнализация

Вопрос № 32
В результате внедрения системы электронного документооборота удается достичь:

повышения оперативности получения необходимой информации
увеличения затрат на хранение бумажных документов
повышения заработной платы бухгалтеров
отказа от использования SQL-технологии

Примерная тематика рефератов

1. Доктрина информационной безопасности РФ.
2. Угрозы информационной безопасности и их классификация.
3. Глава 28 Уголовного кодекса Российской Федерации. Закон «О государственной тайне» от 21 июля 1993 года N 5486-1.
4. Закон «О коммерческой тайне» №98-ФЗ от 2004 года. Закон «О персональных данных» №152-ФЗ от 2006 года Закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года N 149-ФЗ.
5. Закон «О лицензировании отдельных видов деятельности». Основные лицензирующие органы и их функции.
6. Гражданский кодекс Российской Федерации.
7. Кодекс об административных правонарушениях Российской Федерации. Уголовный кодекс Российской Федерации.
8. «Оранжевая книга» как оценочный стандарт.
9. Информационная безопасность распределенных систем. Рекомендации X.800.
10. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».
11. Интерпретация «Оранжевой книги» для сетевых конфигураций. Руководящие документы Гостехкомиссии России.
12. Процедурный уровень обеспечения ИБ.
13. Программно-технический уровень обеспечения ИБ.
14. Сеть Фейстеля.
15. Криптоанализ.
16. Самошифрование и полиморфичность.
17. Антивирусное программное обеспечение.
18. Место информационной безопасности экономических систем в национальной безопасности страны.
19. Три вида возможных нарушений информационной системы. Защита.

20. История появления компьютерных вирусов и факторы, влияющие на их распространение.

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

Вопросы к экзамену
(1 семестр, очная форма обучения)

1. Доктрина информационной безопасности РФ.
2. Угрозы информационной безопасности и их классификация.
3. Основные угрозы доступности.
4. Основные угрозы целостности.
5. Основные угрозы конфиденциальности.
6. Объектно-ориентированный подход к информационной безопасности.
7. Глава 28 Уголовного кодекса Российской Федерации. Закон «О государственной тайне» от 21 июля 1993 года N 5486-1.
8. Закон «О коммерческой тайне» №98-ФЗ от 2004 года. Закон «О персональных данных» №152-ФЗ от 2006 года Закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года N 149-ФЗ.
9. Закон «О лицензировании отдельных видов деятельности». Основные лицензирующие органы и их функции.
10. Гражданский кодекс Российской Федерации.
11. Кодекс об административных правонарушениях Российской Федерации. Уголовный кодекс Российской Федерации.
12. «Оранжевая книга» как оценочный стандарт.
13. Информационная безопасность распределенных систем. Рекомендации X.800.
14. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».
15. Гармонизированные критерии Европейских стран.
16. Интерпретация «Оранжевой книги» для сетевых конфигураций. Руководящие документы Гостехкомиссии России.
17. Процедурный уровень обеспечения ИБ.
18. Программно-технический уровень обеспечения ИБ.
19. Сеть Фейстеля.
20. Криптоанализ.
21. Самошифрование и полиморфичность.
22. Программные закладки.
23. Антивирусное программное обеспечение.
24. Место информационной безопасности экономических систем в национальной безопасности страны.
25. Три вида возможных нарушений информационной системы. Защита.
26. История появления компьютерных вирусов и факторы, влияющие на их распространение.

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 : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.
2. Введение в информационную безопасность и защиту информации : учебное пособие : [16+] / В.А. Трушин, Ю.А. Котов, Л.С. Левин, К.А. Донской ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2017. – 132 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=575113 (дата обращения: 01.09.2021). – Библиогр.: с. 49-50. – ISBN 978-5-7782-3233-4.

4.2. Дополнительная литература

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557.
2. Ковалев, Д.В. Информационная безопасность: учебное пособие / Д.В. Ковалев, Е.А. Богданова. - Ростов-на-Дону: Издательство Южного федерального университета, 2016. - 74 с. [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=493175 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-9275-2364-1. – Текст : электронный.
3. Прохорова, О.В. Информационная безопасность и защита информации: учебник / О.В. Прохорова. - Самара: Самарский государственный архитектурно-строительный университет, 2014. - 113 с. [Электронный ресурс]. - URL: https://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.

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/	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 про-	Свободный доступ

		грамм.	
3.	https://www.intuit.ru/	Национальный открытый университет - организация, предоставляющая с помощью собственного сайта услуги дистанционного обучения по нескольким образовательным программам, многие из которых касаются информационных технологий. Сайт содержит несколько сотен открытых образовательных курсов, по прохождении которых можно бесплатно получить электронный сертификат. Также возможно платное получение сертификатов о повышении квалификации. Кроме того, организация действует как издательство, выпуская учебную литературу по курсам.	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	www.school.edu.ru	Российский общеобразовательный портал	Свободный доступ.
2.	www.garant.ru	Гарант.РУ – информационно-правовой портал	Свободный доступ.
3.	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
4.	www.garant.ru	Информационно-правовой портал	Свободный доступ
5.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
6.	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;
- - 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.

Предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.