ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.01.14 Защита информации

Направление подготовки: 09.03.01 Информатика и вычислительная техника
Направленность (профиль): Информатика и вычислительная техника
Квалификация (степень): бакалавр
Форма обучения: очная

Институт: математики, естествознания и техники
Кафедра: математического моделирования и компьютерных технологий

	очная форма	очно-заочная форма	заочная форма
Курс	**4**		
Семестр/триместр	**7**		

Лекции	**20**		
Лабораторные занятия	**20**		
Практические (семинарские) занятия	**-**		
Консультации	**2**		
Форма(ы) промежуточной аттестации	**Экзамен – 0,3**		
Контроль	**36**		
Иные формы работы	**-**		
Самостоятельная работа	**65,7**		

Всего часов: 144
Трудоемкость: 4 зачетные единицы.

Разработчик(и) рабочей программы:
старший преподаватель кафедры ММиКТ Д.И. Максимов

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины: обучение студентов методам и средствам обеспечения информационной безопасности объектов профессиональной деятельности и объектов проектирования.

Задачи изучения дисциплины:

- освоить технологии диагностики опасностей и угроз для информационных систем и методов работы с моделями безопасности;
- изучить основные типы 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);
- разъяснить значение 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 части, формируемой участниками образовательных отношений, блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ПКС-1	**Знать:** – возможности существующей программно-технической архитектуры; – методологию разработки программного обеспечения и технологию программирования; – методы и средства проектирования программного обеспечения; – методы и средства проектирования баз данных; – типовые решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке программного обеспечения.	**Знает:** – методы и средства защиты информации при использовании программного обеспечения.
	Уметь: – проводить оценку и обоснование рекомендуемых решений; – вырабатывать варианты реализации программного обеспечения;	**Умеет:** – применять методы и средства обеспечения информационной безопасности.

	– применять методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов.	
	Владеть: – анализом возможностей реализации требований к программному обеспечению; – навыками распределения заданий между программистами в соответствии с техническими спецификациями; – навыками осуществления обучения и наставничества; – методами проектирования структур данных; – методами проектирования программных интерфейсов.	**Владеет:** – навыками осуществления защиты информации в программных продуктах.

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. «Защита информации. Основные понятия и определения.»	**21,7**	**6**		**4**	**11,7**
1.	**Тема 1. «**Информационные ресурсы и документирование информации Безопасность информационных ресурсов.»	6,7	2		2	2,7
2.	**Тема 2.** «Государственные информационные ресурсы. Персональные данные о гражданах. Права на доступ к информации. Вычислительные сети и защита информации.»	5	2			3
3.	**Тема 3. «**Нормативно-правовая база функционирования систем защиты информации.»	5	2			3
4.	**Тема 4. «**Компьютерные преступления и особенности их расследования. Промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.»	5			2	3
	Раздел 2. «Законодательный уровень обеспечения информационной безопасности.»	**18**	**4**		**2**	**12**
5.	**Тема 1. «**Глава 28 Уголовного кодекса Российской Федерации. Закон «О государственной тайне» от 21 июля 1993 года N	6	2			4

	5486-1. Закон «О коммерческой тайне» №98-ФЗ от 2004 года. Закон “О персональных данных” №152-ФЗ от 2006 года.»					
6.	**Тема 2. «**Закон "Об информации, информационных технологиях и о защите информации"от 27 июля 2006 года N 149-ФЗ. Закон "О лицензировании отдельных видов деятельности". Основные лицензирующие органы и их функции. Гражданский кодекс Российской Федерации.»	6	2			4
7.	**Тема 3. «**Кодекс об административных правонарушениях Российской Федерации. Уголовный кодекс Российской Федерации.»	6			2	4
	Раздел 3. Стандарты и технические спецификации в области информационной безопасности.	**12**	**2**		**2**	**8**
8.	**Тема 1. «**Оранжевая книга как оценочный стандарт. Информационная безопасность распределенных систем.» Рекомендации X.800. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".	6	2			4
9.	**Тема 2. «**Гармонизированные критерии Европейских стран. Интерпретация "Оранжевой книги" для сетевых конфигураций. Руководящие документы Гостехкомиссии России.»	6			2	4
	Раздел 4. «Криптографические модели. Симметричные и ассиметричных криптосистемы для защиты компьютерной информации.»	**18**	**4**		**2**	**12**
10.	**Тема 1. «**Криптографические модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации.»	6	2			4
11.	**Тема 2. «**Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки. Блочные и поточные шифры.»	6			2	4
12.	**Тема 3. «**Методы генерации псевдослучайных последовательностей чисел.»	6	2			4
	Раздел 5. «Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем.»	**20**	**4**		**4**	**12**
13.	**Тема 1. «**Стандартные алгоритмы шифрования. Основные понятия и определения. Шифры перестановки. Шифрующие таблицы. Применение магических квадратов.»	8	2		2	4
14.	**Тема 2. «**Концепция криптосистемы с открытым ключом. Криптосистема шифрования	6			2	4

	данных RSA. Безопасность и быстродействие криптосистемы RSA.»					
15.	**Тема 3. «**Изучение американского стандарта шифрования данных DES. Основные режимы работы алгоритма DES. Отечественный стандарт шифрования данных.»	6	2			4
	Раздел 6. «Защита информации в компьютерных сетях, антивирусная защита.»	**16**			**6**	**10**
16.	**Тема 1. «**Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия.»	4			2	2
17.	**Тема 2. «**Модели взаимодействия прикладной программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок. Компьютерные вирусы как особый класс разрушающих программных воздействий.»	6			2	4
18.	**Тема 3. «**Защита от разрушающих программных воздействий. Антивирусная защита в сетях. Понятие изолированной программной среды. Рекомендации по защите информации в Internet.»	6			2	4
	Консультации	2				
	Экзамен	0,3				
	Контроль	36				
	Итого за 7 семестр	*144*	*20*	*0*	*20*	*65,7*
	ИТОГО:	**144**	**20**	**0**	**20**	**65,7**

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

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 также 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 выгод 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 авторского 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 лицензия
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

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

Вопросы к экзамену
(7 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.
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. Место информационной безопасности экономических систем в национальной безопасности страны.
34. Три вида возможных нарушений информационной системы.
35. Факторы, влияющие на распространение компьютерных вирусов.
36. Безопасность информационных ресурсов.
37. Оранжевая книга" как оценочный стандарт.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1 Основная литература

1. Горбенко, А.О. Основы информационной безопасности (введение в профессию) : учебное пособие / А.О. Горбенко. – Санкт-Петербург : ИЦ "Интермедия", 2017. – 336 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=482788 (дата обращения: 29.10.2020). – ISBN 978-5-4383-0136-3. – Текст : электронный.

4.2 Дополнительная литература

1. Ажмухамедов, И.М. Основы организационно-правового обеспечения информационной безопасности : учебное пособие / И.М. Ажмухамедов, О.М. Князева. – Санкт-Петербург : ИЦ "Интермедия", 2017. – 264 с. : табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481107 (дата обращения: 29.10.2020). – Библиогр.: с. 248-256. – ISBN 978-5-4383-0160-8. – 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;
- 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.