ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.06 Программно-аппаратные средства защита информации

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	**3**		
Семестр	**5**		

Лекции	**18**		
Лабораторные занятия	**18**		
Практические (семинарские) занятия	**18**		
в т. ч. практическая подготовка			
Форма(ы) промежуточной аттестации	**зачет**		
Контроль			
Иные формы работы			
Самостоятельная работа	**54**		

Всего часов: 108
Трудоемкость: 3 зачетных единицы.

Разработчик(и) рабочей программы:
кандидат физико-математических наук, доцент С.А. Рощупкин

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

формирование знаний в области теоретических основ информационной безопасности и навыков практического обеспечения программно-аппаратных средств для защиты информации.

Задачи изучения дисциплины:

– ознакомление со стандартами, методическими и нормативными материалами, которые определяют проектирование и разработку объектов профессиональной деятельности;

– изучение моделей, методов и форм организации процесса разработки объектов профессиональной деятельности;

– изучение методов и средств анализа и моделирования объектов профессиональной деятельности и их компонентов.

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

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-7	Знать: - типы алгоритмов и способы их написания, основные языки программирования и современные программные среды разработки автоматизированных систем и технологий для решения задач профессиональной деятельности.	Знает: - типы алгоритмов и способы их написания для обеспечения информационной безопасности с помощью программно-аппаратных средств защиты информации.
	Уметь: - составлять алгоритмы, писать и проводить отладку кода на языке программирования, тестировать работоспособность программы.	Умеет: - составлять алгоритмы, писать на языке программирования для обеспечения информационной безопасности с помощью программно-аппаратных средств защиты информации.
	Владеть: - навыками программирования, отладки и тестирования программных продуктов для решения задач профессиональной деятельности.	Владеет: - навыками программирования, отладки и тестирования программных продуктов для программно-аппаратных средств защиты информации.
ОПК-9	Знать: - особенности технических и криптографических средств защиты информации, механизмы функционирования основных технических и криптографических средств защиты, характеристики криптографических протоколов.	Знает: - особенности технических программно-аппаратных средств защиты информации.
	Уметь: - проводить анализ технических и	Умеет: - проводить анализ технических про-

	криптографических средств защиты автоматизированных систем, определять виды информации, подверженной внешним и внутренним угрозам, производить правильный выбор параметров средств защиты информации.	граммно-аппаратных средств защиты информации.
	Владеть: - базовыми навыками использования технических и криптографических средств защиты информации при решении задач профессиональной деятельности.	Владеет: - базовыми навыками использования технических программно-аппаратных средств защиты информации.
ОПК-2.2	Знать: - источники и классификацию возможных деструктивных воздействий на информационные ресурсы; - программные и аппаратные средства защиты информации, направленные на оптимизацию структуры и функциональных процессов объекта защиты и его информационных составляющих.	Знает: - принципы обеспечения информационной безопасности с помощью программно-аппаратных и технических средств защиты информации.
	Уметь: - анализировать и оценивать вероятный ущерб от деструктивных воздействий на информационные ресурсы, - применять программные и аппаратные средства защиты информации для оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих.	Умеет: - определять необходимый инструментарий, программно-аппаратные и технические средства защиты информации.
	Владеть: - методами и средствами выявления деструктивных воздействий на информационные ресурсы; - способами установки, настройки и использования программных и аппаратных средств защиты информации в автоматизированной системе.	Владеет: - навыками установки, настройки и методами, инструментами тестирования программно-аппаратных и технических средств 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

№	Наименование разделов и тем	Всего часов	Аудиторные занятия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
Раздел 1. «Основные понятия и определения»		**26**	**4**	**4**	**4**	**14**
1	Тема 1. Предмет и объект защиты информации. Объект защиты информации. Санкционированный и несанкционированный доступ. Базовые свойства безопасности информации. Угрозы безопасности и каналы реализации угроз.	12	2	2	2	6
2	Тема 2. Классификация угроз информационной безопасности. Основные принципы обеспечения информационной безопасности. Ценность информации. Стандарты информационной безопасности. Методы обеспечения безопасности компьютерных систем.	14	2	2	2	8
Раздел 2. «Комплексный подход к построению систем защиты от нарушения свойств информации»		**22**	**4**	**4**	**4**	**10**
3	Тема 3. Построение систем защиты от угроз нарушения конфиденциальности информации, нарушения целостности и нарушения доступности	22	4	4	4	10
Раздел 3. «Модели контроля конфиденциальности и целостности информации»		**16**	**2**	**2**	**2**	**10**
4	Тема 4. Понятие политики безопасности. Модели контроля конфиденциальности информации	16	2	2	2	10
Раздел 4. «Идентификация и аутентификация»		**16**	**2**	**2**	**2**	**10**
5	Тема 5. Парольная аутентификация. Аутентификация на основе сертификатов. Использование аутентифицирующих устройств. Биометрические методы аутентификации	16	2	2	2	10
Раздел 5. «Контроль целостности информации. Понятие электронной подписи»		**10**	**2**	**2**	**2**	**4**
6	Тема 6. Сертификаты открытых ключей. Удостоверяющий центр. Технологии электронной подписи на основе иок. Подтверждение доверия электронной подписи. Доверенные корневые удостоверяющие центры. Обеспечение юридической значимости	10	2	2	2	4
Раздел 6. «Защита информации в компьютерных сетях. Информационная безопасность в операционных системах»		**18**	**4**	**4**	**4**	**6**
7	Тема 7. Основные типы сетевых атак и методы противодействия им. Обеспечение информационной безопасности сетей.	9	2	2	2	3
8	Тема 8. Применение технологии межсетевых экранов. Угрозы безопасности операционной системы. Административные меры защиты.	9	2	2	2	3

	Форма отчетности	зачет				
	Контроль					
	Экзамен					
	Итого за 5 семестр	***108***	***18***	***18***	***18***	***54***
	в т.ч. практическая подготовка					
	ИТОГО	**108**	**18**	**18**	**18**	**54**

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.

Типовой вариант контрольной работы

1. Кратко опишите модель потенциального нарушителя.
2. Основные каналы утечки информации.
3. Охарактеризуйте свойства достоверности и своевременности информации.
4. Приведите классификацию конфиденциальной информации. Чем определяется ценность информации?
5. Предмет защиты информации
6. Охарактеризуйте информацию и ее свойства.
7. Электронный документ (ЭД). Понятие ЭД. Типы ЭД.
8. Виды информации в КС. Информационные потоки в КС. Понятие исполняемого модуля.
9. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа.
10. Понятие несанкционированного доступа (НСД), классы и виды НСД. Несанкционированное копирование программ как особый вид НСД.
11. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).
12. Политика безопасности в компьютерных системах. Оценка защищенности.
13. Способы защиты конфиденциальности, целостности и доступности в КС.
14. Руководящие документы Гостехкомиссии по оценке защищенности от НСД.
15. Понятие идентификации пользователя. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация (понятие, способы хранения, связь с ключевыми системами).
16. Основные подходы к защите данных от НСД. Шифрование. Контроль доступа. Разграничение доступа.
17. Файл как объект доступа. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости.
18. Организация доступа к файлам. Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам различных ОС.
19. Защита сетевого файлового ресурса на примерах организации доступа в различных ОС.
20. Способы фиксации факторов доступа. Журналы доступа и критерии их информативно-

сти.

21. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.

22. Доступ данных со стороны процесса (понятие; отличия от доступа со стороны пользователя).

23. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.

24. Защита массивов информации от изменения (имитозащита). Криптографическая постановка защиты от изменения данных. Подходы к решению задачи защиты данных от изменения.

25. Защита от разрушающих программных воздействий. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия. Понятие изолированной программной среды.

26. Построение программно-аппаратных комплексов шифрования.

27. Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носителя алгоритма шифрования.

28. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.

29. Необходимые и достаточные функции аппаратного средства криптозащиты. Проектирование модулей криптопреобразований на основе сигнальных процессов.

30. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ.

31. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей. Механизмы расширения BIOS. Преимущества и недостатки программных и аппаратных средств.

32. Способы защиты информации на съемных дисках. Организация прозрачного режима шифрования.

33. Надежность средств защиты компонент. Понятие временной и гарантированной надежности.

34. Несанкционированное копирование программ. Юридические аспекты несанкционированного копирования программ. Несанкционированное копирование программ как тип НСД.

35. Защита программ от несанкционированного копирования (общее понятие защиты от копирования). Разновидности задач защиты от копирования.

36. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования ПО.

37. Привязка программ к гибким машинным дискам (ГМД). Структура данных на ГМД. Управление контроллером ГМД.

38. Способы создания некопируемых меток. Точное измерение характеристик форматирования дорожки. Технология «слабых битов».

39. Физические метки и технология работы с ними.

40. Привязка программ к жестким магнитным дискам (ЖМД). Особенности привязки к ЖМД. Виды меток на ЖМД. Привязка к прочим компонентам штатного оборудования ПЭВМ.

41. Привязка к портовым ключам. Использование дополнительных плат расширения. Методы «водяных знаков» и методы «отпечатков пальцев».

42. Хранение ключей информации.

43. Секретная информация, используемая для контроля доступа: ключи и пароли.

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. Понятие «Информационная безопасность». Основные методологические и нормативно-правовые документы по информационной безопасности.
2. Основные понятия по защите компьютерных данных. Доступ к информации, санкционированный доступ, несанкционированный доступ, конфиденциальность данных, субъект и объект информационных технологий, доступность компонента или ресурса системы, угроза безопасности автоматизированной информационной системе, ущерб безопасности, уязвимость АСОИ, атака на компьютерную систему, политика безопасности.
3. Основные виды угроз безопасности компьютерных систем, Угрозы нарушения целостности информации, угрозы нарушения работоспособности АСОИ и отказы в работе.
4. Структурные составляющие гипотетической модели нарушителя, Преднамеренные потенциальные угрозы. Классификация каналов несанкционированного доступа.
5. Наиболее распространенные способы несанкционированного доступа в компьютерных технологиях. Перехват паролей, маскарад, незаконное использование привилегий, пассивное вторжение в АСОИ, активное вторжение.
6. Основные подходы для парирования и нейтрализации угроз информационной безопасности: фрагментарный подход и комплексный подход.
7. Политика безопасности. Виды политики безопасности: избирательная политика безопасности, полномочная политика безопасности.
8. Этапы построения системы защиты автоматизированных информационных систем. Составляющие отдельных этапов.
9. Основные задачи методов защиты информации в автоматизированных информационных системах. Принципы системы защиты информации в АСОИ.
10. Идентификация и проверка подлинности электронных документов и пользователей компьютерных технологий.
11. . Идентификация и механизмы подтверждения подлинности пользователя. Взаимная проверки подлинности пользователей.
12. Процедура «рукопожатия».
13. Протоколы аутентификации с нулевой передачей знаний.
14. Параллельная идентификация с нулевой передачей знаний.
15. Система идентификации Гиллоу-Куискуотера.
16. Управление криптографическими ключами. Генерация и хранение ключей.
17. Иерархия ключей шифрования данных в корпоративных компьютерных системах.
18. Распределение ключей в корпоративных компьютерных системах. Использование одного или нескольких центров распределении ключей. Прямой обмен сеансовыми ключами между санкционированными пользователями.
19. Механизм запроса – ответа в сетевых технологиях, механизм отметки времени.
20. Распределение ключей с участием Центра распределении ключей.
21. Протокол для симметричных криптосистем с использованием отметки времени.
22. Протокол для асимметричных криптосистем с использованием сертификатов открытых ключей.
23. Алгоритм открытого распределения ключей Диффи-Хелмана.
24. Протокол SKIP управления криптоключами.
25. Аутентификация пользователей как основной компонент межсетевых экранов.
26. Схема защиты компьютерных сетевых технологий на основе межсетевых экранов: фильтрующий маршрутизатор, межсетевой экран на основе двупортового шлюза, межсетевой экран на основе экранированного шлюза, экранированная подсеть, межсетевые экраны для организации виртуальных корпоративных сетей.
27. Программные методы защиты сетевых технологий в Internet структурах.

28. Защита данных в электронных платежных системах.

29. Принципы функционирования электронных платежных систем.

30. Электронные пластиковые карты. Пассивные и активные пластиковые карты. Основные типы активных пластиковых карт: карты-счетчики, карты с памятью, карты с микропроцессором, карты с контактным считыванием, карты с индукционным считванием.

31. Персональный идентификационный номер (PIN). Обеспечение безопасности электронно-платежной системы POS (Point-of-Sale), схема функционирования POS.

32. Обеспечение безопасности банкоматов в электронных платежных системах, схема обмена сообщениями между банкоматом и хост-ЭВМ банка рои идентификации и платеже, схема прохождения данных с PIN клиента между банкоматом, банком-эквайером и банком-эмитентом.

33. Универсальная платежная система UEPS (Universal Electronic Payment System), состав и архитектура платежной системы, распределение ключей и паролей, цикл платежной транзакции.

34. Торговые терминалы, формирование сессионных ключей, эмиссия карточек, разграничение ответственности между банками-участниками общей платежной системы, двойное шифрование записи о транзакции на ключах банка-эквайера и банка-эмитента.

35. Обеспечение безопасности электронных платежей через сеть Internet.

36. Авторизация и шифрование финансовой информации в сети Internet.

37. Протоколы шифрования SSL (Secure Socket Layer) и SET (Secure Electronic Transactions), использование сертификатов.

38. Отечественные программно-аппаратные средства криптографической защиты компьютерных систем.

39. Средства и системы управления контролем доступа в компьютерных технологиях.

40. Основные подходы к защите данных от несанкционированного доступа. Шифрование. Контроль доступа. Разграничения доступа к файлам.

41. Защита программного продукта от несанкционированного копирования.

42. Несанкционированное копирование программ как тип НСД.

43. Юридические аспекты несанкционированного копирования программ. Общее понятие защиты от копирования.

44. Разновидности задач защиты от копирования. Подходы к задаче защиты от копирования.

45. Привязка ПО к аппаратному окружению и физическим носителям как единственное средство защиты от копирования.

46. Привязка к внешним (добавляемым) элементам ПЭВМ. Привязка к портовым ключам. Использование дополнительных плат расширения.

47. Методы «водяных знаков» и методы «отпечатков пальцев».

48. Защита программного продукта от изучения.

49. Изучение и обратное проектирование программного обеспечения: понятие изучения и обратного проектирования программного обеспечения, способы изучения программного обеспечения (статическое и динамическое изучение), временная надежность (невозможность обеспечения гарантированной надежности).

50. Задачи защиты программного продукта от изучения и способы их решений: защита от отладки, динамическое преобразование кода,

51. Итеративный программный замок А. Долгина

52. Принцип ловушек и принцип избыточного кода, защита от дизассемблирования, принцип внешней загрузки файлов, динамическая модификация программы, защита от трассировки по прерываниям.

53. Аспекты защиты от исследования: способы ассоцианирования защиты и программного обеспечения, оценка надежности защиты от отладки.

54. Защита от разрушающих программных воздействий.

55. Вирусы как особый класс разрушающих программных воздействий. Необходимые и достаточные условия недопущения разрушающего воздействия.

56. Понятие изолированной программной среды.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Программно-аппаратные средства защиты информации : учебное пособие / Л.Х. Мифтахова, А.Р. Касимова, В.Н. Красильников и др. – Санкт-Петербург : ИЦ "Интермедия", 2018. – 408 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481123 (дата обращения: 01.09.2021). – Библиогр.: с. 404-405. – ISBN 978-5-4383-0157-8. – Текст : электронный.

4.2. Дополнительная литература

1. Прокушев, Я.Е. Программно-аппаратные средства защиты информации : учебное пособие / Я.Е. Прокушев. – Санкт-Петербург : ИЦ "Интермедия", 2017. – 168 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=481158 (дата обращения: 01.09.2021). – Библиогр.: с. 154. – ISBN 978-5-4383-0147-9. – Текст : электронный
2. Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю.Ю. Громов, О.Г. Иванова, К.В. Стародубов, А.А. Кадыков ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499013 (дата обращения: 01.09.2021). – Библиогр.: с. 190. – ISBN 978-5-8265-1737-6. – 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.	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
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	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.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	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.