Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Вишневский Дмитрий Александрович
Должность: Ректор
Дата подписания: 30.04.2025 11:55:50
Уникальный программный ключ:
03474917c4d012283e5ad996a48a5e70b68d057

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНОБРНАУКИ РОССИИ)

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ДонГТУ»)

Факультет информационных технологий и автоматизации производственных процессов

Кафедра интеллектуальных систем и информационной безопасности

УТВЕРЖДАЮ
И.о. проректора
по учебной работе
_____Д.В. Мулов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации
(наименование дисциплины)

10.05.03 Информационная безопасность автоматизированных систем
(код, наименование специальности)

Безопасность открытых информационных систем
(специализация)

Квалификация специалист по защите информации
(бакалавр/специалист/магистр)

Форма обучения очная
(очная, очно-заочная, заочная)

Алчевск, 2024

1 Цели и задачи изучения дисциплины

Цели дисциплины. Целью изучения дисциплины «Программно-аппаратные средства защиты информации» является формирование системы понятий, знаний, умений и навыков в области разработки приложений для мобильных устройств.

Задачи изучения дисциплины:

–изучение теоретических основ разработки приложений для мобильных устройств;

– формирование представлений о современных тенденциях в области информатики, связанных с использованием мобильных устройств.

Дисциплина направлена на формирование общепрофессиональной (ОПК-14) компетенции выпускника.

2 Место дисциплины в структуре образовательной программы

Логико-структурный анализ дисциплины – курс входит в обязательную часть в БЛОКА 1 «Дисциплины (модули)» студентов по направлению 10.05.03 Информационная безопасность автоматизированных систем (Безопасность открытых информационных систем).

Дисциплина реализуется кафедрой интеллектуальных систем и информационной безопасности.

Основывается на базе дисциплин: «Физика», «Высшая математика», «Общая электротехника», «Информатика», «Основы информационной безопасности».

Является основой для изучения следующих дисциплин: «Управление информационной безопасностью», «Методы проектирования защищенных открытых информационных систем», «Интеллектуальные системы информационной безопасности».

Для изучения дисциплины необходимы компетенции, сформированные у студента для решения профессиональных задач деятельности, связанных с разработкой программного обеспечения.

Курс является фундаментом для ориентации студентов в сфере разработки программного обеспечения информационных систем.

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 ак.часа.

Программой дисциплины предусмотрены следующие виды занятий: лекционные (36 часов), практические (36 ч.), самостоятельная работа обучающегося составляет 72 часа.

Дисциплина изучается на 5 курсе в 9 семестре. Форма промежуточной аттестации – экзамен. По дисциплине выполняется курсовой проект.

3 Перечень результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины «Программно-аппаратные средства защиты информации» направлен на формирование компетенции, представленной в таблице 1.

Таблица 1 –Компетенции, обязательные к освоению

Содержание компетенции	Код компетенции	Код и наименование индикатора достижения компетенции
Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений	ОПК-14	ОПК-14.1 Осуществляет разработку и внедрение автоматизированных систем с учетом требований по защите информации

4 Объём и виды занятий по дисциплине

Общая трудоёмкость учебной дисциплины составляет 4 зачётных единицы, 144 ак.ч.

Самостоятельная работа студента (СРС) включает проработку материалов лекций, подготовку к практическим занятиям, текущему контролю, выполнение индивидуального задания, самостоятельное изучение материала и подготовку к экзамену и дифференцированному зачету.

При организации внеаудиторной самостоятельной работы по данной дисциплине используются формы и распределение бюджета времени на СРС для очной формы обучения в соответствии с таблицей 2.

Таблица 2 – Распределение бюджета времени на СРС

Вид учебной работы	Всего ак.ч.	Ак.ч. по семестрам
		9
Аудиторная работа, в том числе:	72	72
Лекции (Л)	36	36
Практические занятия (ПЗ)	–	–
Лабораторные работы (ЛР)	36	36
Курсовая работа/курсовой проект	-	-
Самостоятельная работа студентов (СРС), в том числе:	72	72
Подготовка к лекциям	9	9
Подготовка к лабораторным работам	18	18
Подготовка к практическим занятиям / семинарам	-	-
Выполнение курсовой работы / проекта	20	20
Расчетно-графическая работа (РГР)	-	-
Реферат (индивидуальное задание)	-	-
Домашнее задание	-	-
Подготовка к контрольным работам	-	-
Подготовка к коллоквиуму	-	-
Аналитический информационный поиск	-	-
Работа в библиотеке	5	5
Подготовка к экзамену и диф.зачету	20	20
Промежуточная аттестация – экзамен (Э), диф.зачет (Д/З)	Э, Д/З	Э, Д/З
Общая трудоемкость дисциплины		
ак.ч.	144	144
з.е.	4	4

5 Содержание дисциплины

С целью освоения компетенции, приведенной в п.3 дисциплина разбита на 3 темы:

– тема 1 (Назначение и функции программно аппаратных средств обеспечения информационной безопасности);

– тема 2 (Политика и модели информационной безопасности);

– тема 3 (Программно-аппаратные комплексы защиты информации).

Виды занятий по дисциплине и распределение аудиторных часов для очной формы приведены в таблице 3.

Таблица 3 – Виды занятий по дисциплине и распределение аудиторных часов (очная форма обучения)

№ п/п	Наименование темы (раздела) дисциплины	Содержание лекционных занятий	Трудоемкость в ак.ч.	Темы практических занятий	Трудоемкость в ак.ч.	Тема лабораторных занятий	Трудоемкость в ак.ч.
1	2	3	4	5	6	7	8
1	Назначение и функции программно аппаратных средств обеспечения информационной безопасности	Стандарты нформационной безопасности. Назначение и функции программно аппаратных средств обеспечения информационной безопасности	6	–	–	–	–
2	Политика и модели информационной безопасности	Программные закладки. Модели воздействий программных закладок на вычислительные системы. Обнаружение программных закладок. Методы защиты от программных закладок. Политика информационной безопасности. Модели безопасности компьютерных систем. Технологии идентификации, аутентификации и авторизации	6 4 6 4	–	–	Выявление и предотвращение утечек информации Симметричное и ассиметричное шифрование данных Создание криптографических сообщений Аппаратная реализация криптографических средств защиты информации	4 4 4 8

Завершение таблицы 3

1	2	3	4	5	6	7	8
3	Программно-аппаратные комплексы защиты информации	Программно-аппаратные комплексы защиты информации.	12	–	–	Программно-аппаратный комплекс «Аккорд» Система защиты нформации «Secret Net» Программное средство PGP Средства защиты информации Dallas Lock	4 4 4 4
Всего аудиторных часов			36	–		36	

6 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

6.1 Критерии оценивания

В соответствии с Положением о кредитно-модульной системе организации образовательного процесса ФГБОУ ВО «ДонГТУ» (https://www.dstu.education/images/structure/license_certificate/polog_kred_modul.pdf) при оценивании сформированности компетенций по дисциплине используется 100-балльная шкала.

Перечень компетенций по дисциплине и способы оценивания знаний приведены в таблице 4.

Таблица 4 – Перечень компетенций по дисциплине и способы оценивания знаний

Код и наименование компетенции	Способ оценивания	Оценочное средство
ОПК-14	Экзамен, дифзачет	Комплект контролирующих материалов для экзамена

Всего по текущей работе в семестре студент может набрать 100 баллов, в том числе:

– защита лабораторных работ – всего 100 баллов;

Зачет проставляется автоматически, если студент набрал в течении семестра не менее 60 баллов и отчитался за каждую контрольную точку. Минимальное количество баллов по каждому из видов текущей работы составляет 60% от максимального.

Зачет по дисциплине «Программно-аппаратные средства защиты информации» проводится по результатам работы в семестре. В случае, если полученная в семестре сумма баллов не устраивает студента, во время сессии студент имеет право повысить итоговую оценку либо в форме устного собеседования по приведенным ниже вопросам (п.п. 6.5), либо в результате тестирования.

Шкала оценивания знаний при проведении промежуточной аттестации приведена в таблице 5.

Таблица 5 –Шкала оценивания знаний

Сумма баллов за все виды учебной деятельности	Оценка по национальной шкале зачёт/экзамен
0-59	Не зачтено/неудовлетворительно
60-73	Зачтено/удовлетворительно
74-89	Зачтено/хорошо
90-100	Зачтено/отлично

6.2 Домашнее задание

Домашние задания не предусмотрены.

6.3 Темы для рефератов (презентаций) – индивидуальное задание

Рефераты (индивидуальные задания) не предусмотрены.

6.4 Оценочные средства для самостоятельной работы и текущего контроля успеваемости

Тема 1. Назначение и функции программно аппаратных средств обеспечения информационной безопасности.

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

а) защита информации

б) компьютерная безопасность

в) защищенность информации

г) безопасность данных

2. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:

а) информационная война

б) информационное оружие

в) информационное превосходство

3. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:

а) конфиденциальность

б) целостность

в) доступность

г) аутентичность

д) аппелируемость

4. Гарантия точного и полного выполнения команд в АС:

а) надежность

б) точность

в) контролируемость

г) устойчивость

д) доступность

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

а) конфиденциальность

б) целостность

в) доступность

г) аутентичность

д)аппелируемость

Тема 2. Политика и модели информационной безопасности.

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

а) комплексное обеспечение ИБ

б) безопасность АС

в) угроза ИБ

г) атака на АС

д) политика безопасности

2. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.

а) комплексное обеспечение информационной безопасности

б) безопасность АС

в) угроза информационной безопасности

г) атака на автоматизированную систему

д) политика безопасности

3. Возможные воздействия на АС, которые прямо или косвенно могут нанести ущерб ее безопасности:

а) комплексное обеспечение информационной безопасности

б) безопасность АС

в) угрозы информационной безопасности

г) атака на автоматизированную систему

д) политика безопасности

4. Защищенность АС от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов:

а) комплексное обеспечение информационной безопасности

б) безопасность АС

в) угроза информационной безопасности

г) атака на автоматизированную систему

д) политика безопасности

5. Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий:

а) комплексное обеспечение информационной безопасности

б) безопасность АС
в) угроза безопасности
г) атака на автоматизированную систему
д) политика безопасности

Тема 3. Программно-аппаратные комплексы защиты информации.

1. Под системой защиты информации в КС понимается:

а) состояние всех компонент компьютерной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне

б) одно из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы

в) единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности

2. Контроллер - это...

а) основное устройство системы, производящее идентификацию пользователя и дающее разрешение на проход, в случае если считанный с идентификатора код совпадает с кодом, хранящимся в памяти контроллера

б) это набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа

в) это известность ее содержания только имеющим соответствующие полномочия субъектам

3. Множество объектов и типов доступа к ним субъекта может изменяться:

а) в соответствии с некоторыми правилами, существующими в данной системе

б) статично т.е. не может изменяться вообще

в) это никак не связано с субъектами

4. На каком уровне сетевой модели OSI не работает межсетевой экран:

а) физический
б) сеансовый
в) сетевой
г) транспортный

5. На каком этапе заканчивается жизненный цикл автоматизированной системы?

а) бета-тестирование системы
б) внедрение финальной версии системы в эксплуатацию
в) прекращение сопровождения и технической поддержки системы
г) альфа-тестирование системы

6.5 Вопросы для подготовки к экзамену

1) Как бы Вы дали определение понятию «угроза безопасности» вычислительной системы (ВС)?

2) Какие Вы знаете виды угроз безопасности ВС?

3) Как бы Вы дали определение понятию«программная закладка»?

4) Какие Вы знаете методы внедрения программных закладок?

5) Какие Вы знаете виды негативных воздействий программных закладок на ВС?

6) Какие Вы знаете виды вредоносного программного обеспечения?

7) Как бы Вы дали определение понятию «Rootkit»?

8) Как бы Вы дали описание методик внедрения UserModeруткитов?

9) Как бы Вы дали описание методик внедрения KernelModeруткитов?

10) Как бы Вы дали определение понятию «изолированная программная среда» (ИПС)?

11) Как бы Вы дали определение понятию «монитор безопасности объектов» (МБО)?

12) Как бы Вы дали определение понятию «монитор безопасности субъектов» (МБС)?

13) Как бы Вы объяснили, почему для реализации ИПС необходимо требовать наличие контроля порождения субъектов и объектов?

14) Как бы Вы дали определение понятию «политика информационной безопасности»?

15) Какие Вы знаете компоненты политики безопасности?

16) Как бы Вы дали определение понятию «процедуры безопасности»

17) Как бы Вы дали описание какие проблемы решает верхний уровень политики безопасности?

18) Как бы Вы дали описание какие проблемы решает средний уровень политики безопасности?

19) Как бы Вы дали описание какие проблемы решает нижний уровень политики безопасности?

20) Как бы Вы дали описание, что представляют собой специализированные политики безопасности?

21) Как бы Вы дали определение понятиям «идентификация», «аутентификация»и «авторизация»?

22) Какие Вы знаете способы аутентификации?

23) Как бы Вы дали описание методы аутентификации на основе

пароля?

24) Как бы Вы дали описание методы аутентификации на основесмарт-карт?

25) Как бы Вы дали описание методы биометрической аутентификации?

6.6 Примерная тематика курсовых проектов

Примерные темы курсовых проектов представлены в таблице 6.

Таблица 6 – Примерные темы курсовых работ

№ п/п	Наименование темы и краткое содержание
1	Комплекс программных продуктов защиты корпоративных информационных систем «Застава». Реализация программных средств обеспечения информационной безопасности с использованием криптографических пакетов и интерфейсов
2	Программно-аппаратный комплекс обнаружения вторжений «ViPNet IDS». Реализация программных средств обеспечения информационной Безопасности с использованием криптографических пакетов и интерфейсов
3	Персональное средство криптографической защиты информации ШИПКА. Основные этапы установки, настройки и функционирования ПСКЗИ Шипка.
4	Система автоматического распознавания лиц Face-Интеллект. Основные методы и подходы к распознаванию лиц.
5	Программно-аппаратный комплекс средств защиты информации «Аккорд - АМДЗ». Установка и основы работы с комплексом.
6	Аутентификация пользователя по отпечаткам пальцев с помощью программно-аппаратных средств Biolink.
7	Средство защиты информации SecretNet. Установка и основы работы со средством контроля каналов распространения конфиденциальной информации.
8	Персональное средство аутентификации eToken: аутентификация с помощью электронных ключей
9	Персональное средство аутентификации Rutoken: аутентификация с помощью электронных ключей
10	Программно-аппаратный комплекс предотвращения несанкционированного доступа к ресурсам компьютера «Соболь»: установка, настройка и эксплуатация комплекса.

Индивидуальное задание, касающееся конкретной задачи, выдается студенту преподавателем.

7 Учебно-методическое и информационное обеспечение дисциплины

7.1 Рекомендуемая литература

Основная литература

1. Программно-аппаратные средства защиты информации [Электронный ресурс] : учебное пособие : в 3-х ч. / В. А. Гриднев, Ю. А. Губсков, А. С. Дерябин, А. В. Яковлев. – Тамбов : Издательский центр ФГБОУ ВО «ТГТУ». URL: https://znanium.ru/catalog/document?id=419393&ysclid=m4znrcnu53328882974. (Дата обращения - 26.08.2024).

Дополнительная литература

1. Программно-аппаратные средства обеспечения информационной безопасности [Текст] : учебное пособие / В.И. Петров, Н.Д. Пригонюк. – М. : ИД Академии Жуковского, 2020. – 88 с. – URL: http://storage.mstuca.ru/xmlui/handle/123456789/8839. (Дата обращения - 26.08.2024).

7.2 Базы данных, электронно-библиотечные системы, информационно-справочные и поисковые системы

1. Научная библиотека ДонГТУ : официальный сайт.— Алчевск. — URL: library.dstu.education .— Текст : электронный.

2. Научно-техническая библиотека БГТУ им. Шухова : официальный сайт. — Белгород. — URL: http://ntb.bstu.ru/jirbis2/ .— Текст : электронный.

3. Консультант студента : электронно-библиотечная система.— Москва. — URL: http://www.studentlibrary.ru/cgi-bin/mb4x.— Текст : электронный.

4. Университетская библиотека онлайн : электронно-библиотечная система.— URL: http://biblioclub.ru/index.php?page=main_ub_red.— Текст : электронный.

5. Сайт кафедры ИСИБ http://scs.dstu.education.

8 Материально-техническое обеспечение дисциплины

Материально-техническая база обеспечивает проведение всех видов деятельности в процессе обучения, соответствует требованиям ФГОС ВО.

Материально-техническое обеспечение представлено в таблице 9.

Таблица 9 – Материально-техническое обеспечение

Наименование оборудованных учебных кабинетов	Адрес (местоположение) учебных кабинетов
Специальные помещения: *Мультимедийная аудитория. (60 посадочных мест)*, оборудованная специализированной (учебной) мебелью (скамья учебная –20 шт., стол– 1 шт., доска аудиторная– 1 шт.), учебное ПК (монитор + системный блок), мультимедийная стойка с оборудованием – 1 шт., широкоформатный экран. Аудитории для проведения лекций:	ауд. *207* корп. *4*
Компьютерные классы (22 посадочных места), оборудованный учебной мебелью, компьютерами с неограниченным доступом к сети Интернет, включая доступ к ЭБС: ПК– 12 шт.; Доска – 1 шт.	ауд. *211* корп. *4*

Лист согласования рабочей программы дисциплины

Разработал:
и.о заведующего кафедрой
интеллектуальных систем
и информационной безопасности _____ Е.Е.Бизянов
(должность) (подпись) Ф.И.О.)

и.о. заведующего кафедрой интеллектуальных систем
и информационной безопасности _____ Е.Е.Бизянов
(подпись Ф.И.О.)

Протокол № 1 заседания кафедры интеллектуальных систем и информационной безопасности от 27.08.2024 г

И.о. декана факультета
информационных технологий и
автоматизации производственных
процессов _____ В.В Дьячкова
(подпись) Ф.И.О.)

Согласовано:

Председатель методической
комиссии по специальности 10.05.03
Информационная безопасность
автоматизированных систем _____ Е.Е. Бизянов
(подпись Ф.И.О.)

Начальник учебно-методического центра _____ О.А. Коваленко
(подпись Ф.И.О.)

Лист изменений и дополнений

<table>
<tr><td colspan="2">Номер изменения, дата внесения изменения, номер страницы для внесения изменений</td></tr>
<tr><td>ДО ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td><td>ПОСЛЕ ВНЕСЕНИЯ ИЗМЕНЕНИЙ:</td></tr>
<tr><td colspan="2">Основание:</td></tr>
<tr><td colspan="2">Подпись лица, ответственного за внесение изменений</td></tr>
</table>