Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра автономных информационных и управляющих систем

“УТВЕРЖДАЮ”
ДЕКАН ФЛА
д.т.н. Саленко С. Д.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Программно-аппаратные средства защиты информации

Образовательная программа: 27.03.04 Управление в технических системах, профиль: Автономные информационные и управляющие системы

Курс: 4, семестр : 8

Факультет летательных аппаратов,

		Семестр
№	**Вид деятельности**	**8**
1	Всего зачетных единиц (кредитов)	4
2	Всего часов	144
3	Всего занятий в контактной форме, час.	37
4	Лекции, час.	12
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	12
7	из них в активной и интерактивной форме, час.	16
8	Аттестация, час.	2
9	Консультации, час.	11
10	Самостоятельная работа, час.	107
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	ДЗ

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 27.03.04 Управление в технических системах

ФГОС введен в действие приказом №1171 от 20.10.2015 г. , дата утверждения: 12.11.2015 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная, по выбору студента

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 27.03.04 Управление в технических системах

Рабочая программа обсуждена на заседании кафедры

АИУС, протокол заседания кафедры №7 от 20.06.2017

Утверждена на совете факультета летательных аппаратов, протокол № 5 от 21.06.2017

Программу разработал:

старший преподаватель, Шумейко В. А.

Заведующий кафедрой:

доцент, д.т.н. Легкий В. Н.

Ответственный за образовательную программу:

заведующий кафедрой Легкий В. Н.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ОПК.9 способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности; *в части следующих результатов обучения*:**
з10. знать современные аппаратные средства защиты систем ЭВМ
з8. знать возможные угрозы информационной безопасности при передаче информации в сетях ЭВМ
з9. знать методы защиты передаваемой информации в сетях ЭВМ
у3. уметь работать с программно-аппаратными комплексами защиты ЭВМ
***Компетенция ФГОС*: ПК.3 готовность участвовать в составлении аналитических обзоров и научно-технических отчетов по результатам выполненной работы, в подготовке публикаций по результатам исследований и разработок; *в части следующих результатов обучения*:**
у1. представлять итоги проделанной работы в виде отчетов, рефератов, статей, оформленных в соответствии с имеющимися требованиями, с привлечением современных средств редактирования и печати

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Программно-аппаратные средства защиты информации	
ОПК.9.з8 знать возможные угрозы информационной безопасности при передаче информации в сетях ЭВМ	
1.о способах безопасной передачи данных в сети ЭВМ	Самостоятельная работа
ОПК.9.з9 знать методы защиты передаваемой информации в сетях ЭВМ	
2.современные методы разграничения доступа в компьютерных системах	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.9.з10 знать современные аппаратные средства защиты систем ЭВМ	
3.возможные угрозы при передаче информации в сетях ЭВМ	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.9.у3 уметь работать с программно-аппаратными комплексами защиты ЭВМ	
4.методы защиты информационных ресурсов от вирусных воздействий	Лабораторные работы; Самостоятельная работа
ОПК.9.з8 знать возможные угрозы информационной безопасности при передаче информации в сетях ЭВМ	
5.методы защиты информационных ресурсов от вирусных воздействий	Лабораторные работы; Самостоятельная работа
ОПК.9.з10 знать современные аппаратные средства защиты систем ЭВМ	
6.методы защиты передаваемой информации в сетях ЭВМ	Лабораторные работы; Самостоятельная работа
ОПК.9.у3 уметь работать с программно-аппаратными комплексами защиты ЭВМ	
7.современные методы разграничения доступа в компьютерных системах	Лекции; Лабораторные работы; Самостоятельная работа
ОПК.9.з10 знать современные аппаратные средства защиты систем ЭВМ	
8.возможные угрозы при передаче информации в сетях ЭВМ	Лекции; Лабораторные работы; Самостоятельная работа
ПК.3.у1 представлять итоги проделанной работы в виде отчетов, рефератов, статей, оформленных в соответствии с имеющимися требованиями, с привлечением современных средств редактирования и печати	

9.у1. представлять итоги проделанной работы в виде отчетов, рефератов, статей, оформленных в соответствии с имеющимися требованиями, с привлечением современных средств редактирования и печати	Лекции; Лабораторные работы; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 8			
Дидактическая единица: раздел 1			
1. Предмет защиты. Информация общедоступная и ограниченного доступа. Категории ценности информации. Информация как объект права собственности. Назначение и задачи в сфере обеспечения информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной и коммерческой тайны. Международный стандарт безопасности информационных систем ISO 17799. Цели и задачи курса.	0	2	3, 7, 8, 9
2. Основные термины и определения. Угрозы безопасности информационных систем. Классификация угроз безопасности: угрозы преднамеренные и случайные; каналы утечки информации прямые и косвенные; угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами. Модель нарушителя. Классификация методов и средств защиты информации. Службы защиты информации: обеспечение, аутентичности субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации.	0	2	2, 8, 9
3. Требования к защищенности ИС на уровне Защиты объектов Защита подсистем управления Организационных мер	0	2	7, 8, 9
4. Принципы защиты информации от НСД Идентификация, аутентификация и авторизация. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Схема Kerberos. Несимметричные методы аутентификации субъекта. Аутентификация объекта. Разграничение и контроль доступа к информации. Контроль и управление доступом средствами операционной системы.	0	2	2, 3, 7, 8, 9
5. Дискреционный метод организации разграничения доступа. Мандатный метод организации разграничения доступа. Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности. Защищенные операционные системы. Средства защиты программного обеспечения от несанкционированной загрузки. Защита информации на машинных носителях. Защита остатков информации.	0	2	2, 7, 8, 9
6. Средства ПА защиты фирм «Информзащита», «Конфидент», и др.	0	2	3, 7, 8, 9

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность

Семестр: 8				
Дидактическая единица: раздел 1				
1. Firewalls (Освоение принципов защиты АС файрволом типа 3+)	4	2	3, 4, 5, 6, 8, 9	Лабораторная работа «Kerio PF» 1. Установить программу X Spider 2. Отсканировать машину без защиты файрволом 3. Установить Kerio Personal Firewall 4. Отсканировать машину с установленным файрволом 5. проанализировать полученные результаты и произвести настройку файрвола для устранения найденных уязвимостей 6. Объяснить природу обнаруженных уязвимостей
4. SecretNet 4.0 (Освоение принципов защиты АС данным программно-аппаратным комплексом, отработка навыков администрирования данного комплекса)	8	2	2, 7, 8, 9	1. Установить систему SecretNet на испытуемый компьютер 2. Настроить систему SecretNet для работы 2х пользователей (суперпользователь и пользователь) 3. Настроить систему журналирования 4. Настроить «Замкнутую среду» работы 5. Включить «Жесткий режим» работы системы 6. Настроить систему контроля целостности 7. Настроить систему маркировки при выводе на печать
5. Знакомство с аппаратным маршрутизатором компании CISCO либо D-LINK, Построение безопасной ЛВС	4	4	2, 3, 4, 8, 9	управляемому маршрутизатору используя Web-интерфейс 2. Подключиться к управляемому маршрутизатору используя ssh-интерфейс 3. Подключиться к управляемому маршрутизатору используя консольный кабель 4. В трех предыдущих режимах настроить VLAN, и указанные преподавателем

6. АККОРД 2000 (Освоение принципов защиты АС данным программно-аппаратным продуктом)	0	4	3, 7, 8, 9	1. Установить на испытуемый компьютер ПАСЗИ "АККОРД 2000" 2. Произвести настройку ПАСЗИ 3. Проверить предложенные преподавателем аспекты безопасности 4. Корректно деинсталировать систему

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 8				
1	ргз по вариантам	1, 2, 3, 4, 5, 6, 7, 8, 9	44	4
: Менжулин С. А. Системное администрирование [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Менжулин ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235094. - Загл. с экрана.				
2	изучение теории	1, 2, 3, 4, 5, 6, 7, 8, 9	63	7
: Менжулин С. А. Системное администрирование [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Менжулин ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235094. - Загл. с экрана.				

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Личный типовой сайт; Социальные сети
Консультирование	e-mail; Личный типовой сайт; Социальные сети
Контроль	e-mail; Личный типовой сайт; Социальные сети
Размещение учебных материалов	e-mail; Личный типовой сайт; Социальные сети

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Максимальный балл
Семестр: 8	
Лабораторная:	80
Зачет:	20

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля			
		Защита Л/Р	Защита РГЗ	Зачет	Прочее
ОПК.9	з10. знать современные аппаратные средства защиты систем ЭВМ	+	+	+	+
	з8. знать возможные угрозы информационной безопасности при передаче информации в сетях ЭВМ		+	+	+
	з9. знать методы защиты передаваемой информации в сетях ЭВМ	+	+		+
	у3. уметь работать с программно-аппаратными комплексами защиты ЭВМ	+	+	+	+
ПК.3	у1. представлять итоги проделанной работы в виде отчетов, рефератов, статей, оформленных в соответствии с имеющимися требованиями, с привлечением современных средств редактирования и печати		+		+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Кропачев Ю. У. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / Ю. У. Кропачев, М. Г. Черепанов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2007. - 69, [1] с. : ил.. - Режим доступа: http://www.ciu.nstu.ru/fulltext/textbooks/2007/2007_krop.rar

2. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2009. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-91134-353-8 - Режим доступа: http://znanium.com/catalog.php?bookinfo=169345 - Загл. с экрана.

Дополнительная литература

1. Программно-аппаратные средства и математическое обеспечение вычислительных систем : [сборник статей] / под ред. Л. Н. Королева, В. М. Репина. - М., 1989. - 176, [2] с. : ил.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Менжулин С. А. Системное администрирование [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Менжулин ; Новосиб. гос. техн. ун-т. - Новосибирск, [2017]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000235094. - Загл. с экрана.

8.2 Специализированное программное обеспечение

1 Windows
2 Office

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	описание

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра автономных информационных и управляющих систем

“УТВЕРЖДАЮ”
ДЕКАН ФЛА
д.т.н., профессор С.Д. Саленко
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Образовательная программа: 27.03.04 Управление в технических системах, профиль: Автономные информационные и управляющие системы

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по **дисциплине** Программно-аппаратные средства защиты информации приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ОПК.9 способность использовать навыки работы с компьютером, владеть методами информационных технологий, соблюдать основные требования информационной безопасности	з8. знать возможные угрозы информационной безопасности при передаче информации в сетях ЭВМ	Firewalls (Освоение принципов защиты АС файрволом типа 3+) ргз по вариантам	РГЗ Основная часть	Зачет, вопросы №1-15
ОПК.9	з9. знать методы защиты передаваемой информации в сетях ЭВМ	SecretNet 4.0 (Освоение принципов защиты АС данным программно-аппаратным комплексом, отработка навыков администрирования данного комплекса) Дискреционный метод организации разграничения доступа. Мандатный метод организации разграничения доступа. Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности. Защищенные операционные системы. Средства защиты программного обеспечения от несанкционированной загрузки. Защита информации на машинных носителях. Защита остатков информации. Знакомство с аппаратным маршрутизатором компании CISCO либо D-LINK, Построение безопасной ЛВС Основные термины и определения. Угрозы безопасности информационных систем. Классификация угроз безопасности: угрозы преднамеренные и случайные; каналы утечки информации прямые и косвенные; угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами. Модель нарушителя. Классификация	Отчет по лабораторной работе №1-3 РГЗ Основная часть	

		методов и средств защиты информации. Службы защиты информации: обеспечение, аутентичности субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации. Принципы защиты информации от НСД Идентификация, аутентификация и авторизация. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Схема Kerberos. Несимметричные методы аутентификации субъекта. Аутентификация объекта. Разграничение и контроль доступа к информации. Контроль и управление доступом средствами операционной системы. ргз по вариантам		
ОПК.9	з10. знать современные аппаратные средства защиты систем ЭВМ	Firewalls (Освоение принципов защиты АС файрволом типа 3+) SecretNet 4.0 (Освоение принципов защиты АС данным программно-аппаратным комплексом, отработка навыков администрирования данного комплекса) АККОРД 2000 (Освоение принципов защиты АС данным программно-аппаратным продуктом) Дискреционный метод организации разграничения доступа. Мандатный метод организации разграничения доступа. Контроль целостности информации. Имитозащита информации. Криптографические методы контроля целостности. Защищенные операционные системы. Средства защиты программного обеспечения от несанкционированной загрузки. Защита информации на машинных носителях. Защита остатков информации. Знакомство с аппаратным маршрутизатором компании CISCO либо D-LINK, Построение безопасной ЛВС Основные термины и определения. Угрозы безопасности информационных систем. Классификация угроз безопасности: угрозы	Отчет по лабораторной работе №1-3 РГЗ Основная часть	Зачет, вопросы №1-15

		преднамеренные и случайные; каналы утечки информации прямые и косвенные; угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами. Модель нарушителя. Классификация методов и средств защиты информации. Службы защиты информации: обеспечение, аутентичности субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации. Предмет защиты. Информация общедоступная и ограниченного доступа. Категории ценности информации. Информация как объект права собственности. Назначение и задачи в сфере обеспечения информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной и коммерческой тайны. Международный стандарт безопасности информационных систем ISO 17799. Цели и задачи курса. Принципы защиты информации от НСД Идентификация, аутентификация и авторизация. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Схема Kerberos. Несимметричные методы аутентификации субъекта. Аутентификация объекта. Разграничение и контроль доступа к информации. Контроль и управление доступом средствами операционной системы. ргз по вариантам Средства ПА защиты фирм «Информзащита», «Конфидент», и др. Требования к защищенности ИС на уровне Защиты объектов Защита подсистем управления Организационных мер		
ОПК.9	у3. уметь работать с программно-аппаратными комплексами защиты ЭВМ	Firewalls (Освоение принципов защиты АС файрволом типа 3+) SecretNet 4.0 (Освоение принципов защиты АС данным программно-аппаратным	Отчет по лабораторной работе №1-3 РГЗ Основная часть	Зачет, вопросы №1-15

		комплексом, отработка навыков администрирования данного комплекса) АККОРД 2000 (Освоение принципов защиты АС данным программно-аппаратным продуктом) Знакомство с аппаратным маршрутизатором компании CISCO либо D-LINK, Построение безопасной ЛВС Предмет защиты. Информация общедоступная и ограниченного доступа. Категории ценности информации. Информация как объект права собственности. Назначение и задачи в сфере обеспечения информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной и коммерческой тайны. Международный стандарт безопасности информационных систем ISO 17799. Цели и задачи курса. Принципы защиты информации от НСД Идентификация, аутентификация и авторизация. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Схема Kerberos. Несимметричные методы аутентификации субъекта. Аутентификация объекта. Разграничение и контроль доступа к информации. Контроль и управление доступом средствами операционной системы. ргз по вариантам Средства ПА защиты фирм «Информзащита», «Конфидент», и др. Требования к защищенности ИС на уровне Защиты объектов Защита подсистем управления Организационных мер		
ПК.3/НИ готовность участвовать в составлении аналитических обзоров и научно-технических отчетов по результатам выполненной работы, в подготовке публикаций по результатам исследований и	у1. представлять итоги проделанной работы в виде отчетов, рефератов, статей, оформленных в соответствии с имеющимися требованиями, с привлечением современных средств редактирования и печати	Firewalls (Освоение принципов защиты АС файрволом типа 3+) АККОРД 2000 (Освоение принципов защиты АС данным программно-аппаратным продуктом) Дискреционный метод организации разграничения доступа. Мандатный метод организации разграничения доступа. Контроль целостности информации. Имитозащита информации. Криптографические методы	Отчет по лабораторной работе №1-3 РГЗ Основная часть	

разработок		контроля целостности. Защищенные операционные системы. Средства защиты программного обеспечения от несанкционированной загрузки. Защита информации на машинных носителях. Защита остатков информации. Основные термины и определения. Угрозы безопасности информационных систем. Классификация угроз безопасности: угрозы преднамеренные и случайные; каналы утечки информации прямые и косвенные; угрозы, обусловленные человеческим фактором, техническими средствами, форс-мажорными обстоятельствами. Модель нарушителя. Классификация методов и средств защиты информации. Службы защиты информации: обеспечение, аутентичности субъектов информационного взаимодействия, управление доступом, обеспечение секретности и конфиденциальности информации, обеспечение целостности информации. Принципы защиты информации от НСД Идентификация, аутентификация и авторизация. Аутентификация субъекта. Парольные схемы защиты. Симметричные методы аутентификации. Схема Kerberos. Несимметричные методы аутентификации субъекта. Аутентификация объекта. Разграничение и контроль доступа к информации. Контроль и управление доступом средствами операционной системы. Средства ПА защиты фирм «Информзащита», «Конфидент», и др. Требования к защищенности ИС на уровне Защиты объектов Защита подсистем управления Организационных мер		

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 8 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ОПК.9, ПК.3/НИ.

Зачет проводится в устной форме, по билетам .

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 8 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе учебной дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОПК.9, ПК.3/НИ, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра автономных информационных и управляющих систем

Паспорт зачета

по дисциплине «Программно-аппаратные средства защиты информации», 8 семестр

1. Методика оценки

Зачет проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-10, второй вопрос из диапазона вопросов 11-18 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет ФЛА

Билет № _____
к зачету по дисциплине «Программно-аппаратные средства защиты информации»

1. Вопрос 1
2. Вопрос 2.
3. Задача.

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

Пример Билета для зачета

1. Циклы в языке С
2. Массивы и работа с массивами
3. Написать цикл for через while.

2. **Критерии оценки**

- Ответ на билет для зачета считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки,

оценка составляет 10 *баллов.*

- Ответ на билет для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные,
  оценка составляет 15 *баллов.*
- Ответ на билет для зачета билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить качественные характеристики процессов, не допускает ошибок при решении задачи,
  оценка составляет 20 *баллов.*
- *Ответ на билет для зачета билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет 30 и более баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее 20 баллов (из 40 возможных).

В общей оценке по дисциплине баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** зачету **по дисциплине «**Программно-аппаратные средства защиты информации**»**

1. Назначение программно-аппаратной защиты
2. Защита от несанкционированного доступа
3. Электронные ключи
4. Аппаратная защита компьютера и информации
5. Назначение SecretNet
6. Состав и функционирование системы Secret Net NT
7. Состав серверной части системы Secret Net NT
8. Сервер управления доступом (ACS)
9. Подсистема ведения базы данных системы защиты
10. Состав клиентской части системы Secret Net NT
11. Агент сервера управления доступом
12. Локальная база данных системы защиты
13. Подсистема опознавания пользователя
14. Подсистема контроля целостности
15. Подсистема полномочного управления доступом
16. Общий механизм взаимодействия компонент системы Secret Net NT
17. Поддержка криптографической защиты данных в системе Secret Net NT
18. Криптографические ключи в системе Secret Net NT
19. Криптографическая защита информационного содержания файлов
20. Формальное понятие защищенности АС
21. Методы тестирования системы защиты
22. Средства тестирования системы защиты

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра автономных информационных и управляющих систем

Паспорт
расчетно-графического задания (работы)

по дисциплине «Программно-аппаратные средства защиты информации», 8 семестр

1. **Методика оценки**

Расчетно-графическое задание (РГЗ) по дисциплине «Программно-аппаратные средства защиты информации» нацелено на формирование практических умений и навыков в области прикладного программирования.
Методические указания по выполнению расчетно-графического задания на тему «Проектирование защищенной сети предприятия по вариантам» включают в себя совокупность связанных расчетных заданий.
Расчетно-графическое задание включает выполнение задания и его защиту:
Пример задания: Разработать схему и системы защиты сети предприятия исходя из следующих данных(по вариантам).
Расчетно-графическое (РГЗ) задание выполняется студентами во внеаудиторное время.
Расчетно-графическое задание должно содержать:
1. Титульный лист установленной формы (представлен в приложении).
2. Оглавление.
3. Цель и задачи РГЗ по своему варианту.
4. Листинг и описание готовой программы

Требования к оформлению отчета о выполнении расчетно-графического задания:
- текст должен содержать заголовки в соответствии со структурой отчета;
- формат А4;
- шрифт – Times New Roman;
- размер шрифта – 12-14 пт;
- цвет шрифта – черный;
- межстрочный интервал – 1-1,5;
- размеры полей: верхнее – 20 мм, нижнее – 20 мм, левое – 30 мм, правое – 10 мм;
- абзацный отступ – 1,25 мм; выравнивание текста – по ширине;
- страницы работы нумеруются арабскими цифрами в нижней части листа, начиная с титульного листа, номер на котором не ставится.

2. **Критерии оценки**

- работа считается **не выполненной,** если оценка составляет меньше 30 баллов.
- работа считается выполненной **на пороговом** уровне, если оценка составляет 50 баллов.
- работа считается выполненной **на базовом** уровне, если оценка составляет 60-79 баллов.
- **работа считается выполненной на продвинутом уровне, если оценка составляет больше 80 баллов.**

3. **Шкала оценки**

В общей оценке по дисциплине баллы за работы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

Таблица 1 - Критерии оценки защиты РГЗ

Диапазон баллов	Характеристика ответа студента
100	Студент отлично владеет терминологией, демонстрирует хорошие аналитические способности, легко оперирует категориями, дает полные ответы на дополнительные вопросы.
80-90	Студент хорошо владеет терминологией, с трудом определяет причинно-следственные связи явлений и объектов, на дополнительные вопросы дает не полные ответы.
50-70	Студент плохо владеет терминологией, дает ответы в краткой или затянутой форме, с наводящими вопросами.
0-40	Студент не владеет терминологией, дает ответы в краткой или затянутой форме, с наводящими вопросами. На дополнительные вопросы отвечает выборочно.