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

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Программно-аппаратные средства защиты информации

Образовательная программа: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Курс: 3, семестр : 5

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**5**
1	Всего зачетных единиц (кредитов)	4
2	Всего часов	144
3	Всего занятий в контактной форме, час.	80
4	Лекции, час.	36
5	Практические занятия, час.	18
6	Лабораторные занятия, час.	18
7	из них в активной и интерактивной форме, час.	8
8	Аттестация, час.	2
9	Консультации, час.	6
10	Самостоятельная работа, час.	64
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	контр.
12	Вид аттестации	Э

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.03.01 Информационная безопасность

ФГОС введен в действие приказом №1515 от 01.12.2016 г. , дата утверждения: 20.12.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, базовая

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.03.01 Информационная безопасность

Рабочая программа обсуждена на заседании кафедры

ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

старший преподаватель, Туманов С. А.

Заведующий кафедрой:

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

заведующий кафедрой Трушин В. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ПК.1** **способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации; *в части следующих результатов обучения*:**
з4. знать программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей
***Компетенция ФГОС*: ПК.10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; *в части следующих результатов обучения*:**
у1. уметь выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации
***Компетенция ФГОС*: ПК.12 способность принимать участие в проведении экспериментальных исследований системы защиты информации; *в части следующих результатов обучения*:**
з3. знать основыные параметры и характеристики средств защиты
***Компетенция ФГОС*: ПК.3 способность администрировать подсистемы информационной безопасности объекта защиты; *в части следующих результатов обучения*:**
у1. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

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	
ПК.1.з4 знать программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей	
1.-операционные системы персональных ЭВМ;	Лекции; Практические занятия; Лабораторные работы; Самостоятельная работа
ПК.10.у1 уметь выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	
2.-выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах;	Лекции; Практические занятия; Самостоятельная работа
ПК.3.у1 уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	
3.Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику	Лекции; Самостоятельная работа
ПК.12.з3 знать основыные параметры и характеристики средств защиты	
4.-ашаратные средства вычислительной техники;	Лекции; Практические занятия; Лабораторные работы; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения
Семестр: 5			
Дидактическая единица: основные принципы создания программно-аппаратных средств обеспечения информационной безопасности, концепция диспетчера доступа			

1. Введение. Постановка задачи защиты информации от НСД. Классификация каналов утечки информации в ПЭВМ; Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности, концепция диспетчера доступа;	0	3	1
Дидактическая единица: программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем			
2. Традиционные и дополнительные методы и средства защиты от НСД к информации; Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем;	0	3	2, 4
Дидактическая единица: методы и средства ограничения доступа к компонентам вычислительных систем			
3. Угрозы безопасности и методы защиты локальной ПЭВМ от НСД к информации; Методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям	0	3	1, 2, 4
4. Угрозы безопасности и методы защиты рабочей станции в сети от НСД к информации; Методы и средства хранения ключевой информации	0	3	1
Дидактическая единица: методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям			
5. Расширенное применение программно-аппаратных средств защиты информации; Изменения и контроль целостности, построение изолированной программной среды	0	3	3, 4
Дидактическая единица: методы и средства хранения ключевой информации			
6. Применение программно-аппаратных средств для идентификации и аутентификации субъектов и хранения ключевой информации	0	3	1, 3
Дидактическая единица: защита программ от изучения, способы встраивания средств защиты в программное обеспечение			
7. Методы защиты от несанкционированного копирования информации, методы защиты программ от изучения, изменения и искажения	0	3	1, 3, 4
8. Интеграция программно-аппаратных средств защиты информации в комплексную систему безопасности автоматизированной системы; Способы встраивания средств защиты в программное обеспечение;	0	3	2
Дидактическая единица: защита от разрушающих программных воздействий, защита программ от изменения и контроль целостности, построение изолированной программной среды			
9. Методы защиты от разрушающих программных воздействий	0	2	1
Дидактическая единица: задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности			

10. Проектирование и разработка программно-аппаратных средств защиты информации. Стандарты безопасности. Сертификация средств защиты информации; Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности	0	3	1, 4
Дидактическая единица: основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности			
11. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности	0	3	2
Дидактическая единица: программно-аппаратные средства защиты информации в сетях передачи данных			
12. Программно-аппаратные средства защиты информации в сетях передачи данных	0	4	1, 4

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 5				
Дидактическая единица: методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям				
2. Изучение методов защиты локальной ПЭВМ от НСД к информации, от несанкционированного копирования информации, идентификации и аутентификации субъектов в АС при помощи программно-аппаратного комплекса Secret Net и электронного замка "Соболь", Аккорд NT/2000	0	18	1, 4	Студенты изучают методы идентификации и аутентификации субъектов при помощи программно-аппаратного комплекса Secret Net, Аккорд NT/2000

Таблица 3.3

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 5				
Дидактическая единица: методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям				
3. Изучение методов защиты локальной ПЭВМ от НСД к информации при помощи программно-аппаратного комплекса при помощи программно-аппаратного комплекса Dallas Lock .	2	10	4	Студенты изучают методы защиты от несанкционированного копирования и НСД
Дидактическая единица: методы и средства хранения ключевой информации				
1. Изучение криптографических методов защиты при помощи программно-аппаратного комплекса Secret Disk	4	4	1, 2	Студенты изучают криптографические методы защиты при помощи программно-аппаратного комплекса Secret Disk

Дидактическая единица: защита от разрушающих программных воздействий, защита программ от изменения и контроль целостности, построение изолированной программной среды				
4. Изучение методов защиты от разрушающих программных воздействий при помощи программных комплексов "Ла-боратория Касперского" и "Dr. Web"	2	4	2, 4	Студенты изучают методы защиты от разрушающих программных воздействий в среде программных комплексов "Лаборатория Касперского" и "Dr. Web"

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 5				
1	Контрольные работы	1, 2, 3	22	4
: Аппаратно-программный комплекс шифрования "Континент" : методические указания по выполнению лабораторных работ по специальности 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем" / Новосиб. гос. техн. ун-т ; [сост.: И. В. Минин, О. В. Минин]. - Новосибирск, 2010. - 25 с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000148424				
2	Подготовка к занятиям	1, 4	16	0
: 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://elibrary.nstu.ru/source?bib_id=vtls000066407				
3	Дополнительная учебная деятельность	1, 4	8	0
: Туманов С. А. Система защиты информации от несанкционированного доступа на основе "SecretNet 7" : учебно-методическое пособие / С. А. Туманов, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 89, [2] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000226348 Туманов С. А. Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" : учебно-методическое пособие / С. А. Туманов, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 54, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000227592				
4	Подготовка к аттестации	1, 4	18	2
: Аппаратно-программный комплекс шифрования "Континент" : методические указания по выполнению лабораторных работ по специальности 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем" / Новосиб. гос. техн. ун-т ; [сост.: И. В. Минин, О. В. Минин]. - Новосибирск, 2010. - 25 с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000148424				

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
Консультирование	Социальные сети
Контроль	e-mail
Размещение учебных материалов	Портал НГТУ

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: 5	
Лабораторная:	20
Практические занятия:	10
Контрольные работы:	30
Экзамен:	40

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

Таблица 6.2

Коды компетенций ФГОС	**Результаты обучения**	**Формы контроля**	
		Контр. раб.	**Экзамен**
ПК.1	з4. знать программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей		+
ПК.10	у1. уметь выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации		+
ПК.12	з3. знать основыные параметры и характеристики средств защиты		+
ПК.3	у1. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	+	+

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

7. Литература

Основная литература

1. Мельников В. П. Информационная безопасность и защита информации : [учебное пособие для вузов по специальности 230201 "Информационные системы и технологии"] / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - Москва, 2009. - 330, [1] с. : ил., табл.

2. Зайцев А. П. Технические средства и методы защиты информации : лабораторный практикум : учебное пособие / А. П. Зайцев, А. А. Шелупанов. - Томск, 2005. - 119 с. : ил.

Дополнительная литература

1. Проскурин В. Г. Защита в операционных системах : Учеб. пособие для вузов по спец. : "Защитные телекоммуникационные системы", "Организация и технология защиты информации". . . / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. - М., 2000. - 166 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. Туманов С. А. Система защиты информации от несанкционированного доступа на основе "DallasLock 8.0" : учебно-методическое пособие / С. А. Туманов, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 54, [1] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000227592

2. Туманов С. А. Система защиты информации от несанкционированного доступа на основе "SecretNet 7" : учебно-методическое пособие / С. А. Туманов, И. Л. Рева ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 89, [2] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000226348

3. 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://elibrary.nstu.ru/source?bib_id=vtls000066407

4. Аппаратно-программный комплекс шифрования "Континент" : методические указания по выполнению лабораторных работ по специальности 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем" / Новосиб. гос. техн. ун-т ; [сост.: И. В. Минин, О. В. Минин]. - Новосибирск, 2010. - 25 с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000148424

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)	Материалы лекций

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

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Программно-аппаратные средства защиты информации

Образовательная программа: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

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)**
ПК.1/Э способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	з4. знать программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей	Введение. Постановка задачи защиты информации от НСД. Классификация каналов утечки информации в ПЭВМ; Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности, концепция диспетчера доступа; Изучение криптографических методов защиты при помощи программно-аппаратного комплекса Secret Disk Изучение методов защиты локальной ПЭВМ от НСД к информации, от несанкционированного копирования информации, идентификации и аутентификации субъектов в АС при помощи программно-аппаратного комплекса Secret Net и электронного замка "Соболь", Аккорд NT/2000 Методы защиты от несанкционированного копирования информации, методы защиты программ от изучения, изменения и искажения Методы защиты от разрушающих программных воздействий Применение программно-аппаратных средств для идентификации и аутентификации субъектов и хранения ключевой информации Программно-аппаратные средства защиты информации в сетях передачи данных Проектирование и разработка программно-аппаратных средств защиты информации. Стандарты безопасности. Сертификация средств защиты информации; Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной		Экзамен, вопросы...

		безопасности Угрозы безопасности и методы защиты локальной ПЭВМ от НСД к информации; Методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям Угрозы безопасности и методы защиты рабочей станции в сети от НСД к информации; Методы и средства хранения ключевой информации		
ПК.10/ЭИ способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	у1. уметь выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации	Изучение криптографических методов защиты при помощи программно-аппаратного комплекса Secret Disk Изучение методов защиты от разрушающих программных воздействий при помощи программных комплексов "Ла-боратория Касперского" и "Dr. Web" Интеграция программно-аппаратных средств защиты информации в комплексную систему безопасности автоматизированной системы; Способы встраивания средств защиты в программное обеспечение; Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности Угрозы безопасности и методы защиты локальной ПЭВМ от НСД к информации; Методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям		Экзамен, вопросы...
ПК.12/ЭИ способность принимать участие в проведении экспериментальных исследований системы защиты информации	з3. знать основыные параметры и характеристики средств защиты	Изучение методов защиты локальной ПЭВМ от НСД к информации при помощи программно-аппаратного комплекса при помощи программно-аппаратного комплекса Dallas Lock . Изучение методов защиты локальной ПЭВМ от НСД к информации, от несанкционированного копирования информации, идентификации и аутентификации субъектов в АС при помощи программно-аппаратного комплекса Secret		Экзамен, вопросы...

		Net и электронного замка "Соболь", Аккорд NT/2000 Изучение методов защиты от разрушающих программных воздействий при помощи программных комплексов "Ла-боратория Касперского" и "Dr. Web" Методы защиты от несанкционированного копирования информации, методы защиты программ от изучения, изменения и искажения Программно-аппаратные средства защиты информации в сетях передачи данных Проектирование и разработка программно-аппаратных средств защиты информации. Стандарты безопасности. Сертификация средств защиты информации; Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности Расширенное применение программно-аппаратных средств защиты информации; Изменения и контроль целостности, построение изолированной программной среды Традиционные и дополнительные методы и средства защиты от НСД к информации; Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем;		
ПК.3/Э способность администрировать подсистемы информационной безопасности объекта защиты	у1. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Методы защиты от несанкционированного копирования информации, методы защиты программ от изучения, изменения и искажения Применение программно-аппаратных средств для идентификации и аутентификации субъектов и хранения ключевой информации Расширенное применение программно-аппаратных средств защиты информации; Изменения и контроль целостности, построение изолированной программной среды		Экзамен, вопросы...

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 5 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ПК.1/Э, ПК.10/ЭИ, ПК.12/ЭИ, ПК.3/Э.

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

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 ПК.1/Э, ПК.10/ЭИ, ПК.12/ЭИ, ПК.3/Э, 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 защиты информации

Паспорт экзамена

по дисциплине «Программно-аппаратные средства защиты информации», 5 семестр

1. Методика оценки

Экзамен проводится в устной (письменной) форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-21, второй вопрос из диапазона вопросов 22-43 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

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

---

1. Вопрос 1
2. Вопрос 2.

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

2. Критерии оценки

- Ответ на экзаменационный билет (тест) 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 *55 баллов.*
- Ответ на экзаменационный билет (тест) 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 *65 баллов.*

- Ответ на экзаменационный билет (тест) 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 *75 баллов.*
- Ответ на экзаменационный билет (тест) 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 90 *баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее 100 баллов (из 180 возможных).

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

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

1. Объектно-ориентированный подход к информационной безопасности и рассмотрению защищаемых систем.

2. Информационная безопасность распределенных систем. Рекомендации X.800. Стандарт ISO/IEC 15408.

3. Административный уровень информационной безопасности. Политика безопасности и программа безопасности. Вопросы технической безопасности.

4. Техническая безопасность и управление рисками.

5. Классы мер процедурного уровня и принципы, позволяющие обеспечить надежную защиту.

6. Программно-технические меры и сервис безопасности.

7. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность.

8. Протоколирование и аудит, шифрование, контроль целостности их место в общей архитектуре безопасности.

9. Структура Windows NT. Реализация встраивания систем защиты. Защищенные подсистемы. Исполнительная система. Система приоритетов.

10. Структура Windows NT. Реализация встраивания систем защиты. Унифицированная модель драйвера.

11. Структура Windows NT. Реализация встраивания систем защиты. Установка, удаление, запуск и остановка драйвера.

12. Сетевая архитектура Windows NT. Реализация встраивания систем защиты. Сетевые API.

13. Сетевая архитектура Windows NT. Реализация встраивания систем защиты. Сетевые программные компоненты ОС Windows NT.

14. Сетевая архитектура Windows NT. Реализация встраивания систем защиты. Возможности реализации средств защиты сетевой информации на пользовательском уровне.

15. Сетевая архитектура Windows NT. Реализация встраивания систем защиты. Возможности реализации средств защиты сетевой информации на уровне ядра.

16. Механизм идентификации и аутентификации в ОС Windows NT. Процесс Winlogon и библиотека GINA.

17. Обеспечения безопасности программного обеспечения. Угрозы безопасности программного обеспечения. Технологическая и эксплуатационная безопасность программ.

18. Модели угроз безопасности программного обеспечения.

19. Формальные методы доказательства правильности программ и их спецификаций. Прикладное значение доказательства безопасности программных комплексов.

20. Конфиденциальные вычисления. Примитивы, схемы и протоколы. Обобщенные модели для сети синхронно и асинхронно взаимодействующих процессоров.

21. Конфиденциальное вычисление функции. Проверяемые схемы разделения секрета как конфиденциальное вычисление функции. Синхронные и асинхронные конфиденциальные вычисления.

22. Самотестирующиеся и самокорректирующиеся программы. Общие принципы создания двухмодульных вычислительных процедур и методология самотестирования. Области применения.

23. Защита программ и забывающее моделирование на ram-машинах.

24. Методы и средства анализа безопасности программного обеспечения. Контрольно-испытательные методы.

25. Методы и средства анализа безопасности программного обеспечения. Способы тестирования программного обеспечения при испытаниях его на технологическую безопасность.

26. Методы обеспечения надежности программ для контроля их технологической безопасности. Анализ существующих моделей надежности программного обеспечения и оценка уровня технологической безопасности программных комплексов.

27. Подходы к защите разрабатываемых программ от автоматической генерации инструментальными средствами программных закладок.

28. Методы защиты программного обеспечения от исследования. Защита от отладчиков, дизассемблеров, программы просмотра.

29. Методы и средства обеспечения целостности и достоверности используемого программного кода. Методы обнаружения ошибок передачи данных.

30. Основные подходы к защите программ от несанкционированного копирования. Автоматические распаковщики. Пристыковочный механизм защиты программ. Электронные ключи.

31. Механизмы и сервисы безопасности компьютерных сетей. Основные понятия и инфраструктура Открытого Ключа.

32. Безопасное сетевое взаимодействие. Приложения, обеспечивающие безопасность сетевого взаимодействия

33. Безопасное сетевое взаимодействие. Протокол удаленного безопасного входа SSH.

34. Архитектура безопасности для IP. Общие процедуры и форматы пакетов для ведения переговоров об установлении, изменении и удалении SA.

35. Безопасность корпоративных сетей. Особенности корпоративных сетей. Структура управления безопасностью сети. Анализ уровня защищенности.

36. Безопасность корпоративных сетей. Виртуальные частные сети.

37. Внутренние злоумышленники в корпоративных сетях. Методы воздействия.

38. Методы и средства защиты от удаленных атак через сеть Internet.

39. Защита информации в электронных платежных системах.

40. Методы и средства защиты от нелегальной рассылки по электронной почте.

41. Защита вычислительных систем от взлома с использованием руткитных технологий. Аппаратно-программные руткиты.

42. Защита вычислительных систем от взлома с использованием руткитных технологий. Методы защиты BIOS. Распознавание инфицированной BIOS.

43. Защита распределенных баз данных: транзакция, репликация, резервирование и другие особенности по надежности.

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

Паспорт контрольной работы

по дисциплине «Программно-аппаратные средства защиты информации», 5 семестр

1. Методика оценки

Контрольная работа проводится по теме (темам) 3, 4, 5-, включает 10 заданий.

Выполняется устно (письменно) и т.д.

2. Критерии оценки

Каждое задание контрольной работы оценивается в соответствии с приведенными ниже критериями.

Контрольная работа считается **невыполненной,** если если выполнены не все части. Оценка составляет **55** баллов.

Работа выполнена на **пороговом** уровне, если выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы. Оценка составляет **65** баллов.

Работа выполнена на **базовом** уровне, если выполнен в полном объеме, признаки и параметры диагностирования не обоснованы. Оценка составляет **75** баллов.

Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме. Оценка составляет **90** баллов.

3. Шкала оценки

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

4. Пример варианта контрольной работы

1. Модель контроля целостности Кларка-Вилсона.
2. Модель безопасности на основе матрицы доступов HRU.
3. Модель распространения прав доступа TAKE-GRANT.
4. Модель системы безопасности Белла-Лападула.
5. Модель безопасности информационных потоков.
6. Модели нарушителя информационных систем.
7. Модели нарушения целостности программ и данных в электронно-вычислительных машинах.
8. Теория безопасных систем. ТСВ.
9. Политики безопасности. Домены безопасности. Основные типы.
10. Парольная защита Требования и атаки.

11. Криптографические методы защиты. Основные требования, модели, способы и реализации.

12. Асимметричное шифрование. Модели и алгоритмы.

13. Симметричное шифрование. Модели и алгоритмы.

14. Электронно-цифровая подпись. Модели, требования, атаки, способы обмана, реализация ЭЦП.

15. Криптографические атаки на схемы шифрования.

16. Критерии оценки безопасности компьютерных систем министерства обороны США ("Оранжевая книга").

17. Европейские критерии безопасности информационных технологий.

18. Федеральные критерии безопасности информационных технологий.

19. Руководящие документы Государственной Технической Комиссии при Президенте РФ.

20. Защита распределенных баз данных: транзакция, репликация, резервирование и другие особенности по надежности.