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-аппаратное обеспечение информационной безопасности на критически важных объектах

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Курс: 5, семестр : 9

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**9**
1	Всего зачетных единиц (кредитов)	5
2	Всего часов	180
3	Всего занятий в контактной форме, час.	89
4	Лекции, час.	36
5	Практические занятия, час.	36
6	Лабораторные занятия, час.	0
7	из них в активной и интерактивной форме, час.	8
8	Аттестация, час.	2
9	Консультации, час.	15
10	Самостоятельная работа, час.	91
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): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС введен в действие приказом №1509 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): 10.05.03 Информационная безопасность автоматизированных систем

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*: ПСК.31 способность проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов; *в части следующих результатов обучения*:**
з1. знать характеристики основных каналов утечки информации на критически важных объектах
з2. знать способы и средства защиты информации и контроля эффективности защиты информации на критически важных объектах
у1. уметь составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер по технической защите информации на критически важных объектах
***Компетенция ФГОС*: ПСК.32 способность участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов; *в части следующих результатов обучения*:**
з1. знать средства защиты информации, используемые на критически важных объектах
у2. уметь формулировать основные требования к методам и средствам технической защиты информации на критически важных объектах
***Компетенция ФГОС*: ПСК.34 способность разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов; *в части следующих результатов обучения*:**
у1. уметь формировать политики безопасности для критически важных объектов

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-аппаратное обеспечение информационной безопасности на критически важных объектах	
ПСК.31.з1 знать характеристики основных каналов утечки информации на критически важных объектах	
1.характеристики основных технических каналов утечки информации на критически важных объектах;	Лекции; Самостоятельная работа
ПСК.32.з1 знать средства защиты информации, используемые на критически важных объектах	
2.средства защиты информации, используемые на критически важных объектах;	Лекции; Практические занятия; Самостоятельная работа
ПСК.31.з2 знать способы и средства защиты информации и контроля эффективности защиты информации на критически важных объектах	
3.внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов;	Лекции; Практические занятия; Самостоятельная работа
ПСК.31.у1 уметь составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер по технической защите информации на критически важных объектах	
4.всевозможные средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов.	Лекции; Самостоятельная работа
ПСК.32.у2 уметь формулировать основные требования к методам и средствам технической защиты информации на критически важных объектах	

5.восстанавливать работоспособность средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов.	Лекции; Практические занятия
ПСК.34.у1 уметь формировать политики безопасности для критически важных объектов	
6.Определять меры (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для защиты информации в автоматизированных системах.	Лекции; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 9				
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	2	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	2	2	
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. Угрозы безопасности и методы защиты рабочей станции в сети от НСД к информации; Методы и средства хранения ключевой информации	0	2	2	
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	5, 6	
Дидактическая единица: методы и средства хранения ключевой информации				
6. Применение программно-аппаратных средств для идентификации и аутентификации субъектов и хранения ключевой информации	0	4	4	
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	4	1	
8. Интеграция программно-аппаратных средств защиты информации в комплексную систему безопасности автоматизированной системы; Способы встраивания средств защиты в программное обеспечение;	0	3	5	
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	2	
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	1	4	3	Принципы организации и структура систем защиты
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	4	4	
Дидактическая единица: программно-аппаратные средства защиты информации в сетях передачи данных				
12. Программно-аппаратные средства защиты информации в сетях передачи данных	0	4	2, 6	
13. Осуществление оценки защищенности критической информационной инфраструктуры Российской Федерации и ее объектов	0	2	4	

Таблица 3.2

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 9				
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	2	8	2	Студенты изучают методы идентификации и аутентификации субъектов при помощи программно-аппаратного комплекса Secret Net, Аккорд NT/2000
3. Изучение методов защиты локальной ПЭВМ от НСД к информации при помощи программно-аппаратного комплекса при помощи программно-аппаратного комплекса Dallas Lock .	2	10	3	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	2	8	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"	1	10	5	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: 9				
1	РГЗ	2, 4, 6	17	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				
2	Подготовка к занятиям	2	15	0
: 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 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 Минин И. В. Криптографические методы защиты информации : учебно-методическое пособие / И. В. Минин, О. В. Минин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2009. - 31, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000121807				
3	Дополнительная учебная деятельность	1, 2, 3	40	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	Подготовка к аттестации	1, 2, 3	19	9
: Минин И. В. Криптографические методы защиты информации : учебно-методическое пособие / И. В. Минин, О. В. Минин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2009. - 31, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000121807				

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

Таблица 5.2

Активные и интерактивные формы проведения занятий

№	Наименование активных форм
1	Лекция в форме дискуссии
Краткое описание применения: Разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем	
Подробная информация об использовании технологии приводится в "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"	

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	Мин. балл	Максимальный балл
Семестр: 9		
Практические занятия:	15	20
РГЗ:	45	60
Зачет:	15	20
Контролирующие материалы - список вопросов		

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 РГЗ	Зачет	Прочее
ПСК.31	з1. знать характеристики основных каналов утечки информации на критически важных объектах		+	
	з2. знать способы и средства защиты информации и контроля эффективности защиты информации на критически важных объектах		+	

	у1. уметь составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер по технической защите информации на критически важных объектах	+	+	
ПСК.32	з1. знать средства защиты информации, используемые на критически важных объектах		+	
	у2. уметь формулировать основные требования к методам и средствам технической защиты информации на критически важных объектах		+	
ПСК.34	у1. уметь формировать политики безопасности для критически важных объектов			+

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

7. Литература

Основная литература

1. Защита информации в персональных ЭВМ / А. В. Спесивцев [и др.]. - М., 1993. - 191 с.

2. Ищейнов В. Я. Защита конфиденциальной информации : [учебное пособие для вузов по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации"] / В. Я. Ищейнов, М. В. Мецатунян. - М., 2009. - 254 с. : ил., табл.

3. 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.

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. 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. 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

3. 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

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

5. Минин И. В. Криптографические методы защиты информации : учебно-методическое пособие / И. В. Минин, О. В. Минин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2009. - 31, [1] с. : табл.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000121807

6. 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

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)	Презентация материалов

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-аппаратное обеспечение информационной безопасности на критически важных объектах

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Новосибирск 2017

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

Обобщенная структура фонда оценочных средств по **дисциплине** Программно-аппаратное обеспечение информационной безопасности на критически важных объектах 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)**
ПСК.31 способность проводить оценку эффективности средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	з1. знать характеристики основных каналов утечки информации на критически важных объектах	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; Методы защиты от несанкционированного копирования информации, методы защиты программ от изучения, изменения и искажения		Зачет, вопросы...
ПСК.31	з2. знать способы и средства защиты информации и контроля эффективности защиты информации на критически важных объектах	Изучение методов защиты локальной ПЭВМ от НСД к информации при помощи программно-аппаратного комплекса при помощи программно-аппаратного комплекса Dallas Lock . 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		Зачет, вопросы...
ПСК.31	у1. уметь составлять и оформлять акты контрольных проверок, анализировать результаты проверок и разрабатывать предложения по совершенствованию и повышению эффективности применения мер по технической защите информации на критически важных объектах	Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности Применение программно-аппаратных средств для идентификации и аутентификации субъектов и хранения ключевой информации	РГЗ, разделы...	Зачет, вопросы...

ПСК.32 способность участвовать в разработке, осуществлять внедрение и эксплуатацию средств защиты информации, использующихся на критически важных объектах и в автоматизированных системах критически важных объектов	з1. знать средства защиты информации, используемые на критически важных объектах	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 разрушающих программных воздействий Программно-аппаратные средства защиты информации в сетях передачи данных 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; 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		Зачет, вопросы...
ПСК.32	у2. уметь формулировать основные требования к методам и средствам технической защиты информации на критически важных объектах	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; Расширенное применение программно-аппаратных средств защиты информации; Изменения и контроль		Зачет, вопросы...

		целостности, построение изолированной программной среды		
ПСК.34 способность разрабатывать технические регламенты для различных видов деятельности по обеспечению информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	у1. уметь формировать политики безопасности для критически важных объектов	Программно-аппаратные средства защиты информации в сетях передачи данных	Прочее, разделы...	

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 9 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ПСК.31, ПСК.32, ПСК.34.

Зачет проводится в устной (письменной) форме, по билетам (тестам) варианты теста составляются из вопросов, приведенных в паспорте зачета,позволяющих оценить показатели сформированности соответствующих компетенций

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

В 9 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 ПСК.31, ПСК.32, ПСК.34, 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 зачета

по дисциплине «Программно-аппаратное обеспечение информационной безопасности на критически важных объектах», 9 семестр

1. Методика оценки

Зачет проводится в устной (письменной) форме, по билетам (тестам). 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 билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «Программно-аппаратное обеспечение информационной безопасности на критически важных объектах»

---

1. Вопрос 1
2. Вопрос 2.

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

2. Критерии оценки

- Ответ на билет (тест) 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 *40 баллов.*
- Ответ на билет (тест) 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 *55 баллов.*

- Ответ на билет (тест) 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 *75 баллов.*
- Ответ на билет (тест) 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 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 баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. **Вопросы к** зачету **по дисциплине «**Программно-аппаратное обеспечение информационной безопасности на критически важных объектах**»**

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.

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

Паспорт
расчетно-графического задания (работы)

по дисциплине «Программно-аппаратное обеспечение информационной безопасности на критически важных объектах», 9 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны освоить разработку и применение программно-аппаратных средств защиты информации для решения различных задач обеспечения безопасности информации.

При выполнении расчетно-графического задания (работы) студенты должны провести анализ объекта диагностирования, выбрать и обосновать диагностические признаки и параметры, разработать алгоритмы диагностирования, выбрать аппаратные средства.

Обязательные структурные части РГЗ.

Изучение нормативно-методических документов Гостехкомиссии России (ФСТЭК России) по защите информации от несанкционированного доступа. Руководящих документов Гостехкомиссии России "Общие критерии безопасности информационных технологий", положения "О сертификации средств защиты информации по требованиям безопасности информации"

Оцениваемые позиции:

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), отсутствует анализ объекта, диагностические признаки не обоснованы, аппаратные средства не выбраны или не соответствуют современным требованиям, оценка составляет 55 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы, аппаратные средства не соответствуют современным требованиям, оценка составляет 65 баллов.
- Работа считается выполненной **на базовом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны ,но не оптимизированы, аппаратные средства выбраны без достаточного обоснования, оценка составляет 75 баллов.
- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования обоснованы, алгоритмы разработаны и оптимизированы, выбор аппаратных средств обоснован, оценка составляет 90 баллов.

3. Шкала оценки

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

4. **Примерный перечень тем РГЗ(Р)**

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.