

«

»

“ ”

“ ”

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Безопасность операционных систем

: 10.03.01

, :

: 2, : 4

		4
1	()	4
2		144
3	, .	66
4	, .	36
5	, .	0
6	, .	18
7	, .	18
8	, .	2
9	, .	10
10	, .	78
11	(, ,)	.
12		

(): 10.03.01

1515 01.12.2016 . , : 20.12.2016 .

: 1,

(): 10.03.01

, 6 20.06.2017
, 6 20.06.2017

, 6 21.06.2017

:

, . -

:

. . . ,
,

:

. . .

1.

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; <i>в части следующих результатов обучения:</i>	
4.	,
Компетенция ФГОС: ПК.2 способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач; <i>в части следующих результатов обучения:</i>	
2.	,
Компетенция ФГОС: ПК.3 способность администрировать подсистемы информационной безопасности объекта защиты; <i>в части следующих результатов обучения:</i>	
3.	,

2.

2.1

	(
--	---

.1. 4	
1. знать программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей	;
.2. 2	
2. уметь выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах	;
.3. 3	
3. уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	;

3.

3.1

	,	.	
: 4			
:			
1.	0	2	1, 2, 3
2.	0	3	1, 2, 3
3.	0	3	1, 2, 3

4.		0	4	1, 2, 3
5.		0	4	1, 2, 3
6.		0	4	1, 2, 3
7.		0	4	1, 2, 3
8.	UNIX Windows NT.	0	4	1, 2, 3
9.		0	4	1, 2, 3
10.		0	4	1, 2, 3

3.2

: 4				
:				
11. Windows	4	4	1, 2, 3	Windows
12. Windows Script	4	4	1, 2, 3	Windows Script
13.	4	4	1, 2, 3	
14.	6	6	1, 2, 3	

4.

: 4				
1		1, 2, 3	8	1
: 4 / 1: ; [.] . - , 2010. - 35, [1] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768				
2		1, 2, 3	30	5
: 4 / 1: ; [.] . - , 2010. - 35, [1] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768				
3		1, 2, 3	20	0
: 4 / 1: ; [.] . - , 2010. - 35, [1] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768				
4		1, 2, 3	20	4

4 / [] - ; [] - . 1: , 2010. - 35, [1] .: .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768

5.

(. 5.1).

5.1

	-
	e-mail
	e-mail

6.

(),

15-

ECTS.

. 6.1.

6.1

: 4	
<i>Лабораторная:</i>	20
(/) " ; [] - , 2010. - 35, [1] .: .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768"	
<i>Контрольные работы:</i>	20
(/) " ; [] - , 2010. - 35, [1] .: .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768"	
<i>РГЗ:</i>	40
(/) " ; [] - , 2010. - 35, [1] .: .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768"	
<i>Зачет:</i>	20
(/) " ; [] - , 2010. - 35, [1] .: .. - : http://elibrary.nstu.ru/source?bib_id=vtls000146768"	

6.2

6.2

		/	.		
.1	4.	+	+	+	+
.2	2.	+	+	+	+

.3	3.	+	+	+	+
-----------	----	---	---	---	---

1

7.

1. Вихман В. В. Методы и средства защиты компьютерной информации [Электронный ресурс] : электронный учебно-методический комплекс / В. В. Вихман ; Новосиб. гос. техн. ун-т. - Новосибирск, [2011]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000156312. - Загл. с экрана.

1. Раводин О. М. Безопасность операционных систем : учебное пособие / О. М. Раводин, В. О. Раводин ; Томский гос. ун-т систем управления и радиоэлектроники. - Томск, 2005. - 226 с. : ил.

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.

8.1

1. Методы и средства защиты компьютерной информации. Ч. 1 : методические указания к лабораторным работам для 4 курса АВТФ / Новосиб. гос. техн. ун-т ; [сост. Ю. А. Котов]. - Новосибирск, 2010. - 35, [1] с. : ил. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000146768

8.2

1 Windows

2 Office

9.

1	(- , ,)	

--	--	--

1	(
	Internet)	

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

Кафедра вычислительной техники
Кафедра защиты информации

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

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Безопасность операционных систем

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

1. Обобщенная структура фонда оценочных средств учебной дисциплины

Обобщенная структура фонда оценочных средств по дисциплине Безопасность операционных систем 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	з3. знать программные и аппаратные средства защиты информации для типовых операционных систем, систем управления базами данных, компьютерных сетей	Предмет и задачи защиты информации. Основные виды угроз и методы защиты информации Администрирование защиты в условиях дискреционного доступа Защита ОС и оболочка Windows Script Криптографическая защита и аутентификация Криптографическая защита информации. Классификация шифров Назначение и задачи операционных систем. Архитектура ОС. Классификация ОС Организация данных в ОС. Организация файлов в ОС. Файловая система. Многоуровневая модель. Архитектура файловых систем Организация памяти в ОС. Принцип локальности Основные принципы построения и состав ОС. Начальная загрузка ОС. Интерфейсы ОС Параллельные процессы, критические ресурсы и участки. Понятие тупика. Алгоритмы предотвращения и обхода тупиков Подсистема защиты ОС Windows Понятие процесса и его применение в ОС. Система прерываний в ОС Ресурсы ОС Управление заданиями на уровне внешнего планирования в ОС. Алгоритмы внутреннего планирования в ОС Элементы безопасности ОС Windows NT. Элементы безопасности ОС UNIX	Контрольные работы Отчет по лабораторной работе РГЗ, разделы 1-5	Зачет, вопросы 1-10
ПК.2/Э способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы	у2. уметь выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах	Предмет и задачи защиты информации. Основные виды угроз и методы защиты информации Администрирование защиты в условиях дискреционного доступа Защита ОС и оболочка Windows Script Криптографическая защита и аутентификация Криптографическая защита	Контрольные работы Отчет по лабораторной работе РГЗ, разделы 1-5	Зачет, вопросы 11-20

<p>программирования для решения профессиональных задач</p>		<p>информации. Классификация шифров Назначение и задачи операционных систем. Архитектура ОС. Классификация ОС Организация данных в ОС. Организация файлов в ОС. Файловая система. Многоуровневая модель. Архитектура файловых систем Организация памяти в ОС. Принцип локальности Основные принципы построения и состав ОС. Начальная загрузка ОС. Интерфейсы ОС Параллельные процессы, критические ресурсы и участки. Понятие тупика. Алгоритмы предотвращения и обхода тупиков Подсистема защиты ОС Windows Понятие процесса и его применение в ОС. Система прерываний в ОС Ресурсы ОС Управление заданиями на уровне внешнего планирования в ОС. Алгоритмы внутреннего планирования в ОС Элементы безопасности ОС Windows NT. Элементы безопасности ОС UNIX</p>		
<p>ПК.3/Э способность администрировать подсистемы информационной безопасности объекта защиты</p>	<p>уз. уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе</p>	<p>Предмет и задачи защиты информации. Основные виды угроз и методы защиты информации Администрирование защиты в условиях дискреционного доступа Защита ОС и оболочка Windows Script Криптографическая защита и аутентификация Криптографическая защита информации. Классификация шифров Назначение и задачи операционных систем. Архитектура ОС. Классификация ОС Организация данных в ОС. Организация файлов в ОС. Файловая система. Многоуровневая модель. Архитектура файловых систем Организация памяти в ОС. Принцип локальности Основные принципы построения и состав ОС. Начальная загрузка ОС. Интерфейсы ОС Параллельные процессы, критические ресурсы и участки. Понятие тупика. Алгоритмы предотвращения и обхода тупиков Подсистема защиты ОС Windows Понятие процесса и его применение в ОС. Система прерываний в ОС Ресурсы ОС Управление</p>	<p>Контрольная работа Отчет по лабораторной работе РГЗ, разделы 1-5</p>	<p>Зачет, вопросы 20-40</p>

		заданиями на уровне внешнего планирования в ОС. Алгоритмы внутреннего планирования в ОС Элементы безопасности ОС Windows NT. Элементы безопасности ОС UNIX		
--	--	--	--	--

В разделе 2 необходимо дать краткую характеристику мероприятиям текущего и промежуточного контроля, применяемым для оценки компетенций в рамках дисциплины. Далее в ФОС по дисциплине должны быть приведены паспорта тех мероприятий текущего и промежуточного контроля, которые указаны в последних столбцах таблицы с обобщенной структурой ФОС. Если дисциплина многосеместровая, то паспорта должны быть для всех видов промежуточной и текущей аттестации в каждом семестре.

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 4 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ПК.1/Э, ПК.2/Э, ПК.3/Э.

Зачет проводится в устной форме по билетам

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

В 4 семестре обязательным этапом текущей аттестации являются расчетно-графическое задание (работа) (РГЗ(Р)), контрольная работа. Требования к выполнению РГЗ(Р), контрольной работы, состав и правила оценки сформулированы в паспорте РГЗ(Р), контрольной работы.

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

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ПК.1/Э, ПК.2/Э, 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 вычислительной техники
Кафедра защиты информации

Паспорт зачета

по дисциплине «Безопасность операционных систем», 4 семестр

1. Методика оценки

Зачет проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-20, второй вопрос из диапазона вопросов 21-40 (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 «Безопасность операционных систем»

1. Организация файлов в ОС
2. Основные проблемы криптографической защиты и способы их решения.
3. Зашифровать свою фамилию, имя и отчество, используя шифр простой перестановки

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 4 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 10 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 *_15_ 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 *_20 баллов*.

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее *_5_ баллов* (из *_20_* возможных).

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

4. Вопросы и задачи к зачету по дисциплине «Безопасность операционных систем»

1. Назначение и задачи операционных систем (ОС).
2. Классификация ОС.
3. Основные принципы построения и состав ОС.
4. Начальная загрузка ОС.
5. Интерфейсы ОС.
6. Понятие процесса и его применение в ОС.
7. Система прерываний в ОС.
8. Ресурсы ОС.
9. Управление заданиями на уровне внешнего планирования в ОС.
10. Алгоритмы внутреннего планирования в ОС.
11. Параллельные процессы, критические ресурсы и участки.
12. Понятие тупика. Алгоритмы предотвращения и обхода тупиков.
13. Организация памяти в ОС,
14. Принцип локальности.
15. Организация данных в ОС.
16. Организация файлов в ОС.
17. Файловая система. Многоуровневая модель.
18. Архитектура файловых систем.
19. Элементы безопасности ОС Windows NT.
20. Элементы безопасности ОС UNIX.
21. Предмет и задачи защиты информации.
22. Основные виды угроз и методы защиты информации.
23. Криптографическая защита информации. Классификация шифров.
24. Шифры замены.
25. Шифры перестановки.
26. Шифр гаммирования.
27. Шифр DES.
28. Шифр ГОСТ.

29. Криптосистемы с открытым ключем. Принцип Шеннона. Основные особенности и характеристики.
30. Шифр RSA.
31. Шифр Эль Гаммала.
32. Основные проблемы криптографической защиты и способы их решения.
33. Методы идентификации/аутентификации, назначение и особенности.
34. Стандартные методы идентификации и аутентификации.
35. Доказательство с нулевой передачей знаний.
36. Электронная цифровая подпись.
37. Антивирусные программы и межсетевые экраны.
38. Методы доступа – основные виды и способы реализации.
39. Протоколирование и аудит.
40. Меры защищенности информационных систем.

ЗАДАЧИ К ЗАЧЕТУ

1. Зашифровать свою фамилию, имя и отчество, используя шифр простой перестановки.
2. Зашифровать свою фамилию, имя и отчество, используя шифр одиночной перестановки по ключу. В качестве ключа взять свое имя.
3. Зашифровать свою фамилию, имя и отчество, используя шифр двойной перестановки по ключу. В качестве ключей взять свое имя и отчество.
4. Зашифровать свою фамилию, имя и отчество, используя «полибианский» квадрат, составленный на основе алфавита включенных в ФИО букв.
5. Зашифровать свою фамилию, имя и отчество, используя произвольную перестановку по таблице.
6. Зашифровать свою фамилию, имя и отчество, используя шифр Гронсфельда. В качестве ключа использовать свое имя.
7. Зашифровать свою фамилию, имя и отчество, используя шифр Виженера. В качестве алфавита взять буквы, включенные в ФИО, а в качестве ключа использовать свое отчество.
8. Определить длину ключа в каждом случае: 0101 0101 0101 0101, 0000 0000 0000 0000, FEFE FEFE FEFE FEFE. Ключи даны в 16-ричной системе.
9. Для метода RSA и $p=3$, $q=5$ сформировать ключи «d» и «e».
10. Зашифровать открытый текст 1101011001101010110101 методом гаммирования, используя ключ 1011101011. Исходная информация и ключ даны в двоичной системе.
11. Зашифровать открытый текст 1101011001101010110101 методом гаммирования с обратной связью, используя ключ 1011101011 и блок длиной 4 бита. Исходная информация и ключ даны в двоичной системе.
12. Определить, сколько различных электронных документов можно представить с помощью хэш-значения длиной 16 бит.

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

Паспорт контрольной работы

по дисциплине «Безопасность операционных систем», 4 семестр

1. Методика оценки

Контрольная работа проводится по теме Безопасность ОС включает 10 заданий.

Выполняется письменно.

2. Критерии оценки

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

Контрольная работа считается **невыполненной**, если Оценка составляет **_4_** баллов.

Работа выполнена на **пороговом** уровне, если. Оценка составляет **_5_** баллов.

Работа выполнена на **базовом** уровне, если Оценка составляет **__10__** баллов.

Работа считается выполненной **на продвинутом** уровне, если Оценка составляет **20** 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

Паспорт расчетно-графического задания (работы)

по дисциплине «Безопасность операционных систем», 4 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны рассчитать параметры элементов защиты операционной системы.

При выполнении расчетно-графического задания (работы) студенты должны провести анализ объекта, выбрать и обосновать способы НСД, разработать процедуру НСД, выбрать программные средства.

Обязательные структурные части РГЗ: постановка задачи, описание уязвимости, процедуры НСД.

Оцениваемые позиции: полнота анализа уязвимости и оригинальность НСД:

2. Критерии оценки

- Работа считается **не выполненной**, если выполнены не все части РГЗ(Р), отсутствует анализ объекта, не обоснованы способы НСД, программные средства не выбраны или не соответствуют современным требованиям, оценка составляет 10 баллов.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ объекта выполнен без декомпозиции, диагностические признаки недостаточно обоснованы, программные средства не соответствуют современным требованиям, оценка составляет 20 баллов.
- Работа считается выполненной **на базовом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры диагностирования уязвимости обоснованы, процедуры НСД разработаны, но не оптимизированы, программные средства выбраны без достаточного обоснования, оценка составляет 30 баллов.
- Работа считается выполненной **на продвинутом** уровне, если анализ объекта выполнен в полном объеме, признаки и параметры уязвимости обоснованы, процедуры НСД разработаны и реализованы, выбор программных средств обоснован, оценка составляет 40 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)

Обход пароля учетной записи Windows с помощью программы Kon Boot
Вскрытие пароля учетной записи Windows с помощью программы Ophcrack
Повышение прав пользователя Windows с использованием системного реестра
Блокирование сайтов и обход системы блокировки в ОС Windows
Блокирование USB портов и обход блокировки в ОС Windows
Сброс пароля администратора ОС Windows и создание нового администратора без использования дополнительных программ

Включение изначально скрытой учётной записи «Администратор» в ОС Windows
Вскрытие пароля локального администратора компьютера под управлением ОС Windows7
Изменение прав пользователя в ОС Windows
Сброс пароля администратора в ОС Windows и создание нового администратора
Получение логина и пароля удаленного компьютера
Перехват логина и пароля по протоколу Telnet в локальной сети
Организация скрытого входа в ОС Windows (подмена процессов)
Получение несанкционированного доступа в ОС Windows