

«

»

“ ”

“ ”

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Международные и российские стандарты и нормативные акты по информационной безопасности

: 10.05.03

, :

: 4, : 7

		7
1	()	4
2		144
3	, .	84
4	, .	36
5	, .	36
6	, .	0
7	, .	18
8	, .	2
9	, .	10
10	, .	60
11	(, ,)	
12		

(): 10.05.03

1509 01.12.2016 ., : 20.12.2016 .

: 1,

(): 10.05.03

, 6 20.06.2017

, 6 21.06.2017

:

, . . .

:

. . . ,

:

. . .

1.

1.1

Компетенция ФГОС: ОПК.6 способность применять нормативные правовые акты в профессиональной деятельности; в части следующих результатов обучения:	
1.	-
Компетенция ФГОС: ПК.1 способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке; в части следующих результатов обучения:	
3.	
Компетенция ФГОС: ПК.16 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации; в части следующих результатов обучения:	
3.	,
Компетенция ФГОС: ПК.21 способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем; в части следующих результатов обучения:	
2.	
Компетенция ФГОС: ПК.7 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ; в части следующих результатов обучения:	
1.	-
Компетенция ФГОС: ПК.9 способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности; в части следующих результатов обучения:	
1.	-

2.

2.1

()
---	---

.1. 3	
1.знать основные источники получения нормативных и методических материалов	; ;
.6. 1 -	
2.уметь осуществлять реализацию нормативно-правовых актов в сфере профессиональной деятельности	; ;
.7. 1 -	
3.знать нормативно-методические документы по оформлению и содержанию научно-технической документации, отчетов, публикации	; ;
.9. 1 -	
4.уметь применять нормативно-методическую базу по разработке защищенных автоматизированных систем	; ;

.16. 3		,
5.знать организацию работы, нормативные правовые акты и стандарты по аттестации объектов информатизации		; ;
.21. 2		
6.знать правила аттестации автоматизированных систем с учетом нормативных требований по защите информации		;

3.

3.1

: 7				
:				
1.	0	4	1, 3, 5	
:				
2.	0	4	1, 2, 3, 5	
:				
3.	0	2	1, 3, 4, 5	
:				
4.	0	2	1, 2, 3, 4, 5	
: ISO27000.				
5.	0	8	1, 3, 4, 5	
: ISO15408 (Common Criteria)				
/ 15408				

6.	ISO15408 (Common Criteria) / 15408	0	4	1, 2, 3, 5	ISO15408 (Common Criteria) / 15408
: NIST. NIST SP 800-60.					
7.	NIST. NIST SP 800-60. ISO 27000	0	4	1, 3, 5	
:					
8.		0	2	1, 2, 4, 5	
:					
9.	-	0	2	1, 3, 4, 5	
: , . SOX, Basel II, HIPAA					
10.	, . SOX, Basel II, HIPAA	0	4	1, 5, 6	

3.2

		,	.		
: 7					
: ISO27000.					
1.	/ ISO27001	6	10	2, 3, 4, 5	/ ISO27001
: ISO15408 (Common Criteria) / 15408					
2.	ISO 27000	6	8	2, 3, 4, 5	ISO 27000
: NIST. NIST SP 800-60.					
3.	-	2	8	2, 3, 4, 5, 6	-
:					
4.		4	10	1, 2, 3, 4, 5	

4.

: 7				

1		2, 3, 4	20	4
<p>3 : . . . / . . . ; . . . - . - , 2016. - 29, [4] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000234013</p>				
2		1, 3, 5	10	0
<p>1 : . . . / . . . ; . . . - . - , 2016. - 29, [4] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000234013</p>				
3		1, 2, 3, 4	30	6
<p>2 : . . . / . . . ; . . . - . - , 2016. - 29, [4] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000234013</p>				

5.

- , (. 5.1).

5.1

	-
	e-mail
	e-mail;

6.

(),

- 15- ECTS.

. 6.1.

6.1

: 7	
<i>Дополнительная учебная деятельность:</i>	
<i>Практические занятия:</i>	30
<i>РГЗ:</i>	30
<p>- / . . . ; . . . - . - , 2016. - 29, [4] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000234013</p>	
<i>Экзамен:</i>	40
<p>() " . . . - . - , 2016. - 29, [4] . : .. - : http://elibrary.nstu.ru/source?bib_id=vtls000234013</p>	

.6	1.	-	+ +
.1	3.		+ +
.16	3.	,	+ +
.21	2.		+ +
.7	1.	- , ,	+ +
.9	1.	-	+ +

1

7.

1. Галатенко В. А. Стандарты информационной безопасности : курс лекций : учебное пособие для студентов вузов, обучающихся по специальностям в области информационных технологий / В. А. Галатенко ; под ред. В. Б. Бетелина. - М., 2006. - 262, [1] с. : табл.

2. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности / Федер. агентство по техн. регулированию и метрологии. - М., 2010. - IV, 35 с. : табл.

1. Грибков Д. О формировании системы международной информационной безопасности / Д. Грибков // Международная жизнь. - 2015. - № 8. - С. 86-92.

2. Курило А. П. О новой редакции Стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы. Общие положения" / А. П. Курило // Деньги и кредит. - 2009. - № 2. - С. 3-7.

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. Моделирование и прогнозирование количества инцидентов в системе информационной безопасности при помощи динамической модели : методические указания к выполнению лабораторных работ по специальностям 090105 - Комплексное обеспечение информационной безопасности автоматизированных систем и 090104 - Комплексная защита объектов информатизации / Новосиб. гос. техн. ун-т ; [сост.: А. Ж. Абденов, Р. Н. Заркумова]. - Новосибирск, 2012. - 26 с. : табл., ил.. - Режим доступа:
http://elibrary.nstu.ru/source?bib_id=vtls000173267

2. Дронов В. Ю. Международные и отечественные стандарты по информационной безопасности : учебно-методическое пособие / В. Ю. Дронов ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 29, [4] с. : ил.. - Режим доступа:
http://elibrary.nstu.ru/source?bib_id=vtls000234013

8.2

1 Windows

2 Office

9.

-

1	(-) , ,	

1. Обобщенная структура фонда оценочных средств учебной дисциплины

Обобщенная структура фонда оценочных средств по дисциплине Международные и российские стандарты и нормативные акты по информационной безопасности приведена в Таблице.

Таблица

Формируемые компетенции	Показатели сформированности компетенций (знания, умения, навыки)	Темы	Этапы оценки компетенций	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	Промежуточная аттестация (экзамен, зачет)
ОПК.6 способность применять нормативные правовые акты в профессиональной деятельности	у1. уметь осуществлять реализацию нормативно-правовых актов в сфере профессиональной деятельности	Международные и российские законодательные акты и стандарты, требования регуляторов, отраслевые требования, требования бизнеса. Перечень организационно-технических требований к системе ИБ. Перечень не применимости.	РГР, разделы 1.1, 1.2, 1.3	Экзамен, Вопросы 1.1 – 1.10, 2.1 – 2.10, 3.1 – 3.10
ПК.1/НИ способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	з3. знать основные источники получения нормативных и методических материалов	Законодательство в области информационных технологий и защиты информации. Международные и отечественные стандарты в сфере ИБ. Требования регуляторов. Отраслевые требования.	РГР, разделы 1.1, 1.2, 1.3	Экзамен, Вопросы 1.1 – 1.10, 2.1 – 2.10, 3.1 – 3.10
ПК.16/КА способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	з3. знать организацию работы, нормативные правовые акты и стандарты в области защиты информации	Семейство международных стандартов ISO/IEC 27000 и их отечественные аналоги. Стандарт кибербезопасности ISO/IEC 27032. Стандарт ISO/IEC 15408 (Common Criteria) и его отечественный аналог. Семейство стандартов NIST SP 800. Стандарты по управлению рисками, жизненным циклом систем. Стандарты и положения кредитно-финансовых организация, предприятий энергетики. Стандарты и законодательные акты, влияющие на требования ИБ. SOX, Basel II, HIPAA.	РГР, разделы 1.1, 1.2, 1.3	Экзамен, Вопросы 1.1 – 1.10, 2.1 – 2.10, 3.1 – 3.10
ПК.21/ОУ способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной	з2. знать принципы использования требований законодательства, стандартов, регуляторов при построении СУИБ организации	Классификация и категорирование информационных ресурсов. Разработка организационно-технических требований СУИБ организации.	РГР, разделы 1.1, 1.2, 1.3	Экзамен, Вопросы 1.1 – 1.10, 2.1 – 2.10, 3.1 – 3.10

безопасности автоматизированных систем				
ПК.7/НИ способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	з1. знать нормативно-методические документы по разработке внутренних документов организации в сфере защиты информации	Классификация и категорирование информационных ресурсов. Разработка организационно-технических требований СУИБ организации. Перечень организационно-технических требований к системе ИБ. Перечень не применимости.	РГР, разделы 1.1, 1.2, 1.3	Экзамен, Вопросы 1.1 – 1.10, 2.1 – 2.10, 3.1 – 3.10
ПК.9/ПК способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	у1. уметь применять нормативно-методическую базу по разработке защищенных автоматизированных систем	Классификация и категорирование информационных ресурсов. Разработка организационно-технических требований СУИБ организации. Перечень организационно-технических требований к системе ИБ. Перечень не применимости.	РГР, разделы 1.1, 1.2, 1.3	Экзамен, Вопросы 1.1 – 1.10, 2.1 – 2.10, 3.1 – 3.10

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 7 семестре - в форме экзамена, который направлен на оценку сформированности компетенций ОПК.6, ПК.1/НИ, ПК.16/КА, ПК.21/ОУ, ПК.7/НИ, ПК.9/ПК.

Экзамен проводится по форме, приведенной в соответствующем паспорте.

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

В 7 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 дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОПК.6, ПК.1/НИ, ПК.16/КА, ПК.21/ОУ, ПК.7/НИ, ПК.9/ПК, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Теоретическое содержание курса освоено частично, пробелы носят существенный характер, уровень выполнения работы не отвечает большинству основных требований, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, предусмотренное программой обучения учебное задание не выполнено.

Пороговый. Теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, уровень выполнения работы отвечает большинству основных требований, необходимые практические навыки работы с освоенным материалом в основном сформированы.

Базовый. Теоретическое содержание курса освоено полностью, без пробелов, уровень выполнения работы отвечает всем основным требованиям, 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. Теоретическое содержание курса освоено полностью, без пробелов, уровень выполнения работы отвечает всем требованиям, 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 «Международные и российские стандарты и нормативные акты по
информационной безопасности», 7 семестр

1. Методика оценки

Экзамен проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1, второй вопрос из диапазона вопросов 2, третий вопрос выбирается из диапазона вопросов 3 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня вопросов (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____

к экзамену по дисциплине «Международные и российские стандарты и нормативные
акты по информационной безопасности»

1. Вопрос 1.
2. Вопрос 2.
3. Вопрос 3.

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

(дата)

2. Критерии оценки

- Ответ на экзаменационный билет считается **неудовлетворительным**, если студент при ответе на вопросы не показывает знаний стандартов.
Оценка составляет 0 баллов.
- Ответ на экзаменационный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы показывает знание отдельных международных и российских стандартов, законодательных актов РФ в области ИБ, но не способен предложить методы решения проблем ИБ на основе стандартов.
Оценка составляет 30 баллов.
- Ответ на экзаменационный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы показывает знание международных и российских стандартов, законодательных актов РФ в области ИБ, предлагает методы решения проблем ИБ на основе стандартов, но не способен обосновать свой выбор.
Оценка составляет 50 баллов.
- Ответ на экзаменационный билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы показывает знания широкого спектра международных

и российских стандартов, законодательных актов РФ в области ИБ, проводит сравнительный анализ подходов в стандартах разных семейств, предлагает методы решения проблем ИБ на основе стандартов и способен обосновать свой выбор. Оценка составляет 70 баллов.

3. Шкала оценки

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 «Международные и российские стандарты и нормативные акты по информационной безопасности»

Диапазон 1.

1. Семейство стандартов NIST SP 800. Состав, положения, использование
2. Семейство стандартов ISO 27000. Состав, положения, использование
3. Стандарт ISO/IEC 15408 (Common Criteria). Состав, положения, использование
4. Информационные ресурсы. Активы и их. Положения стандарта ISO/IEC 13335
5. Стандарт платежных банковских карт PCI DSS
6. Положения стандарта Банка России СТО БР ИББС-1.0
7. Персональные данные. Международные и российские законодательные акты
8. Стандарт по управлению рисками ИБ
9. Стандарты по управлению жизненным циклом систем
10. Стандарты по ИБ для систем АСУ ТП

Диапазон 2.

1. Положения стандарта ISO27001
2. Положения стандарта ISO27002
3. Положения стандарта ISO27032
4. Стандарты NIST SP 800. Требования к системе ИБ
5. Роль информационной безопасности (на основе ГОСТ 15408)
6. Стандарты в области обработки рисков
7. Законы РФ №149 "Об информации, информационных технологиях и защите информации", №152 "О персональных данных", №98 "О коммерческой тайне",
8. Закон РФ №63 "Об электронной подписи", законодательные акты в области криптографии
9. Категорирование информационных ресурсов. Нормативные документы
10. Классификация информационных ресурсов. Нормативные документы

Диапазон 3.

1. Свойства информации - соответствие и подотчетность
2. Свойства информации - неотказуемость и аутентичность
3. Свойства информации - целостность и доступность
4. Свойства информации - полезность и эффективность
5. Свойства информации - конфиденциальность и надежность
6. Что такое информационные ресурсы
7. Стратегическая задача ИБ
8. Требования к ИБ SOX
9. Требования к ИБ Basel II
10. Требования к ИБ HIPAA

Паспорт расчетно-графического задания (работы)

по дисциплине «Международные и российские стандарты и нормативные акты по
информационной безопасности», 7 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны разработать документ (политику информационной безопасности второго уровня), содержащий перечень организационно-технических требований по информационной безопасности (далее - ОТТ) одной из данных преподавателем организации.

При выполнении расчетно-графического задания (работы) студенты должны провести анализ действующих международных и отечественных стандартов в области информационной безопасности, применительно к предоставленной преподавателем организации, выбрать и зафиксировать в документе (политике информационной безопасности) набор ОТТ, сформировать перечень неприменимости.

Обязательные структурные части РГЗ.

1. Политика информационной безопасности, определяющая организационно-технические требования обеспечения безопасности информационных ресурсов.
2. Перечень неприменимости ОТТ.
3. Перечень использованных стандартов.

Оцениваемые позиции:

1. Перечень выбранных ОТТ (применительно к предложенной организации).
2. Документ "Политика безопасности, определяющая организационно-технические требования обеспечения безопасности информационных ресурсов".
3. Перечень неприменимости.
4. Перечень используемых международных и отечественных стандартов по ИБ.

2. Критерии оценки

- Работа считается **не выполненной**, если выполнены не все части РГЗ(Р), отсутствует анализ ОТТ, применяемые/неприменяемые меры не обоснованы.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: анализ ОТТ выполнен не в полном объеме, обязательность применения/неприменения ОТТ недостаточно обоснована, перечень использованных стандартов ограничен одним, политика и перечень неприменимости сделаны формально, оценка составляет 10 баллов.
- Работа считается выполненной **на базовом** уровне, если анализ ОТТ выполнен в полном объеме, но применяемые и неприменяемые ОТТ не достаточно обоснованы, перечень использованных стандартов ограничен одним-двумя, политика и перечень неприменимости сделаны с недочетами, оценка составляет 20 баллов.
- Работа считается выполненной **на продвинутом** уровне, если анализ ОТТ выполнен в полном объеме, применяемые и неприменяемые ОТТ обоснованы, перечень использования стандартов включает более двух, политика и перечень неприменимости сделаны в полном объеме, оценка составляет 30 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)

На основе стандартов ISO 27000 и NIST SP 800 разработать и документировать в текстовом редакторе "Политику безопасности, определяющую организационно-технические требования обеспечения безопасности информационных ресурсов" для одной из нижеприведенных компаний.

Вариант I. Крупное авиастроительное предприятие.

Вариант II. Среднее машиностроительное предприятие.

Вариант III. Государственная организация.

Вариант IV. Небольшое частное предприятие.