МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(РГГУ)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности
Кафедра информационной безопасности

СПЕЦИАЛЬНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ И СТАНДАРТЫ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

По направлению подготовки 10.03.01 «Информационная безопасность»
профиль «Организация и технология защиты информации»
Уровень квалификации выпускника (*бакалавр*)

Форма обучения (*очная*)

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2017

Специальные нормативные документы и стандарты по информационной безопасности
Рабочая программа дисциплины
Составитель:
д.т.н, профессор В.В. Арутюнов

Ответственный редактор
к.и.н., доцент, заведующая кафедрой
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры информационной безопасности
№ 5 от 24.01.2017 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля): формирование у обучающихся знаний об отечественных и зарубежных нормативных актах, стандартах и нормативных документах-регуляторов в области обеспечения безопасности информационных систем и сетей.

Задачи дисциплины:

- рассмотреть задачи нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности, структуру и содержание системы нормативного обеспечения безопасности;

- раскрыть вопросы нормативного регулирования развития терминологии в области обеспечения безопасности информационных систем и сетей, нормативного регулирования технической и криптографической защиты информации;

- рассмотреть и освоить обучающимися стандарты в области обеспечения функциональной безопасности информационных систем и сетей, управления информационной безопасностью.

1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине *(модулю)*:

Коды компе--тенции	**Содержание компетенций**	**Перечень планируемых результатов обучения по дисциплине**
ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	Знать: основные нормативно-правовые документы в профессиональной деятельности; Уметь: пользоваться нормативно-правовыми документами; Владеть: навыками работы с нормативно-правовыми документами
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Знать: базовые международные и российские регуляторы по информационной безопасности; Уметь: работать со стандартами и нормативными документами; Владеть: навыками использования международных и национальных стандартов в своей профессиональной деятельности
ПК-10	способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Знать: основные документы, выпускаемые регуляторами по информационной безопасности; Уметь: работать со стандартами и нормативными документами; Владеть: навыками использования международных и национальных стандартов в своей профессиональной деятельности
ПСК-2.4	способность организовать контроль защищенности объекта информатизации в соответствии с	Знать: основные документы, выпускаемые регуляторами по информационной безопасности; Уметь: пользоваться мерами нормативно-правовой поддержки регулирования вопросов защиты

	нормативными документами	информации в РФ; Владеть: навыками обоснования и принятия решений по применению специальных нормативных документов и стандартов в области информационной безопасности

1.3. Место дисциплины (модуля) в структуре основной образовательной программы

Дисциплина (модуль) «Специальные нормативные документы и стандарты по информационной безопасности» относится к базовой части блока дисциплин учебного плана.

Для освоения дисциплины (модуля) необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: Основы информационной безопасности, Правовое обеспечение информационной безопасности, Экономика защиты информации.

В результате освоения дисциплины (модуля) формируются знания, умения и владения, необходимые для прохождения преддипломной практики и подготовки и защиты ВКР и дисциплин: Комплексное обеспечение безопасности объекта информатизации. Управление службой защиты информации, а также Аудит информационной безопасности.

2. Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 4 з. е., 144 ч., в том числе контактная работа обучающихся с преподавателем 56 ч., самостоятельная работа обучающихся 70 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Основы технического регулирования и стандартизации в Российской Федерации	7	6		4			14	опрос
2	Национальные и международные стандарты в области информационной безопасности	7	6		8			20	опрос
3	Национальные стандарты Российской Федерации в области информационной	7	10		6			22	опрос, контрольная работа 1

	безопасности								
4	Нормативные документы ФСТЭК России	7	10		4			14	опрос, контрольная работа 2
5	Экзамен	7					18		Экзамен по билетам
	Итого		**32**		**24**		**18**	**70**	

3. Содержание дисциплины (модуля)

Тема 1. Основы технического регулирования и стандартизации в Российской Федерации

Предмет и содержание дисциплины, методы изучения, основная литература, контроль освоения дисциплины. Основные термины в области защиты информации.

Основная задача стандартов в сфере информационной безопасности. Категории сторон, заинтересованных в создании и развитии стандартов в сфере информационной безопасности.

Федеральный закон Российской Федерации "О техническом регулировании". Правила разработки национальных стандартов (ГОСТ Р 1.2-2014).

Тема 2. Национальные и международные стандарты в области информационной безопасности

Основные базовые требования к безопасности, впервые сформулированные в "Оранжевой книге".

Международный стандарт ISO/IEC 15408-99 («Общие критерии»).

Национальный стандарт ГОСТ Р ИСО/МЭК 15408—2002 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

Международная серия стандартов ISO/IEC 27000.

Национальный стандарт по менеджменту инцидентов информационной безопасности ГОСТ Р ИСО/МЭК ТО 184044-2007.

Тема 3. Национальные стандарты Российской Федерации в области информационной безопасности

Национальный стандарт ГОСТ Р ИСО/МЭК 15408-1-2012. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-2-2012. Национальный стандарт ГОСТ Р ИСО/МЭК 15408-3-2012.

Национальные стандарты серии ГОСТ Р 34.10 для криптографической защиты систем обработки информации.

Национальные стандарты по биометрической аутентификации серий ГОСТ Р ИСО/МЭК 19784 и ГОСТ Р 52633.

Национальные стандарты в сфере управления информационной безопасностью серии ГОСТ Р ИСО/МЭК 27000.

Тема 4. Нормативные документы ФСТЭК России

Защита от НСД - несанкционированного доступа к информации: термины и определения. Концепция защиты средств вычислительной техники (СВТ) и автоматизированных систем от НСД к информации.

Классификация автоматизированных систем и требования по защите информации.

Показатели защищённости межсетевых экранов от НСД.

Классификация межсетевых экранов по уровню защищённости от несанкционированного доступа к информации.

Контроль отсутствия недекларированных возможностей в программном обеспечении.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебной работы	Информационные и образовательные технологии
1	**2**	**3**	**5**
1.	Основы технического регулирования и стандартизации в Российской Федерации	Лекция 1 Семинар 1	Вводная лекция с использованием видеопроектора Опрос
2.	Национальные и международные стандарты в области информационной безопасности	Лекция 2 Семинар 2	Лекция с использованием видеопроектора опрос
3.	Национальные стандарты Российской Федерации в области информационной безопасности	Лекция 3 Семинар 3	Лекция с использованием видеопроектора опрос
4.	Нормативные документы ФСТЭК России	Лекция 4 Семинар 4 Контрольная работа 2	Лекция с использованием видеопроектора Опрос Подготовка к контрольной с использованием материалов лекций и литературы

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос* *- контрольная работа (темы 3-4)*	 *10 баллов* *20 баллов*	 *40 баллов* *20 баллов*
Промежуточная аттестация *(традиционная форма)*		*40 баллов*
Итого за семестр *экзамен*		*100 баллов*

Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины представляется в виде таблицы:

№ п/п	***Контролируемые разделы дисциплины***	***Код контролируемой компетенции***	***Наименование оценочного средства***
1.	1	ПК-5, ОПК-5	План практического занятия
2.	2	ПК-10, ПСК-2.4	План практического занятия
3.	3	ОПК-5, ПК-5	План практического занятия
4.	4	ПК-10, ПСК-2.4	План практического занятия Контрольная работа

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	отлично	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	хорошо	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D, E	удовлетворительно	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине.

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
		Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F, FX	неудовлетворительно	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине *(модулю)*

Текущий контроль (вариант опросного задания)

Вопросы	***Реализуемая компетенция***
1. Базовые органы - генераторы правовых документов в сфере ИБ в России на федеральном уровне	***ОПК-5***
2. Основные категории сторон, заинтересованные в создании и развитии национальных стандартов в сфере информационной безопасности.	***ПК-5***
3. Базовые задачи стандартов в сфере информационной безопасности.	***ПК-10***
4. Объекты информатизации, аттестуемые по требованиям безопасности информации.	***ПСК-2.4***

Примерная тематика контрольной работы - проверка сформированности компетенций ОПК-5, ПК-5, ПК-10, ПСК-2.4

1. Классификация стандартов ИБ.
2. Базовые нормативные документы по техническому регулированию и стандартизации в РФ.
3. Классификация источников норм в стандартизации.
4. Базовые категории сторон, заинтересованные в создании и развитии национальных стандартов в сфере информационной безопасности.
5. Основные группы классификация автоматизированных систем в соответствии с требованиями по защите информации.
6. Базовые этапы разработки национальных стандартов в РФ.
7. Классификация МЭ по уровню контроля отсутствия незадекларированных возможностей.
8. Структура системы стандартов по защите информации.

Промежуточная аттестация (примерные контрольные вопросы по курсу) - проверка сформированности компетенций ОПК-5, ПК-5, ПК-10, ПСК-2.4

1. Основные федеральные органы РФ, формирующие нормативно-правовые документы в области информационной безопасности.
2. Содержание ФЗ "О техническом регулировании".
3. Основные принципы стандартизации в России.
4. Базовые объекты стандартизации в России.
5. Основные правила разработки национальных стандартов в России.
6. Структура стандартов России в области защиты информации.
7. Основные задачи системы стандартизации в России в области защиты информации.
8. Порядок разработки и утверждения стандартов организаций.
9. Базовые этапы разработки стандарта в России.
10. Краткая характеристика международных стандартов серии ISO/IEC 27000.
11. Базовые национальные стандарты России для криптографической защиты систем обработки информации.
12. Классификация автоматизированных систем в соответствии с требованиями по защите информации.
13. Классификация СВТ в соответствии с требованиями по защите информации.
14. Основные требования по защите, предъявляемые к межсетевым экранам.
15. Классификация программного обеспечения по уровню контроля отсутствия недекларированных возможностей.

16. Классификация межсетевых экранов по уровню защищённости от несанкционированного доступа к информации.

17. Основные уровни контроля отсутствия НДВ в программном обеспечении, установленные в РД ФСТЭК России.

18. Основные классы защищенности, установленные для средств антивирусной защиты.

19. Базовые классы защищенности, установленные для средств обнаружения вторжений.

20. Основные классы защищенности, установленные для средств контроля съемных машинных носителей информации.

21. Основные положения документа «Политика информационной безопасности».

22. Этапы работ по защите от угроз, использующих скрытые каналы.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

а) источники:

1. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ // СЗ РФ 31.07.2006, N 31 (1 ч.). - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон Российской Федерации от 27.12.2002 г. № 184-ФЗ «О техническом регулировании». «Собрание законодательства РФ», 30.12.2002, № 52 (ч.1), ст. 5140. - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_40241/

б) основная литература:

1. Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info

дополнительная:

1.Кузнецов И.Н., Бизнес-безопасность. - М.: Дашков и К, 2016. - 416 с. - Режим доступа: URL: http://znanium.com/catalog/product/430343

6.2. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru

2. Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/

3. Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru

4. Национальный открытый университет ИНТУИТ - Режим доступа: URL: http://www.intuit.ru

6.3.Перечень БД и ИСС

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен Microsoft Office 2010, включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

Перечень ПО

№ п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 7 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

- письменные задания оформляются увеличенным шрифтом;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

- письменные задания выполняются на компьютере в письменной форме;

- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;
  - принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

  - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

  - передвижными, регулируемыми эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий - *проверка сформированности компетенций ПК-5, ОПК-5, ПК-10, ПСК-2.4*

Планы практических занятий

Практическое занятие 1. (Тема 1). Содержание Федерального закона Российской Федерации "О техническом регулировании" - **(2 часа)** - ***проверка сформированности компетенций ПК-5, ОПК-5***

Вопросы для изучения и обсуждения:

1. Базовые органы - генераторы в России на федеральном уровне правовых документов в сфере ИБ.

2. Цели Федерального закона Российской Федерации "О техническом регулировании".

3. Основные документы в области стандартизации, действующие на территории Российской Федерации после ввода в действие ФЗ "О техническом регулировании".

4. Базовые принципы технического регулирования в России.

Контрольные вопросы:

1. Сущность стандарта и технического регламента.
2. Какие вопросы регулируются ФЗ "О техническом регулировании"?
3. Цели принятия технических регламентов.
4. Порядок разработки и утверждения национальных стандартов.

Список литературы

Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ // СЗ РФ 31.07.2006, N 31 (1 ч.). - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_61798/

Федеральный закон Российской Федерации от 27.12.2002 г. № 184-ФЗ «О техническом регулировании». «Собрание законодательства РФ», 30.12.2002, № 52 (ч.1), ст. 5140. - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_40241/

Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info

Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru

Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/

Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru

Национальный открытый университет ИНТУИТ - Режим доступа: URL: http://www.intuit.ru

Практическое занятие 2. (Тема 2). Международная серия стандартов ISO/IEC 27000 - **(8 часов)** - ***проверка сформированности компетенций - ПК-10, ПСК-2.4***

Вопросы для изучения и обсуждения:

1. Основные причины подготовки и выпуска стандартов серии ISO/IEC 2700.
2. Категории пользователей стандартов серии ISO/IEC 2700.

3. Сферы информационной безопасности, в которой действуют стандарты серии ISO/IEC 27000.

4. Основные кластеры стандартов, выделяемые во множестве стандартов серии ISO/IEC 27000.

5. Национальные стандарты России, гармонизированные со стандартами серии ISO/IEC 27000.

6. Основные разработчики стандартов серии ISO/IEC 27000.

Контрольные вопросы:

1. Какие первые стандарты в сфере ИБ были приняты в мире?
2. По каким признакам классифицируются стандарты серии ISO/IEC 27000?
3. В каком стандарте и каким образом определяется система менеджмента информационной безопасности (СМИБ)?
4. Основные принципы успешной реализации СМИБ.
5. В чём суть процессного подхода для СМИБ «План — Осуществление — Проверка — Действие»?
6. Основные действия организации для разработки СМИБ.

Список литературы

Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info

Кузнецов И.Н., Бизнес-безопасность. - М.: Дашков и К, 2016. - 416 с. - Режим доступа: URL: http://znanium.com/catalog/product/430343

Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru

Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/

Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru

Национальный открытый университет ИНТУИТ - Режим доступа: URL: http://www.intuit.ru

Практическое занятие 3. (Тема 3). Национальные стандарты по биометрической аутентификации серии ГОСТ Р 52633 - **(2 часа)** - ***проверка сформированности компетенций - ПК-10, ПСК-2.4***

Вопросы для изучения и обсуждения:

1. Основные области стандартизации, относящиеся к биометрии.
2. Базовые подсистемы биометрической системы защиты информации.
3. Основные функции обобщённой биометрической системы.
4. Формат записи биометрической информации.

Вопросы для изучения и обсуждения:

1. Базовые стандарты серии ГОСТ Р 52633.
2. Основные физиологические и поведенческие биометрические идентификаторы.

3. На основе каких биометрических идентификаторов функционируют современные системы защиты информации?

4. Какое количество национальных стандартов в сфере биометрической защиты информации на начало 2017 г. действует в России и о чём оно свидетельствует?

Список литературы

Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info

Кузнецов И.Н., Бизнес-безопасность. - М.: Дашков и К, 2016. - 416 с. - Режим доступа: URL: http://znanium.com/catalog/product/430343

Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru

Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/

Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru

Национальный открытый университет ИНТУИТ - Режим доступа: URL: http://www.intuit.ru

Практическое занятие 4. (Тема 4). Классификация автоматизированных систем с учётом требований по защите информации - **(2 часа) - *проверка сформированности компетенций* - ПК-10, ОПК-5**

Вопросы для изучения и обсуждения:

1. Основные группы автоматизированных систем с учетом уровня их защищённости.

2. Базовые требования к автоматизированным системам для декомпозиции их на различные классы.

3. Классификация автоматизированных систем с учетом уровня их защищённости.

4. Базовые подсистемы в составе автоматизированной системы 1-го класса защищённости.

Контрольные вопросы:

1. Какие основные стандарты в России посвящены средствам защиты автоматизированных систем?

2. Основные признаки группировки автоматизированных систем в различные классы с учётом уровня защиты в них информации.

3. Базовые группы, на которые декомпозируется в России множество автоматизированных систем с учетом уровня их защищённости.

4. Какие основные подсистемы должна содержать автоматизированная система для обеспечения защиты информации?

Список литературы

Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info

Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru

Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/

Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru

10. Методические рекомендации по организации самостоятельной работы

Трудоемкость освоения дисциплины «Гуманитарные аспекты информационной безопасности. Информационное противоборство» составляет 144 часа, из них 70 часов отведены на самостоятельную работу студента (СР).

Вид работы	**Содержание (перечень вопросов)**	**Трудоемкость самостоятельной работы (в часах)**	**Рекомендации**
Подготовка к практическому занятию Тема 1. «Содержание Федерального закона Российской Федерации "О техническом регулировании" »	Базовые органы - генераторы в России на федеральном уровне правовых документов в сфере ИБ. Цели Федерального закона Российской Федерации "О техническом регулировании". Основные документы в области стандартизации, действующие на территории Российской Федерации после ввода в действие ФЗ "О техническом регулировании". Базовые принципы технического регулирования в России.	14	Проанализировать материал из законодательных, нормативных документов, учебников: Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // СЗ РФ 31.07.2006, N 31 (1 ч.). - Режим доступа: URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ Федеральный закон Российской Федерации от 27.12.2002 г. № 184-ФЗ «О техническом регулировании». «Собрание законодательства РФ», 30.12.2002, № 52 (ч.1), ст. 5140. - Режим доступа: URL: http://www.consultant.ru/docu

			ment/cons_doc_LAW_40241/ Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/ Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru Национальный открытый университет ИНТУИТ - Режим доступа: URL: http://www.intuit.ru
Подготовка к практическому занятию Тема 2. «Международная серия стандартов ISO/IEC 27000»	Основные причины подготовки и выпуска стандартов серии ISO/IEC 2700. Категории пользователей стандартов серии ISO/IEC 2700. Сферы информационной безопасности, в которой действуют стандарты серии ISO/IEC 27000. Основные кластеры стандартов, выделяемые во множестве стандартов серии ISO/IEC 27000. Национальные стандарты России, гармонизированные со стандартами серии ISO/IEC 27000.	20	Проанализировать материал из законодательных, нормативных документов, учебников: Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info Кузнецов И.Н., Бизнес-безопасность. - М.: Дашков и К, 2016. - 416 с. - Режим доступа: URL: http://znanium.com/catalog/product/430343 Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru

	Основные разработчики стандартов серии ISO/IEC 27000.		Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/ Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru Национальный открытый университет ИНТУИТ - Режим доступа: URL: http://www.intuit.ru
Подготовка к практическому занятию Тема 3. «Национальные стандарты по биометрической аутентификации серии ГОСТ Р 52633»	Основные области стандартизации, относящиеся к биометрии. Базовые подсистемы биометрической системы защиты информации. Основные функции обобщённой биометрической системы. Формат записи биометрической информации.	22	Проанализировать материал из законодательных, нормативных документов, учебников: Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info Кузнецов И.Н., Бизнес-безопасность. - М.: Дашков и К, 2016. - 416 с. - Режим доступа: URL: http://znanium.com/catalog/product/430343 Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/ Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru Национальный открытый университет ИНТУИТ -

			Режим доступа: URL: http://www.intuit.ru
Подготовка к практическому занятию Тема 4. «Классификация автоматизированных систем с учётом требований по защите информации»	Основные группы автоматизированных систем с учетом уровня их защищённости. Базовые требования к автоматизированным системам для декомпозиции их на различные классы. Классификация автоматизированных систем с учетом уровня их защищённости. Базовые подсистемы в составе автоматизированной системы 1-го класса защищённости.	14	Проанализировать материал из законодательных, нормативных документов, учебников: Галатенко В.А. Стандарты информационной безопасности [Электронный ресурс] - Режим доступа: URL: https://www.intuit.ru/studies/courses/30/30/info Информационный портал в области защиты информации - Режим доступа URL: http://www.securitylab.ru Портал Росстандарта - Режим доступа: URL: https://www.gost.ru/portal/gost/ Портал ФСТЭК России - Режим доступа: URL: http://fstec.ru

Приложение 1

АННОТАЦИЯ

Дисциплина (модуль) «Специальные нормативные документы и стандарты по информационной безопасности» реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.

Целью дисциплины (модуля) является формирование у обучающихся знаний об отечественных и зарубежных нормативных актах, стандартах и нормативных документах-регуляторов в области обеспечения безопасности информационных систем и сетей.

Задачи дисциплины:

- рассмотреть задачи нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения безопасности, структуру и содержание системы нормативного обеспечения безопасности;
- раскрыть вопросы нормативного регулирования развития терминологии в области обеспечения безопасности информационных систем и сетей, нормативного регулирования технической и криптографической защиты информации;
- рассмотреть и освоить обучающимися стандарты в области обеспечения функциональной безопасности информационных систем и сетей, управления информационной безопасностью.

Дисциплина (модуль) направлена на формирование следующих компетенций:

- ОПК-5 - способность использовать нормативные правовые акты в профессиональной деятельности
- ПК-5 - способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
- ПК-10 - способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;
- ПСК-2.4 - способность организовать контроль защищенности объекта информатизации в соответствии с нормативными документами.

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

- базовые международные и российские регуляторы по информационной безопасности;
- основные документы, выпускаемые регуляторами по информационной безопасности;

Уметь:

- работать со стандартами и нормативными документами;
- пользоваться мерами нормативно-правовой поддержки регулирования вопросов защиты информации в Российской Федерации.

Владеть:

- навыками работы с нормативно-правовыми документами;
- навыками использования международных и национальных стандартов в своей профессиональной деятельности;
- навыками обоснования и принятия решений по применению специальных нормативных документов и стандартов в области информационной безопасности.

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, контрольных работ; промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.06.2017 г.*	*10*
2	*Обновлена основная литература*	*26.06.2018 г.*	***20***
3	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*26.06.2018 г.*	***20***
4	*Обновлена основная литература*	*29.08.2019 г.*	***1***
5	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*29.08.2019 г.*	***1***
6	*Обновлена структура дисциплины (модуля) для очной формы обучения (2020 г.)*	*23.06.2020 г*	***14***
7	*Обновлена основная и дополнительная литература*	*23.06.2020 г*	***14***
8	*Обновлен раздел п.4 Образовательные технологии*	*23.06.2020 г*	***14***
9	*Обновлен состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС)*	*23.06.2020 г*	***14***

Приложение 1
к листу изменений

1. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2017 г.)

Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	MicrosoftOffice 2013	Microsoft	лицензионное
2	Windows XP	Microsoft	лицензионное
3	KasperskyEndpointSecurity	Kaspersky	лицензионное
4	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2017 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2017 г. Журналы Oxford University Press
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:
д.т.н, профессор В.В. Арутюнов

Приложение 2
к листу изменений

2. Обновление основной и дополнительной литературы (2018 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел *Основная литература*

Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учеб. пособие. — М. : ИНФРА-М, 2018. — 223 с. - Режим доступа: URL: http://znanium.com/catalog/product/979415

3. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2018 г.)

Перечень ПО

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

Перечень БД и ИСС

Таблица 2

№п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной

	подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:
д.т.н, профессор В.В. Арутюнов

Приложение 3
к листу изменений

4. Обновление основной и дополнительной литературы (2019 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

Дополнить раздел *Дополнительная литература*

Арутюнов В.В., Курышева М.С. О кластеризации национальных стандартов России и нормативно-правовых документов ФСТЭК в области информационной безопасности. В сборнике: Информационная безопасность: вчера, сегодня, завтра. Сборник статей по материалам Международной научно-практической конференции. - М.: РГГУ, 2019. С. 7-16. - Режим доступа: URL: https://elibrary.ru/download/elibrary_41274548_67690255.pdf

5. Состав программного обеспечения (ПО), современных профессиональных баз данных (БД) и информационно-справочные систем (ИСС) (2019 г.)

Перечень ПО

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках

	национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Составитель:
д.т.н, профессор В.В. Арутюнов

Приложение 4
к листу изменений

6. Обновление структуры дисциплины (модуля) для очной формы обучения (2020 г.)

Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 4 з. е., 152 ч., в том числе контактная работа обучающихся с преподавателем 56 ч., самостоятельная работа обучающихся 78 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Основы технического регулирования и стандартизации в Российской Федерации	7	6		4			16	опрос
2	Национальные и международные стандарты в области информационной безопасности	7	6		8			20	опрос
3	Национальные стандарты Российской Федерации в области информационной безопасности	7	10		6			22	опрос, контрольная работа 1
4	Нормативные документы ФСТЭК России	7	10		6			20	опрос, контрольная работа 2
5.	Экзамен						**18**		Экзамен по билетам
	Итого		**32**		**24**		**18**	**78**	

7. Обновление основной литературы (2020 г.)

В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:

1. Дополнить раздел **Основная литература**

Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие / Ю.Н. Сычев. — Москва: ИНФРА-М, 2020. — 223 с. — ISBN 978-5-16-015718-4. - Текст: электронный. - URL: https://znanium.com/catalog/product/1048121

2. Дополнить раздел **Дополнительная литература**

Шишмарев В. Ю. Метрология, стандартизация, сертификация, техническое регулирование и документоведение: Учебник / В.Ю. Шишмарев. — Москва: КУРС: ИНФРА-М, 2020. — 312 с. — ISBN 978-5-906923-15-8. - Текст: электронный. - URL: https://znanium.com/catalog/product/952310

8. В элемент рабочей программы **п.4 Образовательные технологии** вносятся следующие изменения:

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции;

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

9. В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

В элемент рабочей программы **7. Материально-техническое обеспечение дисциплины/модуля** вносятся следующие изменения:

Состав программного обеспечения (ПО)

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или*

			свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

Составитель:

д.т.н, профессор, В.В. Арутюнов