Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ИНСТИТУТ ЭКОНОМИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АНАЛИЗА ДАННЫХ
ОТДЕЛЕНИЕ ПРИКЛАДНОЙ ИНФОРМАТИКИ

кафедра Системного анализа и информатики

УТВЕРЖДЕНА

решением кафедры Системного анализа и информатики

Протокол №6 от «2» сентября 2019г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.03.01 СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

направление подготовки
09.03.03 «Прикладная информатика»
направленность (профиль)
«Прикладная информатика в информационной безопасности»
квалификация
бакалавр
очная форма обучения

Год набора – 2020

Москва, 2020 г.

Автор–составитель: к.т.н.
доцент кафедры Системного анализа и информатики Каширская Е.Н.

Заведующий кафедрой
Системного анализа и информатики Маруев С.А

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина «Стандарты информационной безопасности» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-18	способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	ПК-18.2	Способен определять основные требования стандартов ИБ и различать угрозы ИБ применительно к функционированию ИС
ПК-21	способен проводить оценку экономических затрат и рисков при создании информационных систем	ПК-21.2	Способен оценивать риски при создании ИС

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта)	Код этапа освоения компетенции	Результаты обучения
	ПК-18.2	на уровне знаний: знать виды угроз безопасности, методы и средства обеспечения информационной безопасности, подходы к организации ИТ - инфраструктуры;
		на уровне умений: уметь организовывать защиту информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение);
		на уровне навыков: иметь навыки обеспечения информационной безопасности и защиты информации, организации ИТ – инфраструктуры.
	ПК-21.2	на уровне знаний: знать экономические основы информатизации и автоматизации решения прикладных задач;
		на уровне умений: уметь использовать международные и отечественные модели и методы оценки экономических затрат на проекты по информатизации и автоматизации;
		на уровне навыков: иметь навыки анализа затрат и рисков в сфере информатизации.

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Объем дисциплины в ЗЕ и академических/астрономических часах – 4 ЗЕ (144/108 ч).

Количество академических/астрономических часов, выделенных на контактную работу по очной форме обучения – 64/48 часов (в т.ч. лекц. - 32 ч., практ.-32 ч.); на самостоятельную работу обучающихся на очной форме –44/33 часов.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.03.01 «Стандарты информационной безопасности» относится к дисциплинам по выбору вариативной части учебного плана по направлению подготовки 09.03.03 Прикладная информатика.

Дисциплина изучается на 2 курсе в 4 семестре (очная форма обучения)

Дисциплина опирается на объём знаний, полученных при изучении таких дисциплин, как Информатика, Программирование и алгоритмизация, Математический анализ, Теоретические основы компьютерной безопасности, Операционные системы, Основы информационной безопасности.

Форма промежуточной аттестации – экзамен.

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Раздел 1	Общие положения о стандартах в области информационной безопасности.	20	6		6		8	Д, О
Раздел 2	Российские международные, национальные и отраслевые стандарты в области информационной безопасности.	40	12		12		16	Д, О
Раздел 3	Международные стандарты в сфере обеспечения информационной безопасности бизнеса и кибербезопасности.	48	14		14		20	Д, О
Промежуточная аттестация		36						экзамен
Всего академ./астроном.часов:		**144/108**	**32/24**		**32/24**		**44/33**	

Примечание: * – формы текущего контроля успеваемости: доклад(ы) (Д), опрос (О).

Содержание дисциплины

№ п/п	Название раздела	Основные вопросы и положения, раскрывающие содержание тем
Раздел 1.	Общие положения о стандартах в области информационной безопасности.	Тема I. Нормативно-правовые и методические документы в области информационной безопасности. Роль и понятие стандартов в области информационной безопасности. Основные группы стандартов и спецификаций. Исторические аспекты создания стандартов в области информационной безопасности. Суть и содержание Оранжевой книги «Критерии оценки доверенных компьютерных систем» Министерства обороны США. Тема 2. Международные стандарты в области информационной безопасности. Международная организация по стандартизации (ISO). Связь ISO с другими международными организация по стандартизации. Основные международные стандарты (ISO) по информационной безопасности. Международная электротехническая комиссия (МЭК). Основные международные стандарты (МЭК) по информационной безопасности (NIST). Тема 3. Российские международные, национальные и отраслевые стандарты в области информационной безопасности. Российские международные стандарты (ГОСТ Р ИСО/МЭК). Национальные стандарты. Отраслевые стандарты. Стандарты Банка России. Нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в области информационной безопасности.
Раздел 2.	Российские международные, национальные и отраслевые стандарты в области информационной безопасности.	Тема 1. Российский международный стандарт ГОСТ Р ИСО/МЭК 15408-1-2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель». Область применения стандарта. Основное содержание. Объект оценки. Активы и контрмеры. Профили защиты (ПЗ) и пакеты. Использование ПЗ и пакетов. Тема 2. Российский международный стандарт ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. «Функциональные требования безопасности») и «Требования доверия к

		безопасности». Область применения стандарта. Основное содержание. Парадигма, используемая в функциональных компонентах безопасности данной части ИСО/МЭК 15408. Каталог функциональных компонентов. Пояснительная информация для потенциальных пользователей функциональных компонентов. Требования доверия и оценочные уровни. Компоненты доверия. Тема 3. Российский международный стандарт ГОСТ Р ИСО/МЭК 13335 «Информационная технология. Методы и средства обеспечения безопасности». Общие сведения о стандарте ГОСТ Р ИСО/МЭК 13335. Область применения. Основное содержание частей стандарта. Тема 4. Российские международные стандарты в области оценки деятельности по управлению информационной безопасностью. ГОСТ Р ИСО/МЭК 27004-2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения», ГОСТ Р ИСО/МЭК 27006-2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента ИБ», Стандарт ISO/IEC 27007:2011 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по аудиту систем менеджмента информационной безопасности». Общие сведения о стандартах. Области применения. Термины и определения. Основное содержание стандартов. Тема 5. Стандарты Банка России. СТО БР ИББС-1.0-2014 (Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения), СТО БР ИББС-1.1-2007 (Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности), СТО БР ИББС-1.2-2010 (Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям), СТО БР ИББС-2.2.-2009. (Стандарт Банка России. Обеспечение

		информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности). Общие сведения о стандартах. Области применения стандарта. Основное содержание.
Раздел 3.	Международные стандарты в сфере обеспечения информационной безопасности бизнеса и кибербезопасности	Тема 1. Стандарт информационной безопасности ISO/IEC 17799 «Информационные технологии — Технологии безопасности — Практические правила менеджмента ин-формационной безопасности». Общие сведения о стандарте. Область применения. Термины и определения. Основное содержание стандарта. Тема 2. Стандарт ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности». Общая характеристика стандарта. Основное содержание и особенности стандарта. Формулировка киберпространства. Рекомендации по оценке и отработке рисков в киберпространстве, по соблюдению требований безопасности пользователями, по обеспечению кибербезопасности для организаций-провайдеров. Базовые меры, направленные на решение задач: обеспечения безопасности приложений, обеспечения безопасности серверов, обеспечения безопасности конечных пользователей, защиты от атак методами социальной инженерии, повышения готовности.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости.

4.1.1. В ходе реализации дисциплины «Стандарты Информационной безопасности» используются следующие методы текущего контроля успеваемости обучающихся:

Тема (раздел)	Методы текущего контроля успеваемости
Раздел 1	Доклады с презентацией, опрос на практическом занятии
Раздел 2	Доклады с презентацией, опрос на практическом занятии
Раздел 3	Доклады с презентацией, опрос на практическом занятии

4.1.2. Экзамен проводится в форме устного ответа на билеты (по 2 вопроса в билете).

4.2. Материалы текущего контроля успеваемости обучающихся

Текущий контроль успеваемости осуществляется непрерывно, на протяжении всего курса. Прежде всего, это устный опрос по ходу лекции, выполняемый для оперативной активизации внимания обучающихся и оценки их уровня восприятия. Помимо этого, контроль самостоятельной работы обучающихся осуществляется при опросе на практических занятиях, докладах с презентацией.

4.3. Оценочные средства для промежуточной аттестации

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-18	способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью	ПК-18.2	Способен определять основные требования стандартов ИБ и различать угрозы ИБ применительно к функционированию ИС
ПК-21	способен проводить оценку экономических затрат и рисков при создании информационных систем	ПК-21.2	Способен оценивать риски при создании ИС

4.3.2. Типовые оценочные средства

Промежуточный контроль проводится в форме экзамена и предусматривает устный ответ на вопросы по билету.

Код и наименование этапа освоения компетенции	Результаты обучения	Оценочное средство
ПК-18.2 Способен определять основные требования стандартов ИБ и различать угрозы ИБ применительно к функционированию ИС	на уровне знаний: знать виды угроз безопасности, методы и средства обеспечения информационной безопасности, подходы к организации ИТ - инфраструктуры;	устный опрос
	на уровне умений: уметь организовывать защиту информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение);	устный опрос
	на уровне навыков: иметь навыки обеспечения информационной безопасности и защиты информации, организации ИТ – инфраструктуры.	устный опрос
ПК-21 Способен оценивать риски при создании ИС	на уровне знаний: знать экономические основы информатизации и автоматизации решения прикладных задач;	устный опрос
	на уровне умений: уметь использовать международные и отечественные модели и методы оценки экономических затрат на проекты по информатизации и автоматизации;	устный опрос устный опрос
	на уровне навыков: иметь навыки анализа затрат и рисков в сфере информатизации.	

Перечень вопросов к экзамену по дисциплине
«Стандарты информационной безопасности

1. Функции стандартов в области информационной безопасности.
2. Основные области стандартизации информационной безопасности.
3. Классификации стандартов в области информационной безопасности.
4. Федеральный закон РФ от 27.12.2002 г №184-ФЗ «О техническом регулировании» о принципах применения международных стандартов.
5. Основные группы стандартов и спецификаций в области информационной безопасности.
6. Суть и содержание Оранжевой книги «Критерии оценки доверенных компьютерных систем» Министерства обороны США.
7. Основные международные стандарты (ISO) по информационной безопасности.
8. Российские международные стандарты (ГОСТ Р ИСО/МЭК).
9. Основные международные стандарты (МЭК) по информационной безопасности (NIST).
10. Российские государственные стандарты в области информационной безопасности.
11. Основные стандарты Банка России в области информационной безопасности.
12. Основные действующие нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в области информационной безопасности.
14. Область применения ГОСТ Р ИСО/МЭК 15408-1-2012. Часть 1. «Введение и общая модель». Основное содержание.
15. Область применения ГОСТ Р ИСО/МЭК 15408-1-2012. Часть 2. «Функциональные требования безопасности»). Основное содержание.
16. Область применения ГОСТ Р ИСО/МЭК 15408-1-2012. Часть 3. «Требования доверия к безопасности». Основное содержание.
17. Основное содержание стандарта ГОСТ Р ИСО/МЭК 27001-2006 «Информационные технологии. Методы безопасности. Система управления безопасностью. Требования».
18. Основное содержание стандарта ГОСТ Р ИСО/МЭК 27002-2012. «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».
19. Основное содержание стандарта ГОСТ Р ИСО/МЭК 27003-2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности».
20. Основное содержание стандарта ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».
21. Основное содержание стандарта ГОСТ Р ИСО/МЭК 27004-2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения».
22. Основное содержание стандарта ГОСТ Р ИСО/МЭК 27006-2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента ИБ».
23. Основное содержание стандарта Стандарт ISO/IEC 27007:2011 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по аудиту систем менеджмента информационной безопасности».
24. Основное содержание стандарта ГОСТ Р ИСО/МЭК 27031-2012 «Информационные технологии. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса».
25. Основное содержание стандарта ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», ГОСТ Р 53647.4-2011

«Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности».
26. Обеспечение информационной безопасности организаций банковской системы Российской Федерации.
27. Стандарт Банка России СТО БР ИББС-2.2.-2009
28. Стандарт Банка России СТО БР ИББС-1.2-2010.
29. Стандарт Банка России СТО БР ИББС-1.0-2014.

30. Стандарт информационной безопасности ISO/IEC 17799 «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной без-опасности».

31. Основное содержание стандарта ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности».

32. Определение киберпространства в соответствии со стандартом ISO/IEC 27032:2012.

33. Рекомендации по оценке и отработке рисков в киберпространстве.

34. Базовые меры, направленные на решение задач кибербезопасности.

35. Схема таксономии киберугроз.
36. Варианты darknet-мониторинга киберпространства.

4.4. Методические материалы

4.4.1. Методические материалы, определяющие процедуру оценивания ответов обучающихся на вопросы на понимание лекционного материала

Критериями оценки ответа обучающихся на лекционном занятии выступают:

- правильность ответов на вопросы преподавателя по изученному материалу;
- полнота и лаконичность ответа;
- степень понимания тематики предмета;
- логика и аргументированность изложения материала;
- приведение примеров, демонстрирующих умение и владение полученными знаниями по темам предмета в раскрытии поставленных вопросов.

4.4.2. Методические материалы, определяющие процедуру оценивания при проведении опроса на практическом занятии

Оценки **«отлично»** заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание вопроса, умение свободно ориентироваться в теме, усвоивший основную, и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется обучающимся, усвоившим взаимосвязь основных понятий в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного

материала;

Оценки **«хорошо»** заслуживает обучающийся, обнаруживший полное знание темы, успешно выполняющий предусмотренные программой задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется обучающимся, показавшим систематический характер знаний по пройденному материалу и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности;

Оценки **«удовлетворительно»** заслуживает обучающийся, обнаруживший знание основного материала в объеме, необходимом для дальнейшего усвоения материала и предстоящей работы по профессии, знакомый с основной литературой, рекомендованной программой.

Оценка **«неудовлетворительно»** выставляется обучающемуся, обнаружившему пробелы в знаниях основного материала темы, допустившему принципиальные ошибки в понимании и изложении учебного материала.

4.4.3. Методические материалы, определяющие процедуру оценивания промежуточной аттестации по дисциплине

Экзамен принимается в устной форме, по билетам. Задание для экзамена включает два теоретических вопроса. Оценка знаний обучающегося на зачет с оценкой носит комплексный характер и определяется его:

- ответом на экзамене;
- учебными достижениями в семестровый период.

Знания, умения, навыки обучающегося на экзамене оцениваются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

Оценивание студента на экзамене по дисциплине
«Стандарты информационной безопасности»

Оценка	Требования к знаниям
Отлично	«Отлично» выставляется обучающемуся, если он показал полные, глубокие и систематические знания, знакомство с основной и дополнительной литературой, полный и правильный ответ, творческий подход в понимании и изложении учебного материала, полное выполнение мероприятий текущего контроля.
Хорошо	«Хорошо» выставляется обучающемуся, если он показал достаточные и систематизированные знания, знакомство с основной и отчасти с дополнительной литературой, дал в целом правильный ответ, показал понимание и изложении учебного материала, полностью выполнил мероприятий текущего контроля. Допустимы погрешности при выполнении мероприятий промежуточного контроля и при ответе.
Удовлетвори тельно	«Удовлетворительно» выставляется обучающемуся, если он выполнил не все предусмотренные программой задания, не полностью отработал практические или лабораторные занятия, необходимые дополнительные занятия по соответствующей дисциплине, допустил непринципиальные ошибки при ответе. Допустимо знание основного

	учебного материала в минимальном объеме, необходимом для дальнейшей учебы и работы, имеются погрешности при выполнении мероприятий промежуточного контроля и при ответе.
Недовлетворительно	«Неудовлетворительно» выставляется обучающемуся, если он не выполнил предусмотренные программой задания, не отработал практические или лабораторные занятия, необходимые дополнительные занятия по соответствующей дисциплине, нарушил академические нормы, имеет существенные погрешности при выполнении мероприятий текущего контроля, допущены существенные ошибки при ответе, необходима некоторая дополнительная работа.

5. Методические указания для обучающихся по освоению дисциплины

5.1. Методические указания по вопросам на понимание лекционного материала

На лекциях рекомендуется слушать предлагаемый лектором материал, при этом параллельно конспектировать основные положения, поскольку это дает наибольший результат в усвоении материала. Предоставляется возможность задавать вопросы на уточнение понимания темы и принимать участие в ее обсуждении.

Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям. Во время самостоятельной проработки лекционного материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. Все такие моменты следует выделить или выписать отдельно для дальнейшего обсуждения на практическом занятии. В случае необходимости следует обращаться к преподавателю за консультацией. Полный список литературы по дисциплине приведен в разделе 6 настоящей программы.

5.2. Методические указания по подготовке вопросов для самостоятельного изучения к занятиям практического (семинарского) типов

Подготовка обучающегося к практическому занятию осуществляется на основании плана раскрытия темы практического занятия, которое разрабатывается преподавателем на основе рабочей программы и доводится до сведения обучающегося своевременно.

При подготовке к практическому занятию обучающемуся необходимо изучить внимательно основные вопросы темы семинара. Важным условием успешной подготовки к практическому занятию является четкая организация самостоятельной работы студентов по изучению учебной и дополнительной литературы. Умение анализировать и применять для ответов на вопросы и решения задач и заданий полученные знания при самостоятельной подготовке в значительной степени определяет успешность освоения материала по дисциплине и формирование у обучающихся соответствующих компетенций.

Подготовка вопросов для самостоятельного изучения включает: изучение необходимой литературы (обязательной, дополнительной литературы, специальных периодических изданий, Интернет-ресурсов), подготовку конспекта ответа, ответы на вопросы.

При подготовке к практическим занятиям важно:

– использовать достаточно широкий диапазон массива информации, провести обзор литературы и специальных изданий, составить каталог Интернет-ресурсов;

– представить различные подходы, четко и полно определить рассматриваемые понятия, выявить взаимосвязи понятий и явлений, взаимозависимости и связи с другими вопросами;

– грамотно структурировать материал, ясно, четко и логично его излагать,

приводить соответствующие примеры из практики, для иллюстрации положений, тезисов и выводов использовать таблицы, схемы, графики, диаграммы.

Вопросы для самостоятельной подготовки к занятиям практического (семинарского) типа указаны в разделе 4.2.

5.2.1. Учебно-методическое обеспечение самостоятельной работы.

Самостоятельная работа студентом осуществляется для закрепления изученного материала после практических занятий для выполнения домашних заданий, для подготовки к контрольным работам, для изучения дополнительных материалов.

№ п/п	Тип занятия	Указания
Раздел 1. Общие положения о стандартах и рекомендациях в области информационной безопасности.		
1	СРС	Российские международные стандарты (ГОСТ Р ИСО/МЭК). Государственные стандарты. Отраслевые стандарты. Стандарты Банка России**.**
2	СРС	Нормативные методические документы Федеральной службы безопасности Российской Феде-рации, Федеральной службы по техническому и экспортному контролю в области информационной безопасности.
Раздел 2. Российские международные стандарты в области информационной безопасности.		
3	СРС	Предназначение, суть и содержание стандарта. Основные сведения о стандарте ГОСТ Р ИСО/МЭК 15408.Содержание стандарта, термины и определения, используемые в стандарте. Путеводитель по критериям оценки без-опасности ИТ.
4	СРС	ГОСТ Р ИСО/МЭК 27031-2012 «Информационные технологии. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных техно-логий к обеспечению непрерывности бизнеса»
5	СРС	ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»,
6	СРС	ГОСТ Р 53647.4-2011 «Менеджмент непрерывности бизнеса.
7	СРС	Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности».
8	СРС	Общие сведения о стандартах. Области применения. Термины и определения. Основное содержание стандартов.
9	СРС	СТО БР ИББС-1.0-2014 (Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения). СТО БР ИББС-1.1-2007 (Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности). СТО БР ИББС-1.2-2010 (Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям). СТО БР ИББС-2.2.-2009. (Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности).

№ п/п	Тип занятия	Указания
Раздел 3. Стандарты и рекомендации в сфере обеспечения информационной безопасности бизнеса и кибербезопасности.		
10	СРС	Общая характеристика стандарта. Основное содержание и особенности стандарта. Формулировка киберпространства. Рекомендации по оценке и отработке рисков в киберпространстве, по соблюдению требований безопасности пользователями, по обеспечению кибербезопасности для организаций-провайдеров.
11	СРС	Базовые меры, направленные на решение задач: обеспечения безопасности приложений, обеспечения безопасности серверов, обеспечения безопасности конечных пользователей, защиты от атак методами социальной инженерии, повышения готовности.
12	СРС	Необходимость введения стандартов безопасности компьютерных систем. Использовать конспект лекции и рекомендованную литературу.

5.3. Методические рекомендации по подготовке к зачету с оценкой по дисциплине

Ответ на экзамен предусматривает устный ответ на теоретические вопросы.

При подготовке к экзамену обучающийся обращается к пройденному материалу, сосредоточенному в конспектах лекций, учебниках и других источниках информации. Повторяя, обобщая, закрепляя и дополняя полученные знания, поднимает их на качественно новый уровень — уровень системы совокупных данных, что позволяет ему понять логику всего предмета в целом. Новые знания обучающийся получает в ходе самостоятельного изучения того, что не было изложено в лекциях и на семинарских занятиях.

Экзамен как особая форма учебного процесса имеет свои особенности, специфические черты и некоторые аспекты, которые необходимо обучающемуся знать и учитывать в своей работе. Это, прежде всего:

- что и как запоминать при подготовке к зачету;
- по каким источникам и как готовиться;
- на чем сосредоточить основное внимание;
- каким образом в максимальной степени использовать программу курса;
- что и как записать, а что выучить дословно и т. п.

На экзамене, как правило, проверяется не столько уровень запоминания обучающимся учебного материала, сколько то, насколько успешно он оперирует теми или иными научными понятиями и категориями, систематизирует факты, как умеет мыслить, аргументировано отстаивать определенную позицию, объясняет и пересказывает заученную информацию.

Программу курса необходимо максимально использовать как в ходе подготовки, так и на самом экзамене. Ведь она включает в себя разделы, темы и основные проблемы, в рамках которых и формируются вопросы для зачета с оценкой.

Оптимальным для подготовки к экзамену является вариант, когда обучающийся начинает подготовку к нему с первых занятий по данному курсу.

При подготовке к экзамену по наиболее сложным вопросам, ключевым проблемам и важнейшим понятиям необходимо сделать краткие письменные записи в виде тезисов, планов, определений. Особое внимание в ходе подготовки к экзамену следует уделять конспектам лекций, ибо они обладают рядом преимуществ по сравнению с печатной продукцией. Как правило, они более детальные, что позволяет оценивать современную ситуацию, отражать самую свежую научную и оперативную информацию, отвечать на вопросы, интересующие аудиторию, в данный момент, тогда как при написании и опубликовании печатной продукции проходит определенное время, и материал быстро устаревает, особенно в таких областях знаний, как инфокоммуникационные технологии и

информационная безопасность.

В то же время подготовка по одним конспектам лекций недостаточна, необходимо использовать и иную учебную литературу. Не следует бояться дополнительных и уточняющих вопросов на экзамене. Они, как правило, задаются или помимо теоретического вопроса для выявления общей подготовленности, или в рамках билета для уточнения высказанной мысли.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет, включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

1. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю. Н. Сычев. — Саратов : Вузовское образование, 2018. — 195 c. — ISBN 978-5-4487-0128-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72345.html
2. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности: Учебное пособие. Стандарт третьего поколения СПб: Питер, 2017. 256 с.

6.2. Дополнительная литература

1. Галатенко В.А. Стандарты информационной безопасности (2-е изд.). М.: НОУ "Интуит", 2016г. – 307с.
2. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 c. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72341.html

6.3. Нормативные правовые документы.

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.07.2017) «Об информации, информационных технологиях и о защите информации». Статья 16. Защита информации. СПС Консультант.
2. Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности». СПС Консультант.
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». СПС Консультант.
4. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи». СПС Консультант.
5. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». СПС Консультант.
6. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». СПС Консультант.
7. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации». СПС Консультант.

6.4. Интернет-ресурсы

http://www.infosecurity. report.ru/
• http://meganorm.ru/list/14-0.htm
• http://dsbb.imf.org.
• http://www.infoforum.ru/
• http:// www.iwars.su/
• http://www.itsec.ru/main.php/
• http://www.un.org/russian/online/loc1.htm.

6.5. Иные источники.

Не предусмотрены

7.Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Название лаборатории/класса, оснащенного необходимым, в соответствии с требованиями ФГОС/ СУОС, оборудованием	Наименование оборудования	Перечень лицензионного программного обеспечения
учебная аудитория для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации	Рабочие места студентов: столы и стулья – соответственно количеству студентов. Рабочее место для инвалида и лиц с ОВЗ: парта с телескопической столешницей на электромеханическом приводе - 1 шт., кресло-коляска для инвалидов 18" - 1 шт., индукционная петля - 1 шт., компьютер с версией для слабовидящих - 1 шт., кнопка вызова сотрудников - 1 шт. Рабочее место преподавателя: стол – 1 шт., стул – 1 шт, кафедра - 1 шт. Доска меловая и маркерная. Экран, ноутбук Lenovo ideapad 100/15, проектор	Мультимедийный проектор КонсультантПлюс
информационно-аналитическая лаборатория - учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций	Рабочие места: столы компьютерные – в соответствии с количеством студентов, кресло Престиж Profi -B-20 Самба бордо в рубчик - 15 шт., подставка для ног Fellowes FS-48121 Standard черный - 15 шт. Рабочее место преподавателя: стол компьютерный - 1 шт., стул - 1 шт. Доска меловая или маркерная Персональные компьютеры	Мультимедийный проектор КонсультантПлюс
библиотека - помещение для самостоятельной работы	Рабочие места: столы и стулья. Рабочее место преподавателя: стол – 1 шт., стул - 1 шт., кафедра библиотечная - 1 шт. Телефон – 1 шт., цифровой многофункциональный копир - 1 шт., копировальный аппарат МФУ – 1 шт., принтер - 1 шт., сканер – 1 шт. Шкаф –	Мультимедийный проектор КонсультантПлюс

	7 шт, стеллаж-33 шт, библиотечная стойка – 2 шт., стенд – 2 шт. Меловая или маркерная доска. Персональные компьютеры	

Программное обеспечение:
В процессе лекционных и семинарских занятий используется следующее программное обеспечение:
- программы, обеспечивающие доступ в сеть Интернет (например, «Google chrome») и локальную сеть Академии;
- программы, демонстрации видео материалов (например, проигрыватель «Windows Media Player»);
- программы для демонстрации и создания презентаций (например, «Microsoft PowerPoint»).

Информационные справочные системы:
Информационно-правовой портал «Консультант плюс» (правовая база данных). [Электронный ресурс]. – URL: http://www.consultant.ru/
Информационно-правовой портал «Гарант» (правовая база данных). [Электронный ресурс]. – URL: http://www.garant.ru/