МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по учебной работе

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Нормативное обеспечение защиты информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль) / специализация: **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **8**
Учебный план набора 2020 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Практические занятия	36	36	часов
3	Всего аудиторных занятий	54	54	часов
4	Самостоятельная работа	90	90	часов
5	Всего (без экзамена)	144	144	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	180	180	часов
		5.0	5.0	З.Е.

Экзамен: 8 семестр

Томск

Согласована на портале № 51569

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от «26» 11 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем, утвержденного 01.12.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчики:

доцент кафедра КИБЭВС _____ А. К. Новохрестов

старший преподаватель кафедра КИБЭВС _____ А. И. Гуляев

Заведующий обеспечивающей каф. КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф. КИБЭВС _____ А. А. Шелупанов

Эксперты:

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ А. А. Конев

Доцент кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) _____ К. С. Сарин

Согласована на портале № 51569

1. Цели и задачи дисциплины

1.1. Цели дисциплины

формирование знаний по организационному обеспечению информационной безопасности и навыков по их определению для конкретных условий.

1.2. Задачи дисциплины

– дать актуальные знания по законодательству РФ в области информационной безопасности, защите персональных данных и критической информационной инфраструктуры;

– дать актуальные знания по международному законодательству в области защиты информации.

–

–

2. Место дисциплины в структуре ОПОП

Дисциплина «Нормативное обеспечение защиты информации» (Б1.В.02.03) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Организационное и правовое обеспечение информационной безопасности.

Последующими дисциплинами являются: Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;

– ПК-9 способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности;

– ПК-15 способностью участвовать в проведении экспериментально-исследовательских работ по сертификации средств защиты информации автоматизированных систем;

– ПК-16 способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации;

– ПК-21 способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;

В результате изучения дисциплины обучающийся должен:

– **знать** основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях; организацию работы и нормативные правовые акты, и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.

– **уметь** применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности; разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

– **владеть** профессиональной терминологией в области информационной безопасности; навыками работы с нормативными правовыми актами; навыками организации и обеспечения режима секретности; методами организации и управления деятельностью служб защиты информации на предприятии; методами формирования требований по защите информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 5.0 зачетных единицы и представлена в таблице 4.1.

Согласована на портале № 51569

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		8 семестр
Аудиторные занятия (всего)	54	54
Лекции	18	18
Практические занятия	36	36
Самостоятельная работа (всего)	90	90
Проработка лекционного материала	45	45
Подготовка к практическим занятиям, семинарам	45	45
Всего (без экзамена)	144	144
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	180	180
Зачетные Единицы	5.0	5.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Нормативное обеспечение безопасности персональных данных	6	12	30	48	ПК-21, ПК-4, ПК-9
2 Нормативное обеспечение безопасности критической информационной инфраструктуры	6	12	30	48	ПК-21, ПК-4, ПК-9
3 Нормативное обеспечение по технической защите информации	6	12	30	48	ПК-15, ПК-16, ПК-9
Итого за семестр	18	36	90	144	
Итого	18	36	90	144	

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Нормативное обеспечение безопасности персональных данных	152-ФЗ О персональных данных. Правила организации и осуществления государственного контроля и надзора за обработкой персональных данных. Требования и методы по обезличиванию персональных данных. Требования к защите персо-	6	ПК-21, ПК-4, ПК-9

Согласована на портале № 51569

	нальных данных при их обработке в информационных системах персональных данных. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Конвенция о защите физических лиц при автоматизированной обработке персональных данных. Директива Европейского Союза № 2002/58/ЕС "О приватности и электронных коммуникациях"		
	Итого	6	
2 Нормативное обеспечение безопасности критической информационной инфраструктуры	187-ФЗ О безопасности критической информационной инфраструктуры РФ. Правила подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ. Порядок ведения реестра значимых объектов КИИ. Требования к созданию систем безопасности значимых объектов КИИ и обеспечение их функционирования. Требования по обеспечению безопасности значимых объектов КИИ. Требования к обеспечениюзащиты информации в автоматизированных системах управления производственными и технологическими процессами на объектах КИИ. Государственная система обнаружения, предупреждения и ликвидации последствийкомпьютерных атак, направленных на информационные ресурсы РФ (ГосСОПКА). Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Совершенствование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Национальный координационный центр по компьютерным инцидентам. Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ.	6	ПК-21, ПК-4, ПК-9
	Итого	6	
3 Нормативное обеспечение по технической защите	Перечень органов по аттестации. Реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабо-	6	ПК-15, ПК-16, ПК-9

Согласована на портале № 51569

информации	раторий. Государственный реестр сертифицированных средств защиты информации. Документы по лицензионной деятельности ФСТЭК России в области технической защиты информации. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации.		
	Итого	6	
Итого за семестр		18	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин		
	1	2	3
Предшествующие дисциплины			
1 Организационное и правовое обеспечение информационной безопасности	+	+	+
Последующие дисциплины			
1 Преддипломная практика	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Прак. зан.	Сам. раб.	
ПК-4	+	+	+	Экзамен, Опрос на занятиях, Тест, Отчет по практическому занятию
ПК-9	+	+	+	Экзамен, Опрос на занятиях, Тест, Отчет по практическому занятию
ПК-15	+	+	+	Опрос на занятиях, Тест, Отчет по практическому занятию

Согласована на портале № 51569

ПК-16	+	+	+	Опрос на занятиях, Тест, Отчет по практическому занятию
ПК-21	+	+	+	Экзамен, Опрос на занятиях, Тест, Отчет по практическому занятию

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Нормативное обеспечение безопасности персональных данных	Подготовка нормативных актов, необходимых для реализации Федерального закона «О персональных данных». Уведомлению уполномоченного органа о начале обработки персональных данных и внесении изменений в ранее представленные сведения	12	ПК-21, ПК-4, ПК-9
	Итого	12	
2 Нормативное обеспечение безопасности критической информационной инфраструктуры	Категорирование объектов КИИ. Формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерныхатак. Обмен информацией о компьютерных инцидентах между субъектами КИИ. Информирование ФСБ России о компьютерных инцидентах, реагирование на них, принятие мер по ликвидации последствий компьютерных атак.	12	ПК-21, ПК-4, ПК-9
	Итого	12	
3 Нормативное обеспечение по технической защите информации	Сертификация средств защиты информации. Формы заявления об аккредитации, формы и требования к содержанию прилагаемых к заявлению об аккредитации документов и документов, необходимых для организации и проведения аккредитации, а также документов, подтверждающих соответствие заявителя (аккредитованного лица) критериям аккредитации. Правила выполнения работ по аккредитации орга-	12	ПК-15, ПК-16, ПК-9

Согласована на портале № 51569

	нов по сертификации и испытательных лабораторий, выполняющих работы по оценке соответствия в отношении продукции, используемой в целях защиты сведений, составляющих государственную тайну.		
	Итого	12	
Итого за семестр		36	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
8 семестр				
1 Нормативное обеспечение безопасности персональных данных	Подготовка к практическим занятиям, семинарам	15	ПК-21, ПК-4, ПК-9	Опрос на занятиях, Отчет по практическому занятию, Тест, Экзамен
	Проработка лекционного материала	15		
	Итого	30		
2 Нормативное обеспечение безопасности критической информационной инфраструктуры	Подготовка к практическим занятиям, семинарам	15	ПК-21, ПК-4, ПК-9	Опрос на занятиях, Отчет по практическому занятию, Тест
	Проработка лекционного материала	15		
	Итого	30		
3 Нормативное обеспечение по технической защите информации	Подготовка к практическим занятиям, семинарам	15	ПК-15, ПК-16, ПК-9	Опрос на занятиях, Отчет по практическому занятию, Тест
	Проработка лекционного материала	15		
	Итого	30		
Итого за семестр		90		
	Подготовка и сдача экзамена	36		Экзамен
Итого		126		

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр

Согласована на портале № 51569

8 семестр				
Опрос на занятиях	3	3	3	9
Отчет по практическому занятию	15	15	15	45
Тест			16	16
Итого максимум за период	18	18	34	70
Экзамен				30
Нарастающим итогом	18	36	70	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт — Режим доступа: https://urait.ru/bcode/469235 (дата обращения: 23.06.2021).

12.2. Дополнительная литература

1. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 [Электронный ресурс]: — Режим доступа: https://fstec.ru/component/attachments/download/2919 (дата обращения: 23.06.2021).

Согласована на портале № 51569

2. Методика оценки угроз безопасности информации. Методический документ. Утвержден ФСТЭК России 5 февраля 2021 г. [Электронный ресурс]: — Режим доступа: https://fstec.ru/component/attachments/download/566 (дата обращения: 23.06.2021).

3. Меры защиты информации в государственных информационных системах. Методический документ. Утвержден ФСТЭК России 11 февраля 2014 г. [Электронный ресурс]: — Режим доступа: https://fstec.ru/component/attachments/download/675 (дата обращения: 23.06.2021).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Организационно-правовое обеспечение информационной безопасности [Электронный ресурс]: Методические указания по практическим занятиям и самостоятельной работе / Э. В. Семенов - 2012. 13 с. — Режим доступа: https://edu.tusur.ru/publications/2506 (дата обращения: 23.06.2021).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. http://www.elibrary.ru - научная электронная библиотека;
2. https://fstec.ru/ - Федеральная служба по техническому и экспортному контролю
3. https://rkn.gov.ru/ - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Аудитория Интернет-технологий и информационно-аналитической деятельности

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Экран раздвижной;
- Мультимедийный проектор View Sonic PJD5154 DLP;
- Компьютеры: AMD A8-5600K/ ASUS A88XM-A/ DDR3 4 Gb/ WD5000AAKX 500 Gb/

Согласована на портале № 51569

мышь/ клавиатура/ монитор (15шт.);

- Компьютеры: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор (6шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 10

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

Согласована на портале № 51569

14.1.1. Тестовые задания

Вопрос 1

Что такое информация в соответствии с Федеральным законом №149-ФЗ?

1. Сообщения и данные
2. Изображения
3. Сведения об интеллектуальной собственности
4. Сведения (сообщения, данные) независимо от формы их представления

Вопрос 2

Дата принятия Конституции Российской федерации?

1. 01 января 1991
2. 10 декабря 1992
3. 12 декабря 1993
4. 15 ноября 1994

Вопрос 3

Конфиденциальность информации это?

1. Целостность и доступность информации при ее обработке в автоматизированных системах управления технологическими процессами.

2. Сохранность персональных данных субъекта персональных данных при попытках доступа третьих лиц в информационную систему персональных данных.

3. Обязательное для выполнения лицом, получившим доступ к определенной информации,требование не передавать такую информацию третьим лицам без согласия ее обладателя.

4. Обязательно требование для выполнения лицом, получившим доступа к сведениям, содержащим государственную тайну.

Вопрос 4

Обладатель информации это?

1. Лицо, оформившее права на интеллектуальную собственность в соответствии с законодательством Российской Федерации об интеллектуальной собственности.

2. Лицо, самостоятельно создавшее информацию либо получившее на основании закона илидоговора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

3. Юридическое лицо, оформляющее право на интеллектуальную собственность физических лиц и юридических лиц за исключением резидентов иностранных государств.

4. Юридическое лицо, зарегистрированное за пределами Российской Федерации и регистрирующее право интеллектуальной собственности на территории Российской Федерации.

Вопрос 5

Дата принятия Доктрины информационной безопасности Российской Федерации?

1. 21 июля 1993
2. 09 сентября 2000
3. 27 июня 2006
4. 05 декабря 2016

Вопрос 6

Обеспечение информационной безопасности в соответствии с Доктриной информационной безопасности Российской Федерации?

1. Совокупность правовых, организационно-технических и экономических методов.

2. Совокупность правовых, организационных и технических методов.

3. Совокупность оперативно-розыскных, научно-технических, информационно-аналитических мер.

4. Совокупность оперативно-розыскных, научно-технических, информационно-аналитических и иных мер.

Вопрос 7

Основные компоненты справочно-правовой системы?

1. Программная оболочка, экспертная группа юристов.

2. Программная оболочка, информационный банк.

Согласована на портале № 51569

3. Информационный банк, техническая поддержка.
4. Техническая поддержка, экспертная группа правоведов.
Вопрос 8
Каким образом делиться информация по категориям доступа?
1. Государственная тайна и персональные данные.
2. Общедоступная информация и информация ограниченного доступа.
3. Служебная тайна и адвокатская тайна.
4. Конфиденциальная информация и государственная тайна.
Вопрос 9
Пометка коммерческая тайна содержит:
1. Фамилия, имя, отчество индивидуального предпринимателя.
2. Наименование юридического лица.
3. Место нахождения юридического лица.
4. Наименование и место нахождения юридического лица.
Вопрос 10
Режим коммерческой тайны считается установленным?
1. После устного распоряжения генерального директора.
2. После собрания совета директоров юридического лица.
3. После письменного распоряжения уполномоченного лица.
4. После назначения лица, ответственного за защиту коммерческой тайны.
Вопрос 11
Какое количество типов актуальных угроз персональным данным описывается в постановлении Правительства РФ от 01.11.2012 №1119?
1. Один
2. Два
3. Три
4. Четыре
Вопрос 12
Контроль за выполнением требований к защите персональных данных, утвержденный постановлением Правительства РФ от 01.11.2012 №1119 выполняется не реже чем 1 раз в:
1. 1 год
2. 3 года
3. 5 лет
4. На усмотрение оператора персональных данных
Вопрос 13
Постановление Правительства РФ от 01.11.2012 №1119 устанавливает:
1. Классы защищенности персональных данных
2. Уровни защищенности персональных данных
3. Уровни значимости персональных данных
4. Все выше перечисленное
Вопрос 14
Выбор класса средств криптографической защиты информации в соответствии с приказом ФСБ от 10.07.2014 №378 основывается на:
1. Модели актуальных угроз персональных данных
2. Типе актуальных угроз персональных данных
3. Уровне защищенности персональных данных
4. Ни один из выше перечисленных пунктов
Вопрос 15
Какое минимальное число сотрудников устанавливает постановление Правительства от 03.02.2012 №79 соискателю лицензии на деятельность по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну) являющемуся юридическим лицом:
1. 1 сотрудник
2. 2 сотрудника

Согласована на портале № 51569

3. 3 сотрудника

4. 5 сотрудников

Вопрос 16

Какие требования к работникам соискателя лицензии на деятельность по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну) предъявляет постановление Правительства от 03.02.2012 №79:

1. Работа в штате по основному месту работы

2. Работа в штате по внешнему совместительству и высшее образование по направлению-подготовки (специальности) в области информационной безопасности и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 3 лет

3. Высшее образование и стаж работы в области проводимых работ по лицензируемомувиду деятельности не менее 3 лет, прошедших обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности

4. Работа в штате по основному месту работы и высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области проводимых работ по лицензируемому виду деятельности не менее 5 лет

Вопрос 17

Для выполнения работ и услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации лицензиат ФСТЭК должен иметь в наличии:

1. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от

11.02.2013 N 17 и ГОСТ 2.103-2013 ЕСКД Стадии разработки

2. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11.02.2013 N 17 и ГОСТ 2.119-2013 ЕСКД Эскизный проект

3. ГОСТ 2.503-2013 ЕСКД Правила внесения изменений и ГОСТ 2.610-2006 ЕСКД Правилавыполнения эксплуатационных документов

4. ГОСТ Р 8.563-2009 Государственная система обеспечения единства измерений. Методики(методы) измерений и ГОСТ 28195-89 Оценка качества программных средств. Общие положения

Вариант 18

Для выполнения работ мониторингу информационной безопасности средств и систем информатизации лицензиат ФСТЭК должен иметь в наличии:

1. Средства управления информацией об угрозах безопасности информации

2. Программные средства контроля целостности

3. Программные средства формирования и контроля полномочий доступа в информационных (автоматизированных) системах

4. Осциллографы

Вопрос 19

Для какого вида деятельности в соответствии с постановление Правительства от 16.04.2012 №313 не требуется получение лицензии:

1. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем

2. Монтаж шифровальных (криптографических) средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну

3. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем

4. Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств

Вопрос 20

Какое требование предъявляется к руководителю и (или) лицу, уполномоченное руководить

Согласована на портале № 51569

работами по модернизации шифровальных (криптографических) средств

1. Высшее профессиональное образование по направлению подготовки "Информационная-безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 3 лет

2. Высшее профессиональное образование по направлению подготовки "Информационная-безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 500 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет

3. Высшее профессиональное образование по направлению подготовки "Информационная-безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет

4. Любой из перечисленных пунктов

Вопрос 21

Какое требование предъявляется к руководителю и (или) лицу, уполномоченное руководить работами по передаче шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации

1. Высшее профессиональное образование по направлению подготовки "Информационная-безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 3 лет

2. Высшее профессиональное образование по направлению подготовки "Информационная-безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 500 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет

3. Высшее профессиональное образование по направлению подготовки "Информационная-безопасность" и (или) прошедшие переподготовку по одной из специальностей этого направления (нормативный срок - свыше 1000 аудиторных часов), а также имеющие стаж в области выполняемых работ в рамках лицензируемой деятельности не менее 5 лет

4. Любой из перечисленных пунктов

Вопрос 22

Какие организации создают свои системы сертификации средств защиты информации?

1. Федеральная служба безопасности Российской Федерации

2. Федеральная служба по техническому и экспортному контролю Российской Федерации

3. Министерство обороны Российской Федерации

4. Все вышеперечисленные

Вопрос 23

Какие из перечисленных функций не входят в перечень компетенций федерального органа по сертификации?

1. выдает сертификаты и лицензии на применение знака соответствия

2. приостанавливает или отменяет действие выданных сертификатов

3. формируют фонд нормативных документов, необходимых для сертификации

4. организует работы по формированию системы сертификации и руководство ею, координирует деятельность органов по сертификации средств защиты информации и испытательных лабораторий, входящих в систему сертификации

Вопрос 24

В компетенцию какого ведомства входит сертификация средств криптографической защиты информации?

1. Федеральная служба безопасности Российской Федерации

2. Федеральная служба по техническому и экспортному контролю Российской Федерации

3. Министерство обороны Российской Федерации

Согласована на портале № 51569

4. Все вышеперечисленные

Вопрос 25

В каком случае аттестация объекта информатизации является добровольной?

1. обработка государственной тайны
2. при защите государственного информационного ресурса
3. управление экологически опасными объектами
4. ведение конфиденциальных переговоров

Вопрос 26

Кто создает организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации

1. Федеральная служба безопасности Российской Федерации
2. Федеральная служба по техническому и экспортному контролю Российской Федерации
3. Министерство обороны Российской Федерации
4. Все вышеперечисленные

Вопрос 27

Какое действие не является обязательным при аттестации объектов информатизации по требованиям безопасности информации

1. подачу и рассмотрение заявки на аттестацию
2. разработка программы и методики аттестационных испытаний
3. испытание несертифицированных средств и систем защиты информации
4. оформление, регистрация и выдача "Аттестата соответствия"

Вопрос 28

Максимальный срок действия аттестата объекта информатизации в соответствии с "Положение по аттестации объектов информатизации по требованиям безопасности информации" утвержденного Гостехкомиссией РФ от 25.11.1994

1. 1 год
2. 2,5 года
3. 3 года
4. 5 лет

Вопрос 29

Какое постановление Правительства РФ регламентирует лицензирование деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну?

1. Постановление Правительства РФ от 03.02.2012 N 79
2. Постановление Правительства РФ от 16.04.2012 N 313
3. Постановление Правительства РФ от 12.04.2012 N 287
4. Постановление Правительства РФ от 15.04.1995 N 333

Вопрос 30

Чем является защита государственной тайны?

1. видом основной деятельности
2. совокупностью органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях
3. техническими, криптографическими, программными и другими средствами, предназначенными для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средствами контроля эффективности защиты информации
4. процедурой оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений

14.1.2. Экзаменационные вопросы

1. Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации.
2. Конституционные гарантии прав граждан на информацию и механизм их реализации.
3. Понятие и виды защищаемой информации по законодательству РФ.

Согласована на портале № 51569

4. Государственная тайна как особый вид защищаемой информации.

5. Конфиденциальная информация.

6.Система защиты государственной тайны.

7.Правовой режим защиты государственной тайны.

8. Правовое регулирование взаимоотношений администрации и персонала в области защиты информации.

9. Правовые режимы конфиденциальной информации.

10. Лицензирование и сертификация в области защиты информации, в том числе государственной тайны.

11. Правовые основы защиты информации с использованием технических средств (защита от технических разведок, применение и разработка шифровальных средств, электронная цифровая подпись и т.д.).

12. Защита интеллектуальной собственности.

13. Правовая регламентация охранной деятельности.

14. Международное законодательство в области защиты информации.

15. Преступления в сфере компьютерной информации.

16. Экспертиза преступлений в области компьютерной информации.

17. Криминалистические аспекты проведения расследований.

14.1.3. Темы опросов на занятиях

152-ФЗ О персональных данных. Правила организации и осуществления государственного контроля и надзора за обработкой персональных данных. Требования и методы по обезличиванию персональных данных. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Особенности обработки персональных данных, осуществляемой без использования средств автоматизации. Конвенция о защите физических лиц при автоматизированной обработке персональных данных. Директива Европейского Союза № 2002/58/ЕС "О приватности и электронных коммуникациях"

187-ФЗ О безопасности критической информационной инфраструктуры РФ. Правила подготовки и использования ресурсов единой сети электросвязи РФ для обеспечения функционирования значимых объектов КИИ. Порядок ведения реестра значимых объектов КИИ. Требования к созданию систем безопасности значимых объектов КИИ и обеспечение их функционирования. Требования по обеспечению безопасности значимых объектов КИИ. Требования к обеспечению

защиты информации в автоматизированных системах управления производственными и технологическими процессами на объектах КИИ. Государственная система обнаружения, предупреждения и ликвидации последствий

компьютерных атак, направленных на информационные ресурсы РФ (ГосСОПКА). Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Совершенствование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Национальный координационный центр по компьютерным инцидентам. Порядок обмена информацией о компьютерных инцидентах между субъектами КИИ.

Перечень органов по аттестации. Реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий. Государственный реестр сертифицированных средств защиты информации. Документы по лицензионной деятельности ФСТЭК России в области технической защиты информации. Документы по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации.

14.1.4. Вопросы для подготовки к практическим занятиям, семинарам

Подготовка нормативных актов, необходимых для реализации Федерального закона «О персональных данных». Уведомлению уполномоченного органа о начале обработки персональных данных и внесении изменений в ранее представленные сведения

Категорирование объектов КИИ. Формы направления сведений о результатах присвоения

Согласована на портале № 51569

объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных

атак. Обмен информацией о компьютерных инцидентах между субъектами КИИ. Информирование ФСБ России о компьютерных инцидентах, реагирование на них, принятие мер по ликвидации последствий компьютерных атак.

Сертификация средств защиты информации. Формы заявления об аккредитации, формы и требования к содержанию прилагаемых к заявлению об аккредитации документов и документов, необходимых для организации и проведения аккредитации, а также документов, подтверждающих соответствие заявителя (аккредитованного лица) критериям аккредитации. Правила выполнения работ по аккредитации органов по сертификации и испытательных лабораторий, выполняющих работы по оценке соответствия в отношении продукции, используемой в целях защиты сведений, составляющих государственную тайну.

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адапти-

Согласована на портале № 51569

рованных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

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

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 51569