МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Нормативная база обеспечения информационной безопасности банковской организации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7**
Учебный план набора 2016 года

Распределение рабочего времени

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	28	28	часов
3	Всего аудиторных занятий	56	56	часов
4	Из них в интерактивной форме	16	16	часов
5	Самостоятельная работа	52	52	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е

Зачет: 7 семестр

Томск 2017

Согласована на портале № 17040

Рассмотрена и одобрена на заседании кафедры
протокол № 4 от «10» 5 2017 г.

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа 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 декабря 2016 года, рассмотрена и утверждена на заседании кафедры «___» _____ 20__ года, протокол №_____.

Разработчик:
МНС каф. КИБЭВС _____ Н. С. Егошин

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

Рабочая программа согласована с факультетом, профилирующей и выпускающей кафедрами направления подготовки (специальности).

Декан ФБ _____ Е. М. Давыдова

Заведующий выпускающей каф.
КИБЭВС _____ А. А. Шелупанов

Эксперт:

доцент каф. КИБЭВС _____ А. А. Конев

Согласована на портале № 17040

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины «Нормативная база обеспечения информационной безопасности банковской организации» является ознакомление с основными стандартами и регламентами, регулирующими информационную безопасность в сфере банковского дела.

1.2. Задачи дисциплины

– Задачи изучения дисциплины – получение студентами:

– – знаний о стандартах и регламентах, регулирующих работу банковских организаций в сфере информационной безопасности;

– – умений и навыков формирования и применения комплекса мер для обеспечения информационной безопасности автоматизированной банковской системы;

– – навыков по разработке и реализации политики информационной безопасности автоматизированных банковских систем;

– – навыков применения нормативных документов, относящихся к обеспечению информационной безопасности автоматизированных банковских систем

2. Место дисциплины в структуре ОПОП

Дисциплина «Нормативная база обеспечения информационной безопасности банковской организации» (Б1.Б.33.6) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются следующие дисциплины: Моделирование автоматизированных информационных систем, Организационное и правовое обеспечение информационной безопасности, Основы информационной безопасности, Основы управленческой деятельности, Правоведение, Системный анализ.

Последующими дисциплинами являются: Безопасность систем пластиковых карт, Документоведение, Защита информации в банковских системах.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПСК-5.5 способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы;

– ПСК-5.2 способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем;

– ПСК-5.1 способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;

В результате изучения дисциплины студент должен:

– **знать** Документацию, регламентирующую деятельности банковских организация в сфере информационной безопасности.

– **уметь** Применять нормативные правовые акты и нормативно-методические документы по обеспечению информационной безопасности автоматизированных банковских систем.

– **владеть** Навыками практического применения нормативно-правовых актов в сфере информационной безопасности касательно деятельности банковских организаций.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		7 семестр
Аудиторные занятия (всего)	56	56
Лекции	28	28
Практические занятия	28	28

Согласована на портале № 17040

Из них в интерактивной форме	16	16
Самостоятельная работа (всего)	52	52
Проработка лекционного материала	10	10
Подготовка к практическим занятиям, семинарам	42	42
Всего (без экзамена)	108	108
Общая трудоемкость ч	108	108
Зачетные Единицы	3.0	3.0

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	Лекции	Практические занятия	Самостоятельная работа	Всего часов (без экзамена)	Формируемые компетенции
7 семестр					
1 Общее описание деятельности службы безопасности банковской организации.	2	0	1	3	ПСК-5.1, ПСК-5.5
2 Становление стандартов ИБ Банка России	2	0	1	3	ПСК-5.2
3 Информационная безопасность банков с учетом СТО БР ИББС-2014	16	24	42	82	ПСК-5.1, ПСК-5.2, ПСК-5.5
4 Защита персональных данных в банках	2	0	1	3	ПСК-5.1
5 Информационная безопасность национальной платежной системы	2	0	1	3	ПСК-5.1, ПСК-5.2
6 Информационная безопасность платежных систем	2	0	1	3	ПСК-5.1, ПСК-5.2
7 Формирование СОИБ банковской организации.	2	4	5	11	ПСК-5.1, ПСК-5.2, ПСК-5.5
Итого за семестр	28	28	52	108	
Итого	28	28	52	108	

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

Согласована на портале № 17040

7 семестр			
1 Общее описание деятельности службы безопасности банковской организации.	Цели создания службы безопасности.-Средства деятельности службы безопасности.Нормативно-правовые акты, регулирующие деятельность службы безопасности.	2	ПСК-5.1, ПСК-5.5
	Итого	2	
2 Становление стандартов ИБ Банка России	История появления и развития стандартов ИБ Банка России	2	ПСК-5.2
	Итого	2	
3 Информационная безопасность банков с учетом СТО БР ИББС-2014	Подробный разбор СТО БР ИББССТО БР ИББС-1.0-2014. «Общие положения (5 редакция)».СТО БР ИББС-1.1-2007. «Аудит информационной безопасности».СТО БР ИББС-1.2-2014. «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 (4 редакция)».СТО БР ИББС-1.3-2016 «Сбор и анализ технических данных при выявлении и расследовании инцидентов информационной безопасности при осуществлении переводов денежных средств».РС БР ИББС-2.0-2007. «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствие с требованиями СТО БР ИББС-1.0».РС БР ИББС-2.1-2007. «Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности».РС БР ИББС-2.5-2014. «Менеджмент инцидентов информационной безопасности».РС БР ИББС-2.6-2014. «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем».РС БР ИББС-2.7-2015. «Ресурсное обеспечение информационной безопасности».РС БР ИББС-2.8-2015. «Обеспечение информационной безопасности при использовании технологии виртуализации».РС БР ИББС-2.9-2016. «Предотвращение утечек информации».РС БР ИББС-2.3-2010. «Требования по обеспечению безопасности	16	ПСК-5.1, ПСК-5.2, ПСК-5.5

Согласована на портале № 17040

	персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации».РС БР ИББС-2.4-2010 «Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации»		
	Итого	16	
4 Защита персональных данных в банках	Разбор Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных» в контексте информационной безопасности банковской организации.	2	ПСК-5.1
	Итого	2	
5 Информационная безопасность национальной платежной системы	Разбор вопроса о необходимости разработки национальной платёжной системы (НПС).Разбор подзаконных актов, направленных на обеспечение безопасности НПС.	2	ПСК-5.1, ПСК-5.2
	Итого	2	
6 Информационная безопасность платежных систем	Разбор стандарта PCI DSS.	2	ПСК-5.1, ПСК-5.2
	Итого	2	
7 Формирование СОИБ банковской организации.	Разбор этапов формирования СОИБ банковской организации.Знакомство с Циклом Деминга.	2	ПСК-5.1, ПСК-5.2, ПСК-5.5
	Итого	2	
Итого за семестр		28	

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	4	5	6	7
Предшествующие дисциплины							
1 Моделирование автоматизированных информационных систем			+				
2 Организационное и правовое обеспечение информационной безопасности			+	+	+	+	
3 Основы информационной безопасности	+						
4 Основы управленческой дея-							+

Согласована на портале № 17040

тельности							
5 Правоведение		+					
6 Системный анализ			+	+			
Последующие дисциплины							
1 Безопасность систем пластиковых карт					+	+	
2 Документоведение		+					
3 Защита информации в банковских системах			+	+			

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 и видов занятий, формируемых при изучении дисциплины

Компетенции	Виды занятий			Формы контроля
	Лекции	Практические занятия	Самостоятельная работа	
ПСК-5.5	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Зачет, Выступление (доклад) на занятии
ПСК-5.2	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Зачет, Выступление (доклад) на занятии
ПСК-5.1	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Зачет, Выступление (доклад) на занятии

6. Интерактивные методы и формы организации обучения

Технологии интерактивного обучения при разных формах занятий в часах приведены в таблице 6.1

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий в часах

Методы	Интерактивные практические занятия	Интерактивные лекции	Всего
7 семестр			
Презентации с использованием видеофильмов с обсуждением		2	2
Презентации с использованием слайдов с обсуждением		6	6

Согласована на портале № 17040

IT-методы	8		8
Итого за семестр:	8	8	16
Итого	8	8	16

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
7 семестр			
3 Информационная безопасность банков с учетом СТО БР ИББС-2014	Подробный разбор разделов СТО БР ИББС	24	ПСК-5.1, ПСК-5.2, ПСК-5.5
	Итого	24	
7 Формирование СОИБ банковской организации.	Формирования пакета документов, регламентирующих деятельность банковской организации в сфере информационной безопасности.	4	ПСК-5.1, ПСК-5.2, ПСК-5.5
	Итого	4	
Итого за семестр		28	

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
7 семестр				
1 Общее описание деятельности службы безопасности банковской организации.	Проработка лекционного материала	1	ПСК-5.1, ПСК-5.5	Зачет, Опрос на занятиях
	Итого	1		
2 Становление стандартов ИБ Банка России	Проработка лекционного материала	1	ПСК-5.2	Зачет, Опрос на занятиях
	Итого	1		
3 Информационная безопасность банков с учетом СТО БР ИББС-2014	Подготовка к практическим занятиям, семинарам	38	ПСК-5.1, ПСК-5.2, ПСК-5.5	Выступление (доклад) на занятии, Зачет, Опрос на занятиях
	Проработка лекционного материала	4		

Согласована на портале № 17040

	Итого	42		
4 Защита персональных данных в банках	Проработка лекционного материала	1	ПСК-5.1	Выступление (доклад) на занятии, Зачет, Опрос на занятиях
	Итого	1		
5 Информационная безопасность национальной платежной системы	Проработка лекционного материала	1	ПСК-5.1, ПСК-5.2	Выступление (доклад) на занятии, Зачет, Опрос на занятиях
	Итого	1		
6 Информационная безопасность платежных систем	Проработка лекционного материала	1	ПСК-5.1, ПСК-5.2	Выступление (доклад) на занятии, Зачет, Опрос на занятиях
	Итого	1		
7 Формирование СОИБ банковской организации.	Подготовка к практическим занятиям, семинарам	4	ПСК-5.1, ПСК-5.2, ПСК-5.5	Выступление (доклад) на занятии, Зачет, Опрос на занятиях, Отчет по индивидуальному заданию
	Проработка лекционного материала	1		
	Итого	5		
Итого за семестр		52		
Итого		52		

10. Курсовая работа (проект)

Не предусмотрено РУП

11. Рейтинговая система для оценки успеваемости студентов

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
7 семестр				
Выступление (доклад) на занятии			20	20
Зачет			30	30
Опрос на занятиях	5	5	10	20
Отчет по индивидуальному заданию			30	30
Итого максимум за период	5	5	90	100
Нарастающим итогом	5	10	100	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

Согласована на портале № 17040

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. Основы информационной безопасности: Учебное пособие / Голиков А. М. - 2007. 201 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1024, дата обращения: 10.05.2017.

2. Информационные технологии в экономике и управлении / В. В. Трофимов. – М.: Юрайт . – 2013. – 479 с. (наличие в библиотеке ТУСУР - 20 экз.)

12.2. Дополнительная литература

1. Банковское дело: Учебное пособие / Черская Р. В. - 2015. 160 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/6794, дата обращения: 10.05.2017.

2. Информационные системы в банковской деятельности: учебное пособие / С. Ю. Золотов, Е. Б. Грибанова; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра автоматизированных систем управления. – Томск: ТМЦДО, 2008. – 103 с (наличие в библиотеке ТУСУР - 20 экз.)

12.3 Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Информационные системы и технологии в экономике: Методические указания по выполнению лабораторных и самостоятельных работ / Афанасьева И. Г., Дубровин А. В. - 2011. 89 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2264, дата обращения: 10.05.2017.

2. МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ [Электронный ресурс]. - http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god

3. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1017, дата обращения: 10.05.2017.

Согласована на портале № 17040

12.3.2 Учебно-методические пособия для лиц с ограниченными возможностями здоровья

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа 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. Базы данных, информационно-справочные, поисковые системы и требуемое программное обеспечение

1. Консультант Плюс

13. Материально-техническое обеспечение дисциплины

13.1. Общие требования к материально-техническому обеспечению дисциплины

13.1.1. Материально-техническое 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 наглядные пособия в виде презентаций по лекционным разделам дисциплины.

13.1.2. Материально-техническое обеспечение для практических занятий

Для проведения практических занятий используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью.

13.1.3. Материально-техническое обеспечение для самостоятельной работы

Для проведения самостоятельных работ используется учебная аудитория, с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью.

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

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения.

При обучении студентов **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах для студентов с нарушениями слуха, мобильной системы обучения для студентов с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой обучаются студенты с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При обучении студентов **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 удаленного просмотра.

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

14. Фонд оценочных средств

14.1. Основные требования к фонду оценочных средств и методические рекомендации

Фонд оценочных средств и типовые контрольные задания, используемые для оценки сформированности и освоения закрепленных за дисциплиной компетенций при проведении текущей,

Согласована на портале № 17040

промежуточной аттестации по дисциплине приведен в приложении к рабочей программе.

14.2 Требования к фонду оценочных средств для лиц с ограниченными возможностями здоровья

Для студентов с инвалидностью предусмотрены дополнительные оценочные средства, перечень которых указан в таблице.

Таблица 14 – Дополнительные средства оценивания для студентов с инвалидностью

Категории студентов	Виды дополнительных оценочных средств	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 средствам для лиц с ограниченными возможностями здоровья

Для студентов с ОВЗ 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.

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов 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 инвалидов по дисциплине предусматривает предоставление информации 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.

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 17040

Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П. Е. Троян
«___» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Нормативная база обеспечения информационной безопасности банковской организации

Уровень образования: **высшее образование - специалитет**
Направление подготовки (специальность): **10.05.03 Информационная безопасность автоматизированных систем**
Направленность (профиль): **Информационная безопасность автоматизированных банковских систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7**

Учебный план набора 2016 года

Разработчик:
- МНС каф. КИБЭВС Н. С. Егошин

Зачет: 7 семестр

Томск 2017

Согласована на портале № 17040

1. Введение

Фонд оценочных средств (ФОС) является приложением к рабочей программе дисциплины (практики) и представляет собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.) и методов их использования, предназначенных для измерения уровня достижения студентом установленных результатов обучения.

ФОС по дисциплине (практике) используется при проведении текущего контроля успеваемости и промежуточной аттестации студентов.

Перечень закрепленных за дисциплиной (практикой) компетенций приведен в таблице 1.

Таблица 1 – Перечень закрепленных за дисциплиной компетенций

Код	Формулировка компетенции	Этапы формирования компетенций
ПСК-5.5	способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы	Должен знать Документацию, регламентирующую деятельности банковских организация в сфере информационной безопасности.; Должен уметь Применять нормативные правовые акты и нормативно-методические документы по обеспечению информационной безопасности автоматизированных банковских систем.; Должен владеть Навыками практического применения нормативно-правовых актов в сфере информационной безопасности касательно деятельности банковских организаций.;
ПСК-5.2	способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем	
ПСК-5.1	способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем	

Общие характеристики показателей и критериев оценивания компетенций на всех этапах приведены в таблице 2.

Таблица 2 – Общие характеристики показателей и критериев оценивания компетенций по этапам

Показатели и критерии	Знать	Уметь	Владеть
Отлично (высокий уровень)	Обладает фактическими и теоретическими знаниями в пределах изучаемой области с пониманием границ применимости	Обладает диапазоном практических умений, требуемых для развития творческих решений, абстрагирования проблем	Контролирует работу, проводит оценку, совершенствует действия работы
Хорошо (базовый уровень)	Знает факты, принципы, процессы, общие понятия в пределах изучаемой области	Обладает диапазоном практических умений, требуемых для решения определенных проблем в области исследования	Берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем
Удовлетворительно (пороговый уровень)	Обладает базовыми общими знаниями	Обладает основными умениями, требуемыми для выполнения простых задач	Работает при прямом наблюдении

2 Реализация компетенций

2.1 Компетенция ПСК-5.5

ПСК-5.5: способностью формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированной банковской системы.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания пред-

Согласована на портале № 17040

ставлены в таблице 3.

Таблица 3 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Принципы организации нормативно-правовых актов	Формировать комплекс мер для обеспечения информационной безопасности автоматизированной банковской системы	Навыками применения комплекса мер для обеспечения информационной безопасности автоматизированной банковской системы
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по индивидуальному заданию; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Отчет по индивидуальному заданию; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Отчет по индивидуальному заданию; • Выступление (доклад) на занятии; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 4.

Таблица 4 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• Знает в полном объёме принципы организации нормативно-правовых актов;	• В полном объёме умеет формировать комплекс мер для обеспечения информационной безопасности автоматизированной банковской системы;	• В полном объёме владеет навыками применения комплекса мер для обеспечения информационной безопасности автоматизированной банковской системы;
Хорошо (базовый уровень)	• Знает на продвинутом уровне принципы организации нормативно-правовых актов;	• На продвинутом уровне умеет формировать комплекс мер для обеспечения информационной безопасности автоматизированной банковской системы;	• На продвинутом уровне владеет навыками применения комплекса мер для обеспечения информационной безопасности автоматизированной банковской системы;
Удовлетворительно (пороговый уровень)	• Знает на базовом уровне принципы организации нормативно-правовых актов;	• На базовом уровне умеет формировать комплекс мер для обеспечения информационной безопасности автоматизированной	• На базовом уровне владеет навыками применения комплекса мер для обеспечения информационной безопасности автоматизирован-

Согласована на портале № 17040

		банковской системы;	ной банковской системы;

2.2 Компетенция ПСК-5.2

ПСК-5.2: способностью разрабатывать и реализовывать политики информационной безопасности автоматизированных банковских систем.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 5.

Таблица 5 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Способы разработки и реализации политики информационной безопасности автоматизированных банковских систем	Разрабатывать политики информационной безопасности автоматизированных банковских систем	Навыками реализации политики информационной безопасности автоматизированных банковских систем
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по индивидуальному заданию; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Отчет по индивидуальному заданию; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Отчет по индивидуальному заданию; • Выступление (доклад) на занятии; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 6.

Таблица 6 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• В полном объёме знает способы разработки и реализации политики информационной безопасности автоматизированных банковских систем;	• В полном объёме умеет разрабатывать политики информационной безопасности автоматизированных банковских систем;	• В полном объёме владеет навыками реализации политики информационной безопасности автоматизированных банковских систем;
Хорошо (базовый уровень)	• На продвинутом уровне знает способы разработки и реализации политики информационной безопасности автоматизированных банковских систем;	• На продвинутом уровне умеет разрабатывать политики информационной безопасности автоматизированных банковских систем;	• На продвинутом уровне владеет навыками реализации политики информационной безопасности автоматизированных банковских систем;
Удовлетворительн	• На базовом уровне	• На базовом уровне	• На базовом уровне

Согласована на портале № 17040

о (пороговый уровень)	знает способы разработки и реализации политики информационной безопасности автоматизированных банковских систем;	умеет разрабатывать политики информационной безопасности автоматизированных банковских систем;	владеет навыками реализации политики информационной безопасности автоматизированных банковских систем;

2.3 Компетенция ПСК-5.1

ПСК-5.1: способностью на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем.

Для формирования компетенции необходимо осуществить ряд этапов. Этапы формирования компетенции, применяемые для этого виды занятий и используемые средства оценивания представлены в таблице 7.

Таблица 7 – Этапы формирования компетенции и используемые средства оценивания

Состав	Знать	Уметь	Владеть
Содержание этапов	Структуру нормативных документов, относящихся к обеспечению информационной безопасности автоматизированных банковских систем	Применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем	Навыками использования нормативных документов, относящизся к обеспечению информационной безопасности автоматизированных банковских систем
Виды занятий	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Интерактивные лекции; • Практические занятия; • Лекции; • Самостоятельная работа;	• Интерактивные практические занятия; • Самостоятельная работа;
Используемые средства оценивания	• Отчет по индивидуальному заданию; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Отчет по индивидуальному заданию; • Опрос на занятиях; • Выступление (доклад) на занятии; • Зачет;	• Отчет по индивидуальному заданию; • Выступление (доклад) на занятии; • Зачет;

Формулировка показателей и критериев оценивания данной компетенции приведена в таблице 8.

Таблица 8 – Показатели и критерии оценивания компетенции на этапах

Состав	Знать	Уметь	Владеть
Отлично (высокий уровень)	• В полном объёме знает структуру нормативных документов, относящихся к обеспечению информационной безопасности автоматизированных банковских систем;	• В полном объёме умеет применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;	• В полном объёме владеет навыками использования нормативных документов, относящизся к обеспечению информационной безопасности автоматизированных банковских систем;
Хорошо (базовый уровень)	• На продвинутом уровне знает структуру	• На продвинутом уровне умеет приме-	• На продвинутом уровне владеет навыка-

Согласована на портале № 17040

	нормативных документов, относящихся к обеспечению информационной безопасности автоматизированных банковских систем;	нять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;	ми использования нормативных документов, относящизся к обеспечению информационнобъй безопасности автоматизированных банковских систем;
Удовлетворительно (пороговый уровень)	• На базовом уровне знает структуру нормативных документов, относящихся к обеспечению информационной безопасности автоматизированных банковских систем;	• На базовом уровне умеет применять нормативные документы, относящиеся к обеспечению информационной безопасности автоматизированных банковских систем;	• На базовом уровне владеет навыками использования нормативных документов, относящизся к обеспечению информационнобъй безопасности автоматизированных банковских систем;

3 Типовые контрольные задания

Для реализации вышеперечисленных задач обучения используются типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы, в следующем составе.

3.1 Зачёт

– Какими нормативно-правовыми актами регулируется деятельность службы безопасности банковской организации?

3.2 Темы индивидуальных заданий

– Разработка пакета документов, регулирующих информационную безопасность на примере выдуманной студентом банковской организации

3.3 Темы опросов на занятиях

– История появления и развития стандартов ИБ Банка России
– Подробный разбор СТО БР ИББС
– СТО БР ИББС-1.0-2014. «Общие положения (5 редакция)».
– СТО БР ИББС-1.1-2007. «Аудит информационной безопасности».
– СТО БР ИББС-1.2-2014. «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 (4 редакция)».
– СТО БР ИББС-1.3-2016 «Сбор и анализ технических данных при выявлении и расследовании инцидентов информационной безопасности при осуществлении переводов денежных средств».
– РС БР ИББС-2.0-2007. «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствие с требованиями СТО БР ИББС-1.0».
– РС БР ИББС-2.1-2007. «Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».
– РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности».
– РС БР ИББС-2.5-2014. «Менеджмент инцидентов информационной безопасности».
– РС БР ИББС-2.6-2014. «Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем».
– РС БР ИББС-2.7-2015. «Ресурсное обеспечение информационной безопасности».
– РС БР ИББС-2.8-2015. «Обеспечение информационной безопасности при использовании технологии виртуализации».

Согласована на портале № 17040

– РС БР ИББС-2.9-2016. «Предотвращение утечек информации».

– РС БР ИББС-2.3-2010. «Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации».

– РС БР ИББС-2.4-2010 «Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации»

– Разбор Федерального закона РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных» в контексте информационной безопасности банковской организации.

– Разбор вопроса о необходимости разработки национальной платёжной системы (НПС).

– Разбор подзаконных актов, направленных на обеспечение безопасности НПС.

– Разбор стандарта PCI DSS.

– Разбор этапов формирования СОИБ банковской организации.

– Знакомство с Циклом Деминга.

3.4 Темы докладов

– Один из разделов СТО БР ИББС

4 Методические материалы

Для обеспечения процесса обучения и решения задач обучения используются следующие материалы:

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы фор-мирования компетенций, согласно п. 12 рабочей программы.

4.1. Основная литература

1. Основы информационной безопасности: Учебное пособие / Голиков А. М. - 2007. 201 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1024, свободный.

2. Информационные технологии в экономике и управлении / В. В. Трофимов. – М.: Юрайт . – 2013. – 479 с. (наличие в библиотеке ТУСУР - 20 экз.)

4.2. Дополнительная литература

1. Банковское дело: Учебное пособие / Черская Р. В. - 2015. 160 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/6794, свободный.

2. Информационные системы в банковской деятельности: учебное пособие / С. Ю. Золотов, Е. Б. Грибанова; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра автоматизированных систем управления. – Томск: ТМЦДО, 2008. – 103 с (наличие в библиотеке ТУСУР - 20 экз.)

4.3. Обязательные учебно-методические пособия

1. Информационные системы и технологии в экономике: Методические указания по выполнению лабораторных и самостоятельных работ / Афанасьева И. Г., Дубровин А. В. - 2011. 89 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/2264, свободный.

2. МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ [Электронный ресурс]. - http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god

3. Основы информационной безопасности: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. [Электронный ресурс] - Режим доступа: https://edu.tusur.ru/publications/1017, свободный.

4.4. Базы данных, информационно справочные и поисковые системы

1. Консультант Плюс

Согласована на портале № 17040