МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА 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) / 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: **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

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 23.08.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск 2018

Согласована на портале № 36616

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от « 15 » 5 2018 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 №_____.

Разработчик:

Доцент каф. КИБЭВС _____ Е. Ю. Костюченко

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 каф. КИБЭВС _____ Е. М. Давыдова

Доцент каф. КИБЭВС _____ А. А. Конев

Согласована на портале № 36616

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

– получение знаний о стандартах и регламентах, регулирующих работу банковских организаций в

– сфере информационной безопасности;

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

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

– получение 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: 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, Подготовка к сдаче и сдача государственного экзамена, Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– 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;

– 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;

В результате изучения дисциплины обучающийся 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

Согласована на портале № 36616

Лекции	28	28
Практические занятия	28	28
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	Лек., ч	Прак. зан., ч	Сам. раб., ч	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
7 семестр			
1 Общее описание деятельности службы безопасности банковской	Цели создания службы безопасности.-Средства деятельности службы без-опасности.Нормативно-правовые акты,регулирующие деятельность	2	ПСК-5.1, ПСК-5.5

Согласована на портале № 36616

организации.	службыбезопасности		
	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 персональных данных в информационных системах персональных	16	ПСК-5.1, ПСК-5.2, ПСК-5.5

Согласована на портале № 36616

	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 Организационное и правовое обеспечение информационной безопасности			+	+	+	+	
2 Основы информационной безопасности	+						
3 Основы управленческой деятельности							+
4 Правоведение		+					

Согласована на портале № 36616

5 Системный анализ			+	+			
Последующие дисциплины							
1 Безопасность систем пластиковых карт					+	+	
2 Документоведение		+					+
3 Защита информации в банковских системах		+	+		+		+
4 Подготовка к сдаче и сдача государственного экзамена	+	+	+	+	+	+	+
5 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.	
ПСК-5.2	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Зачет, Выступление (доклад) на занятии, Тест
ПСК-5.1	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Зачет, Выступление (доклад) на занятии, Тест
ПСК-5.5	+	+	+	Отчет по индивидуальному заданию, Опрос на занятиях, Зачет, Выступление (доклад) на занятии, Тест

6. Интерактивные методы и формы организации обучения

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

Таблица 6.1 – Технологии интерактивного обучения при разных формах занятий

Методы	Интерактивные практические занятия, ч	Интерактивные лекции, ч	Всего, ч
7 семестр			
Презентации с использованием видеофильмов с обсуждением		2	2
Презентации с использованием слайдов с обсуждением		6	6
IT-методы	8		8
Итого за семестр:	8	8	16
Итого	8	8	16

7. Лабораторные работы

Не предусмотрено РУП.

Согласована на портале № 36616

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 БРИББС	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, Тест
	Итого	1		
2 Становление стандартов ИБ Банка России	Проработка лекционного материала	1	ПСК-5.2	Зачет, Опрос на занятиях, Тест
	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, Тест
	Проработка лекционного материала	4		
	Итого	42		
4 Защита персональных данных в банках	Проработка лекционного материала	1	ПСК-5.1	Выступление (доклад) на занятии, Зачет, Опрос на занятиях, Тест
	Итого	1		
5 Информационная безопасность национальной платежной	Проработка лекционного материала	1	ПСК-5.1, ПСК-5.2	Выступление (доклад) на занятии, Опрос на занятиях, Тест
	Итого	1		

Согласована на портале № 36616

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

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
7 семестр				
Выступление (доклад) на занятии			20	20
Зачет			30	30
Опрос на занятиях	5	5	10	20
Отчет по индивидуальному заданию			20	20
Тест			10	10
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
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

Согласована на портале № 36616

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 [Электронный ресурс]: Учебное пособие / Голиков А. М. - 2007. 201 с. — Режим доступа: https://edu.tusur.ru/publications/1024 (дата обращения: 19.05.2018).

12.2. Дополнительная литература

1. Информационные технологии в экономике и управлении / В. В. Трофимов. – М.: Юрайт. – 2013. – 479 с. (наличие в библиотеке ТУСУР - 16 экз.)
2. Банковское дело [Электронный ресурс]: Учебное пособие / Черская Р. В. - 2015. 160 с. — Режим доступа: https://edu.tusur.ru/publications/6794 (дата обращения: 19.05.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Информационные системы и технологии в экономике [Электронный ресурс]: Методические указания по выполнению лабораторных и самостоятельных работ / Афанасьева И. Г., Дубровин А. В. - 2011. 89 с. — Режим доступа: https://edu.tusur.ru/publications/2264 (дата обращения: 19.05.2018).
2. МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ [Электронный ресурс]: — Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380 (дата обращения: 19.05.2018).
3. Основы информационной безопасности [Электронный ресурс]: Учебное пособие для практических и семинарских занятий / Голиков А. М. - 2007. 154 с. — Режим доступа: https://edu.tusur.ru/publications/1017 (дата обращения: 19.05.2018).

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:

Согласована на портале № 36616

– 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. Гарант, Консультант Плюс

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

Лаборатория "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 (15 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security
– Microsoft Windows 10
– VirtualBox
– Visio

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.

Согласована на портале № 36616

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:

14.1.1. Тестовые задания

1. Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС) – это …

• законодательный акт Российской Федерации, принимаемый в соответствии с Конституцией Российской Федерации по предметам ведения Российской Федерации и по предметам совместного ведения Российской Федерации и её субъектов

• разрешение на право, либо право на выполнение некоторых действий

• комплекс документов Банка России, описывающий единый подход к построению системы обеспечения ИБ организаций банковской сферы с учётом требований российского законодательства

• стандарт по информационной безопасности опубликованный совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC)

2. Какой нормативный документ регулирует права банков в сфере обработки персональных данных?

• СТО БР ИББС

• 152-ФЗ

• ISO 27000

• УК 159

3. Стандарт безопасности данных индустрии платёжных карт, разработанный Советом по стандартам безопасности индустрии платежных карт, учреждённым международными платёжными системами Visa, MasterCard, American Express, JCB и Discover – это …

• EMV

• PCI DSS

Согласована на портале № 36616

• GSM
• RSA

4. Как называется серия международных стандартов, включающая стандарты по информационной безопасности опубликованные совместно Международной Организацией по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC)?

• ISO 9000
• ГОСТ 34025-2016
• ISO/IEC 27000
• RSA 20189

5. Как называется банк, выпускающий в обращение денежные знаки или ценные бумаги, а также банковские карты, выдаваемые клиенту в пользование?

• Хозяин
• Держатель
• Плательщик
• Эмитент

6. НПС – это …

• Номинальная пропускная способность
• Национальная платежная система
• Национальное платежное средство
• Нормативно правовой стандарт

7. Национальная система платёжных карт России носит название …

• Союз
• Спутник
• Мир
• Труд

8. СОИБ – это …

• Стандарт обеспечения информационной безопасности
• Система обеспечения информационной безопасности
• Стратегическая оборонная инициатива безопасности
• Средство ограничения использования бюджета

9. Согласно СТО БР ИББС-1.0-2014 что заложено в основу работы СОИБ?

• Цикл Деминга
• Цикл Леминга
• Цикл Фурье
• Цикл Качи

10. Что из нижесказанного не присутствует в Цикле Деминга для СОИБ?

• Планирование СОИБ
• Реализация СОИБ
• Совершенствование СОИБ
• Утилизация СОИБ

11. Как называется международный стандарт для операций по банковским картам с чипом, разработанный совместными усилиями компаний Europay, MasterCard и Visa, чтобы повысить уровень безопасности финансовых операций?

• CVV
• GSM
• EMV
• Des

12. Как называется система, предназначенная для оценки финансовых транзакций в Интернете на предмет подозрительности с точки зрения мошенничества и предлагающая рекомендации по их дальнейшей обработке?

• Изолированная среда
• Антивирус
• Антифрод система
• Платёжный шлюз

Согласована на портале № 36616

13. Как называется аппаратно-программный комплекс, который позволяет автоматизировать процесс приема платежей в Интернете?

• Криптошлюз
• Фишинговый сайт
• Платежный шлюз
• Медиапортал

14. Как называется аппаратно-программный комплекс криптографической защиты трафика данных, голоса, видео на основе шифрования пакетов при установлении соединения?

• Медиашлюз
• Платежный шлюз
• Криптошлюз
• Файловый шлюз

15. Коммерческая тайна – это ...

• информация по счетам или вкладам своих клиентов и корреспондентов;
• любая информация, обеспечивающая достижение преимуществ над конкурентами и извлечение прибыли;
• информация об объемах и структуре предоставленных и полученных кредитов и депозитов;

16. Механизм электронной подписи реализует следующие функции:

• Шифрование, сертификация;
• Аутентификация, шифрование;
• Сертификация, аутентификация.

17. Промышленный шпионаж – это ...

• получение обманным путем конфиденциальной информации, используемой в различных противоправных целях;
• уголовно наказуемое и иное противоправное деяние, посягающее на имущественные и приравненные к ним права и интересы банка либо на порядок его функционирования;
• присвоение кредитов по фиктивным банковским гарантиям подставными фирмами.

18. Данные составляющие банковскую тайну - это ...

• объёмы инвестиций, планы маркетинга;
• базы данных об акционерах и специалистах;
• информация банковского вклада, операций по счёту и сведений о клиенте.

19. Задача проведения анализа уязвимости информационной банковской системы сводится к ...

• рассмотрению всех возможных угроз и оценка размеров возможного ущерба;
• определению всех возможных слабых мест информационной банковской системы;
• регламентации деятельности кредитной организации.

20. Аутентификация – это ...

• проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности;
• реквизит электронного документа, предназначенный для защиты данного документа от модификации;
• наука о методах обеспечения конфиденциальности и аутентичности информации.

14.1.2. Темы индивидуальных заданий

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

14.1.3. Зачёт

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

Назовите этапы формирования СОИБ банковской организации

Опишите стандарт PCI DSS

Для чего используется цикл Деминга?

Согласована на портале № 36616

14.1.4. 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».

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»

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

Необходимость разработки национальной платёжной системы (НПС)

Разбор подзаконных актов, направленных на обеспечение безопасности НПС

Стандарт PCI DSS

Этапы формирования СОИБ банковской организации

Цикл Деминга

14.1.5. Темы докладов

Один из разделов СТО БР ИББС

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.

Согласована на портале № 36616

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

Согласована на портале № 36616