Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.
“___”_____ _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Информационная безопасность банковской деятельности

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Курс: 4, семестр : 7

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**7**
1	Всего зачетных единиц (кредитов)	3
2	Всего часов	108
3	Всего занятий в контактной форме, час.	61
4	Лекции, час.	18
5	Практические занятия, час.	36
6	Лабораторные занятия, час.	0
7	из них в активной и интерактивной форме, час.	12
8	Аттестация, час.	2
9	Консультации, час.	5
10	Самостоятельная работа, час.	47
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	3

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС введен в действие приказом №1509 от 01.12.2016 г. , дата утверждения: 20.12.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, вариативная, по выбору студента

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

Рабочая программа обсуждена на заседании кафедры

ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

старший преподаватель, Дронов В. Ю.

Заведующий кафедрой:

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

заведующий кафедрой Трушин В. А.

1. Внешние требования

Таблица 1.1

***Компетенция ФГОС*: ОК.2 способность использовать основы экономических знаний в различных сферах деятельности; *в части следующих результатов обучения*:**
з3. знать основы организации и управления предприятием в условиях рынка
***Компетенция ФГОС*: ПК.11 способность разрабатывать политику информационной безопасности автоматизированной системы; *в части следующих результатов обучения*:**
з1. знать принципы формирования политики информационной безопасности в автоматизированных системах
***Компетенция ФГОС*: ПК.23 способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа; *в части следующих результатов обучения*:**
у2. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
у3. уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем
***Компетенция ФГОС*: ПСК.33 способность применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов; *в части следующих результатов обучения*:**
у2. уметь работать с нормативными правовыми актами в области технической защиты информации ограниченного доступа на предприятии (в организации, учреждении)

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	**Формы организации занятий**
Информационная безопасность банковской деятельности	
ОК.2.з3 знать основы организации и управления предприятием в условиях рынка	
1.знать основы организации и управления предприятием в условиях рынка	Лекции; Практические занятия; Самостоятельная работа
ПК.11.з1 знать принципы формирования политики информационной безопасности в автоматизированных системах	
2.знать принципы формирования политики информационной безопасности в автоматизированных системах	Лекции; Практические занятия; Самостоятельная работа
ПК.23.у2 уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	
3.уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Лекции; Практические занятия; Самостоятельная работа
ПК.23.у3 уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем	
4.уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем	Лекции; Практические занятия; Самостоятельная работа
ПСК.33.у2 уметь работать с нормативными правовыми актами в области технической защиты информации ограниченного доступа на предприятии (в организации, учреждении)	
5.уметь работать с нормативными правовыми актами в области технической защиты информации ограниченного доступа на предприятии (в организации, учреждении)	Лекции; Практические занятия; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Общие понятия об информационных технологиях				
1. Основные понятия, применяемые в информационных технологиях	0	3	1, 2	Аппаратное и программное обеспечение вычислительной техники, информационные процессы и информационные технологии. Системное и прикладное программное обеспечение, понятие информационных ресурсов (объектов) и пользователей данных ресурсов (субъектов). Основные функции операционной системы ПЭВМ, встроенные возможности разграничения доступа, блокировка доступа к рабочей станции. Идентификация и аутентификация пользователей автоматизированных систем, понятие учетных записей, полномочия администраторов и пользователей систем (привилегии, роли), автоматическая блокировка/разблокировка учетных записей. Использование паролей, понятие структуры пароля, правила выбора стойких паролей, подбор паролей с использование специализированных программ. Использование локально-вычислительных сетей, понятие сетевых ресурсов, изолированность сегментов локально-вычислительных сетей, разграничение прав доступа к сетевым ресурсам (на примере сети Windows), анализ системных журналов, резервирование и архиви-
Дидактическая единица: Обеспечение информационной безопасности и защита автоматизированных систем.				

2. Средства криптографической защиты информации.	0	3	3, 4	Шифрование данных при хранении и передачи (симметричное/асимметричное шифрование). Понятие электронно-цифровой подписи, цифровых сертификатов, описание механизмов аутентификации. Средства криптографической защиты информации в банковской системе
3. Основные понятия информационной безопасности.	0	3	1, 2, 4	Политика безопасности в системе, критичные информационные ресурсы. Разграничение доступа к ресурсам, понятие несанкционированного доступа и несанкционированного воздействия. Понятие целостности и лицензионной чистоты программного обеспечения
Дидактическая единица: Информационная безопасность в системе Банка России				
4. История банковского дела	0	3	2, 3, 4, 5	Ростовщики. Трапезиты. История банков в России. Виды банков. Функции банков. Правовое регулирование банковской деятельностью
5. Автоматизированные банковские системы	0	2	1, 2, 3, 4, 5	Особенности автоматизированных банковских систем, используемых в российских банках. Информационное обеспечение автоматизированных банковских систем. Техническое оснащение современных автоматизированных банковских систем. Программное обеспечение автоматизированных банковских систем.
6. Пластиковые карты, электронные деньги	0	2	1, 2, 3, 4, 5	История развития пластиковых карт. История банковских карт в России. Виды электронных денег и их применение.

7. Реализация требований информационной безопасности в системе Банка России.	0	2	1, 2, 3, 4, 5	Основные направления политики информационной безопасности и нормативная база Банка России. Стандарты Банка России. Применяемые в ТУ Банка России меры и средства защиты информации, функции администраторов информационной безопасности подразделений. Особенности использования средств защиты информации от несанкционированного доступа. Организация бесперебойного функционирования информационных систем.

Таблица 3.2

Темы практических занятий	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Информационная безопасность в системе Банка России				
1. Идентификация и аутентификация пользователей автоматизированных систем, блокировка/разблокировка учетных записей.	2	6	3, 4, 5	Информационное обеспечение автоматизированных банковских систем.
2. Создание электронно-цифровой подписи, работа с цифровыми сертификатами.	2	6	1, 2, 5	Организация бесперебойного функционирования информационных систем.
3. Разграничение доступа к ресурсам, целостность и лицензионная чистоты программного обеспечения	2	6	1, 3, 5	Особенности использования средств защиты информации от несанкционированного доступа.
4. Программное обеспечение автоматизированных банковских систем, установка и настройка.	2	6	2, 5	Стандарты Банка России. Применяемые в ТУ Банка России меры и средства
5. Работа с ПО для пластиковых карт.	2	6	2, 4	Виды электронных денег и их применение.
6. Работа под администратором информационной безопасности с ПО.	2	6	1, 2, 3	Основные направления политики информационной безопасности и нормативная база

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 7				
1	РГЗ	1, 3, 4, 5	12	3
РГЗ: Дронов В. Ю. Информационная безопасность банковской деятельности : учебно-методическое пособие / В. Ю. Дронов, В. В. Анюшин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 12, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234007				
2	Подготовка к занятиям	1, 2	20	0
, подробная информация приведена в приложении №1 : Дронов В. Ю. Информационная безопасность банковской деятельности : учебно-методическое пособие / В. Ю. Дронов, В. В. Анюшин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 12, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234007				
3	Подготовка к аттестации	1, 2, 3, 4, 5	15	2
: Дронов В. Ю. Информационная безопасность банковской деятельности : учебно-методическое пособие / В. Ю. Дронов, В. В. Анюшин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 12, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234007				

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	e-mail; Социальные сети
Консультирование	e-mail; Социальные сети

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставлять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Мин. балл	Максимальный балл
Семестр: 7		
Дополнительная учебная деятельность:	0	
РГЗ:	10	60
Контролирующие материалы (список вопросов) приводятся в "Дронов В. Ю. Информационная безопасность банковской деятельности : учебно-методическое пособие / В. Ю. Дронов, В. В. Анюшин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 12, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234007"		
Зачет:	10	40
Контролирующие материалы (список вопросов) приводятся в "Дронов В. Ю. Информационная безопасность банковской деятельности : учебно-методическое пособие / В. Ю. Дронов, В. В. Анюшин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 12, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234007"		

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля	
		Защита РГЗ	Зачет
ОК.2	з3. знать основы организации и управления предприятием в условиях рынка	+	+
ПК.11	з1. знать принципы формирования политики информационной безопасности в автоматизированных системах	+	+
ПК.23	у2. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	+	+
	у3. уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем	+	+
ПСК.33	у2. уметь работать с нормативными правовыми актами в области технической защиты информации ограниченного доступа на предприятии (в организации, учреждении)	+	+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Белоглазова Г. Н. Банковское дело. Организация деятельности коммерческого банка : учебник / Г. Н. Белоглазова, Л. П. Кроливецкая ; С.-Петерб. гос. ун-т экономики и финансов (ФИНЭК). - М., 2009. - 422 с.

2. Ольхова Р. Г. Банковское дело: управление в современном банке : [учебное пособие для вузов по специальностям "Финансы и кредит", "Бухгалтерский учет, анализ и аудит"] / Р. Г. Ольхова. - Москва, 2009. - 303, [1] с. : ил., табл.

3. Банковское дело : [учебник для вузов / Е. Ф. Жуков и др.] ; под ред. Е. Ф. Жукова, Н. Д. Эриашвили ; Междунар. банк. об-ние. - Москва, 2007. - 574, [2] с. : ил., табл.. - Авт. указаны на 576-й с..

Дополнительная литература

1. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : [учебное пособие для вузов по специальности 075400 - "Комплексная защита объектов информации"] / А. А. Малюк. - М., 2004. - 280 с. : ил., табл.

2. Ярочкин В. И. Информационная безопасность : [учебник для вузов по гуманитарным и социально-экономическим специальностям] / В. И. Ярочкин. - М., 2004. - 542, [1] с. : ил., табл.

Интернет-ресурсы

1. ЭБС НГТУ : http://elibrary.nstu.ru/

2. ЭБС «Издательство Лань» : https://e.lanbook.com/

3. ЭБС IPRbooks : http://www.iprbookshop.ru/

4. ЭБС "Znanium.com" : http://znanium.com/

5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Дронов В. Ю. Информационная безопасность банковской деятельности : учебно-методическое пособие / В. Ю. Дронов, В. В. Анюшин ; Новосиб. гос. техн. ун-т. - Новосибирск, 2016. - 12, [4] с. : ил.. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000234007

8.2 Специализированное программное обеспечение

1 Windows

2 Office

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Для демонстрации основных положений курса

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“___”_____ _____ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность банковской деятельности

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Новосибирск 2017

1. **Обобщенная структура фонда оценочных средств учебной дисциплины**

Обобщенная структура фонда оценочных средств по дисциплине **Информационная безопасность банковской деятельности** приведена в Таблице.

Таблица

Формируемые компетенции	**Показатели сформированности компетенций (знания, умения, навыки)**	**Темы**	**Этапы оценки компетенций**	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	**Промежуточная аттестация (экзамен, зачет)**
ОК.2 способность использовать основы экономических знаний в различных сферах деятельности	з3. знать основы организации и управления предприятием в условиях рынка	История банковского дела Современный рынок кредитно-финансовых услуг, тенденции и тренды Формы и модели организации банковского бизнеса ИБ как бизнес процесс организации		Зачет, Вопросы 1.1, 1.2, 2.1, 2.4
ПК.11/ПК способность разрабатывать политику информационной безопасности автоматизированной системы	з1. знать принципы формирования политики информационной безопасности в автоматизированных системах	Современные угрозы бизнесу КФО, эволюция угроз, аналитика перспектив развития методов кибератак Модель угроз и модель нарушителя Требования к СОИБ со стороны государства, регуляторов, международных финансовых институтов Методология создания политик ИБ различного уровня	РГЗ, разделы 1.1-1.3	Зачет, Вопросы 1.4, 2.3
ПК.23/ОУ способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	у3. уметь определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем	Наличные и безналичные финансовые средства, платежные системы, виртуальные деньги, ДБО, пластиковые карты, электронные кошельки ИТ-архитектура КФО Виды и характеристики кибератак на КФО Определение уязвимостей, оценка угроз, управление рисками Модель угроз и модель нарушителя Нормативная база ИБ, требования регуляторов, стандарты Организационно-технические требования, методы разработки, реализации, контроля	РГЗ, разделы 1.1-1.3	Зачет, Вопросы 1.3, 1.5-1.10, 2.2, 2.5-2.10
ПК.23/ОУ	у2. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Определение уязвимостей, оценка угроз, управление рисками Классы технических систем защиты информации, способы применения, контроль результативности	РГЗ, разделы 1.1-1.3	Зачет, Вопросы 1.3, 1.5-1.10, 2.2, 2.5-2.10

ПСК.33 способность применять современную нормативную базу, регламентирующую деятельность критически важных объектов и обеспечение информационной безопасности критически важных объектов и автоматизированных систем критически важных объектов	у2. уметь работать с нормативными правовыми актами в области технической защиты информации ограниченного доступа на предприятии (в организации, учреждении)	Требования международных организаций, государства, регуляторов в области защиты информации Требования Банка России, их реализация Лучшие практики обеспечения ИБ	РГЗ, разделы 1.1-1.3	Зачет, Вопросы 1.3, 1.5-1.10, 2.2, 2.5-2.10

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по **дисциплине** проводится в 7 семестре - в форме зачета, который направлен на оценку сформированности компетенций ОК.2, ПК.11/ПК, ПК.23/ОУ, ПСК.33.

Зачет проводится в устной форме, по билетам.

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

В 7 семестре обязательным этапом текущей аттестации является расчетно-графическое задание (работа) (РГЗ(Р)). Требования к выполнению РГЗ(Р), состав и правила оценки сформулированы в паспорте РГЗ(Р).

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе учебной дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ОК.2, ПК.11/ПК, ПК.23/ОУ, ПСК.33, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Теоретическое содержание курса освоено частично, пробелы носят существенный характер, уровень выполнения работы не отвечает большинству основных требований, необходимые практические навыки работы с освоенным материалом сформированы не достаточно, предусмотренное программой обучения учебное задание не выполнено.

Пороговый. Теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, уровень выполнения работы отвечает большинству основных требований, необходимые практические навыки работы с освоенным материалом в основном сформированы.

Базовый. Теоретическое содержание курса освоено полностью, без пробелов, уровень выполнения работы отвечает всем основным требованиям, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Теоретическое содержание курса освоено полностью, без пробелов, уровень выполнения работы отвечает всем требованиям, необходимые практические навыки работы с

освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт зачета

по дисциплине «**Информационная безопасность банковской деятельности**», 7 семестр

1. **Методика оценки**

Зачет проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов __1__, второй вопрос из диапазона вопросов __2__, (список вопросов приведен ниже). В ходе зачета преподаватель вправе задавать студенту дополнительные вопросы из общего перечня вопросов (п. 4).

Форма зачетного билета

НОВОСИБИРСКИЙГОСУДАРСТВЕННЫЙТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет №_____
к зачету по дисциплине «**Информационная безопасность банковской деятельности**»

1. Вопрос 1.
2. Вопрос 2.

Утверждаю: зав. кафедрой ____должность, ФИО
(подпись)
(дата)

2. **Критерии оценки**

- Ответ на зачетный билет считается **неудовлетворительным**, если студент при ответе на вопросы показывает слабые знания основных понятий ИБ кредитно-финансовых организаций (КФО), не понимает их взаимосвязь.
  Оценка составляет _*0*_ *баллов.*
- Ответ на зачетный билет засчитывается на **пороговом** уровне, если студент при ответе на вопросы показывает знание основных понятий ИБ КФО, способен показать их взаимовлияние и зависимости, но не показывает понимания построения ИБ КФО, роль и состав системы обеспечения ИБ.
  Оценка составляет __*30*__ *баллов*
- Ответ на зачетный билет засчитывается на **базовом** уровне, если студент при ответе на вопросы показывает знание основных понятий ИБ КФО, может показать их взаимозависимость, имеет понимание процессности в построении ИБ КФО, роль, состав и построение системы обеспечения ИБ.
  Оценка составляет __*50*__ *баллов.*

- Ответ на зачетный билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы показывает знание основных понятий ИБ, может показать их взаимозависимость, имеет понимание процессности в построении ИБ КФО, роль, состав и построение системы обеспечения ИБ, организационной и технической составляющих ИБ, способен обосновать применение организационных мер и технических средств в процессах ИБ КФО.
  Оценка составляет _70_ *баллов.*

3. Шкала оценки

В общей оценке по дисциплине зачетные баллы учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Вопросы к зачету по дисциплине «Информационная безопасность банковской деятельности»

Диапазон 1.

1. Основные понятия ИБ и их взаимосвязь (на основе СТО БР ИББС)
2. Роль и задачи СОИБ и ее составляющих - СИБ, СУИБ
3. Требования по обеспечению ИБ при назначении и распределении ролей и обеспечении доверия к персоналу
4. Требования по обеспечению ИБ автоматизированных банковских систем на стадиях жизненного цикла
5. Требования по обеспечению ИБ при управлении доступом и регистрацией
6. Требования по обеспечению ИБ средствами антивирусной защиты
7. Требования по обеспечению ИБ при использовании ресурсов сети Интернет
8. Требования по обеспечению ИБ при использовании средств криптографической защиты информации
9. Требования по обработке персональных данных в организации банковской системы РФ
10. Требования по обеспечению ИБ банковских платежных и банковских информационных технологических процессов

Диапазон 2.

1. Организация и функционирование службы ИБ организации банковской системы Российской Федерации
2. Оценка рисков нарушения ИБ, выбор подходов к оценке рисков
3. Разработка внутренних документов, регламентирующих деятельность в области обеспечения ИБ
4. Требования к организации реализации планов внедрения СОИБ
5. Разработка, организация реализации программ по обучению и повышению осведомленности персонала в области ИБ
6. Организация обнаружения и реагирования на инциденты ИБ
7. Организация обеспечения непрерывности бизнеса и его восстановления после прерываний
8. Контроль защитных мер. Мониторинг ИБ
9. Контроль защитных мер. Самооценка ИБ
10. Контроль защитных мер. Аудит ИБ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт
расчетно-графического задания (работы)

по дисциплине «Информационная безопасность банковской деятельности», 7 семестр

1. Методика оценки

В рамках расчетно-графического задания (работы) по дисциплине студенты должны разработать и документировать перечень организационно-технических мер защиты информации.

При выполнении расчетно-графического задания (работы) студенты должны провести анализ действующих требований к защите информации кредитно-финансовой организации (требований законодательства, Банка России, международных и отечественных стандартов).

Обязательные структурные части РГЗ.

1. Перечень организационно-технических мер защиты информации кредитно-финансовой организации.
2. Перечень использованных нормативных документов.

Оцениваемые позиции:

1. Перечень организационных мер защиты информации.
2. Перечень технических систем защиты информации.
3. Перечень международных и российских законодательных актов, нормативных документов регуляторов, стандартов, действующих в области ИБ.

2. Критерии оценки

- Работа считается **не выполненной,** если выполнены не все части РГЗ(Р), техническая подсистема полностью не соответствует требованиям, отсутствует перечень мер по управлению технической подсистемой ИБ.
- Работа считается выполненной **на пороговом** уровне, если части РГЗ(Р) выполнены формально: техническая подсистема не закрывает наиболее важные уязвимости, система управления технической подсистемой отсутствует, законодательные требования, требования регуляторов не использованы. Оценка составляет __10__ баллов.
- Работа считается выполненной **на базовом** уровне, если техническая подсистема не полностью закрывает уязвимости, законодательные требования и требования регуляторов использованы в полном объеме, управлящие мероприятия разработаны не в полном объеме. Оценка составляет __20__ баллов.
- Работа считается выполненной **на продвинутом** уровне, если техническая подсистема полностью закрывает уязвимости, законодательные требования и требования регуляторов использованы в полном объеме, управляющие мероприятия разработаны в полном объеме. Оценка составляет __30__ баллов.

3. Шкала оценки

В общей оценке по дисциплине баллы за РГЗ(Р) учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

4. Примерный перечень тем РГЗ(Р)

На основе действующих требований к системе информационной безопасности кредитно-финансовой организации разработать перечень организационно-технических мер по защите информации.