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: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

Курс: 4, семестр : 7

Факультет автоматики и вычислительной техники,

		Семестр
№	**Вид деятельности**	**7**
1	Всего зачетных единиц (кредитов)	5
2	Всего часов	180
3	Всего занятий в контактной форме, час.	66
4	Лекции, час.	36
5	Практические занятия, час.	18
6	Лабораторные занятия, час.	0
7	из них в активной и интерактивной форме, час.	18
8	Аттестация, час.	2
9	Консультации, час.	10
10	Самостоятельная работа, час.	114
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	РГЗ
12	Вид аттестации	Э

Новосибирск 2017

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.03.01 Информационная безопасность

ФГОС введен в действие приказом №1515 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): 10.03.01 Информационная безопасность

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*: ПК.10 способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности; *в части следующих результатов обучения*:**
з1. знать методологию создания систем защиты информации
***Компетенция ФГОС*: ПК.12 способность принимать участие в проведении экспериментальных исследований системы защиты информации; *в части следующих результатов обучения*:**
у2. уметь выявлять уязвимости сисем защиты информации и проводить их исследование
***Компетенция ФГОС*: ПК.3 способность администрировать подсистемы информационной безопасности объекта защиты; *в части следующих результатов обучения*:**
у1. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
***Компетенция ФГОС*: ПК.4 способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты; *в части следующих результатов обучения*:**
з4. знать принципы формирования политики информационной безопасности на объекте защиты
у5. уметь контролировать эффективность принятых мер по реализации частных политик информационной безопасности на объекте защиты

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	
ПК.3.у1 уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	
1.уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Лекции; Практические занятия; Самостоятельная работа
ПК.4.з4 знать принципы формирования политики информационной безопасности на объекте защиты	
2.знать принципы формирования политики информационной безопасности на объекте защиты	Лекции; Практические занятия; Самостоятельная работа
ПК.4.у5 уметь контролировать эффективность принятых мер по реализации частных политик информационной безопасности на объекте защиты	
3.уметь контролировать эффективность принятых мер по реализации частных политик информационной безопасности на объекте защиты	Лекции; Практические занятия; Самостоятельная работа
ПК.10.з1 знать методологию создания систем защиты информации	
4.знать методологию создания систем защиты информации	Лекции; Практические занятия; Самостоятельная работа
ПК.12.у2 уметь выявлять уязвимости сисем защиты информации и проводить их исследование	
5.уметь выявлять уязвимости сисем защиты информации и проводить их исследование	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	6	1	Аппаратное и программное обеспечение вычислительной техники, информационные процессы и информационные технологии. Системное и прикладное программное обеспече- ние, понятие информационных ресурсов (объектов) и пользователей данных ресурсов (субъ- ектов). Основные функции операционной системы ПЭВМ, встроенные возможности разгра- ничения доступа, блокировка доступа к рабочей станции. Идентификация и аутентификация пользователей автоматизированных систем, понятие учетных записей, полномочия админи- страторов и пользователей систем (привилегии, роли), автоматическая блокиров- ка/разблокировка учетных записей. Использование паролей, понятие структуры пароля, пра- вила выбора стойких паролей, подбор паролей с использование специализированных про- грамм. Использование локально-вычислительных сетей, понятие сетевых ресурсов, изолиро- ванность 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	6	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	6	1, 2, 3, 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	6	4, 5	Ростовщики. Трапезиты. История банков в России. Виды банков. Функции банков. Правовое регулирование банковской деятельности
5. Автоматизированные банковские системы	0	4	2, 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	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	4	2, 3, 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.	3	3	2, 3, 5	Информационное обеспечение автоматизированных банковских систем.
2. Создание электронно-цифровой подписи, работа с цифровыми сертификатами.	3	3	1, 4, 5	Организация бесперебойного функционирования информационных систем.
3. Разграничение доступа к ресурсам, целостность и лицензионная чистоты программного обеспечения	3	3	1, 2, 3	Особенности использования средств защиты информации от несанкционированного доступа.
4. Программное обеспечение автоматизированных банковских систем, установка и настройка.	3	3	4	Стандарты Банка России. Применяемые в ТУ Банка России меры и средства
5. Работа с ПО для пластиковых карт.	3	3	4	Виды электронных денег и их применение.
6. Работа под администратором информационной безопасности с ПО.	3	3	3, 5	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, 2, 4, 5	44	3
РГЗ, подробная информация приведена в приложении №3 : 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, 4	40	2
, 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	30	5
: 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 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"		
Экзамен:	0	40
Контролирующие материалы 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	Экзамен
ПК.10	з1. знать методологию создания систем защиты информации	+	+
ПК.12	у2. уметь выявлять уязвимости сисем защиты информации и проводить их исследование	+	+
ПК.3	у1. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	+	+
ПК.4	з4. знать принципы формирования политики информационной безопасности на объекте защиты	+	+
	у5. уметь контролировать эффективность принятых мер по реализации частных политик информационной безопасности на объекте защиты	+	+

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: 10.03.01 Информационная безопасность, профиль: Комплексная защита объектов информатизации

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)**
ПК.10/ЭИ способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	з1. знать методологию создания систем защиты информации	История банковского дела Основные понятия информационной безопасности. Программное обеспечение автоматизированных банковских си- стем, установка и настройка. Средства криптографической защиты информации.		Экзамен, Вопросы 1.1, 1.2, 2.1, 2.4
ПК.12/ЭИ способность принимать участие в проведении экспериментальных исследований системы защиты информации	у2. уметь выявлять уязвимости сисем защиты информации и проводить их исследование	Реализация требований информационной безопасности в системе Банка России. Автоматизированные банковские системы Идентификация и аутентификация пользователей автоматизиро- ванных систем, блокировка/разблокировка учетных записей. История банковского дела Пластиковые карты, электронные деньги Работа под администратором информационной безопасности с ПО.	РГЗ, разделы 1.1-1.3	Экзамен, Вопросы 1.4, 2.3
ПК.3/Э способность администрировать подсистемы информационной безопасности объекта защиты	у1. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Основные понятия информационной безопасности. Основные понятия, применяемые в информационных технологиях Разграничение доступа к ресурсам, целостность и лицензионная чистоты программного обеспечения Создание электронно-цифровой подписи, работа с цифровыми сер- тификатами.	РГЗ, разделы 1.1-1.3	Экзамен, Вопросы 1.3, 1.5-1.10, 2.2, 2.5-2.10
ПК.4/Э способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной	з4. знать принципы формирования политики информационной безопасности на объекте защиты	Реализация требований информационной безопасности в системе Банка России. Автоматизированные банковские системы Идентификация и аутентификация пользователей автоматизиро- ванных систем, блокировка/разблокировка учетных записей. Основные понятия информационной	РГЗ, разделы 1.1-1.3	Экзамен, Вопросы 1.3, 1.5-1.10, 2.2, 2.5-2.10

безопасности объекта защиты		безопасности. Разграничение доступа к ресурсам, целостность и лицензионная чистоты программного обеспечения		
ПК.4/Э	у5. уметь контролировать эффективность принятых мер по реализации частных политик информационной безопасности на объекте защиты	Реализация требований информационной безопасности в системе Банка России. Идентификация и аутентификация пользователей автоматизиро-ванных систем, блокировка/разблокировка учетных записей. Основные понятия информационной безопасности. Работа под администратором информационной безопасности с ПО. Разграничение доступа к ресурсам, целостность и лицензионная чистоты программного обеспечения Средства криптографической защиты информации.	РГЗ, разделы 1.1-1.3	Экзамен, 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 экзамена, который направлен на оценку сформированности компетенций ПК.10/ЭИ, ПК.12/ЭИ, ПК.3/Э, ПК.4/Э. Экзамен 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 ПК.10/ЭИ, ПК.12/ЭИ, ПК.3/Э, ПК.4/Э 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 экзамена

по дисциплине «Информационная безопасность банковской деятельности», 7 семестр

1. **Методика оценки**

Экзамен проводится в устной форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов __1__, второй вопрос из диапазона вопросов __2__, третий вопрос выбирается из диапазона вопросов __3__ (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня вопросов (п. 4).

Форма экзаменационного билета

НОВОСИБИРСКИЙГОСУДАРСТВЕННЫЙТЕХНИЧЕСКИЙУНИВЕРСИТЕТ
Факультет АВТФ

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

1. Вопрос 1.
2. Вопрос 2.
3. Вопрос 3.

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

2. **Критерии оценки**

- Ответ на экзаменационный 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 экзаменационный 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 процессности в построении ИБ КФО, роль, состав и построение системы обеспечения ИБ.
  Оценка составляет __*30*__ *баллов*
- Ответ на экзаменационный 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 экзаменационный 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.
Оценка составляет _70_ *баллов.*

3. Шкала оценки

В общей оценке по дисциплинеэкзаменационные баллыучитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

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

Диапазон 1.

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

Диапазон 3.

1. Процесс ИБ. Управление рисками
2. Процесс ИБ. Контроль логического доступа

3. Процесс ИБ. Контроль соблюдения требований ИБ персоналом
4. Процесс ИБ. Осведомленность и информирование
5. Процесс ИБ. Физическая безопасность СВТ
6. Процесс ИБ. Управление инцидентами
7. Процесс ИБ. Защита систем и связи
8. Процесс ИБ. Системная и информационная целостность
9. Процесс ИБ. Управление конфигурацией
10. Процесс ИБ. Управление непрерывностью

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.