МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра №34

«УТВЕРЖДАЮ»
Руководитель направления
проф.,д.т.н.,доц.
(должность, уч. степень, звание)
С.В. Беззатеев
(подпись)
«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита банковской информации»
(Название дисциплины)

Код направления	10.05.05
Наименование направления/ специальности	Безопасность информационных технологий в правоохранительной сфере
Наименование направленности	Технологии защиты информации в правоохранительной сфере
Форма обучения	очная

Санкт-Петербург– 2019 г.

Лист согласования рабочей программы дисциплины

Программу составил(а)

доц.,к.э.н.,доц.	24.06.21	Т.Н. Елина
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Программа одобрена на заседании кафедры № 34
«24» июня 2021 г., протокол № 11

Заведующий кафедрой № 34

проф.,д.т.н.,доц.	«24» июня 2021 г.	С.В. Беззатеев
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Ответственный за ОП 10.05.05(01)

доц.,к.т.н.,доц.	24.06.21	В.А. Мыльников
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Заместитель директора института (декана факультета) № 3 по методической работе

доц.,к.э.н.,доц.	24.06.21	Г.С. Армашова-Тельник
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Аннотация

Дисциплина «Защита банковской информации» входит в вариативную часть образовательной программы подготовки обучающихся по специальности «10.05.05 «Безопасность информационных технологий в правоохранительной сфере» специализация «Технологии защиты информации в правоохранительной сфере». Дисциплина реализуется кафедрой №34.

Дисциплина нацелена на формирование у выпускника

профессиональных компетенций:

ПК-4 «способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации»,

ПК-26 «способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные даннные, анализировать и интерпретировать результаты»,

ПК-29 «способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации»,

ПК-31 «способность принимать участие в создании системы защиты информации на объекте информатизации».

Содержание дисциплины охватывает круг вопросов, связанных с привитием обучаемым основ культуры обеспечения информационной безопасности; формированием у обучаемых понимания проблем обеспечения ИБ банковской организации и понимания путей их решения; формированием у обучаемых навыков построения системы управления ИБ, системы менеджмента ИБ и системы обеспечения ИБ банковской организации; навыками использования различных мер защиты информации в системе ИБ банковской организации; формированием у обучаемых представления о современных направлениях повышения эффективности обеспечения ИБ банковских организаций

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента, консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью преподавания дисциплины «Защита информации в банковских системах» является: формирование у студентов правовой культуры, необходимой для эффективного решения задач обеспечения информационной безопасности (ИБ) банковских организаций, на основе изучения лучших практик, накопленных при решении реальных задач.

Задачами дисциплины являются:

- привитие обучаемым основ культуры обеспечения информационной безопасности;
- формирование у обучаемых понимания проблем обеспечения ИБ банковской организации и понимания путей их решения;
- формирования у обучаемых навыков построения системы управления ИБ, системы менеджмента ИБ и системы обеспечения ИБ банковской организации;
- навыков использования различных мер защиты информации в системе ИБ банковской организации;
- формирование у обучаемых представления о современных направлениях повышения эффективности обеспечения ИБ банковских организаций.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ПК-4 «способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации»:

знать - концепцию безопасности банковской организации;
уметь - разрабатывать модели угроз ИБ и модели нарушителей ИБ для банковской организации;
владеть навыками - контроля уровня обеспечения ИБ в банковской организации;
иметь опыт деятельности - обеспечения ИБ банковской организации

ПК-26 «способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные даннные, анализировать и интерпретировать результаты»:

знать - требования нормативных документов уполномоченных государственных организаций в области обеспечения ИБ банковских организаций;
уметь - использовать для обеспечения ИБ банковской организации методы управлении доступом и регистрации, средства антивирусной защиты, методы защиты информации при использовании ресурсов сети Интернет, методы защиты информации в банковских платежных и информационных технологических процессах, методы защиты информации ИБ при обработке персональных данных;
владеть навыками - разработки политик ИБ банковской организации;
иметь опыт деятельности - характеристики системы менеджмента информационной безопасности (СУИБ) банковской организаций;

ПК-29 «способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации»:

знать – виды рабочей технической документации в сфере защиты банковской информации;

уметь – формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности банковской информации;
владеть навыками – использования нормативных актов при разработке систем защиты банковской информации;
иметь опыт деятельности – в применении нормативных актов в сфере защиты информации в банковской сфере;

ПК-31 «способность принимать участие в создании системы защиты информации на объекте информатизации»:
знать – комплексные системы защиты информации в банковской сфере;
уметь – проектировать элементы системы защиты банковской информации;
владеть навыками – работы в защищенных информационных системах;
иметь опыт деятельности – использования методов и моделей защиты информации в информационных системах..

2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Основы электротехники и радиоэлектроники
- Системы и сети передачи данных
- Производственная (эксплуатационная) практика
- Организационная защита информации
- Психология воздействия
- Защита информации в распределенных информационных системах
- Безопасность систем баз данных
- Производственная практика
- Технологии защиты от скрытой передачи данных
- Основы информационной безопасности
- Безопасность сетей ЭВМ
- Защита компьютерных сетей
- Распределенные информационные системы
- Защита и обработка документов ограниченного доступа
- Основы информационной безопасности
- Информационно-психологическое обеспечение правоохранительной деятельности
- Криптографическая защита информации
- Производственная (технологическая) практика

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

- Научно-исследовательская работа
- Производственная преддипломная практика
- Защита информации в распределенных информационных системах

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам

		№9
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час., ***В том числе***	51	51
лекции (Л), (час)	17	17
Практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)	36	36
Самостоятельная работа, всего	21	21
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Экз.	Экз.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ)	ЛР (час)	КП (час)	СРС (час)
Семестр 9					
Введение	1				3
Раздел 1. Концепция обеспечения ИБ банковской организаций	4		8		4
Раздел 2. Система информационной безопасности банковской организации	4		8		4
Раздел 3. Система менеджмента информационной безопасности банковской организации	6		10		4
Раздел 4. Экономика обеспечения информационной безопасности банковской организации	2		8		6
Итого в семестре:	17		34		21
Итого:	17	0	34	0	21

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
	Введение Предмет, цели, содержание дисциплины. Роль дисциплины в формировании специалиста в соответствии с квалификационной характеристикой и образовательным стандартом. Ее место в общем комплексе дисциплин специальности и специализации. Ее взаимосвязь с другими дисциплинами примерного учебного плана. Содержание дисциплины. Виды контроля знаний.
1	Раздел 1. Концепция обеспечения ИБ банковской организаций Тема № 1. Базовые вопросы Концепция безопасности банковской организации как научно обоснованная система взглядов на определение основных направлений, условий и порядка экономичного решения задач защиты банковского дела от противоправных действий и влияния негативных факторов. Документы уполномоченных государственных организаций, их требования. Отраслевые стандарты в области обеспечения ИБ. 3Тема № 2. Политика ИБ банковской организации Определение активов банковской организации, подлежащих защите. Модель угроз ИБ и модели нарушителей ИБ для банковской организации. Принципы обеспечения ИБ. Меры по защите информации. Система ИБ, система менеджмента ИБ, система обеспечения ИБ банковской организации. Разработка и реализация политики ИБ банковской организации.
2	Раздел 2. Система информационной безопасности банковской организации Тема № 3. Определение и характеристики системы информационной безопасности Определение системы информационной безопасности (СИБ) банковской организаций. Характеристики СИБ. Тема № 4. Требования по обеспечению информационной безопасности Общие требования по обеспечению ИБ. Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу. Обеспечение ИБ автоматизированных банковских систем (АБС) на стадиях жизненного цикла. Обеспечение ИБ при управлении доступом и регистрации. Обеспечение ИБ средствами антивирусной защиты. Обеспечение ИБ при использовании ресурсов сети Интернет. Обеспечение ИБ при использовании средств криптографической защиты информации. Обеспечение ИБ банковских платежных и информационных технологических процессов. Обеспечение ИБ при обработки персональных данных в банковской организации.

3	Раздел 3. Система менеджмента информационной безопасности банковской организации Тема № 5. Определение и характеристики системы менеджмента информационной безопасности Определение системы менеджмента информационной безопасности (СМИБ) и системы обеспечения ИБ (СОИБ) банковской организаций. Определение/коррекция области действия системы СОИБ. Тема № 6. Требования по менеджменту информационной безопасности обеспечению информационной безопасности Общие требования по менеджменту ИБ. Требования к организации и функционированию службы ИБ банковской организации. Управление рисками ИБ банковской организации. Управление документооборотом, регламентирующим деятельность в области обеспечения ИБ. Процессы по принятию руководством банковской организации решений о реализации и эксплуатации СОИБ. Организация реализации планов внедрения СОИБ. Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ. Управления инцидентами ИБ в банковской организации. Организация обнаружения и реагирования на инциденты ИБ. Управление непрерывностью основных бизнес-процессов банковской организации их восстановлением после прерываний. Тема № 7. Контроль уровня обеспечения ИБ в банковской организации Мониторинг и контроль защитных мер. Самооценка ИБ. Аудит ИБ. Анализ функционирования СОИБ в том числе и со стороны руководства банковской организации. Требования по тактическому и стратегическому улучшению СОИБ, проверка и оценка ИБ банковской организаций.
4	Раздел 4. Экономика обеспечения информационной безопасности банковской организации Тема № 8. Экономические факторы обеспечения информационной безопасности Анализ современного состояния и существующих подходов к построению систем ИБ с учетом экономических факторов. Учет в общей концепции комплексной защиты информации экономических критериев эффективности. Рационализация процессов проектирования и эксплуатации подсистемы защиты информации банковской организации с точки зрения экономической эффективности и затрат на обеспечение ИБ, посредством использования экономико-математических методов. Тема № 9. Эффективность защиты информации автоматизированных банковских систем Обзор существующих показателей эффективности защиты информации автоматизированных банковских систем (АБС). Анализ эффективности защиты информации АБС по критерию "эффективность-стоимость" и по критерию величины риска информации, содержащейся в АБС. Методика комплексной оценки информационных угроз и рисков информационной безопасности АБС. Создание технологии комплексной оценки экономической эффективности подсистемы информационной безопасности АБС.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисцип-

				лины
Учебным планом не предусмотрено				
Всего:				

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 9				
1	Описание и классификация информационных активов и ресурсов, подлежащих защите	4	4	1
2	Разработка модели угроз ИБ	4	4	1
3	Проектирование СИБ	4	4	2
4	Проектирование СМИБ	4	4	2
5	Разработка программы проведения мониторинга ИБ	4	4	3
6	Разработка плана проведения самооценки ИБ	4	4	3
7	Разработка плана проведения аудита ИБ	2	2	3
8	Расчет показателей ээффективности СОИБ	4	4	4
9	Оценка эффективности СОИБ	4	4	4
Всего:		34	34	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа студентов

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 9, час
1	2	3
Самостоятельная работа, всего	21	21
изучение теоретического материала дисциплины (ТО)	10	10
Отчеты по лаб. работам	5	5
Подготовка к текущему контролю (ТК)	6	6

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы студентов указаны в п.п. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 И 74	Информационный менеджмент [Текст] : учебник / Н. М. Абдикеев [и др.] ; ред. Н. М. Абдикеев. - М. : ИНФРА-М, 2012. - 400 с.	50
681.3 М 48	Мельников, В. П. Информационная безопасность [Текст] : учебное пособие для СПО / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; ред. С. А. Клейменов. - 7-е изд., стер. - М. : Академия, 2012. - 332 с.	40
004 Ф 34	Федотова, Е. Л. Информационные технологии и системы [Текст] : учебное пособие / Е. Л. Федотова. - М. : ФОРУМ : ИНФРА-М, 2012. - 352 с.	50
355/359 О-93	Оценка устойчивости функционирования объектов экономики [Текст] : методические указания к практическим занятиям / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; Сост. А. В. Матвеев, Ю. В. Симагин. - СПб. : Изд-во ГУАП, 2013. - 44 с.	200
Х Т 69	Трифонова, Юлия Викторовна. Организация обработки персональных данных в соответствии с законодательством РФ [Текст] : учебное пособие / Ю. В. Трифонова ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2013. - 99 с.	60
004 М 87	Мошак, Николай Николаевич (проф.). Защищенные инфотелекоммуникации. Анализ и синтез [Текст] : монография / Н. Н. Мошак ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2014. - 197 с.	40
004 М 87	Мошак, Николай Николаевич (проф.). Организация безопасного доступа к информационным ресурсам [Текст] : учебное пособие / Н. Н. Мошак, Т. М. Татарникова ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2014. - 121 с.	40

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004 И 74	Информационные системы и технологии в экономике и управлении [Электронный ресурс] : учебник / С.-Петерб. гос. ун-т экономики и финансов ; ред. В. В. Трофимов. - 3-е изд. перераб. и доп. - Электрон. текстовые дан. - М. : Юрайт, 2012.	1
Х С 50	Смирнов, А. А. Обеспечение информационной безопасности в условиях виртуализации общества : Опыт Европейского Союза [Текст] / А. А. Смирнов. - М. : ЮНИТИ-ДАНА : Закон и право, 2012. - 159 с.	2
004(075) А 91	Астахова, А. В. Информационные системы в экономике и защита информации на предприятиях - участниках ВЭД [Текст] : учебное пособие / А. В. Астахова. - СПб. : Троицкий мост, 2014. - 216 с. : рис., табл. - Библиогр.: с. 210 - 214	5
004	Мельников, В. П. Защита информации [Текст] : учебник / В. П.	10

М 48	Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П. Мельников. - М. : Академия, 2014. - 304 с.	
004 О-54	Олифер, В. Г. Безопасность компьютерных сетей [Текст] : [учебное пособие] / В. Г. Олифер, Н. А. Олифер. - М. : Горячая линия - Телеком, 2014. - 644 с.	10

7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование
www.intuit.ru	Национальный Открытый Университет "ИНТУИТ"

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Компьютерный класс	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных

	средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ПК-4 «способность участвовать в аттестационных испытаниях и аттестации объектов, помещений, технических средств и систем, а также сертификационных программных средств на предмет соответствия требованиям защиты информации»	
3	Основы электротехники и радиоэлектроники
4	Основы электротехники и радиоэлектроники
6	Системы и сети передачи данных
6	Производственная (эксплуатационная) практика
8	Организационная защита информации
9	Комплексные системы защиты информации в правоохранительной сфере
9	Технологии защиты электронных платежей
9	Защита банковской информации
ПК-26 «способность определять задачи исследования, проводить эксперименты по заданной методике, обрабатывать полученные даннные, анализировать и интерпретировать результаты»	
5	Технологии обработки аудио- и видеоданных
5	Мультимедиа технологии
7	Безопасность систем баз данных
8	Производственная практика
8	Технологии защиты от скрытой передачи данных
9	Научно-исследовательская работа
9	Технологии защиты электронных платежей
9	Научно-исследовательская работа
9	Защита банковской информации
10	Научно-исследовательская работа
10	Научно-исследовательская работа
10	Производственная преддипломная практика
ПК-29 «способность формировать рабочую техническую документацию с учетом действующих нормативных и методических документов в области безопасности информации»	
4	Основы информационной безопасности
7	Безопасность сетей ЭВМ
7	Защита компьютерных сетей

7	Распределенные информационные системы
8	Защита и обработка документов ограниченного доступа
9	Компьютерная экспертиза
9	Информационно-аналитическое обеспечение правоохранительной деятельности
9	Технологии защиты электронных платежей
9	Защита банковской информации
9	Технологии защищенного документооборота
ПК-31 «способность принимать участие в создании системы защиты информации на объекте информатизации»	
4	Основы информационной безопасности
4	Производственная (технологическая) практика
5	Криптографическая защита информации
5	Информационно-психологическое обеспечение правоохранительной деятельности
6	Криптографическая защита информации
7	Распределенные информационные системы
7	Защита компьютерных сетей
7	Безопасность сетей ЭВМ
8	Защита информации в распределенных информационных системах
9	Информационно-аналитическое обеспечение правоохранительной деятельности
9	Технологии защиты электронных платежей
9	Защита банковской информации
9	Компьютерная экспертиза
10	Производственная преддипломная практика

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
$85 \le К \le 100$	«отлично» «зачтено»	- обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.

$70 \le К \le 84$	«хорошо» «зачтено»	- обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
$55 \le К \le 69$	«удовлетво-рительно» «зачтено»	- обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
$К \le 54$	«неудовлетво рительно» «не зачтено»	- обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	2. Концепция безопасности банковской организации как научно обоснованная система взглядов на определение основных направлений, условий и порядка экономичного решения задач защиты банковского дела от противоправных действий и влияния негативных факторов. 3. Документы уполномоченных государственных организаций, их требования. 4. Отраслевые стандарты в области обеспечения ИБ. 5. Определение активов банковской организации, подлежащих защите. 6. Модель угроз ИБ и модели нарушителей ИБ для банковской организации. 7. Принципы обеспечения ИБ. 8. Меры по защите информации. 9. Система ИБ, система менеджмента ИБ, система обеспечения ИБ банковской организации. 10. Разработка и реализация политики ИБ банковской организации. 11. Определение системы информационной безопасности (СИБ) банковской организаций. 12. Характеристики СИБ. 13. Общие требования по обеспечению ИБ. 14. Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу. 15. Обеспечение ИБ автоматизированных банковских систем (АБС) на стадиях жизненного цикла. 16. Обеспечение ИБ при управлении доступом и регистрации. 17. Обеспечение ИБ средствами антивирусной защиты. 18. Обеспечение ИБ при использовании ресурсов сети Интернет.

	19. Обеспечение ИБ при использовании средств криптографической защиты информации. 20. Обеспечение ИБ банковских платежных и информационных технологических процессов. 21. Обеспечение ИБ при обработки персональных данных в банковской организации. 22. Определение системы менеджмента информационной безопасности (СМИБ) и системы обеспечения ИБ (СОИБ) банковской организаций. 23. Определение/коррекция области действия системы СОИБ. 24. Общие требования по менеджменту ИБ. 25. Требования к организации и функционированию службы ИБ банковской организации. 26. Управление рисками ИБ банковской организации. 27. Управление документооборотом, регламентирующим деятельность в области обеспечения ИБ. 28. Процессы по принятию руководством банковской организации решений о реализации и эксплуатации СОИБ. 29. Организация реализации планов внедрения СОИБ. 30. Разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ. 31. Управления инцидентами ИБ в банковской организации. 32. Организация обнаружения и реагирования на инциденты ИБ. 33. Управление непрерывностью основных бизнес-процессов банковской организации их восстановлением после прерываний. 34. Мониторинг и контроль защитных мер. 35. Самооценка ИБ. Аудит ИБ. 36. Анализ функционирования СОИБ в том числе и со стороны руководства банковской организации. 37. Требования по тактическому и стратегическому улучшению СОИБ, проверка и оценка ИБ банковской организаций. 38. Анализ современного состояния и существующих подходов к построению систем ИБ с учетом экономических факторов. 39. Учет в общей концепции комплексной защиты информации экономических критериев эффективности. 40. Рационализация процессов проектирования и эксплуатации подсистемы защиты информации банковской организации с точки зрения экономической эффективности и затрат на обеспечение ИБ, посредством использования экономико-математических методов. 41. Обзор существующих показателей эффективности защиты информации автоматизированных банковских систем (АБС). 42. Анализ эффективности защиты информации АБС по критерию "эффективность-стоимость" и по критерию величины риска информации, содержащейся в АБС. 43. Методика комплексной оценки информационных угроз и рисков информационной безопасности АБС. 44. Создание технологии комплексной оценки экономической эффективности подсистемы информационной безопасности АБС.

45. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Учебным планом не предусмотрено

46. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	Учебным планом не предусмотрено

47. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	не предусмотрено

48. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Описание и классификация информационных активов и ресурсов, подлежащих защите. Разработка модели угроз ИБ. Разработка модели нарушителя ИБ. Разработка политики ИБ. Оценка рисков ИБ. Проектирование СИБ. Проектирование СМИБ. Разработка подсистемы обеспечения ИБ. Разработка системы управления инцидентами ИБ. Разработка плана восстановления работоспособности банковских систем после реализации угроз ИБ. Разработка программы проведения мониторинга ИБ. Разработка плана проведения самооценки ИБ. Разработка плана проведения аудита ИБ. Оценка эффективности СОИБ.

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению дисциплины

Целью преподавания дисциплины «Защита информации в банковских системах» является: формирование у студентов правовой культуры, необходимой для эффективного решения задач обеспечения информационной безопасности (ИБ) банковских организаций, на основе изучения лучших практик, накопленных при решении реальных задач.

Задачами дисциплины являются:

- привитие обучаемым основ культуры обеспечения информационной безопасности;
- формирование у обучаемых понимания проблем обеспечения ИБ банковской организации и понимания путей их решения;
- формирования у обучаемых навыков построения системы управления ИБ, системы менеджмента ИБ и системы обеспечения ИБ банковской организации;
- навыков использования различных мер защиты информации в системе ИБ банковской организации;

- формирование у обучаемых представления о современных направлениях повышения эффективности обеспечения ИБ банковских организаций.

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимся лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научится методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Концепция обеспечения ИБ банковской организаций

Раздел 2. Система информационной безопасности банковской организации

Раздел 3. Система менеджмента информационной безопасности банковской организации

Раздел 4. Экономика обеспечения информационной безопасности банковской организации

Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задания для лабораторных работ заключаются в решении задач, рассмотренных в ходе лекций, таких как:
Описание и классификация информационных активов и ресурсов, подлежащих защите.
Разработка модели угроз ИБ.
Разработка модели нарушителя ИБ.
Разработка политики ИБ.
Оценка рисков ИБ.
Проектирование СИБ.
Проектирование СМИБ.
Разработка подсистемы обеспечения ИБ.
Разработка системы управления инцидентами ИБ.
Разработка плана восстановления работоспособности банковских систем после реализации угроз ИБ.
Разработка программы проведения мониторинга ИБ.
Разработка плана проведения самооценки ИБ.
Разработка плана проведения аудита ИБ.
Оценка эффективности СОИБ.

Лабораторные занятия проводятся после чтения лекций, дающих теоретические основы для их выполнения. Допускается выполнение лабораторных занятий до прочтения лекций с целью облегчения изучения теоретического материала при наличии описаний работ, включающих необходимые теоретические сведения или ссылки на конкретные учебные издания, содержащие эти сведения.

Преподаватель имеет право определять содержание лабораторных работ, выбирать методы и средства проведения лабораторных исследований, наиболее полно отвечающие их особенностям и обеспечивающие высокое качество учебного процесса.

Преподаватель формирует рубежные и итоговые результаты (рейтинги) студента по результатам выполнения лабораторных работ.

На лабораторном занятии студент имеет право задавать преподавателю и (или) лаборанту вопросы по содержанию и методике выполнения работы и требовать ответа по существу обращения.

Студент имеет право на выполнение лабораторной работы по оригинальной методике с согласия преподавателя и под его надзором – при безусловном соблюдении требований безопасности.

К выполнению лабораторной работы допускаются студенты, подтвердившие готовность в объеме требований, содержащихся в методических указаниях к лабораторной работе и (или) в устных предварительных указаниях преподавателя.

В ходе лабораторных занятий студенты ведут необходимые записи, составляют (по требованию преподавателя) итоговый письменный отчет. На первом занятии цикла лабораторных работ преподаватель должен дать конкретные указания по составлению и оформлению отчетов с целью обеспечения единообразия. В зависимости от особенностей цикла лабораторных занятий отчет составляется каждым студентом индивидуально, либо общий отчет – подгруппой из 2-3 студентов. По окончании лабораторной работы студенты обязаны представить отчет преподавателю для проверки с последующей защитой. По согласованию с преподавателем допускается представление к защите отчета о лабораторной работе во время следующего лабораторного занятия или в индивидуальные сроки, оговоренные с преподавателем. Допускается по согласованию с преподавателем представлять отчет о лабораторной работе в электронном виде.

Лабораторное занятие состоит из следующих элементов: вводная часть, основная и заключительная.

Вводная часть обеспечивает подготовку студентов к выполнению заданий работы. В ее состав входят:

– формулировка темы, цели и задач занятия, обоснование его значимости в профессиональной подготовке студентов;

– изложение теоретических основ работы;

– характеристика состава и особенностей заданий работы и объяснение методов (способов, приемов) их выполнения;

– характеристика требований к результату работы;

– инструктаж по технике безопасности при эксплуатации технических средств;

– проверка готовности студентов выполнять задания работы;

– указания по самоконтролю результатов выполнения заданий студентами.

Основная часть включает процесс выполнения лабораторной работы, оформление отчета и его защиту. Она может сопровождаться дополнительными разъяснениями по ходу работы, устранением трудностей при ее выполнении, текущим контролем и оценкой результатов отдельных студентов, ответами на вопросы студентов. Возможно пробное выполнение задания(ий) под руководством преподавателя.

Заключительная часть содержит:

– подведение общих итогов занятия;

– оценку результатов работы отдельных студентов;

– ответы на вопросы студентов;

– выдачу рекомендаций по устранению пробелов в системе знаний и умений студентов, по улучшению результатов работы;

– сбор отчетов студентов для проверки, изложение сведений, касающихся подготовки к выполнению следующей работы.

Вводная и заключительная части лабораторного занятия проводятся фронтально. Основная часть может выполняться индивидуально или коллективно (в зависимости от формы организации занятия).

Структура и форма отчета о лабораторной работе

Отчёт по лабораторной работе оформляется индивидуально каждым студентом, выполнившим необходимые (независимо от того, выполнялся ли эксперимент индивидуально или в составе группы студентов). Страницы отчёта следует пронумеровать (титульный лист не нумеруется, далее идет страница 2 и т.д.). Титульный лист отчёта должен содержать фразу: «Отчёт по лабораторной работе «Название работы», чуть ниже: Выполнил студент группы (номер группы) (Фамилия, инициалы)». Внизу листа следует указать текущий год. Например, Отчёт по лабораторной работе № (номер работы) «Введение в спектральный анализ», Выполнил студент группы 5221 Иванов И.И. Вторая страница текста, следующая за титульным листом, должна начинаться с пункта: Цель работы. Отчёт, как правило, должен содержать следующие основные разделы:

1. Цель работы;
2. Теоретическая часть;

3. Программное обеспечение, используемое в работе;
4. Результаты;
5. Выводы.

В случае необходимости в конце отчёта приводится перечень литературы.

Требования к оформлению отчета о лабораторной работе

Теоретическая часть должна содержать минимум необходимых теоретических сведений о предметной области. Не следует копировать целиком или частично методическое пособие (описание) лабораторной работы или разделы учебника.

В разделе Программное обеспечение необходимо описать, с помощью каких инструментальных средств и каким образом были разработаны модели и получены результаты. Рисунки, блок-схемы, описание модели и её особенностей, необходимость отладки – все это должно быть представлено в указанном разделе.

Раздел Результаты включает в себя скриншоты программного приложения, полученные при выполнении лабораторной работы. Рисунки, графики и таблицы нумеруются и подписываются заголовками.

Выводы не должны быть простым перечислением того, что сделано. Здесь важно отметить, какие новые знания о предмете исследования были получены при выполнении работы, к чему привело обсуждение результатов, насколько выполнена заявленная цель работы. Выводы по работе каждый студент делает самостоятельно. В случае необходимости в конце отчёта приводится Список литературы, использованной при подготовке к работе. В тексте отчёта делаются краткие ссылки на литературу (учебники, справочники, иные источники…) номером в квадратных скобках, напр., [1]. Литературные источники нумеруются по мере их появления в тексте отчёта. В конце отчёта даётся их подробный список. На все источники списка литературы должны быть ссылки в тексте отчёта, там, где это необходимо.

При сдаче отчёта преподаватель может сделать устные и письменные замечания, задать дополнительные вопросы. Все ответы на дополнительные вопросы, обсуждения выполняются студентом на отдельных листах, включаемых в отчёт (при этом в тексте основного отчёта делается сноска или другой значок, которому будет соответствовать новый материал). При этом письменные замечания преподавателя должны остаться в тексте для ясности динамики работы над отчётом.

Объём отчёта должен быть оптимальным для понимания того, что и как сделал студент, выполняя работу. Обязательные требования к отчёту включают общую и специальную грамотность изложения, а также аккуратность оформления.

После приёма преподавателем отчёт хранится на кафедре.

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой