Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
_____ Н.В. Бабина
«28» апреля 2020 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«НАЦИОНАЛЬНАЯ СИСТЕМА ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ ПРЕСТУПНЫХ ДОХОДОВ И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

Автор: к.в.н., доцент Сухотерин А.И. Рабочая программа дисциплины: «Национальная система по противодействию легализации преступных доходов и финансированию терроризма». – Королев МО: «Технологический университет», 2020.

Рецензент: **к.в.н., доцент Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания кафедры	Протокол № 8 от 26.03.2020			

Рабочая программа согласована:
Руководитель ОПОП ВО к.в.н., доцент Воронов А.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

2

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является:

1. Усвоение теоретических и практических основ финансового мониторинга экономических процессов, осуществляемого в рамках мероприятий по предупреждению, выявлению и пресечению операций, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

2. Ознакомиться с нормативными документами, регулирующими процесс финансового мониторинга в Российской Федерации, изучить российскую и международную практику противодействия отмыванию денег и финансированию терроризма (далее - ПОД/ФТ).

3. Научиться анализировать информацию об операциях с денежными средствами или иным имуществом, подлежащим контролю в соответствии с законодательством РФ.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общепрофессиональные компетенции:

- (ОПК-1) - способность анализировать физические явления и процессы для решения профессиональных задач;

Профессиональные компетенции:

- (ПК-3) - способность администрировать подсистемы информационной безопасности объекта защиты;
- (ПК-5) – способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации;
- (ПК-6) - способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- (ПК-12) - способность принимать участие в проведении экспериментальных исследований системы защиты информации.

Основными **задачами** дисциплины являются:

- изучение институционально-правовых основ национальной системы противодействия легализации преступных доходов и финансированию терроризма;

- приобретение теоретических и практических навыков выявления операций с денежными средствами или иным имуществом, подлежащих обязательному контролю, и необычных сделок, осуществляемых в целях легализации доходов, полученных преступным путем, или финансирования терроризма;

- приобретение теоретических и практических навыков по надлежащей проверке клиентов, документальному фиксированию и хранению информации, а также разработке правил внутреннего контроля и программы его осуществления;
- выполнение необходимых действий по надлежащей проверке клиентов, документальному фиксированию и хранению информации;
- ознакомление с принципами и способами взаимодействия с уполномоченными в сфере ПОД/ФТ государственными контрольными органами.

После завершения освоения данной дисциплины студент должен:

Знать:

- основы логики;
- перечень нормативно-правовых документов по выбранному профилю;
- источники информации по рынку ценных бумаг и производных финансовых инструментов типовые методики расчета показателей, характеризующих деятельность хозяйствующего субъекта на рынке ценных бумаг;
- информационные ресурсы рынка ценных бумаг и производных финансовых инструментов информационные ресурсы рынка ценных бумаг и производных финансовых инструментов;
- финансовую, бухгалтерскую и иную информацию, содержащуюся в отчетности;
- отечественные и зарубежные источники информации.

Уметь:

- применять понятийно-категориальный аппарат, основные законы гуманитарных и социальных наук в профессиональной деятельности;
- использовать нормативные правовые документы анализировать исходные данные необходимые для расчета экономических показателей на рынке ценных бумаг и производных финансовых инструментов;
- рассчитать типовые показатели на основе действующих методик на рынке ценных бумаг и производных финансовых инструментов

рассчитать типовые показатели на основе действующих методик на рынке ценных бумаг и производных финансовых инструментов;

- собирать, обрабатывать и анализировать данные, необходимые для расчета экономических показателей на рынке ценных бумаг и производных финансовых инструментов;
- собирать и анализировать финансовую, бухгалтерскую и иную информацию, подготавливать отчетность, необходимую на рынке ценных бумаги и производных финансовых инструментов;
- собрать и проанализировать данные, подготовить информационный обзор и/или аналитический отчет по рынку ценных бумаг и производных финансовых инструментов.

Владеть:

- навыками публичной речи, аргументации, ведения дискуссии;
- навыками литературной и деловой письменной речи на русском языке, навыками публичной и научной речи;
- нормативно-правовым понятийным аппаратом;
- методами анализа исходных данных на рынке ценных бумаг и производных финансовых инструментов;
- методами оценки полученных расчетных показателей;
- методами сбора, анализа и обработки данных на рынке ценных бумаг и производных финансовых инструментов;
- способами применения полученных сведений для принятия инвестиционных решений для принятия управленческих решений на рынке ценных бумаг и производных финансовых инструментов;
- способами ввода информации и ее обобщения.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Национальная система по противодействию легализации преступных доходов и финансированию терроризма» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях ранее изученных дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Основы управления информационной безопасностью», «Методы защиты информации на рынке корпоративного контроля»,

«Гуманитарные аспекты (профессиональная этика) информационной безопасности» и компетенциях: ОК-4,9, ОПК-1,5,6,7, ПК-1,4,8,10,13,15.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения всех последующих дисциплин «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», «Защищённые информационные системы банковской деятельности», «Основы расследования нарушений в финансовой сфере», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 4 зачетные единицы, 144 часа.

Таблица1

Виды занятий	**Всего часов**	**Семестр** 7	**Семестр** 8	**Семестр** …	**Семестр** …
Общая трудоемкость	144	144			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	64	64			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	16	16			
Самостоятельная работа	80	80			
Контроль самостоятельной работы	-	-			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	Экзамен	Экзамен			

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Лабораторные занятия, час Очное	Занятия в интерактивной форме, час Очное	Код компетенций
Тема 1: Экономические основы ПОД/ФТ.	2	4	2	3	ОПК-1; ОК-5,-9; ПК-29,-33.

Тема 2: Международная система ПОД/ФТ и международные стандарты в сфере ПОД/ФТ.	2	6	2	3	ОПК-1; ОК-9; ПК-29,-31.
Тема 3: Национальная система ПОД/ФТ	2	6	2	3	ОПК-1; ОК-5,-9; ПК-31,-33.
Тема 4: Государственный финансовый мониторинг.	4	6	4	3	ОПК-1; ОК-5; ПК-29,-33.
Тема 5: Система внутреннего контроля в субъектах первичного финансового мониторинга.	4	6	4	3	ОПК-1; ОК-5,-9; ПК-29,-33.
Тема 6: Ответственность за нарушение законодательства в сфере ПОД/ФТ.	2	4	2	3	ОПК-1; ОК-5,-9; ПК-29,-31,-33.
Итого:	16	32	16	18	

4.2. Содержание тем дисциплины

Тема 1: Экономические основы ПОД/ФТ.

Легализация преступных доходов как фактор негативного воздействия на экономику государства. Причины и условия легализации преступных доходов. Отмывание денег. История возникновения понятия. Определение понятия. Сущность и формы отмывания денег. Финансирование терроризма: понятие и сущность. Причины и условия финансирования терроризма. Основные формы и источники финансирования, их характерные признаки. Связь финансирования терроризма с отмыванием денег.

Тема 2: Международная система ПОД/ФТ и международные стандарты в сфере ПОД/ФТ.

Основные этапы формирования единой международной системы ПОД/ФТ. Международное сотрудничество в сфере ПОД/ФТ. Международная система ПОД/ФТ. Основные черты и компоненты. Институциональные основы международной системы ПОД/ФТ. Организации и специализированные органы. Основные источники международного права

в сфере ПОД/ФТ. Международные стандарты ПОД/ФТ. Сорок и девять рекомендаций ФАТФ. Место и роль России в международной системе ПОД/ФТ.

Тема 3. Национальная система ПОД/ФТ.

Сущность финансового мониторинга. Необходимость финансового мониторинга в решении общегосударственных задач развития народного хозяйства страны. Понятие национальной системы ПОД/ФТ. Её место, роль и основные задачи в системе государственного устройства Российской Федерации и международной системе ПОД/ФТ. Основные этапы становления национальной системы ПОД/ФТ. Современное состояние национальной системы ПОД/ФТ. Институционально-правовые основы национальной системы ПОД/ФТ. Структура национальной системы ПОД/ФТ. Основные источники права в сфере ПОД/ФТ. Общая характеристика нормативных правовых актов РФ

Тема 4: Государственный финансовый мониторинг.

Федеральная служба по финансовому мониторингу (Росфинмониторинг) как ключевой элемент национальной системы ПОД/ФТ. Роль уполномоченного и координирующего органа в системе финансового мониторинга. Правовой статус, полномочия и основные направления деятельности Росфинмониторинга. Надзорная функция Росфинмониторинга. Формы надзора и виды проверок, порядок их проведения. Государственное регулирование в банковской сфере, на страховом рынке, рынке ценных бумаг, на рынке драгоценных металлов и драгоценных камней и в сфере федеральной почтовой связи. Государственное регулирование других организаций, не имеющих надзорных органов. Полномочия и организационная структура надзорных органов и их территориальные органы. Взаимодействие Росфинмониторинга с надзорными органами.

Тема5: Система внутреннего контроля в субъектах первичного финансового мониторинга.

Организации, осуществляющие операции с денежными средствами или иным имуществом: финансовые и нефинансовые организации, представители нефинансовых отраслей и профессий. Основные права и обязанности. Назначение и основные задачи системы внутреннего контроля. Операции подлежащие обязательному контролю. Обязательные процедуры внутреннего контроля. Критерии выявления и признаки необычных сделок как программа системы внутреннего контроля. Типовая структура системы внутреннего контроля. Лица, ответственные за разработку и осуществление правил внутреннего контроля. Правила внутреннего контроля: разработка, ключевые

положения, особенности, связанные с финансово-хозяйственной деятельностью субъекта. Программы осуществления правил внутреннего контроля. Согласование правил внутреннего контроля с надзорным органом. Идентификация клиентов и выгодоприобретателей. Правило «знай своего клиента». Обеспечение конфиденциальности информации. Выявление подозрительных операций. Организация и сроки хранения информации.Порядок взаимодействия системы внутреннего контроля субъекта первичного финансового мониторинга с надзорным органом. Порядок представления информации об операциях, подлежащих контролю, в Росфинмониторинг. Порядок и сроки представления.

Тема 6: Ответственность за нарушение законодательства в сфере ПОД/ФТ.

Виды ответственности за нарушения требований законодательства в сфере ПОД/ФТ (уголовная, административная, гражданско-правовая). Основания для привлечения к ответственности лиц, допустивших нарушения законодательства в сфере ПОД/ФТ. Меры административной ответственности за нарушение законодательства о ПОД/ФТ в рамках Кодекса Российской Федерации об административных правонарушениях и порядок их применения. Полномочия должностных лиц уполномоченного органа уполномоченного органа. Пересмотр решений должностных лиц в порядке обжалования.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Национальная система по противодействию легализации преступных доходов и финансированию терроризма» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Гамза В.А., Ткачук И.Б.. Безопасность банковской деятельности: учебник.- 2 –е изд., перераб. и доп. – М.: Маркет ДС, 2010. (Универсететская серия).

2. В.В. Дик. Банковские информационные системы: учебник. – М.: Маркет ДС, 2013. (Универсететская серия)
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие.— М.:ИНФРА-М.,2008.: - (профессиональное образование).
4. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009.

Дополнительная литература:

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
2. Тихонов В.А., Райх В.В., Информационная безопасность: концептуальные, правовые. Организационные и технические аспекты.: Учебное пособие. -М.: Гелиос АРВ, 2006. -528 с., ил. с.171.
3. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).
4. Кобелев О.А. Электронная коммерция: учебное пособие. – М.: Дашков и К, 2010 – 684 с.
5. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
6. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009 – 552 с.: ил.
7. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).

Рекомендуемая литература:

1. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О центральном банке Российской федерации (Банке России)».
2. Стандарт Банка России СТО БР ИББС 1.0-2006
3. Федеральный закон от 27 июля 2006 г. №149 «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 29 июля 2004 г. № 98-ФЗ (с изменениями и дополнениями от 2 февраля 2006 года № 19-ФЗ; от 24 июля 2007 года № 244 – ФЗ) « О Коммерческой тайне».
5. Федеральный закон от 27 июля 2006 г. № 152 – ФЗ «О персональных данных».
6. Указ Президента РФ от 09 сентября 2000 г. «Доктрина информационной безопасности Российской Федерации».
7. Указ Президента РФ от 16 августа 2004 г. № 1085 « Вопросы Федеральной Службы по техническому и экспортному контролю».

8. Указ Президента РФ от 06 марта 1997 г. № 188 « Об утверждении перечня сведений конфиденциального характера».
9. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
10. Дединев М.А., Дыльнов Д.В. и др. Защита информации в банковском деле и электронном бизнесе. Учебно – справочное пособие – М.: КУДИЦ – ОБРАЗ, 2004. --512 с. (СКБ – специалиту по компьютерной безопасности).

Основные нормативные правовые акты по теме дисциплины:

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.).
2. Конвенция ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ от 19 декабря 1988 г. (Венская).
3. Конвенция совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности от 8 ноября 1990 г. (Страсбургская).
4. Международная конвенция о борьбе с финансированием терроризма от 9 декабря 1999г.
5. Конвенция ООН против транснациональной организованной преступности от 15 ноября 2000г. (Палермская).
6. Конвенция ООН против коррупции от 31 октября 2003 г. (Меридская).
7. Сорок и девять Рекомендаций ФАТФ, 2003 г. (с изменениями от 22 октября 2004 г.).
8. Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ.
9. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. №174-ФЗ.
10. Гражданский кодекс Российской Федерации часть первая 30 ноября 1994 г. №51-ФЗ, часть вторая от 26 января 1996 г. №14-ФЗ, часть третья от 26 ноября 2001 г. №146-ФЗ.
11. Кодекс об административных правонарушениях Российской Федерации от 30 декабря 2001 г. №195-ФЗ.
12. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».
13. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму».
14. Федеральный закон от 2 декабря 1990 г. №395-1 «О банках и банковской деятельности».

15. Федеральный закон от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг».

16. Федеральный закон от 26 марта 1998 г. №41-ФЗ «О драгоценных металлах и драгоценных камнях».

17. Федеральный закон от 17 июля 1999 г. № 176-ФЗ «О почтовой связи».

18. Федеральный закон от 29 октября 1998 г. № 164-ФЗ «О финансовой аренде (лизинге)».

19. Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».

20. Федеральные закон от 8 августа 2001 г. № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей».

21. Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации».

22. Федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

23. Федеральный закон от 11 ноября 2003 г. № 138-ФЗ «О лотереях».

24. Федеральный закон от 29 декабря 2006 г. № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации».

25. Закон Российской Федерации от 27 ноября 1992 г. № 4015-1 «Об организации страхового дела в Российской Федерации».

26. Основы законодательства Российской Федерации о нотариате от 11 февраля 1993 г. № 4462-1.

27. Указ Президента Российской Федерации от 1 ноября 2001 г. № 1263 «Об уполномоченном органе по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

28. Указ Президента Российской Федерации от 17 декабря 1997 г. № 1300 «Об утверждении Концепции национальной безопасности Российской Федерации».

29. Указ Президента Российской Федерации от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти».

30. Указ Президента Российской Федерации от 20 мая 2004 г. № 649 «Вопросы структуры федеральных органов исполнительной власти».

31. Указ Президента Российской Федерации от 15 февраля 2006 г. № 116 «О мерах по противодействию терроризму».

32. Постановление Правительства Российской Федерации от 17 апреля 2002 г. № 245 «Об утверждении Положения о представлении информации в Федеральную службу по финансовому мониторингу

организациями, осуществляющими операции с денежными средствами или иным имуществом».

33. Распоряжение Правительства Российской Федерации от 17 июля 2002 г. №983-р, утвердившее Рекомендации по разработке организациями, совершающими операции с денежными средствами или иным имуществом, правил внутреннего контроля в целях, противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

34. Постановление Правительства Российской Федерации от 8 января 2003 г. № 6 «О порядке утверждения правил внутреннего контроля в организациях, осуществляющих операции с денежными средствами или иным имуществом».

35. Постановление Правительства Российской Федерации от 18 января 2003 г. № 27 «Об утверждении Положения о порядке определения перечня организаций и физических лиц, в отношении которых имеются сведения об их участии в экстремистской деятельности, и доведения этого перечня до сведения организаций, осуществляющих операции с денежными средствами или иным имуществом».

36. Постановление Правительства Российской Федерации от 18 января 2003 г. № 28 «Об утверждении Положения о постановке на учет в Федеральной службе по финансовому мониторингу организаций, осуществляющих операции с денежными средствами или иным имуществом, в сфере деятельности которых отсутствуют надзорные органы».

37. Постановление Правительства Российской Федерации от 26 марта 2003 г. № 173 «О порядке определения и опубликования перечня государств (территорий), которые не участвуют в международном сотрудничестве в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

38. Постановление Правительства Российской Федерации от 23 июня 2004 г. № 307 «Об утверждении Положения о Федеральной службе по финансовому мониторингу».

39. Постановление Правительства Российской Федерации от 16 февраля 2005 г. № 82 «Об утверждении Положения о порядке передачи информации в Федеральную службу по финансовому мониторингу адвокатами, нотариусами и лицами, осуществляющими предпринимательскую деятельность в сфере оказания юридических и бухгалтерских услуг».

40. Постановление Правительства Российской Федерации от 5 декабря 2005 г. № 715 «О квалификационных требованиях к специальным должностным лицам, ответственным за соблюдение правил внутреннего контроля и программ его осуществления, а также требованиях к подготовке и обучению кадров, идентификации клиентов, выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

41. Приказ КФМ России от 16 июня 2003 г. № 72 «Об утверждении Положения об издании КФМ России постановления о приостановлении операции (оперший) с денежными средствами или иным имуществом в случаях, предусмотренных Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

42. Приказ КФМ России от 11 августа 2003 г. № 104 «Об утверждении рекомендаций по отдельным положениям правил внутреннего контроля, разрабатываемых организациями, совершающими операции с денежными средствами или иным имуществом, в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

43. Приказ Росфинмониторинга от 7 нюня 2005 г. № 86 «Об утверждении Инструкции о представлении в Росфинмониторинг информации, предусмотренной Федеральным законом от 7 августа 2001 года № 115-ФЗ О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

44. Приказ Росфинмониторинга от 14 июля 2005 г. № 108 «О должностных лицах Федеральной службы финансового мониторинга, уполномоченных составлять протоколы об административных правонарушениях»,

45. Приказ Федеральной службы по финансовому мониторингу от 1 ноября 2008 г. № 256 «Об утверждении Положения о требованиях к подготовке и обучению кадров организаций, осуществляющих операции с денежными средствами или иным имуществом, в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Электронные книги:

1. Жарковская, Е. П. Финансовый анализ деятельности коммерческого банка [Электронный ресурс]: Учебник / Е.П. Жарковская. - М: Омега-Л, 2010. - 328 с.
http://www.biblioclub.ru/book/54713/

2. Бертунов, А.Э. Внедрение инновационных технологий в сфере банковского дела [Электронный ресурс] / А.Э. Бертунов. — М.: Лаборатория Книги, 2012. — 93 с.
http://www.biblioclub.ru/book/140927/

3. Исаев, Г. Н. Информационные системы в экономике[электронный ресурс]: Учебник.Доп. МО и науки РФ в кач-ве учебника для студентов вузов / Г.Н. Исаев.-3-е изд., стер. - Москва: Омега-Л, 2010. - 464 с.
http://www.biblioclub.ru/book/54663/

4. Шапкин, А. С. Математические методы и модели исследования операций [Электронный ресурс]: учебник / А. С. Шапкин, В. А. Шапкин. —

5-е изд. — М.: Дашков и К, 2012. — 400 с.
http://www.biblioclub.ru/book/112204/

5. Банковское дело [Электронный ресурс]: учебник / А.М. Тавасиева, В.А. Москвин, Н.Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 287 с.
http://www.biblioclub.ru/book/116705/

6. Чикида, А. Деятельность коммерческого банка в современных условиях [Электронный ресурс]: учебное пособие / А. Чикида. — М.: Лаборатория Книги, 2010. — 130 с.
http://www.biblioclub.ru/book/100020/

7. Николаева, И. П. Рынок ценных бумаг [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению «Экономика» / И. П. Николаева. — М.: ЮНИТИ - ДАНА , 2012. — 223 с.
http://www.biblioclub.ru/book/118462/

8. Кириллов, П. К. Основы менеджмента банковских услуг [Электронный ресурс] /П.К. Кириллов. - М: Лаборатория книги, 2010. - 158 с.
http://www.biblioclub.ru/book/88353/

9. Ковалев, П. П. Банковский риск-менеджмент [Электронный ресурс] / П.П. Ковалев. - : Финансы и статистика, 2009. - 303 с.
http://www.biblioclub.ru/book/79604/

10. Насреддинов, Х. Г. Учет определенных операций в банках (эмиссия пластиковых карт, учет счетов, банковские переводы) [электронный ресурс] / Х.Г. Насреддинов. - Саратов: Ай Пи Эр Медиа, 2010. - 72 с.
http://www.biblioclub.ru/book/78803/

11. Финансы организаций (предприятий) [Электронный ресурс]: учебник д л я студентов вузов / Н.В. Колчина [и д р .] ; под ред. Н.В. Колчиной. — 5-е изд., перераб. и доп. — М.: ЮНИТИ-ДАНА, 2012. — 407 с.
http://www.biblioclub.ru/book/118178/

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал
2. **http://informika.ru/** – образовательный портал
3. **www.wikIsec.ru -** Энциклопедия информационной безопасности. –

Публикации, статьи.

1. **www.biblioclub.ru** - Универсальная библиотека онлайн.
2. **www.window.edu.ru** - Единое окно доступа.
3. **http://grebennikov.ru/** - Издательский дом «Гребенников»
4. **www.rucont.ru** - ЭБС «Руконт»
5. **http://www.minfin.ru -** Официальный сайт Министерства финансов Российской Федерации

6. **http://www.gov.ru** -Официальный сервер органов государственной власти Российской Федерации.
7. **http://www.fsb.ru** - Официальный сайт Федеральной Службы Безопасности
8. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

Интернет-ресурсы по теме дисциплины:

1. Федеральной службы по финансовому мониторингу: www.fedsfm.ru.
2. ЕАГ: www.euroasiangroup.org.
3. ФАТФ: www.fatf-gafi.org.
4. Вольфсбергской группы: www.wolfsberg-principles.com.
5. Всемирного банка: www.worldbank.org.
6. ЕС: www.europa.eu.
7. МБРР: www.amlcft.org.
8. Международного валютного фонда: www.imf.org.
9. Совета Европы: www.coe.int.
10. Федеральной службы по финансовым рынкам: www.fcsm.ru.
11. Центрального Банка России www.cbr.ru.
12. Консультант-плюс www.consultant.ru.
13. Министерства финансов РФ www.minfin.ru.
14. Правительства РФ www.government.ru.
15. Государственной думы РФ www.duma.gov.ru.
16. Информационно-издательского центра «Статистика России» www.infostat.ru.
17. Госкомстата РФ www.gks.ru.
18. Организации Объединенных Наций www.un.org.
19. Международной информационной системы по вопросам противодействия легализации доходов, полученных преступным путем www.imolin.org.
20. Азиатско-Тихоокеанской группы по вопросам отмывания денег www.apgml.org.

9. Методичские указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

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

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине: «Национальная система по противодействию легализации преступных доходов и финансированию терроризма»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ «НАЦИОНАЛЬНАЯ СИСТЕМА ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ ПРЕСТУПНЫХ ДОХОДОВ И ФИНАНСИРОВАНИЮ ТЕРРОИЗМА»

(Приложение 1 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-1	способность анализировать физические явления и процессы для решения профессиональных задач	Темы 1, 2,3, 4, 5,6	основные экономические категории и закономерности, методы анализа экономических явлений и процессов.	оценивать эффективность управленческих решений.	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
2..	ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты	Темы 1, 2,3, 4, 5,6	основные экономические категории и закономерности, методы анализа экономических явлений и процессов, специфические черты функционирования хозяйственной системы на (микро- и макро-) уровнях, основные понятия экономической и финансовой деятельности отрасли и ее структурных подразделений	оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
3.	ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Темы 1,2,3, 4, 5,6	основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; характеристик	анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных	навыками обоснования, выбора, реализации и контроля результатов управленческого решения

				у основных отраслей российского права; правовые основы обеспечения национальной безопасности Российской Федерации	прав осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач	
4.	ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Темы 1, 2,3, 4, 5,6	основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации;	отображать предметную область на конкретную модель данных;	навыками организации и обеспечения режима конфиденциальности
5.	ПК-12	способность принимать участие в проведении экспериментальных исследований системы защиты информации	Темы 1, 2,3, 4, 5,6	содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем	выделять сущности и связи предметной области;	навыками разработки, документирования баз данных с учетом требований по обеспечению информационной безопасности;

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-1	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-3	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5

			баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-5	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-6	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).

			Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-12	Контрольная работа	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Международное сотрудничество в сфере ПОД/ФТ.
2. Международная борьба с финансированием терроризма.
3. Формирование единой международной системы ПОД/ФТ.
4. Организация Объединенных Наций. Роль в формировании международной системы ПОД/ФТ.
5. Конвенции ООН и резолюции Совета Безопасности ООН в сфере ПОД/ФТ.
6. Международный валютный фонд и Всемирный банк как участники международной системы ПОД/ФТ.
7. «Группа восьми» и её роль в борьбе с отмыванием денег и финансированием терроризма.

8. Роль ФАТФ в разработке и совершенствовании международных стандартов ПОД/ФТ.
9. Сорок и девять рекомендаций ФАТФ как комплекс международных стандартов в сфере ПОД/ФТ.
10. Проблема не сотрудничающих стран и территорий.
11. Региональные группы по типу ФАТФ.
12. Группа «Эгмонт».
13. Базельский комитет по банковскому надзору.

Примерная тематика заданий на контрольную работу:

1. Международное сотрудничество в сфере ПОД/ФТ.
2. Международная борьба с финансированием терроризма.
3. Формирование единой международной системы ПОД/ФТ.
4. Организация Объединенных Наций. Роль в формировании международной системы ПОД/ФТ.
5. Конвенции ООН и резолюции Совета Безопасности ООН в сфере ПОД/ФТ.
6. Международный валютный фонд и Всемирный банк как участники международной системы ПОД/ФТ.
7. «Группа восьми» и её роль в борьбе с отмыванием денег и финансированием терроризма.
8. Роль ФАТФ в разработке и совершенствовании международных стандартов ПОД/ФТ.
9. Сорок и девять рекомендаций ФАТФ как комплекс международных стандартов в сфере ПОД/ФТ.
10. Проблема несотрудничающих стран и территорий.
11. Региональные группы по типу ФАТФ.
12. Группа «Эгмонт».
13. Базельский комитет по банковскому надзору.
14. Сравнительная характеристика систем финансового мониторинга России и других зарубежных стран (по выбору студента).
15. Понятия и концепция информационной безопасности банка. Банк как объект противоправных посягательств.
16. Система угроз информационной безопасности банка.
17. Банк как субъект борьбы с противоправными посягательствами (информационный аспект).
18. Система правового обеспечения информационной безопасности банка.
19. Правовые акты общего действия, обеспечивающие информационную безопасность банков методами охранительного содержания.
20. Внутренние нормативные акты. Содержание аудита по информационной безопасности технических средств обработки информации.

21. Организация системы информационной безопасности банка. Субъекты обеспечения информационной безопасности банка.
22. Средства и методы обеспечения информационной безопасности банка.
23. Организация внутреннего контроля банка ее информационная безопасность.
24. Организация службы безопасности банка.
25. Система технических средств безопасности банка.
26. Технические средства охраны.
27. Технические средства охраны банковских операций и продуктов.
28. Информационная безопасность при противодействии хищению денежных средств и совершении кредитных операций.
29. Информационная безопасность при противодействии хищению денежных средств с незаконным использованием пластиковых карт.
30. Информационная безопасность при противодействии хищении денежных средств с использованием аккредитивов.
31. Информационная безопасность при противодействии хищению денежных средств с использованием чеков.
32. Информационная безопасность при противодействии хищению денежных средств с использованием платежных поручений
33. Правовая характеристика векселя. Риски в сфере вексельного обращения. Роль информационной безопасности при этом.
34. Преступления против собственности, в которых вексель является предметом посягательств. Роль информационной безопасности при этом.
35. Преступления против собственности, в которых вексель является средством совершения преступления. Роль информационной безопасности при этом.
36. Меры предупреждения преступлений в сфере вексельного обращения. Роль информационной безопасности при этом.
37. Злоупотребления полномочиями. Коммерческий подкуп. Роль информационной безопасности при этом.
38. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну. Роль информационной безопасности при этом.
39. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка. Роль информационной безопасности при этом.
40. Противоправные посягательства на кадровое обеспечение банка. Противоправные посягательства на нематериальные активы банка. Роль информационной безопасности при этом.
41. Информационная безопасность при легализации (отмывания) доходов, полученных преступным путем.
42. Информационная безопасность и система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма
43. Информация, использующая в целях обеспечения безопасности (информационной безопасности) банка, и ее источники.

44. Бюро кредитных историй.
45. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность (информационную безопасность) банка.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Национальная система по противодействию легализации преступных доходов и финансированию терроризма» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ОПК-1; ПК-3; ПК-5; ПК-6; ПК-12	20-40 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ОПК-1; ПК-3; ПК-5; ПК-6; ПК-12	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Экзамен	ОПК-1; ПК-3; ПК-5; ПК-6; ПК-12	3 теоретических вопроса + практическое задание	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 40 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на

						практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных

						понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

Вариант (Технологии межбанковских электронных расчетов)

1. Что такое система межбанковских расчетов?
2. Какой нормативный срок установлен для проведения расчетов в замках субъекта РФ? А в пределах всей территории РФ?
3. С помощью каких видов счетов могут осуществляться расчеты через КО (филиалы)?
4. В какой очередности осуществляется списание денежных средств при недостаточности средств на счете?
5. Что такое операционный день банка?
6. Как осуществляется обработка платежного документа клиента банка?
7. Какие Вы знаете способы обработки электронных документов банком?
8. Какие Вы знаете способы защиты предупреждения ошибок ввода информации.
9. Перечислите основные параметры функционирования платежных систем?
10. Перечислите ключевые принципы для системно значимых платежных систем.
11. Расскажите о рисках, возникающих в процессе функционирования платежной системы.
12. Каковы основные направления решения проблемы распределению ресурсов, выделенных по корреспондентским счетам, участвующим в системе межбанковских расчетов?
13. Какими двумя способами может происходить исполнение платежей в любой платежной системе?

14. Каково главное достоинство брутто-расчетов?

15. Как решается проблема недостаточности средств при брутто - расчетах?

16. По какой причине в Швейцарии большинство банков не является участниками расчетов в национальной платежной системе?

17. Каким положением Банка России регулируется механизм содержания ликвидности кредитной организации в период временного отсутствия денежных средств в РФ?

18. По какой причине не оправдано развитие филиальной сети в России после кризиса 1998 года?

19. Перечислите известные Вам варианты технологий организации расчетов между филиалами внутри одного банка.

20. Каким образом определяется дата перечисления платежа?

21. Какие договоренности должны быть достигнуты между банком - респондентом и банком-корреспондентом?

22. Каким образом производится учет незавершенных расчетов собственным и транзитным платежам банка?

23. Перечислите наиболее часто используемые подходы при выборе окончательного решения кредитной организации по структуре и характеристикам ее корреспондентской сети.

24. Каковы недостатки действующей в настоящее время платежной системы РФ?

25. Каким образом формируется уникальный идентификатор составителя документа электронного документа?

26. В чем различие и особенности электронного платежного документа сокращенного формата и полноформатного?

27. Какова функция РКЦ (ГРКЦ) при организации расчетов через расчетную сеть Банка России?

28. Какой механизм межрегиональных расчетов в расчетной Банка России?

29. Какие Вы знаете преимущества и недостатки технологии клиринга?

30. Перечислите технологии расчетов между филиалами внутри одного банка.

31. Дайте определение и приведите классификацию клиринга?

32. Перечислите основные цели деятельности клиринговых организаций?

33. Какие операции клиринговых учреждений, обеспечивающие выполнение клиринга или способствующие осуществлению клиринговых взаиморасчетов, Вы знаете?

34. Опишите особенности построения коммуникационной сети которые обеспечивает транспорт сообщений между коммерческими банками и расчетными центрами.

35. Каковы основные функции коммуникационного центра?

36. Опишите схему модулей информационной системы автоматизированного расчетного центра и взаимодействия с коммерческим банком на

основе электронной почты.

37. Какими тремя способами может быть организована технология взаимодействия расчетных центров по переводу средств?
38. Какова история появления и развития S.W.I.F.T.?
39. В чем состоят преимущества и недостатки системы S.W.I.F.T.?
40. Когда S.W.I.F.T. появилась в России (СССР)?
41. Какие функции у Российской Национальной Ассоциации ROS-S.W.I.F.T.?
42. Какова схема прохождения платежного поручения клиента в системе S.W.I.F.T.?
43. Что включает в себя стандарт SWIFT-RUR? .
44. По какой причине потребовалось введение стандарта SWIFT-RUR? Укажите текущую версию стандарта.
45. Назовите основные категории сообщений S.W.I.F.T.?
46. Опишите структуру сети S.W.I.F.T.?
47. Какие новые сервисы появились с переходом к SWIFTNet?
48. Перечислите 4 схемы доступа к сети S.W.I.F.T.
49. Какие интерфейсы системы S.W.I.F.T. Вы знаете?

Форма тестов

1. В соответствии с законодательством РФ доходы, полученные преступным путем, определяются как:

a) денежные средства или иное имущество, полученные в результате совершения преступления;*

b) доходы, полученные финансовыми организациями в результате проведения незаконных операций;

c) денежные средства и иное ценное имущество, приобретенное в результате противозаконных действий.

2. Легализация доходов, полученных преступным путем, представляет собой:

a) использование доходов, полученных преступным путем с целью дальнейшего извлечения прибыли;

b) придание правомерного вида владению, пользованию или распоряжению доходами, полученными преступным путем;*

c) уплату налогов с таких доходов и дальнейшее использование средств в законных целях.

3. К мерам, направленным на противодействие легализации доходов, полученных преступным путем, и финансированию терроризма, относятся:

a) обязательные процедуры внутреннего контроля;

b) обязательный контроль;

c) предварительный контроль;

d) запрет на информирование клиентов и иных лиц о принимаемых мерах ПОД/ФТ.

4.2. Типовые вопросы, выносимые на экзамен

1. Понятие легализации преступных доходов и её влияние на экономику государства.
2. Причины и условия легализации преступных доходов.
3. Отмывание денег: понятие и история его возникновения.
4. Сущность и формы отмывания денег.
5. Способы отмывания денег: понятие, типовые схемы, основные тенденции.
6. Трехфазовая модель отмывания преступных доходов.
7. Общественная опасность отмывания денег.
8. Понятие, сущность, основные формы и источники финансирования терроризма.
9. Связь финансирования терроризма с отмыванием денег.
10. Основные этапы формирования единой международной системы ПОД/ФТ.
11. Основные черты и компоненты международной системы ПОД/ФТ.
12. Институциональные основы международной системы ПОД/ФТ.
13. Организация Объединенных Наций и её роль в международной системе ПОД/ФТ.
14. Рекомендации ФАТФ как всеобъемлющий комплекс международных стандартов в сфере ПОД/ФТ.
15. Понятие финансового мониторинга и его роль в развитии экономики страны.
16. Понятие национальной системы ПОД/ФТ.
17. Место системы ПОД/ФТ в системе государственного устройства РФ.
18. Основные этапы становления национальной системы ПОД/ФТ.
19. Структура национальной системы ПОД/ФТ.

20. Основные нормативно правовые акты РФ в сфере ПОД/ФТ.
21. Федеральный закон РФ №115-ФЗ от 07.08.2001г. как основной источник права в сфере финансового мониторинга в РФ.
22. Правовой статус Росфинмониторинга, полномочия и основные направления деятельности.
23. Формы надзора и виды проверок проводимых Росфинмониторингом.
24. Банк России как надзорный орган в сфере ПОД/ФТ. Правовой статус и полномочия.
25. Федеральная служба по финансовым рынкам как надзорный орган в сфере ПОД/ФТ. Правовой статус и полномочия.
26. Росстрахнадзор как надзорный орган в сфере ПОД/ФТ. Правовой статус и полномочия.
27. Организации, осуществляющие операции с денежными средствами или иным имуществом: права и обязанности в сфере ПОД/ФТ.
28. Системы внутреннего контроля: понятие, назначение, основные задачи.
29. Операции подлежащие обязательному контролю.
30. Обязательные процедуры внутреннего контроля.
31. Критерии выявления и признаки необычных сделок.
32. Типовая структура системы внутреннего контроля.
33. Правила внутреннего контроля: разработка, утверждение, согласование и ключевые положения.
34. Программы осуществления правил внутреннего контроля.
35. Идентификация клиентов и выгодоприобретателей. Правило «знай своего клиента».
36. Обеспечение конфиденциальности информации. Организация и сроки хранения информации.
37. Порядок и сроки представления информации об операциях, подлежащих контролю, в Росфинмониторинг.
38. Виды ответственности за нарушение законодательства в сфере ПОД/ФТ.
39. Гражданско-правовая ответственность за нарушение законодательства в сфере ПОД/ФТ.
40. Меры административной ответственности за нарушение законодательства в сфере ПОД/ФТ.
41. Полномочия уполномоченного органа при применении мер административной ответственности.

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ «НАЦИОНАЛЬНАЯ СИСТЕМА ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ ПРЕСТУПНЫХ ДОХОДОВ И ФИНАНСИРОВАНИЮ ТЕРРОИЗМА»

(Приложение 2 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Общие положения

Целью изучения дисциплины является:

1. Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации при проведении кредитно-финансовых операций;
2. Повысить уровень специальных знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
3. Формирование у студентов специализированной базы знаний по основным понятиям в области банковских информационных систем и технологий кредитно- финансовых операций;
4. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере (обеспечение электронной коммерции и интернет – расчетов).

Задачи дисциплины:

- Теоретические основы подготовки студентов для самостоятельного решения поставленных задачи в области применения банковских информационных систем и технологий на основе действующего российского законодательства с помощью с помощью современных принципов, методов, сил и средств в различных организационных структурах;
- Практические аспекты формирования подходов обучаемых к выполнению самостоятельных исследований в области защиты информации в кредитно-финансовых организациях по базовым направлениям защиты банковской тайны и конфиденциальной информации;
- Формирование, у обучающихся системы знаний для применения основных методов и средств защиты информации кредитно-финансовых операций инструментов и технологий функциональных и контролирующих подразделений кредитно-финансовой организации.

2. Указания по проведению практических занятий

Тема 1: Экономические основы ПОД/ФТ.

Практическое занятие 1.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа технологий электронных расчетов.

Основные положения темы занятия:

1. технологии защиты безналичных электронных расчетов на основе систем «Клиент – банк».
2. технологии защиты безналичных электронных расчетов на основе банковских карт.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Информационная безопасность технологий расчетов и их автоматизированные (электронные) формы. Классификация расчетов по субъектам и формам. Структурная схема взаимодействия традиционных и автоматизированных (электронных) форм расчетов. Защита информационных технологий внешних взаимодействий КБ.
2. Назначение и архитектура системы «Клиент – банк». Информационная безопасность передачи информации до компьютерной сети банка. Системы телефонного банкинга. Система «Клиент – банк» на основе технологии «толстого клиента» Понятие и модели Интернет - банкинга. Организация Интернет – банкинга через портал посредника –аутсорсера. Направления удаленного банковского обслуживания и их защита.
3. Информационная безопасность пластиковых карт. Карточные фокусы. Чековые расчеты – основа банковской информационной технологии электронных расчетов. Информационная безопасность карточной платежной системы и схема их работы. Расчеты банковскими картами в Интернете и их информационная безопасность.

Продолжительность занятия – 4 ч.

Тема 2: Международная система ПОД/ФТ и международные стандарты в сфере ПОД/ФТ.

Практическое занятие 2.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа технологий применения ЭП в кредитно-финансовых организациях.

Основные положения темы занятия:

1. технологии защиты с применением ЭП согласно существующего законодательства.
2. технологии защиты с применением ЭП для организации защищенного электронного документооборота в банках.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Место ЭЦП в ряду криптографических механизмов.
2. История возникновения ЭЦП в России.
3. Информационная безопасность при использовании средств ЭЦП в сети межбанковских расчетов.

Продолжительность занятия – 6 ч.

Тема 3. Национальная система ПОД/ФТ.

Практическое занятие 3.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа электронных транзакций.

Основные положения темы занятия:

1. технологии защиты электронных транзакций в банковской деятельности.
2. криптографические методы защиты информации.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1.Информационная безопасность защищенного информационного обмена при использовании симметричных методов.

2.Информационная безопасность защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.

3.Симметричные алгоритмы шифрования. Схема алгоритма работы сети Фейсталя. Режим электронной кодовой книги.

4.Режим сцепления блоков шифротекста. Режим обратной связи по шифротексту. Режим обратной связи по выходу. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.

Продолжительность занятия – 6 ч.

Тема 4: Государственный финансовый мониторинг.

Практическое занятие 4.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа технологий применения ЭП в кредитно-финансовых организациях.

Основные положения темы занятия:

1. технологии защиты электронных транзакций в банковской деятельности.
2. криптографические методы защиты информации в банковской сфере.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
2. Защита электронных транзакций протокол (SSL).
3. Схема работы протокола SET. Управление ключами.
4. Распространение ключей в случае использования только симметричных методов преобразования информации.
5. Распространение ключей в случае использования сертификатов открытых ключей.
6. Информационная безопасность электронных платежей с помощью цифровых денег.

Продолжительность занятия – 6 ч.

Тема5: Система внутреннего контроля в субъектах первичного финансового мониторинга.

Практическое занятие 5.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки в формировании и построении защищенной электронной платежной системы.

Основные положения темы занятия:

1. технологии защиты электронных платежных систем.
2. принципы построения защищенной электронной платежной системыие методы защиты информации в банковской сфере.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1.Расчетная функция банков и ее автоматизация.

2.Схема обработки платежного документа клиентами.

3.Ключевые принципы для системно – значимых платежных систем.

4.Определение количества ресурсов, которые банк будет держать на своих корсчетах.

Продолжительность занятия – 6 ч.

Тема 6: Ответственность за нарушение законодательства в сфере ПОД/ФТ.

Практическое занятие 6.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки в формировании и построении защищенной системы электронного документооборота в кредитно-финансовой организации.

Основные положения темы занятия:

1. ознакомиться с основными правилами работы с электронными документами.
2. принципы построения защищенной СОД.

Вопросы для обсуждения:

Основной доклад (реферат) по теме занятия.

1. Правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
2. Составление и направление ЭД участником – отправителем. Порядок контроля ЭД, полученных от участников – отправителей.
3. Порядок оформления ЭД, подтверждающих исполнение ЭД участников. Порядок приема к исполнению ЭД участником – получателем.
4. Порядок хранения и уничтожения ЭД.

Продолжительность занятия – 4 ч.

3. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области информационной безопасности кредитно-финансовых операций;

2) привить навыки самостоятельного решения задач в области организации защиты кредитно-финансовых операций.

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	**80**
Вопросы, выносимые на самостоятельное изучение	30
Подготовка к практическим занятиям	12
Подготовка к лабораторным занятиям	16
Подготовка докладов	10
Выполнение практических заданий	12

Вопросы, выносимые на самостоятельное изучение:

для очной формы обучения:

1. Понятия и концепция информационной безопасности банка. Банк как объект противоправных посягательств.

2. Система угроз информационной безопасности банка.
3. Банк как субъект борьбы с противоправными посягательствами (информационный аспект).
4. Система правового обеспечения информационной безопасности банка.
5. Правовые акты общего действия, обеспечивающие информационную безопасность банков методами охранительного содержания.
6. Внутренние нормативные акты. Содержание аудита по информационной безопасности технических средств обработки информации.
7. Организация системы информационной безопасности банка. Субъекты обеспечения информационной безопасности банка.
8. Средства и методы обеспечения информационной безопасности банка.
9. Организация внутреннего контроля банка ее информационная безопасность.
10. Организация службы безопасности банка.
11. Система технических средств безопасности банка.
12. Технические средства охраны.
13. Технические средства охраны банковских операций и продуктов.
14. Информационная безопасность при противодействии хищению денежных средств и совершении кредитных операций.

Примерные темы докладов

вариант1:

1. Международное сотрудничество в сфере ПОД/ФТ.
2. Международная борьба с финансированием терроризма.
3. Формирование единой международной системы ПОД/ФТ.
4. Организация Объединенных Наций. Роль в формировании международной системы ПОД/ФТ.
5. Конвенции ООН и резолюции Совета Безопасности ООН в сфере ПОД/ФТ.
6. Международный валютный фонд и Всемирный банк как участники международной системы ПОД/ФТ.
7. «Группа восьми» и её роль в борьбе с отмыванием денег и финансированием терроризма.
8. Роль ФАТФ в разработке и совершенствовании международных стандартов ПОД/ФТ.
9. Сорок и девять рекомендаций ФАТФ как комплекс международных стандартов в сфере ПОД/ФТ.
10. Проблема несотрудничающих стран и территорий.
11. Региональные группы по типу ФАТФ.
12. Группа «Эгмонт».
13. Базельский комитет по банковскому надзору.

вариант2:

1. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
2. Информационная безопасность подсистемы работы с банковскими картами.
3. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.
4. Информационная безопасность подсистемы операций с ценными бумагами.
5. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия.
6. Информационная безопасность подсистемы управления ресурсами (дилинга).
7. Информационная безопасность в подсистеме обеспечения безопасности.
8. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
9. Информационная безопасность подсистема удаленного банковского обслуживания.
10. Информационная безопасность подсистема обеспечения внутренней деятельности кредитно-финансовой операции как субъекта экономики.
11. Информационная безопасность системы электронного документооборота банка.
12. Информационная безопасность традиционных технологий расчетов.
13. Информационная безопасность и архитектура системы «Клиент – банк».
14. Информационная безопасность и способы передачи информации до компьютерной сети кредитно-финансовой организации.
15. Информационная безопасность системы телефонного банкинга.
16. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»

4. Указания по проведению лабораторных работ

Цель проведения лабораторных работ – ознакомление студентов с комплексом показателей для оценки защищённости информационных объектов, систем и ознакомление с программной средой, используемой для моделирования процессов оптимизации применения систем физической защиты.

Задачи выполнения лабораторных работ:

- определение положения механизмов защиты, включение которых в иерархию системы физической защиты информационных объектов повышает уровень их защищённости;

- мониторинг защищённости охраняемых информационных объектов, базирующийся на решении оптимизационных задач на основе рейтинговых показателей, учитывающий разноплановые экспертные оценки, включая экономические;

- анализ существующих систем физической защиты предприятий на предмет определения эффективности их применения исходя из предполагаемых затрат на создание таких систем, их эксплуатацию и реализацию для предотвращения ущерба от выявленных и потенциальных угроз;

- формирование потенциальной структуры защищённых информационных систем и технологий, путём задания иерархии эшелонов и перечня механизмов защиты для нейтрализации требуемого поля угроз и предотвращённого ущерба;

- формирование динамической модели физической защиты информационных систем для анализа последствий реализации угроз, приводящих к ущербу, близкому или превышающему допустимое для данного хозяйствующего субъекта значение.

Методика проведения лабораторных работ определяется моделью решаемых задач по обеспечению физической защиты информационных объектов, исследуемых студентами на занятии по заданию преподавателя.

Средства выполнения лабораторных работ:

- программный комплекс «Эксперт - 2.0»;
- программный комплекс «EASI»;
- инструменты интегрального метода оценки рисков при распределении ограниченных ресурсов;
- программный комплекс «Adobe Photoshop».

Этапы выполнения лабораторных работ:

1. Постановка задачи лабораторной работы.
2. Ознакомление обучаемых с содержанием и объёмом лабораторной работы.
3. Порядок выполнения лабораторной работы.
4. Регистрация результатов и оформление отчёта о лабораторной работе.
5. Заключительная часть лабораторной работы.

Тематика лабораторных работ и задания к ним

Лабораторная работа 1.

Тема: **Выявление и анализ угроз охраняемым объектам с помощью программного комплекса «Эксперт - 2.0».**

Цель занятия: Ознакомление с программным комплексом оценки защищённости информационных систем «Эксперт - 2.0» и получение практических навыков в моделировании и оптимизации определения угроз

безопасности информационным объектам, применения механизмов защиты в ходе осуществления мониторинга деятельности предприятий.

Учебные вопросы.

1. Формирование матрицы экспертных оценок с полями «механизмы защиты-угрозы» и «угрозы-эшелоны» для оценки достоверности активируемых механизмов защиты.
2. Формирование рейтинговых показателей в разрезе использования конкретных механизмов защиты и эшелонов для системы физической защиты в целом, а также показателей активности отдельных эшелонов и механизмов защиты.
3. Анализ активности системы физической защиты в разрезе использования конкретных механизмов и эшелонов защиты, формулирование предложений по улучшению рейтинга исследуемой системы.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №1:

1. Ознакомиться с системой показателей для оценки информационной защищённости исследуемых объектов.

2. Запустить программу «Эксперт - 2.0» и в интерактивном режиме сформировать перечень известных угроз, механизмов защиты и расставить их в иерархии эшелонов защиты для исследуемых объектов.

3. Сформировать матрицы экспертных оценок «Механизмы защиты – Угрозы» и «Угрозы – Эшелоны защиты» для повышения достоверности исходных данных и активации механизмов защиты.

4. Провести расчёт матрицы, определяющей распределение относительного потенциального ущерба по механизмам защиты и эшелонам безопасности на заданном множестве известных угроз.

5. Проанализировать активность системы информационной безопасности в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемого предприятия.

6. Действия пунктов 3-5 повторить для различных частот активизации угроз безопасности.

7. Сформировать рейтинговые показатели при использовании конкретных механизмов защиты и эшелонов информационной безопасности для ука-занных информационных объектов, а также показатели активности отдельных эшелонов и механизмов защиты.

8. Создать отчёт по лабораторной работе и сформулировать выводы.

Лабораторная работа 2.

Тема: **Исследование системы физической защиты с помощью программного комплекса «Эксперт – 2.0».**

Цель занятия: Ознакомление с программным комплексом оценки защищённости информационных систем «Эксперт - 2.0» и получение

практических навыков в моделировании и оптимизации применения механизмов защиты для деятельности отдельных предприятий с учётом рисков и неопределённости внешней среды.

Учебные вопросы.

1. Корректировка матрицы экспертных оценок для достоверности активации механизмов защиты с расчётом матрицы, определяющей распределение достоверности активации по механизмам защиты и эшелонам безопасности для системы физической защиты на заданном множестве известных угроз.
2. Формирование рейтинговых показателей в разрезе использования конкретных механизмов защиты и эшелонов безопасности для системы физической защиты в целом, а также показателей активности отдельных эшелонов и механизмов защиты.
3. Анализ информационной защищенности исследуемых объектов с определением конкретных механизмов защиты, обеспечивающих наибольшую динамику рейтинговых показателей.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №2:

1. Ознакомиться с системой показателей для оценки защищённости исследуемых объектов в деятельности отдельных предприятий с учётом рисков и неопределённости внешней среды.

2. Запустить программу «Эксперт - 2.0» в интерактивном режиме, получить от преподавателя вариант многоуровневой системы защиты исследуемого объекта предприятия с индивидуальным распределением конкретных механизмов защиты по эшелонам безопасности.

3. Провести расчёт матрицы, определяющей распределение относительного ущерба по механизмам защиты и уровням адаптивной системы защищён-ности исследуемых объектов предприятия на заданном множестве известных угроз.

4. Проанализировать активность адаптивной защиты в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемых объектов предприятия.

5. Сформировать рейтинговые показатели в разрезе использования конкретных механизмов защиты и эшелонов безопасности исследуемых объектов предприятия.

6. Проанализировать существующую защищённость и сформулировать предложения по улучшению рейтинга системы физической защиты исследуемых объектов предприятия в рамках реализации адаптивной системы защиты.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

Лабораторная работа 3.

Тема: **Исследование эффективности системы физической защиты**

предприятия по предполагаемым действиям нарушителя при определённых угрозах и состоянии элементов защиты с помощью программного комплекса оценки враждебных проникновений и действий "EASI".

Цель занятия: Ознакомление студентов с комплексом показателей для оценки защищённости объектов предприятий и программным комплексом оценки враждебных проникновений и действий "Estimate of Adversary Sequence Interruption" (EASI), а так же получение практических навыков в моделировании применения механизмов физической защиты и оценки их эффективности на заданном пути нарушителя при определённых угрозах и состоянии самой системы защиты предприятия.

Учебные вопросы.

1. Анализ пути нарушителя при продвижении к охраняемому объекту.
2. Определение критической точки обнаружения и её влияние на параметры оценки прерывания последовательности действий нарушителя.
3. Построение и исследование диаграммы последовательности действий нарушителя для конкретной зоны охраняемого объекта.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №3:

1. Ознакомиться с краткими теоретическими сведениями по оценке физической защищённости охраняемых объектов и основными способами действий злоумышленников.

2. Ознакомиться с методикой применения модели "EASI" по оценке враждебных проникновений и действий нарушителя на охраняемых объектах.

3. Запустить модель "EASI" на персональном компьютере и смоделировать в интерактивном режиме возможные действия нарушителя на предложенном охраняемом объекте с выбором определённых процедур и механизмов защиты.

4. Рассчитать основные показатели эффективности по введённым данным для выбранного пути проникновения нарушителя и сформированной системы защиты охраняемого объекта, оценить её значение.

5. Проанализировать эффективность исходной системы физической защиты охраняемого объекта, выявить её недостатки и сформировать дополнительные мероприятия и средства защиты на пути проникновения нарушителя для повышения основных критериев безопасности все данные занести в рабочую таблицу модели.

6. Оценить эффективность усовершенствованной системы защиты на основе добавленных элементов на охраняемом объекте, обосновать Ваши решения расчётами с занесением данных в рабочую таблицу модели и

сформировать итоговые показатели эффективности системы физической защиты.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

Лабораторная работа 4.

Тема: **Исследование системы физической защиты и охраняемых объектов с помощью интегрального метода оценки рисков при распределении ограниченных ресурсов, имеющихся в распоряжении службы безопасности.**

Цель занятия: Изучение принципов компьютерного моделирования эффективности системы физической защиты на основе общего уравнения для расчёта рисков охраняемого объекта и получение практических навыков в работе со специализированными программными средствами защиты.

Учебные вопросы.

1. Использование общего уравнения для расчёта рисков охраняемого объекта как важного инструмента количественной оценки системы физической защиты.
2. Анализ и оценка рисков для выбора оптимального варианта защиты, допустимого для охраняемого объекта по критерию затраты-прибыль в исследуемой системе физической защиты.

Продолжительность занятия – 4 часа.

Задание на лабораторную работу №4:

1. Ознакомиться с инструментом количественной оценки системы физиической защиты на основе общего уравнения для расчёта рисков охраняемого объекта.

2. Сформировать рейтинговые показатели риска в разрезе использования выбранных механизмов защиты для охраняемых объектов и для системы в целом, а также показатели активности отдельных элементов защиты.

3. Воспользовавшись инструментом количественной оценки системы физиической защиты на основе общего уравнения расчёта рисков проанализировать исходную защищенность исследуемого объекта, выделить конкретные механизмы защиты, обеспечивающие наибольшую динамику рейтинговых показателей риска.

4. Сохранить в файле текущее состояние адаптивной системы физической защиты и показатели риска для дальнейших исследований.

5. Сравнить разнородную структуру системы физической защиты и рейтинговые показатели риска для заданных вариантов адаптивной защиты охраняемых объектов.

6. Результаты работы и итогового анализа сравнения поместить в Вашу папку на ПК.

7. Создать отчёт по лабораторной работе и сформулировать выводы.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. Основная часть работы раскрывает процесс анализа заданной электрической цепи и должна содержать промежуточные и окончательные результаты расчетов, а также соответствующие временные или частотные диаграммы, поясняющие работу электрической цепи.
3. В процессе изложения материала необходимо давать ссылки на используемую литературу.
4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы

основная:

1. Гамза В.А., Ткачук И.Б.. Безопасность банковской деятельности: учебник.- 2 –е изд., перераб. и доп. – М.: Маркет ДС, 2010. (Универсететская серия).
2. В.В. Дик. Банковские информационные системы: учебник. – М.: Маркет ДС, 2013. (Универсететская серия)
3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие.— М.:ИНФРА-М.,2008.: - (профессиональное образование).
4. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009.

дополнительная:

1. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.

2. Тихонов В.А., Райх В.В., Информационная безопасность: концептуальные, правовые. Организационные и технические аспекты.: Учебное пособие. -М.: Гелиос АРВ, 2006. -528 с., ил. с.171.
3. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).
4. Кобелев О.А. Электронная коммерция: учебное пособие. – М.: Дашков и К, 2010 – 684 с.
5. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
6. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009 – 552 с.: ил.
7. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).

рекомендуемая:

1. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О центральном банке Российской федерации (Банке России)».
2. Стандарт Банка России СТО БР ИББС 1.0-2006
3. Федеральный закон от 27 июля 2006 г. №149 «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 29 июля 2004 г. № 98-ФЗ (с изменениями и дополнениями от 2 февраля 2006 года № 19-ФЗ; от 24 июля 2007 года № 244 – ФЗ) « О Коммерческой тайне».
5. Федеральный закон от 27 июля 2006 г. № 152 – ФЗ «О персональных данных».
6. Указ Президента РФ от 09 сентября 2000 г. «Доктрина информационной безопасности Российской Федерации».
7. Указ Президента РФ от 16 августа 2004 г. № 1085 « Вопросы Федеральной Службы по техническому и экспортному контролю».
8. Указ Президента РФ от 06 марта 1997 г. № 188 « Об утверждении перечня сведений конфиденциального характера».
9. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Основные нормативные правовые акты по теме дисциплины:

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.).

2. Конвенция ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ от 19 декабря 1988 г. (Венская).

3. Конвенция совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности от 8 ноября 1990 г. (Страсбургская).

4. Международная конвенция о борьбе с финансированием терроризма от 9 декабря 1999г.

5. Конвенция ООН против транснациональной организованной преступности от 15 ноября 2000г. (Палермская).

6. Конвенция ООН против коррупции от 31 октября 2003 г. (Меридская).

7. Сорок и девять Рекомендаций ФАТФ, 2003 г. (с изменениями от 22 октября 2004 г.).

8. Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ.

9. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. №174-ФЗ.

10. Гражданский кодекс Российской Федерации часть первая 30 ноября 1994 г. №51-ФЗ, часть вторая от 26 января 1996 г. №14-ФЗ, часть третья от 26 ноября 2001 г. №146-ФЗ.

11. Кодекс об административных правонарушениях Российской Федерации от 30 декабря 2001 г. №195-ФЗ.

12. Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

13. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму».

14. Федеральный закон от 2 декабря 1990 г. №395-1 «О банках и банковской деятельности».

15. Федеральный закон от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг».

16. Федеральный закон от 26 марта 1998 г. №41-ФЗ «О драгоценных металлах и драгоценных камнях».

17. Федеральный закон от 17 июля 1999 г. № 176-ФЗ «О почтовой связи».

18. Федеральный закон от 29 октября 1998 г. № 164-ФЗ «О финансовой аренде (лизинге)».

19. Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».

20. Федеральные закон от 8 августа 2001 г. № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей».

21. Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации».

22. Федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

23. Федеральный закон от 11 ноября 2003 г. № 138-ФЗ «О лотереях».

24. Федеральный закон от 29 декабря 2006 г. № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации».

25. Закон Российской Федерации от 27 ноября 1992 г. № 4015-1 «Об организации страхового дела в Российской Федерации».

26. Основы законодательства Российской Федерации о нотариате от 11 февраля 1993 г. № 4462-1.

27. Указ Президента Российской Федерации от 1 ноября 2001 г. № 1263 «Об уполномоченном органе по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

28. Указ Президента Российской Федерации от 17 декабря 1997 г. № 1300 «Об утверждении Концепции национальной безопасности Российской Федерации».

29. Указ Президента Российской Федерации от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти».

30. Указ Президента Российской Федерации от 20 мая 2004 г. № 649 «Вопросы структуры федеральных органов исполнительной власти».

31. Указ Президента Российской Федерации от 15 февраля 2006 г. № 116 «О мерах по противодействию терроризму».

32. Постановление Правительства Российской Федерации от 17 апреля 2002 г. № 245 «Об утверждении Положения о представлении информации в Федеральную службу по финансовому мониторингу организациями, осуществляющими операции с денежными средствами или иным имуществом».

33. Распоряжение Правительства Российской Федерации от 17 июля 2002 г. №983-р, утвердившее Рекомендации по разработке организациями, совершающими операции с денежными средствами или иным имуществом, правил внутреннего контроля в целях, противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

34. Постановление Правительства Российской Федерации от 8 января 2003 г. № 6 «О порядке утверждения правил внутреннего контроля в организациях, осуществляющих операции с денежными средствами или иным имуществом».

35. Постановление Правительства Российской Федерации от 18 января 2003 г. № 27 «Об утверждении Положения о порядке определения перечня организаций и физических лиц, в отношении которых имеются сведения об их участии в экстремистской деятельности, и доведения этого

перечня до сведения организаций, осуществляющих операции с денежными средствами или иным имуществом».

36. Постановление Правительства Российской Федерации от 18 января 2003 г. № 28 «Об утверждении Положения о постановке на учет в Федеральной службе по финансовому мониторингу организаций, осуществляющих операции с денежными средствами или иным имуществом, в сфере деятельности которых отсутствуют надзорные органы».

37. Постановление Правительства Российской Федерации от 26 марта 2003 г. № 173 «О порядке определения и опубликования перечня государств (территорий), которые не участвуют в международном сотрудничестве в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

38. Постановление Правительства Российской Федерации от 23 июня 2004 г. № 307 «Об утверждении Положения о Федеральной службе по финансовому мониторингу».

39. Постановление Правительства Российской Федерации от 16 февраля 2005 г. № 82 «Об утверждении Положения о порядке передачи информации в Федеральную службу по финансовому мониторингу адвокатами, нотариусами и лицами, осуществляющими предпринимательскую деятельность в сфере оказания юридических и бухгалтерских услуг».

40. Постановление Правительства Российской Федерации от 5 декабря 2005 г. № 715 «О квалификационных требованиях к специальным должностным лицам, ответственным за соблюдение правил внутреннего контроля и программ его осуществления, а также требованиях к подготовке и обучению кадров, идентификации клиентов, выгодоприобретателей в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

41. Приказ КФМ России от 16 июня 2003 г. № 72 «Об утверждении Положения об издании КФМ России постановления о приостановлении операции (оперший) с денежными средствами или иным имуществом в случаях, предусмотренных Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

42. Приказ КФМ России от 11 августа 2003 г. № 104 «Об утверждении рекомендаций по отдельным положениям правил внутреннего контроля, разрабатываемых организациями, совершающими операции с денежными средствами или иным имуществом, в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

43. Приказ Росфинмониторинга от 7 нюня 2005 г. № 86 «Об утверждении Инструкции о представлении в Росфинмониторинг информации, предусмотренной Федеральным законом от 7 августа 2001 года № 115-ФЗ О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

44. Приказ Росфинмониторинга от 14 июля 2005 г. № 108 «О должностных лицах Федеральной службы финансового мониторинга, уполномоченных составлять протоколы об административных правонарушениях»,

45. Приказ Федеральной службы по финансовому мониторингу от 1 ноября 2008 г. № 256 «Об утверждении Положения о требованиях к подготовке и обучению кадров организаций, осуществляющих операции с денежными средствами или иным имуществом, в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Электронные книги:

1. Жарковская, Е. П. Финансовый анализ деятельности коммерческого банка [Электронный ресурс]: Учебник / Е.П. Жарковская. - М: Омега-Л, 2010. - 328 с.
http://www.biblioclub.ru/book/54713/
2. Бертунов, А.Э. Внедрение инновационных технологий в сфере банковского дела [Электронный ресурс] / А.Э. Бертунов. — М.: Лаборатория Книги, 2012. — 93 с.
http://www.biblioclub.ru/book/140927/
3. Исаев, Г. Н. Информационные системы в экономике[электронный ресурс]: Учебник.Доп. МО и науки РФ в кач-ве учебника для студентов вузов / Г.Н. Исаев.-3-е изд., стер. - Москва: Омега-Л, 2010. - 464 с.
http://www.biblioclub.ru/book/54663/
4. Шапкин, А. С. Математические методы и модели исследования операций [Электронный ресурс]: учебник / А. С. Шапкин, В. А. Шапкин. — 5-е изд. — М.: Дашков и К, 2012. — 400 с.
http://www.biblioclub.ru/book/112204/
5. Банковское дело [Электронный ресурс]: учебник / А.М. Тавасиева, В.А. Москвин, Н.Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 287 с.
http://www.biblioclub.ru/book/116705/
6. Чикида, А. Деятельность коммерческого банка в современных условиях [Электронный ресурс]: учебное пособие / А. Чикида. — М.: Лаборатория Книги, 2010. — 130 с.
http://www.biblioclub.ru/book/100020/
7. Николаева, И. П. Рынок ценных бумаг [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению «Экономика» / И. П. Николаева. — М.: ЮНИТИ - ДАНА , 2012. — 223 с.
http://www.biblioclub.ru/book/118462/
8. Кириллов, П. К. Основы менеджмента банковских услуг [Электронный ресурс] /П.К. Кириллов. - М: Лаборатория книги, 2010. - 158 с.
http://www.biblioclub.ru/book/88353/
9. Ковалев, П. П. Банковский риск-менеджмент [Электронный ресурс] / П.П. Ковалев. - : Финансы и статистика, 2009. - 303 с.
http://www.biblioclub.ru/book/79604/

10. Насреддинов, Х. Г. Учет определенных операций в банках (эмиссия пластиковых карт, учет счетов, банковские переводы) [электронный ресурс] / Х.Г. Насреддинов. - Саратов: Ай Пи Эр Медиа, 2010. - 72 с. **http://www.biblioclub.ru/book/78803/**
11. Финансы организаций (предприятий) [Электронный ресурс]: учебник д л я студентов вузов / Н.В. Колчина [и д р .] ; под ред. Н.В. Колчиной. — 5-е изд., перераб. и доп. — М.: ЮНИТИ-ДАНА, 2012. — 407 с. **http://www.biblioclub.ru/book/118178/**

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp – научно-образовательный портал**
2. **http://informika.ru/ – образовательный портал**
3. **www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.**
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.window.edu.ru** - Единое окно доступа.
6. **http://grebennikov.ru/** - Издательский дом «Гребенников»
7. **www.rucont.ru** - ЭБС «Руконт»
8. **http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации**
9. **http://www.gov.ru -Официальный сервер органов государственной власти Российской Федерации.**
10. **http://www.fsb.ru - Официальный сайт Федеральной Службы Безопасности**
11. **http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю**

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине «Национальная система по противодействию легализации преступных доходов и финансированию терроризма»