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

«МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА РЫНКЕ КОРПОРАТИВНОГО КОНТРОЛЯ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев

2020

Автор: д.п.н., профессор Шихнабиева Т.Ш. Рабочая программа дисциплины: «Методы защиты информации на рынке корпоративного контроля». – Королев МО: «Технологический университет», 2020.

Рецензент: **к.т.н., доцент Журавлёв С.И.**

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 Солякой 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			

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

Целью изучения дисциплины является формирование у обучаемых специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, а также получение навыков в применении технологий обеспечения информационной безопасности объектов регионального уровня, а также в процессе управления информационной безопасностью защищаемых объектов.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

Общекультурные компетенции:

ОК-9 - способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности.

Общепрофессиональные компетенции:

ОПК-1; способностью анализировать физические явления и процессы для решения профессиональных задач;

ОПК-6: способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности.

Профессиональные компетенции:

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

Основные **задачи** дисциплины являются:

- ознакомить обучаемых с процессами анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества, с теоретическими аспектами построения и развития платежных систем, с составом и структурой национальной платежной системы России, с организацией деятельности субъектов национальной платежной системы;

- дать представление о понятии безналичные расчеты, платежная система как экономической категории, выраженной в ее особенностях, задачах, функциях в современных экономических условиях;
- дать представление об основных категориях и принципах функционирования
- платежных и расчетных систем;
- сформировать комплексное представление об этапах исторического развития платежной системы;
- проанализировать и сравнить отечественную и зарубежную практику законодательного регулирования платежных и расчетных систем;
- раскрыть теоретические и практические основы функционирования платежно-расчетной инфраструктуры, участников платежной системы и возникающих взаимосвязей;
- охарактеризовать применяемые в банковской практике системы управления рисками в платежной системе;
- получить представление о специфике управления рисками платежных и расчетных систем и о технологиях аутентификации для обеспечения безопасности платежей.

После завершения освоения данной дисциплины студент должен:

Знать:

- этапы исторического развития платежной системы;
- состав и структура национальной платежной системы России, с организацией деятельности субъектов национальной платежной системы;
- теоретические и практические основы функционирования платежно-расчетной инфраструктуры, участников платежной системы и возникающих взаимосвязей
- организацию защиты информации в платёжных системах;

Уметь:

- осуществлять организацию защиты компьютерной информации в платёжных системах;
- анализировать физические явления и процессы для решения профессиональных задач;
- применять методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности.

- применять защитные механизмы реализации при построении системы защиты в платежных системах;

Владеть:

- основными понятиями в области защиты информации в платёжных системах;
  методикой анализа систем защиты платёжных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Методы защиты информации на рынке корпоративного контроля» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров 10.03.01 Информационная безопасность.

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее полученных знаниях по дисциплинам: «Социально-психологические основы управленческой деятельности», «Основы управленческой деятельности», «Базы данных, системы управления базами данных», «Организационное и правовое обеспечение информационной безопасности» и компетенциях: ОК-4,6, ОПК-2,4,5 и ПК-2,8,10,14,15.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения всех последующих дисциплин «Информационная безопасность операционных систем и баз данных», «Защита общества от информации, запрещенной к распространению», «Национальная система по противодействию легализации преступных доходов и финансированию терроризма», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины представлена в таблице 1 и составляет 3 зачетные единицы, 108 часов. Дисциплина читается на 3 курсе во втором семестре.

Таблица 1

Виды занятий	Всего часов	Семестр 5 (очная форма обучения)	Семестр 6
Общая трудоемкость	**108**	**108**	
Аудиторные занятия	**48**	**48**	
Лекции (Л)	16	16	
Практические занятия (ПЗ)	16	16	
Лабораторные работы (ЛР) и (или)	16	16	

другие виды аудиторных занятий			
Самостоятельная работа	**60**	**60**	
Расчетно-графические работы	-	-	
Контрольная работа, домашнее задание	+	+	
Текущий контроль знаний	Тестир. (Т1,Т2)	Тестир. (Т1,Т2)	
Вид итогового контроля	Экзамен	Экзамен	

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Темы дисциплины и виды занятий

Темы дисциплины, количество часов на лекции и практические занятия приведены в таблице 2.

Таблица 2

Наименование тем	Лекции, час. Очная форма обуч.	Практ. занятия, час. Очная форма обуч.	Лаб. занятия, час. Очная форма обуч.	Занятия в интерак. форме, час. Очная форма обуч.	Код компетенций
Тема 1. «Понятие платежной системы, ее сущность и структура. Задачи и функции платежной системы. Понятие платежной системы, ее элементы. Принципы построения платежных систем. Классификация и виды платежных систем. Этапы и особенности перехода от системы безналичных расчетов к национальной платежной системе. Роль Центрального банка в платежных системах. Нормативные и законодательные акты, обеспечивающие работу платежных систем. Риски в платежных системах, пути минимизации	4	4	4	2	ОК– 9; ОПК – 1,6
Тема 2: **«Национальная платежная система России»** Платежная система России: структура и институциональная среда. Законодательное регулирование национальных платежных	4	4	4	4	ПК – 1

систем. Национальная платежная система, основы формирования и направления развития. Федеральный закон РФ №161 от 27.06.2011 «О национальной платежной системе РФ». Основные требования к деятельности операторов платежных систем, операторов электронных денег, операторов услуг платежной инфраструктуры, платежных агентов и субагентов, центральных клиринговых контрагентов по денежным обязательствам. Требования к организации и функционированию платежных систем. Критерии значимости платежной системы (системно значимой или социально значимой). Надзор и наблюдение в национальной платежной системе. Стратегия развития национальной платежной системы от15 .03.2013г.					
Тема 3: **«Платежные системы на основе пластиковых карт»** Платежная карточная система, понятие и элементы. Российские платежные системы. Международные платежные системы на основе пластиковых карт, история создания и развития. Операции коммерческих банков с пластиковыми картами. Характеристика инфраструктуры приема и обслуживания банковских карт. Виды карточных программ. Этапы и задачи создания и реализации карточной программы банка. Эмиссия и эквайринг пластиковых карт. Современное состояние рынка пластиковых карт, проблемы и стратегия развития. Методы защиты информации, подлежащие контролю со стороны предприятия.	4	4	4	2	ПК – 1
Тема 4: **Система защищенного электронного документооборота.** Практические аспекты создания единой защищенной системы электронного документооборота для обработки конфиденциальной информации. Построение СЭД без существенных настроек типовой IT – архитектуры. Безоблачный документооборот. Обзор систем электронного документооборота.	4	4	4	4	ОПК–1, 6; ПК – 1
Итого:	**16**	**16**	**16**	**12**	

4.2. Содержание тем дисциплины

Тема 1: «Понятие платежной системы, ее сущность и структура. Задачи и функции платежной системы.

Понятие платежной системы, ее элементы. Принципы построения платежных систем. Классификация и виды платежных систем.

Этапы и особенности перехода от системы безналичных расчетов к национальной платежной системе. Роль Центрального банка в платежных системах.

Нормативные и законодательные акты, обеспечивающие работу платежных систем. Риски в платежных системах, пути их минимизации.

Тема 2: «Национальная платежная система России»

Платежная система России: структура и институциональная среда. Законодательное регулирование национальных платежных систем.

Национальная платежная система, основы формирования и направления развития. Федеральный закон РФ №161 от 27.06.2011 «О национальной платежной системе РФ».

Основные требования к деятельности операторов платежных систем, операторов электронных денег, операторов услуг платежной инфраструктуры, платежных агентов и субагентов, центральных клиринговых контрагентов по денежным обязательствам. Требования к организации и функционированию платежных систем. Критерии значимости платежной системы (системно значимой или социально значимой). Надзор и наблюдение в национальной платежной системе. Стратегия развития национальной платежной системы от15 .03.2013г.

Особенности учёта и регистрации конфиденциальной документированный информации. Обработка поступающих конфиденциальных документов, их учёт и регистрация. Учёт и регистрация внутренних (созданных/изданных) конфиденциальных документов. Технологии исполнения и контроля за исполнением конфиденциальных документов. Учёт и регистрация отправляемых (исходящих) конфиденциальных документов, их экспедиционная обработка и рассылка. Учёт конфиденциальной документированной информации инвентарного (выделенного) хранения. Учёт конфиденциальной информации при ее автоматизированной обработке.

Основные требования к разрешительной системе документа. Особенности доступа к конфиденциальной документированной информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства. Особенности доступа к конфиденциальной документированной информации при ее предоставлении уполномоченным органам государственной власти. Особенности доступа к конфиденциальной документиро-

ванной информации, составляющей персональные данные. Особенности доступа к архивным конфиденциальным документам.

Тема 3: Платежные системы на основе пластиковых карт»

Платежная карточная система, понятие и элементы. Российские платежные системы. Международные платежные системы на основе пластиковых карт, история создания и развития. Операции коммерческих банков с пластиковыми картами. Характеристика инфраструктуры приема и обслуживания банковских карт.

Виды карточных программ. Этапы и задачи создания и реализации карточной программы банка. Эмиссия и эквайринг пластиковых карт. Современное состояние рынка пластиковых карт, проблемы и стратегия развития. Система защиты платежных систем на основе пластиковых карт.

Методы защиты информации корпоративного контроля в банковской сфере. Экспертиза ценности конфиденциальных документов. Подготовка конфиденциальных документов и дел для архивного хранения. Подготовка конфиденциальных документов и дел к уничтожению.

Режим обмена конфиденциальной документированной информацией. Режим сохранности конфиденциальных документов и дел. Режим конфиденциальности при проведении совещаний и переговоров. Проверка наличия носителей конфиденциальной информации.

Тема 4: Система защищенного электронного документооборота. Практические аспекты создания единой защищенной системы электронного документооборота для обработки конфиденциальной информации. Построение СЭД без существенных настроек типовой IT – архитектуры. Безоблачный документооборот. Обзор систем электронного документооборота.

Особенности конфиденциального электронного документооборота. Основные виды угроз информационной безопасности организации. Основные требования и меры по защите конфиденциальной информации, циркулирующей в эксплуатируемой автоматизированной информационной системе. Организация работ при создании системы защиты электронного документооборота. Организация проведения работ по защите конфиденциальной информации при ее автоматизированной обработке. Обеспечение контроля защиты электронного документооборота. Аттестация автоматизированных информационных систем по требования безопасности информации. Защита от вредоносных программ. Защита системы электронных сообщений.

Основные требования к системам электронного документооборота. Краткая характеристика систем электронного документооборота.

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 «Методы защиты информации на рынке корпоративного контроля» приведена в Приложении 1.

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

Основная литература:

1. Положение ЦБ РФ №266-П «Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт» от 24 декабря 2004г. (с изм.и доп). Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. - М.: ИНФРА-М.,2012.-416 с.: ил.-(профессиональное образование).
2. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009 – 552 с.: ил.
3. Банковская система в современной экономике / Под редакцией Лаврушина О.И. М.:Кнорус, 2011. – 360 с.
4. Интернет-технологии в банковском бизнесе: перспективы и риски : учеб.-практ. пособие / Ю. Н. Юденков, Н. А. Тысячникова, И. В. Сандалов [и др.]. - М. : КНОРУС, 2010. - 320 с.
5. Электронные деньги. Интернет-платежи / В. Г. Мартынов, А. Ф. Андреев, В. А. Кузнецов [и др.]. - М.: Маркет ДС: ЦИПСиР, 2010. - 176 с.

Дополнительная литература:

1. Дик В.В. Банковские информационные системы: учебник. – М.: Маркет ДС, 2006.- 816 с. (Университетская серия).
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
3. 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.

4. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).
5. Рудакова О.С.Банковские электронные услуги: учебное пособие для студентов вузов. М.: Вузовский учебник: ИНФРА-М, 2010 -400с.

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).

Электронные книги:

1. Бертунов, А.Э. Внедрение инновационных технологий в сфере банковского дела [Электронный ресурс] / А.Э. Бертунов. — М.: Лаборатория Книги, 2012.
http://www.biblioclub.ru/book/140927/
2. Фабричнов А.Г., Демушкин А.С. и др. Конфиденциальное делопроизводство и защищенный электронный документооборот.- изд. – М.: ЛОГОС, 2011.
http://biblioclub.ru/index.php?page=book_view&book_id=84996

3. 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/
4. Сабанов А.Г., Зыков В.Д., Шелупанов А.А. и др. Защита персональных данных в организациях здравоохранения. М.:Горячая - линия – Телеком .2012
http://biblioclub.ru/index.php?page=book&id=253606&sr=1
5. Журнал Информационная безопасность.ГРОТЕК.2013, №2
http://biblioclub.ru/index.php?page=book&id=210608&sr=1
6. Журнал Информационная безопасность.ГРОТЕК.2012, №2
http://biblioclub.ru/index.php?page=book_view&book_id=211298
7. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс,2010
http://biblioclub.ru/index.php?page=book&id=86475&sr=

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.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации**.**
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
10. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

9. Методические 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: «Методы защиты информации на рынке корпоративного контроля»

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

«МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА РЫНКЕ КОРПОРАТИВНОГО КОНТРОЛЯ»

(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 компетенции	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.	ОК-9	способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности;	Тема:1,3,4	этапы исторического развития платежной системы;	осуществлять организацию защиты компьютерной информации в платёжных системах; анализировать физические явления и процессы для решения профессиональных задач; применять методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций	основными понятиями в области защиты информации в платёжных системах;
2.	ОПК-1	способностью анализировать физические явления и процессы для решения профессиональных задач;	Тема:2,4	состав и структура национальной платежной системы России, с организацией деятельности субъектов национальной платежной системы; теоретические и практические основы функционирования платежно-расчетной инфраструктуры, участников платежной системы и возникающих взаимосвязей	анализировать физические явления и процессы для решения профессиональных задач; применять методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций	основными понятиями в области защиты информации в платёжных системах; методикой анализа систем защиты платёжных систем.

4.	ОПК-6	способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности;	Тема:1,4	теоретические и практические основы функционирования платежно-расчетной инфраструктуры, участников платежной системы и возникающих взаимосвязей	применять математические методы исследования моделей шифров; осуществлять организацию защиты компьютерной информации в платёжных системах;	основными понятиями в области защиты информации в платёжных системах; методикой анализа систем защиты платёжных систем.
5.	ПК-1	способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.	Тема:1,2,3,4	Теоретические и практические основы функционирования платежно-расчетной инфраструктуры, участников платежной системы и возникающих взаимосвязей;	эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; применять защитные механизмы реализации при построении системы защиты в платежных системах; применять методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности.	навыками использования типовых криптографических алгоритмов; методикой анализа систем защиты платёжных систем.

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
ОК-9	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.
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.
ОПК-6	Доклад в форме презентации	A) полностью сформирована **5 баллов** B) частично сформирована **3-4 балла** C) 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-1	Контрольная работа	A) полностью сформирована **5 баллов** B) частично сформирована **3-4 балла** C) не сформирована **2 балла**	Проводится письменно 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.

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. Исследование выбранного объекта защиты информации – локальной вычислительной сети. Описать выбранный объект защиты, провести анализ его защищённости по следующим пунктам: виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения целостности информации; потенциально возможные злоумышленные действия. Разработать план-график создания системы защиты информации защищаемого объекта –

локальной вычислительной сети с использованием специального программного обеспечения и аппаратных средств.

2. Разработка требований к системе защиты информации локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет.

3. Выработать требования к системе защиты информации выбранного объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет. Определить класс защищенности автоматизированной системы. Разработать техническое задание по созданию системы защиты информации.

4. Разработка пояснительной записки по созданию системы защиты информации выбранного объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет.

5. Обосновать создание ЛВС, имеющий выход в сеть Интернет. Осуществить выбор средств и организационно – технических мер по защите информации выбранного объекта защиты (с учетом защиты информации от несанкционированного доступа к СЭД).

6. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.

7. Обоснование необходимости программно - аппаратной системы защиты информации исследуемого объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет при организации СЭД.

8. Проектирование архитектуры системы защиты информации выбранного объекта, от несанкционированного доступа и оценка его уровня защищённости для СЭД.

9. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД.

10. Роль и место стека протоколов TCP/IP в организации защиты информации от НСД для СЭД.

11. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации для СЭД.

12. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) для СЭД и рекомендаций по её эффективному наращиванию.

13. Разработка проекта системы защиты информации локальной вычислительной сети, от несанкционированного доступа для организации СЭД.

14. Разработка проекта подсистемы компьютерной безопасности структурного подразделения предприятия, с учетом применения систем и средств защиты информации от несанкционированного доступа (для СЭД).

Примерная тематика заданий на контрольную работу:

1. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов MICROSOFT. Типовые решения.
2. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов ORACLE и ALADDIN. Типовые решения.
3. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе продуктов компании CITRIX SYSTEMS.
4. Установка и настройка Центра сертификации, использование ключей eToken в домене Windows Server 2003 для СЭД.
5. Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП в СЭД предприятия.
6. Задачи и методы добавочных механизмов в рамках усиления парольной защиты в СЭД.
7. Реализация моделей доступа механизмами добавочной и встроенной защиты для СЭД.
8. Исследование выбранного объекта защиты информации – локальной вычислительной сети для СЭД предприятия.
9. Описать выбранный объект защиты, провести анализ его защищённости по следующим пунктам: виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения целостности информации; потенциально возможные злоумышленные действия.
10. Разработать план-график создания системы защиты информации защищаемого объекта – локальной вычислительной сети с использованием специального программного обеспечения и аппаратных средств.
11. Разработка требований к системе защиты информации локальной вычислительной сети (СЭД), имеющей выход в сеть Интернет.
12. Выработать требования к системе защиты информации выбранного объекта защиты - локальной вычислительной сети, имеющей выход в сеть Интернет. Определить класс защищенности автоматизированной системы. Разработать техническое задание по созданию системы защиты информации.
13. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.
14. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для платежных систем.

15. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.
16. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию (в том числе и СЭД).
17. Разработка, проекта подсистемы компьютерной безопасности структурного подразделения предприятия при обработке информации в платежных системах.
18. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).

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

Формой контроля знаний по дисциплине «Методы защиты на рынке корпоративного контроля» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

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	ОК-9 ОПК-1 ОПК-6 ПК-1	20 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	ОК-9 ОПК-1 ОПК-6 ПК-1	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	ОК-9 ОПК-1 ОПК-6 ПК-1	3 вопроса	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 семинарских занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. **«Хорошо»:** • умение использовать и применять полученные

						знания на практике; • работа на семинарских занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. **«Удовлетворительно»:** • ответ на вопросы билета. • работа на семинарских занятиях; **«Неудовлетворительно»:** • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на семинарских занятиях; • не отвечает на вопросы.

4.1. Задания для письменных контрольных работ

Варианты выбираются по последним двум цифрам номера зачетной книжки (если эти номера больше 15, то выбор нужно делать по последней цифре.

Контрольная работа представляется в письменном виде- 5-10 стр. на компьютере - 5-10 листов А4 в пластиковом файле или скоросшивателе.

Вариант 1

Задание 1

Рассмотрите понятие «национальной платежной системы».

Задание 2.

Используя учебную литературу и статьи периодической печати, опишите виды рисков, возникающих в платежных системах и пути их минимизации.

Задание 3

Используя данные официального сайта ЦБ РФ www.cbr.ru, проследите динамику количества кредитных организаций, осуществляющих эмиссию и эквайринг платежных карт за последние три года. Составьте таблицы, сделайте соответствующие выводы.

Вариант 2

Задание 1

Рассмотрите структуру и элементы «национальной платежной системы».

Задание 2.

Охарактеризуйте систему межбанковских расчетов SWIFT. Каким критериям должны удовлетворять банки, желающие вступить в данную систему?

Задание 3

Составьте кроссворд, используя основные термины и понятия дисциплины «Современные платежные системы».

Вариант 3

Задание 1

Раскройте общие положения Стратегии развития национальной платежной системы (от 15 марта 2013 г).

Задание 2

Опишите особенности депозитно-кредитных НКО, их функции и операции, виды лицензий. Задание 3

Используя данные официального сайта ЦБ РФ www.cbr.ru, охарактеризуйте динамику количества банковских карт, эмитированных кредитными

организациями по типам карт за последние три года. Составьте таблицы, сделайте соответствующие выводы.

Вариант 4

Задание 1

Опишите направления и принципы развития НПС в соответствии со Стратегией развития национальной платежной системы (от 15 марта 2013 г).

Задание 2.

Платежные небанковские кредитные организации (НКО), лицензия**,** функции и операции.

Задание 3.

Используя данные официального сайта ЦБ РФ www.cbr.ru, охарактеризуйте динамику объема операций, совершенных с использованием платежных карт российских коммерческих банков за последние три года. Составьте таблицы, сделайте соответствующие выводы.

Вариант 5

Задание 1

Какие меры будет принимать Банк России по развитию платежных услуг в соответствии со Стратегией развития национальной платежной системы (от 15 марта 2013 г).

Задание 2.

Расчетные НКО, лицензия**,** функции и операции.

Задание 3.

История появления и деятельность S.W.I.F.T. в России, перспективы развития.

Вариант 6

Задание 1

Какие меры будет принимать Банк России по организации надзора и наблюдения за национальной платежной системой.

Задание 2

Используя федеральный закон «О национальной платежной системе» №161 от 27.06 2011г., рассмотрите понятие электронных денег, их характеристики, сфера применения.

Задание 3

Общеевропейская платежная система «ТАРГЕТ», структура, функциональные особенности, схема проведения расчетов.

Вариант 7

Задание 1

Опишите системно значимые платежные системы, ключевые принципы.

Задание 2

Опишите основные этапы эволюции и реформирования системы безналичных расчетов в России.

Задание 3.

Составьте глоссарий по дисциплине «Современные платежные системы».

Вариант 8

Задание 1

Внутрирегиональные электронные расчеты Банка России.

Задание 2

Опишите основные нововведения в связи с принятием Положения Банка России от 19.06.2012 № 383 – П «О правилах осуществления перевода денежных средств»

Задание 3.

Используя данные официального сайта ЦБ РФ www.cbr.ru, охарактеризуйте динамику количества операций, совершенных с использованием платежных карт российских коммерческих банков за последние три года. Составьте таблицы, сделайте соответствующие выводы.

Вариант 9

Задание 1

Опишите историю создания и развития в современных условиях международной платежной системы «VISA».

Задание 2

Опишите основные нововведения в связи с принятием Положения Банка России от 19.06.2012 № 383 – П «О правилах осуществления перевода денежных средств»

Задание 3.

Используя данные официального сайта ЦБ РФ www.cbr.ru, охарактеризуйте динамику количество платежей клиентов кредитных организаций с использованием платежных поручений, поступивших в кредитные организации, по способам поступления.

Вариант 10

Задание 1

Опишите историю создания и развития в современных условиях международной платежной системы «AMERICAN EXPRESS».

Задание 2

Опишите основные нововведения в связи с принятием Положения Банка России от 19.06.2012 № 383 – П «О правилах осуществления перевода денежных средств»

Задание 3.

Используя данные официального сайта ЦБ РФ www.cbr.ru, охарактеризуйте динамику объема платежей клиентов кредитных организаций с использованием платежных поручений, поступивших в кредитные организации, по способам поступления.

Вариант 11

Задание 1

Опишите историю создания и развития в современных условиях международной платежной системы «MASTER CARD».

Задание 2

Опишите основные нововведения в связи с принятием Положения Банка России от 19.06.2012 № 383 – П «О правилах осуществления перевода денежных средств»

Задание 3.

Используя данные официального сайта ЦБ РФ www.cbr.ru, охарактеризуйте динамику клиентов кредитных организаций с использованием платежных поручений, поступивших в кредитные организации, по способам поступления.

Вариант 12

Задание 1

Опишите историю создания и развития российских карточных платежных систем « UNION CARD».

Задание 2

Платежные системы США Законодательное регулирование переводов денежных средств в США. Система валовых расчетов Fedwire.

Задание 3.

Используя данные официального сайта ЦБ РФ www.cbr.ru, охарактеризуйте динамику количества устройств для приема и обслуживания платежных карт за последние три года. Составьте таблицы, сделайте соответствующие выводы.

Вариант 13

Задание 1

Опишите историю создания и развития в современных условиях российской платежной системы «Золотая корона».

Задание 2

Опишите основные нововведения в связи с принятием Положения Банка России от 19.06.2012 № 383 – П «О правилах осуществления перевода денежных средств»

Задание 3.

Используя данные официального сайта ЦБ РФ www.cbr.ru, охарактеризуйте динамику количества устройств для приема и обслуживания платежных карт за последние три года. Составьте таблицы, сделайте соответствующие выводы.

Вариант 14

Задание 1

Опишите историю создания и развития в современных условиях российской платежной системы «STB CARD»

Задание 2

Опишите основные нововведения в связи с принятием Положения Банка России от 19.06.2012 № 383 – П «О правилах осуществления перевода денежных средств»

Задание 3.

Используя данные официального сайта ЦБ РФ www.cbr.ru, охарактеризуйте динамику количества устройств для приема и обслуживания платежных карт за последние три года. Составьте таблицы, сделайте соответствующие выводы.

Вариант 15

Задание 1

Раскройте понятие межбанковских расчетов, их виды и принципы организации

Задание 2

Европейские платежные системы, их виды и принципы функционирования.

Задание 3.

Используя данные официального сайта ЦБ РФ www.cbr.ru и других сайтов, охарактеризуйте динамику развития рынка кредитных карт за последние три года. Составьте таблицы, сделайте соответствующие выводы.

4.2. Типовые вопросы, выносимые на экзамен

1. Понятие платежной системы, ее сущность и структура.
2. Принципы построения платежной системы.
3. Классификация и виды платежных систем.
4. Нормативные и законодательные акты, обеспечивающие работу платежных систем.
5. ФЗ РФ №161от27.06 2011г. «О национальной платежной системе РФ»

7. Ключевые направления и принципы Стратегии развития национальной платежной системы от 15 марта 2013 г.
8. Положения Банка России от 19.06.2012 № 383 – П «О правилах осуществления перевода денежных средств»
9. Особенности реформирования платежной системы. Эволюция расчетной системы России.
10. Риски в платежных системах, пути их минимизации.
11. Назовите процедуры, выполняемые при регистрации пользователя в системе.
12. Что такое аутентификация.
13. Что такое идентификация.
14. Что такое авторизация.
15. Перечислите элементы аутентификации.
16. Для чего служит механизм управления доступом.
17. Перечислите факторы аутентификации.
18. Назовите методы парольной аутентификации.
19. Что такое PIN- код.
20. Назовите области и условие использования PIN- кода.
21. Для чего необходимы парольные политики.
22. Приведите примеры атак на системы, в которых используется аутентификация на основе пароля.
23. Перечислите физиологические биометрические характеристики.
24. Назовите поведенческие биометрические характеристики.
25. Опишите принцип работы биометрических систем.
26. Приведите примеры атак на системы, использующие аутентификацию с помощью биометрических характеристик, и способы защиты от подобных атак.
27. В каких случаях можно использовать криптографию с открытым ключом.
28. Приведите пример использования криптографии с открытым ключом для шифрования сообщения.
29. Приведите примеры атак на системы, использующие аутентификацию с помощью открытых ключей, и способы защиты от подобных атак.
30. Назовите основные особенности протоколов LAN Manager и NT LAN Manager.
31. Сущность и принципы организации безналичных расчетов.
32. Формы безналичных расчетов во внутреннем обороте.
33. Содержание и принципы организации межбанковских расчетов.
34. Расчеты через учреждения Банка России.
35. Система валовых расчетов в режиме реального времени.
36. Расчеты на основе прямых корреспондентских отношений
37. Внутрирегиональные электронные расчеты Банка России;
38. Межрегиональные электронные расчеты Банка России;
39. Платежная карта, как современный инструмент безналичных расчетов.

40. Банковские пластиковые карты, их виды.
41. Операции коммерческих банков с пластиковыми картами.
42. Платежная система на основе пластиковых карт, ее участники.
43. Российские платежные системы на основе пластиковых карт.
44. Международные платежные системы на основе пластиковых карт, история создания и развития.
45. Операции банков с дебетными (расчетными) картами.
46. Операции с дебетными (расчетными) картами.
47. Современное состояние рынка пластиковых карт, проблемы и пути совершенствования расчетов пластиковыми картами.
48. Виды карточных программ. Этапы и задачи создания и реализации карточной программы банка.
49. Банкомат как элемент электронной системы платежей (функции работы, устройство, принципы работы, последовательность действий).
50. Роль и место Центральных банков в платежных системах зарубежных стран;
51. Всемирная межбанковская система SWIFT, история создания и развития, принципы организации и функции.
52. Платежные системы США
53. Автоматизированные системы межбанковских расчетов в России.
54. Автоматизация межбанковских расчетов за рубежом. Национальные платежные системы.
55. Автоматизированный ввод платежных документов в банке.
56. Принципы обеспечения информационной безопасности национальной платежной системы

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ НА РЫНКЕ КОРПОРАТИВНОГО КОНТРОЛЯ»

(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

Цель дисциплины:

- формирование у студентов специализированной базы знаний по основным понятиям в области системных и прикладных вопросов защиты информации в области платежных систем;
- усовершенствовать навыки по основам практического обоснования требований к системе защиты конфиденциальной информации в СЭДО, что позволит студенту ориентироваться на рынке средств информационной защиты при выборе оптимального решения.

Задачи дисциплины:

Научить студентов самостоятельно решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах, по базовым направлениям защиты государственной тайны и конфиденциальной информации и формированием у обучающихся системы знаний, умений и навыков по защите информации, обеспечению информационной безопасности граждан, общества и государства. В том числе:

- построение разрешительной системы доступа к конфиденциальной информации;
- определение номенклатуры дел, формирование и оформление конфиденциальных дел;
- разносторонний обзор систем электронного документооборота;
- раскрытие общих положений по защите информации в банковской сфере;
- научить студентов самостоятельно решать поставленные задачи в области защищенности конфиденциальной информации с применением систем и средств защиты информации с СЭД;
- ознакомить студентов при решении поставленных задач с помощью перспективных технологий и методов защиты информации;
- ознакомить студентов с методикой применения и использования встроенных механизмов защиты информации;
- ознакомить студентов с порядком применения средств добавочной защиты информации.

2. Указания по проведению практических занятий

Тема 1. Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Документирование конфиденциальной информации. Организация конфиденциального документооборота. Разрешительная система доступа к конфиденциальной информации

Практическое занятие 1.

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

Тема и содержание практического занятия:

Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов MICROSOFT. Типовые решения

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.

2. разрешительная система доступа к документам.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Основные сервисы для обеспечения надежной аутентификации и управления доступом

2. Авторизация при доступе к объекту.

3. Система аудита Active Directoru.

4. Назначение и решаемые задачи инфраструктуры открытых ключей.

5.Управление идентификацией (ILM).

6. Microsoft Identity Integration Server (MIIS).

7.Системы обеспечения.

Продолжительность занятия – 4 ч.

Тема 2. Составление номенклатуры дел, формирование и оформление конфиденциальных дел. Подготовка конфиденциальных документов для архивного хранения или уничтожения. Режим конфиденциальности документированной информации

Практическое занятие 2.

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

Тема и содержание практического занятия:

Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов ORACLE и ALADDIN. Типовые решения

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.

2. составление номенклатуры дел и подготовка их для архивного хранения.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Управление доступом в СУБД Oracle с помощью встроенных механизмов безопасности.
2. Управление доступом в СУБД Oracle с помощью криптографических средств защиты.

Продолжительность занятия – 4 ч.

Тема 3: Система защищенного электронного документооборота. Практические аспекты создания единой защищенной СЭД для обработки конфиденциальной информации

Практическое занятие 3.

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

Тема и содержание практического занятия:

Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе продуктов компании CITRIX SYSTEMS

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.

2. создание единой системы защищенной ЭДО.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Описание продуктов компании CITRIX SYSTEMS.

2. Компоненты систем, построенных с использованием XenApp.

Продолжительность занятия – 4 ч.

Тема 4: Построение СЭД без существенных настроек типовой IT – архитектуры. Безоблачный документооборот. Обзор систем электронного документооборота

Практическое занятие 4.

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

Тема и содержание практического занятия:

Часть 1: Установка и настройка Центра сертификации, использование ключей eToken в домене Windows Server 2003

Часть 2: Использование eToken для безопасного доступа к информационным ресурсам, для шифрования и для ЭЦП

Часть 3: Технология программно-аппаратной защиты

Цель работы: Получить практические знания и навыки практического применения нормативно – правовых документов по обработке конфиденциальной информации на предприятии при построении СЭД.

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.

2. создание единой системы защищенной ЭДО.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

Часть1:

1.Общие сведения об аутентификации пользователей в домене Windows Server 2003 с помощью цифровых сертификатов и ключей eToken.

2. Установка и настройка Центра сертификации (CA), подготовка консоли Центра сертификации, издание сертификатов

3. Использование ключей eToken для регистрации в домене, для запуска приложений от имени другого пользователя и для подключения сетевых дисков с использованием прав доступа другого пользователя.

Часть2:

1. Общие сведения о безопасном доступе к информационным ресурсам организации.

2. Удаленный доступ к рабочему столу (RDP).

3. Виртуальные частные сети (VPN).

4. Общие сведения о протоколе EAP.

5. Защищенное подключение к Web – серверу (HTTPS).

6. Шифрование и использование ЭЦП.

Часть3:

1. Реализация программно-аппаратного контроля (мониторинга) активности системы защиты.

2. Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами.

3. Механизм удаленного (сетевого) мониторинга активности системы защиты, как альтернатива применению аппаратной компоненте защиты.

Продолжительность занятия – 2 ч.

Тема 5. Применение метода димензиональной онтологии при выборе средств технической защиты информации от несанкционированного доступа.

Применение аппаратных средств аутентификации и хранения ключевой информации

Практическое занятие 5.

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

Тема и содержание практического занятия:

Часть 1: Метод контроля вскрытия аппаратуры

Часть 2: Электронная цифровая подпись

Цель занятия: ознакомление с принципами защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной цифровой подписи (ЭЦП).

Основные положения темы занятия:

1. характеристика нормативно правовой базы предприятия.

2. создание единой системы защищенной ЭДО.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Общий подход к контролю вскрытия аппаратуры техническими средствами защиты.

2. Реализация системы контроля вскрытия аппаратуры.

3. Принципы комплексирования средств защиты информации.

4.Комплексирование механизмов защиты информации от НСД.

5.Комплексирование в одной системе механизмов технической и объектовой защиты информации с единым сервером безопасности.

Продолжительность занятия – 2 ч.

3. 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 указанных 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 защищённости 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 физической 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.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих современных платёжных систем в банковской сфере;

2) привить навыки самостоятельного решения нестандартных задач в области программных средств защиты информации.

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
	5 семестр	
1	**Понятие и особенности конфиденциальной информации. Общая характеристика нормативной правовой базы. Документирование конфиденциальной информации**	1. Обоснование необходимости программно - аппаратной системы защиты информации исследуемого объекта защиты - локальной вычислительной сети от несанкционированного доступа, имеющей выход в сеть Интернет при организации СЭД. 2. Проектирование архитектуры системы защиты информации выбранного объекта, от несанкционированного доступа и оценка его уровня защищённости для СЭД. 3. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД.
2	**Организация конфиденциального документооборота. Разрешительная система доступа к конфиденциальной информации. Составление номенклатуры дел, формирование и оформление конфиденциальных дел**	1. Роль и место стека протоколов TCP/IP в организации защиты информации от НСД для СЭД. 2. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации для СЭД.
3	**Подготовка конфиденциальных документов для архивного хранения или уничтожения. Режим конфиденциальности документированной информации**	1. Разработка проекта системы защиты информации локальной вычислительной сети, от несанкционированного доступа для организации СЭД.

4	**Система защищенного электронного документооборота. Практические аспекты создания единой защищенной СЭД для обработки конфиденциальной информации. Построение СЭД без существенных настроек типовой IT – архитектуры. Безоблачный документооборот.**	1. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) для СЭД и рекомендаций по её эффективному наращиванию.

Вопросы, выносимые на самостоятельное изучение:

1. Обеспечение безопасности доступа к данным и приложениям информационной системы организации на основе рекомендаций и продуктов MICROSOFT. Типовые решения.
2. Обеспечение безопасности доступа к данным и приложениям информационной системы организации. Типовые решения.
3. Системы валовых расчетов в режиме реального времени. Система расчетов БЭСП. Межфилиальные расчеты. Внутрирегиональные расчеты. Межбанковский клиринг.
4. Мировые тенденции развития платежных систем. Роль и место Центральных банков в платежных системах зарубежных государств.
5. Всемирная межбанковская система SWIFT, история создания и развития. Платежные системы зарубежных государств
6. Самостоятельное изучение по материалам периодических изданий и информации в сети Интернет эффективности национальных и всемирных платежных систем, динамики объемов и структуры платежей. Составление аналитического заключения.
7. Исследование выбранного объекта защиты информации – локальной вычислительной сети для СЭД предприятия.
8. Описать выбранный объект защиты, провести анализ его защищённости по следующим пунктам: виды угроз; характер происхождения угроз; классы каналов несанкционированного получения информации; источники появления угроз; причины нарушения целостности информации; потенциально возможные злоумышленные действия.
9. Разработать план-график создания системы защиты информации защищаемого объекта – локальной вычислительной сети с использованием специального программного обеспечения и аппаратных средств.
10. Разработка требований к системе защиты информации локальной вычислительной сети (СЭД), имеющей выход в сеть Интернет.

11. Выработать требования к системе защиты информации выбранного объекта защиты - локальной вычислительной сети, имеющей выход в сеть Интернет. Определить класс защищенности автоматизированной системы. Разработать техническое задание по созданию системы защиты информации.

12. Исследование объекта защиты информации и анализ его защищённости по видам угроз, классам каналов несанкционированного получения информации, причинам нарушения целостности информации и потенциально возможным злоумышленным действиям.

13. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД.

14. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации.

15. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) и рекомендаций по её эффективному наращиванию (в том числе и СЭД).

16. Разработка, проекта подсистемы компьютерной безопасности структурного подразделения предприятия при обработке информации в СЭД.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	60	Изучение открытых источников
2.	Подготовка к практическим занятиям	16	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	16	Изучение открытых источников
4.	Тематика докладов	12	1. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД. 2. Исследование выбранного объекта защиты информации – локальной вычислительной сети для СЭД предприятия.
5.	Выполнение практических заданий	16	Разработка аппаратного средства вычислительной техники по заданным характеристикам

Примерные темы докладов

1. Обоснование необходимости программно - аппаратной системы защиты информации исследуемого объекта защиты - локальной вычисли-

тельной сети от несанкционированного доступа, имеющей выход в сеть Интернет.

2. Проектирование архитектуры системы защиты информации выбранного объекта, от несанкционированного доступа и оценка его уровня защищённости для СЭД.

3. Средства защиты информации от НСД и основные требования по применению способов и средств защиты для СЭД.

4. Роль и место стека протоколов TCP/IP в организации защиты информации от НСД для СЭД.

5. Совершенствование системы защиты информации предприятия (фирмы) на основе комплексного применения современных средств защиты информации для СЭД.

6. Разработка и обоснование требований к системе защиты информации предприятия (фирмы) для СЭД и рекомендаций по её эффективному наращиванию.

7. Разработка проекта системы защиты информации локальной вычислительной сети, от несанкционированного доступа для организации СЭД.

Разработка проекта подсистемы компьютерной безопасности структурного подразделения предприятия, с учетом применения систем и средств защиты информации от несанкционированного доступа (для СЭД).

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 проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

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 литература:

1. Положение ЦБ РФ №266-П «Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт» от 24 декабря 2004 г (с изм.и доп).Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие.— М.:ИНФРА-М.,2012.- 416 с.: ил.- (профессиональное образование).
2. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009 – 552 с.: ил.
3. Банковская система в современной экономике / Под редакцией Лаврушина О.И. М.:Кнорус, 2011. – 360 с.
4. Интернет-технологии в банковском бизнесе: перспективы и риски : учеб.-практ. пособие / Ю. Н. Юденков, Н. А. Тысячникова, И. В. Сандалов [и др.]. - М. : КНОРУС, 2010. - 320 с.
5. Электронные деньги. Интернет-платежи / В. Г. Мартынов, А. Ф. Андреев, В. А. Кузнецов [и др.]. - М.: Маркет ДС: ЦИПСиР, 2010. - 176 с.

Дополнительная литература:

1. Дик В.В. Банковские информационные системы: учебник. – М.: Маркет ДС, 2006.- 816 с. (Универсететская серия).
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
3. 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.
4. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).
5. Рудакова О.С.Банковские электронные услуги: учебное пособие для студентов вузов. М.: Вузовский учебник: ИНФРА-М, 2010 -400с.

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).

Электронные книги:

1. Бертунов, А.Э. Внедрение инновационных технологий в сфере банковского дела [Электронный ресурс] / А.Э. Бертунов. — М.: Лаборатория Книги, 2012.
http://www.biblioclub.ru/book/140927/
2. Фабричнов А.Г., Демушкин А.С. и др. Конфиденциальное делопроизводство и защищенный электронный документооборот.- изд. – М.: ЛОГОС, 2011.
http://biblioclub.ru/index.php?page=book_view&book_id=84996
3. 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/
4. Сабанов А.Г., Зыков В.Д., Шелупанов А.А. и др. Защита персональных данных в организациях здравоохранения. М.:Горячая - линия – Телеком .2012
http://biblioclub.ru/index.php?page=book&id=253606&sr=1
5. Журнал Информационная безопасность.ГРОТЕК.2013, №2
http://biblioclub.ru/index.php?page=book&id=210608&sr=1
6. Журнал Информационная безопасность.ГРОТЕК.2012, №2

http://biblioclub.ru/index.php?page=book_view&book_id=211298

7. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс,2010 http://biblioclub.ru/index.php?page=book&id=86475&sr=

7. 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.
4. www.biblioclub.ru - Универсальная библиотека онлайн.
5. www.rucont.ru - ЭБС «Руконт».
6. http://www.academy.it.ru/ – академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации**.**
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
10. 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 «Методы защиты информации на рынке корпоративного контроля».