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

«ОСНОВЫ УПРАВЛЕНИЯ В КОРПОРАЦИЯХ»

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: «Основы управления в корпорациях» – 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. Дать студентам концептуальные знания основ финансового управления в корпорациях для региональных информационных объектов с учетом современных требований теории по защите информации;

2. Выработать и закрепить у студентов базовые умения и навыки по практической организации и реализации современных технологий финансового менеджмента в корпорациях как типовых региональных информационных объектах с учетом современных международных и отечественных стандартов.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общекультурные компетенции:

- ОК-4: способность использовать основы правовых знаний в различных сферах деятельности;
- ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

Общепрофессиональные компетенции:

- ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;
- ОПК-5: способность использовать нормативные правовые акты в профессиональной деятельности;

Профессиональные компетенции:

- ПК-6: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
- ПК-9: способность осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения

информационной безопасности по профилю своей профессиональной деятельности.

Основными **задачами** дисциплины являются:

- Теоретические основы подготовки студентов в области криптографических методов защиты информации в компьютерных системах и сетях;
- Практические аспекты формирования подходов к выполнению самостоятельных исследований студентами в области криптографических методов защиты информации в компьютерных системах и сетях.

После завершения освоения данной дисциплины студент должен:

Знать:

- принципы построения системы менеджмента информационной безопасности (СМИБ);
- современные подходы к управлению информационной безопасностью (ИБ) региональных информационных объектов и направления их развития;
- особенности отдельных процессов управления ИБ в рамках СМИБ;
- основные международные и российские стандарты, регламентирующих вопросы управления ИБ;
- принципы разработки процессов управления ИБ;
- основы создания ключевых документов, регламентирующих вопросы управления ИБ;
- подходы к интеграции СМИБ в общую систему управления организации.

Уметь:

- анализировать текущее состояние ИБ на региональных информационных объектах с целью разработки требований к разрабатываемым процессам управления ИБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
- применять процессный подход к управлению ИБ в различных сферах деятельности региона;
- используя современные методы и средства, разрабатывать процессы управления ИБ, учитывающие особенности функционирования регионов и решаемые ими задачи, и оценивать их эффективность;
- практически решать задачи формализации разрабатываемых процессов управления ИБ;

- разрабатывать документационное обеспечение процессов управления ИБ, включая различные политики ИБ и применять его на практике.

Владеть:

- применения терминологии и процессорным подходом построения СМИБ;
- анализа бизнес-активов организации, их угроз и уязвимостей в рамках области действий СМИБ;
- построения как отдельных процессов управления ИБ, так и системы процессов в целом.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Основы управления в корпорациях» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01«Информационная безопасность».

Дисциплина реализуется кафедрой управления.

Изучение данной дисциплины базируется на знаниях ранее изученных дисциплин: «Экономика предприятия и организация производства», «Основы управленческой деятельности», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности» и компетенциях: ОК-2,4,5,6, ОПК-4,5 и ПК-7,8,10,14,15.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения всех последующих дисциплин «Сети и системы передачи информации», «Программно-аппаратные средства защиты информации», «Актуальные проблемы финансов», «Мониторинг рынка страхования», «Информационная безопасность кредитно-финансовых операций», «Налогообложение субъектов финансового мониторинга», «Организация информационно-аналитического обеспечения финансового мониторинга», «Финансовый анализ», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3.Объем дисциплины (модуля) и виды учебной работы

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

Таблица1

Виды занятий	**Всего часов**	**Семестр 5**	**Семестр 6**	**Семестр 7**	**Семестр …**
Общая трудоемкость	144	144			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	16	16			
Самостоятельная работа	96	96			
КСР	-	-			
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	Лабораторная работа, час. Очное	Практические занятия, час Очное	Занятия в интерактивной форме, час	Код компетенций
Тема 1. Безопасность кредитно-финансовых организаций как объекта управления	2	2	2	3	ОК-4,5; ОПК-4,5; ПК-6,9.
Тема 2. Служба безопасности кредитно-финансовых организаций	2	2	2	3	ОК-4,5; ОПК-4,5; ПК-6,9.
Тема 3. Обеспечение информационной безопасности кредитно-финансовых организаций	4	4	4	4	ОК-4,5; ОПК-4,5; ПК-6,9.
Тема 4. Обеспечение безопасности персонала кредитно-финансовых организаций	4	4	4	4	ОК-4,5; ОПК-4,5; ПК-6,9.
Тема 5. Обеспечение имущественной безопасности кредитно-финансовых организаций	4	4	4	4	ОК-4,5; ОПК-4,5; ПК-6,9.
Итого:	16	16	16	18	

4.2. Содержание тем дисциплины

Тема 1. Безопасность кредитно-финансовых организаций как объекта управления

Общее понятие безопасности в финансовой сфере и ее компоненты. Система управления информационной безопасностью организации.

Тема 2. Служба безопасности кредитно-финансовых организаций

Служба безопасности в системе корпоративного управления и возможные подходы к ее организации. Основные аспекты управления корпоративной деятельностью службы безопасности банка. Функции руководителя и основных подразделений службы безопасности.

Тема 3. Обеспечение информационной безопасности кредитно-финансовых организаций

Конфиденциальная информация финансовой организации как объект защиты. Угрозы информационной безопасности финансовой организации. Обеспечение информационной безопасности финансовой организации.

Тема 4. Обеспечение безопасности персонала кредитно-финансовых организаций

Персонал финансовой организации как объект потенциальных угроз. Организация защиты персонала от возможных угроз. Обучение персонала правилам обеспечения безопасности финансовой организации.

Тема 5. Обеспечение имущественной безопасности кредитно-финансовых организаций

Имущество финансовой организации как объект защиты. Защита от угроз с использованием сетей корпоративных компьютерных коммуникаций. Защита от угроз, связанных с использованием электронных банковских карточек. Защита финансовых организаций от мошенничества при получении кредита. Защита финансовых организаций от угрозы хищения высоколиквидных активов. Защита финансовых организаций от ограблений.

5. Основы управления информационной безопасностью 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 приведена в Приложении 1.

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

Основная литература:

1. Основы управления информационной безопасностью. Учебное пособие для вузов/ А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов. А. И. Толстой. - М.: Горячая линия - Телеком, 2012.

2. Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М.: Горячая линия - Телеком, 2012.

3. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М.: Горячая линия - Телеком, 2012.

Дополнительная литература:

1. Управление рисками информационной безопасности. Учебное пособие для вузов / Н. Г. Милославская. М. 10. Сенаторов, А. И. Толстой. - М: Горячая линия-Телеком, 2012.

2. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов. А. И. Толстой. - М.: Горячая линия-Телеком, 2012.

3. Анисимов А.А. Менеджмент в сфере информационной безопасности; Учебное пособие.- М.: БИНОМ. Лаборатория знаний,2012.

Рекомендуемая литература:

1. Белов Е.Б. и др. Основы информационной безопасности: Учеб. пособие. – М: Горячая линия – Телеком, 2006.

2. Гринберг А.С. и др. Защита информационных ресурсов государственного управления: Учеб. пособие. – М.: ЮНИТИ-ДАНА, 2003.
3. Грушо А.А. Теоретические основы компьютерной безопасности. Учеб. пособие. – М.: ИЦ Академия, 2009.
4. Корт С.С. Теоретические основы защиты информации: Учеб. пособие. – М.: Гелиос АРВ, 2004.
5. Организационно-правовое обеспечение информационной безопасности / Под ред. А.А.Стрельцова. – М.: ИЦ Академия, 2008.
6. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. – М: МЦНМО, 2002.
7. Шепитько Г.Е. и др. Комплексная система защиты информации на предприятии: Часть 1. Учеб. пособие. – М.: МФА, 2008.
8. Шепитько Г.Е. Экономика защиты информации: Учеб. пособие. – М.: МФЮУ, 2011.
9. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты: Учеб. пособие. – М.: Книжный мир, 2009.
10. Шульц В.П. и др. Информационное управление в условиях активного противоборства: модели и методы. – М.: Наука, 2011.
11. Шепитько Г.Е. Теория информационной безопасности и методология защиты информации. – М.: РГСУ, 2012.
12. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО "ТИД "СД", 2001.
13. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. М.: СИНТЕГ, 2000.
14. Ярочкин В.И. Информационная безопасность. М.: Международные отношения, 2008

Электронные книги:

1. Управление информационной безопасностью. Практические правила.
http://www.100balov.com/data/ukr/IJnfo_dlya_stydenta__12/1_1743.doc

2. Обеспечение информационной безопасности бизнеса.
http://detectivebooks.ru/author/76454196/

3. Управление информационной безопасностью.
http://romangamma.ucoz.ru/_ld/0/5_____.pdf

4. Политики безопасности компании при работе в Интернет
http://bookz.ru/authors/sergei-petrenko/politiki_424/1-politiki_424.html

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. **http://www.academy.it.ru/ –** академия АЙТИ.

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: «Основы финансового моделирования в корпорациях»

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

«ОСНОВЫ УПРАВЛЕНИЯ В КОРПОРАЦИЯХ»

(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.	ОК-4	способность использовать основы правовых знаний в различных сферах деятельности	Тема:1,4	принципы построения системы менеджмента информационной безопасности (СМИБ)	анализировать текущее состояние ИБ на региональных информационных объектах с целью разработки требований к разрабатываемым процессам управления ИБ;	применения терминологии и процессорным подходом построения СМИБ;
2.	ОК-5	способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Тема:1,2,3	современные подходы к управлению информационной безопасностью (ИБ) региональных информационных объектов и направления их развития;	определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;	анализа бизнес-активов организации, их угроз и уязвимостей в рамках области действий СМИБ
3.	ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для	Тема:3,5	особенности отдельных процессов управления ИБ в рамках СМИБ;	применять процессный подход к управлению ИБ в различных сферах деятельности региона;	построения как отдельных процессов управления ИБ, так и системы процессов в целом

		поиска и обработки информации				
4.	ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности	Тема:1,2,3	основные международные и российские стандарты, регламентирующих вопросы управления ИБ;	используя современные методы и средства, разрабатывать процессы управления ИБ, учитывающие особенности функционирования регионов и решаемые ими задачи, и оценивать их эффективность	построения как отдельных процессов управления ИБ, так и системы процессов в целом
5.	ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Тема:3,5	принципы разработки процессов управления ИБ;	практически решать задачи формализации разрабатываемых процессов управления ИБ;	применения терминологии и процессорным подходом построения СМИБ;
6.	ПК-9	способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Тема:1-5	основы создания ключевых документов, регламентирующих вопросы управления ИБ; подходы к интеграции СМИБ в общую систему управления организации.	разрабатывать документационное обеспечение процессов управления ИБ, включая различные политики ИБ и применять его на практике	анализа бизнес-активов организации, их угроз и уязвимостей в рамках области действий СМИБ

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-4	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.
ОК-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.
ОПК-4	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.
ОПК-5	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-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-9	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств

		сформирована **3-4 балла** С) не сформирована **2 балла**	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. Общее понятие безопасности в финансовой сфере и ее компоненты.
2. Система управления информационной безопасностью организации.
3. Служба безопасности в системе корпоративного управления и возможные подходы к ее организации.
4. Основные аспекты управления корпоративной деятельностью службы безопасности банка.
5. Функции руководителя и основных подразделений службы безопасности.
6. Конфиденциальная информация финансовой организации как объект защиты.
7. Угрозы информационной безопасности финансовой организации.
8. Обеспечение информационной безопасности финансовой организации.

9. Персонал финансовой организации как объект потенциальных угроз.
10. Организация защиты персонала от возможных угроз.
11. Обучение персонала правилам обеспечения безопасности финансовой организации.
12. Имущество финансовой организации как объект защиты.
13. Защита от угроз с использованием сетей корпоративных компьютерных коммуникаций.
14. Защита от угроз, связанных с использованием электронных банковских карточек.
15. Защита финансовых организаций от мошенничества при получении кредита.
16. Защита финансовых организаций от угрозы хищения высоколиквидных активов.
17. Защита финансовых организаций от ограблений.

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

Формой контроля знаний по дисциплине «Основы управления в корпорациях» 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	ОК-4; ОК-5; ОПК-4; ОПК-5; ПК-6; ПК-9.	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-4; ОК-5; ОПК-4; ОПК-5; ПК-6; ПК-9.	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-4; ОК-5; ОПК-4; ОПК-5; ПК-6; ПК-9.	3 вопроса	Экзамен проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 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 «Удовлетвори-тельно»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «Неудовлетворительно»: • 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.

1. Требование безопасности повторного использования объектов противоречит:
инкапсуляции +
наследованию
полиморфизму
2. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
запрет на чтение каких-либо файлов, кроме конфигурационных
запрет на изменение каких-либо файлов, кроме конфигурационных +
запрет на установление сетевых соединений
3. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
меры обеспечения целостности
административные меры +
меры административного воздействия

4. Дублирование сообщений является угрозой:
доступности
конфиденциальности
целостности +
5. Самыми опасными источниками внутренних угроз являются:
некомпетентные руководители +
обиженные сотрудники
любопытные администраторы
6. Для внедрения бомб чаще всего используются ошибки типа:
отсутствие проверок кодов возврата
переполнение буфера +
нарушение целостности транзакций
7. В число целей политики безопасности верхнего уровня входят:
решение сформировать или пересмотреть комплексную программу безопасности +
обеспечение базы для соблюдения законов и правил +
обеспечение конфиденциальности почтовых сообщений
8. В число целей программы безопасности верхнего уровня входят:
управление рисками +
определение ответственных за информационные сервисы
определение мер наказания за нарушения политики безопасности
9. В рамках программы безопасности нижнего уровня осуществляются:
стратегическое планирование
повседневное администрирование +
отслеживание слабых мест защиты +
10. Политика безопасности строится на основе:
общих представлений об ИС организации
изучения политик родственных организаций
анализа рисков +
11. В число целей политики безопасности верхнего уровня входят:
формулировка административных решений по важнейшим аспектам реализации программы безопасности +
выбор методов аутентификации пользователей
обеспечение базы для соблюдения законов и правил +

1.2. Типовые вопросы, выносимые на экзамен

1. Общее понятие безопасности в финансовой сфере и ее компоненты.
2. Система управления информационной безопасностью организации.
3. Служба безопасности в системе корпоративного управления и возможные подходы к ее организации.
4. Основные аспекты управления корпоративной деятельностью службы безопасности банка.

5. Функции руководителя и основных подразделений службы безопасности.
6. Конфиденциальная информация финансовой организации как объект защиты.
7. Угрозы информационной безопасности финансовой организации.
8. Обеспечение информационной безопасности финансовой организации.
9. Персонал финансовой организации как объект потенциальных угроз.
10. Организация защиты персонала от возможных угроз.
11. Обучение персонала правилам обеспечения безопасности финансовой организации.
12. Имущество финансовой организации как объект защиты.
13. Защита от угроз с использованием сетей корпоративных компьютерных коммуникаций.
14. Защита от угроз, связанных с использованием электронных банковских карточек.
15. Защита финансовых организаций от мошенничества при получении кредита.
16. Защита финансовых организаций от угрозы хищения высоколиквидных активов.
17. Защита финансовых организаций от ограблений.

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ОСНОВЫ УПРАВЛЕНИЯ В КОРПОРАЦИЯХ»

(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. Дать студентам концептуальные знания основ финансового управления в корпорациях для региональных информационных объектов с учетом современных требований теории по защите информации;

2. Выработать и закрепить у студентов базовые умения и навыки по практической организации и реализации современных технологий финансового менеджмента в корпорациях как типовых региональных информационных объектах с учетом современных международных и отечественных стандартов.

Задачи дисциплины:

- Ознакомление обучаемых с основными методами управления.
- Изучение правовых, организационных и программно-технических мер обеспечения информационной безопасности.
- Формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем
- Формирование требований к системе управления ИБ конкретного объекта
- Обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации
- Проектирование системы управления ИБ конкретного объекта.

2. Указания по проведению практических занятий

Тема 1. Безопасность кредитно-финансовых организаций как объекта управления

Практическое занятие 1.

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

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки систем и процессов управления информационной безопасностью

Учебные вопросы:

- Управление информационной безопасностью. Комплексная система управления информационной безопасностью.
- Основные определения и критерии классификации угроз. Основные угрозы доступности.

- Основные угрозы целостности.
- Основные угрозы конфиденциальности.
- Источники угроз.

Продолжительность занятия – 2 ч.

Тема 2. Служба безопасности кредитно-финансовых организаций

Практическое занятие 2.

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

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки о политике безопасности отдельных структур

Учебные вопросы:

- Определение политики информационной безопасности
- Принципы политики безопасности
- Виды политики безопасности
- Политики безопасности для
- Уровни политики безопасности.

Продолжительность занятия – 2 ч.

Тема 3. Обеспечение информационной безопасности кредитно-финансовых организаций

Практическое занятие 3.

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

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки в организационно-кадровых и технических аспектах управления информационной безопасностью

Учебные вопросы:

- Основные направления обеспечения информационной безопасности. Законодательно-правовая база обеспечения информационной безопасности на предприятии.
- Нормативные акты предприятия по информационной безопасности.
- Формы правовой защиты информации на предприятии.

Продолжительность занятия – 4 ч.

Тема 4. Обеспечение безопасности персонала кредитно-финансовых организаций

Практическое занятие 4.

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

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

- Метод оценки рисков на основе модели информационных потоков.
- Расчет рисков по угрозе конфиденциальность.
- Расчет рисков по угрозе целостность.
- Методы оценивания информационных рисков.
- Табличные методы оценки рисков.
- Разделение рисков на приемлемые и неприемлемые.

Продолжительность занятия – 4 ч.

Тема 5. Обеспечение имущественной безопасности кредитно-финансовых организаций

Практическое занятие 5.

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

Тема и содержание практического занятия:

Цель работы: Получить практические знания и навыки оценки эффективности управления ИБ

Учебные вопросы:

- Метод оценки рисков на основе модели информационных потоков.
- Расчет рисков по угрозе конфиденциальность.
- Расчет рисков по угрозе целостность.
- Методы оценивания информационных рисков.
- Табличные методы оценки рисков.

Разделение рисков на приемлемые и неприемлемые.

Продолжительность занятия – 4 ч.

3. Указания по проведению лабораторных работ

Используя актуарные расчеты, выполнить задачи:

Пример:

1. Вероятность страхового случая составляет 0,02%. Каждый из 100 объектов застрахован на 500 тыс. руб. Рассчитать размер нетто-ставки?
2. Расчет единовременной тарифной ставки на дожитие по договору страхования человека в возрасте 50 лет (x=50) на срок 10 лет (t=10) со страховой суммы 100 руб. и долей нагрузки в структуре тарифа 30 % (Fr/z = 30%).

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 аппаратных средств вычислительной техники;

2) привить навыки самостоятельного решения нестандартных задач в области аппаратных средств вычислительной техники.

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	96
Вопросы, выносимые на самостоятельное изучение	36
Подготовка к практическим занятиям	16
Подготовка к лабораторным занятиям	12
Подготовка докладов	16
Выполнение практических заданий	16

Вопросы, выносимые на самостоятельное изучение:

1. Общее понятие безопасности в финансовой сфере и ее компоненты.
2. Система управления информационной безопасностью организации.
3. Служба безопасности в системе корпоративного управления и возможные подходы к ее организации.
4. Основные аспекты управления корпоративной деятельностью службы безопасности банка.
5. Функции руководителя и основных подразделений службы безопасности.
6. Конфиденциальная информация финансовой организации как объект защиты.
7. Угрозы информационной безопасности финансовой организации.
8. Обеспечение информационной безопасности финансовой организации.

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	36	Изучение открытых источников
2.	Подготовка к практическим занятиям	16	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	12	Изучение открытых источников
4.	Тематика докладов	16	1. Внутренние аппаратные средства персонального компьютера 2. Внешние периферийные устройства персонального компьютера
5.	Выполнение практических заданий	16	Разработка аппаратного средства вычислительной техники по заданным характеристикам

Примерные темы докладов

1. Персонал финансовой организации как объект потенциальных угроз.
2. Организация защиты персонала от возможных угроз.
3. Обучение персонала правилам обеспечения безопасности финансовой организации.
4. Имущество финансовой организации как объект защиты.
5. Защита от угроз с использованием сетей корпоративных компьютерных коммуникаций.
6. Защита от угроз, связанных с использованием электронных банковских карточек.
7. Защита финансовых организаций от мошенничества при получении кредита.
8. Защита финансовых организаций от угрозы хищения высоколиквидных активов.
9. Защита финансовых организаций от ограблений.

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:

1. Основы управления информационной безопасностью. Учебное пособие для вузов/ А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов. А. И. Толстой. - М.: Горячая линия - Телеком, 2012.

2. Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М.: Горячая линия - Телеком, 2012.

3. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - М.: Горячая линия - Телеком, 2012.

Дополнительная:

1.Управление рисками информационной безопасности. Учебное пособие для вузов / Н. Г. Милославская. М. 10. Сенаторов, А. И. Толстой. - М: Горячая линия-Телеком, 2012.

2. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов. А. И. Толстой. - М.: Горячая линия-Телеком, 2012.

3. Анисимов А.А. Менеджмент в сфере информационной безопасности; Учебное пособие.- М.: БИНОМ. Лаборатория знаний,2012.

Рекомендуемая:

1. Белов Е.Б. и др. Основы информационной безопасности: Учеб. пособие. – М: Горячая линия – Телеком, 2006.

2. Гринберг А.С. и др. Защита информационных ресурсов государственного управления: Учеб. пособие. – М.: ЮНИТИ-ДАНА, 2003.

3. Грушо А.А. Теоретические основы компьютерной безопасности. Учеб. пособие. – М.: ИЦ Академия, 2009.

4. Корт С.С. Теоретические основы защиты информации: Учеб. пособие. – М.: Гелиос АРВ, 2004.

5. Организационно-правовое обеспечение информационной безопасности / Под ред. А.А.Стрельцова. – М.: ИЦ Академия, 2008.

6. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы. – М: МЦНМО, 2002.

7. Шепитько Г.Е. и др. Комплексная система защиты информации на предприятии: Часть 1. Учеб. пособие. – М.: МФА, 2008.

8. Шепитько Г.Е. Экономика защиты информации: Учеб. пособие. – М.: МФЮУ, 2011.

9. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты: Учеб. пособие. – М.: Книжный мир, 2009.

10. Щульц В.П. и др. Информационное управление в условиях активного противоборства: модели и методы. – М.: Наука, 2011.

11. Шепитько Г.Е. Теория информационной безопасности и методология защиты информации. – М.: РГСУ, 2012.

12. Домарев В.В. Безопасность информационных технологий. Методоло¬гия создания систем защиты. К.: ООО "ТИД "СД", 2001.

13. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. М.: СИНТЕГ, 2000.

14. Ярочкин В.И. Информационная безопасность. М.: Международные отношения, 2008

Электронные книги:

1. Иванов М.А., Чугунов И.В. криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие/ под редакцией М.А. Иванова .М.: НИЯУ МИФИ,2012.

http://biblioclub.ru/index.php?page=book_view&book_id=231673

2. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: учебное пособие для вузов. –М. Горячая линия – Телеком,- 2-е изд., стер. 2012.

http://eknigi.org/nauka_i_ucheba/57446-kriptograficheskie-metody-zashhity-informacii.html

3. Жданов О.Н., Золотарев В.В. МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ // Успехи современного естествознания. – 2010.

www.rae.ru/use/?section=content&op=show_article&article_id=7784920

4. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.Технические средства и методы защиты информации. Учебное пособие для вузов.:-4-е издание исправленное и дополненное - –М. Горячая линия – Телеком, 2012.

http://biblioclub.ru/index.php?page=book&id=253208&sr=1

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.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

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 «Основы управления в корпорациях».