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 ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Информационно-аналитические системы финансового мониторинга
Квалификация (степень) выпускника: бакалавр
Форма обучения: очная

Королев
2020

Автор: к.т.н. Журавлев С.И. Рабочая программа дисциплины: «Основы управления информационной безопасностью». – 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 управления информационной безопасностью 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 менеджмента информационной безопасности на типовых региональных информационных объектах с учетом современных международных и отечественных стандартов.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общепрофессиональные компетенции:

- ОПК-7: способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

Профессиональные компетенции:

- ПК-4: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
- ПК-13: способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации.

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 управления информационной безопасности (СУИБ);
- современные подходы к управлению информационной безопасностью (ИБ) региональных информационных объектов и направления их развития;
- особенности отдельных процессов управления ИБ в рамках СУИБ;
- 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 СУИБ 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 СУИБ;
- анализа бизнес-активов организации, их угроз и уязвимостей в рамках области действий СУИБ;
- построения как отдельных процессов управления ИБ, так и системы процессов в целом.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Основы управления информационной безопасностью» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Основы информационной безопасности», «Математический анализ», «Финансовое моделирование», «Основы управления в корпорациях» и компетенциях: ОК-4,5,8, ОПК-2,3,4,5 и ПК-3,6,9.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Управление рисками», «Социотехносферная безопасность объектов информационной защиты», «Правовая охрана результатов интеллектуальной деятельности», «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 3 зачетные единицы, 108 часов;

Таблица1

Виды занятий	**Всего часов**	**Семестр 5**	**Семестр 6**	**Семестр 7**	**Семестр …**
Общая трудоемкость	108	108			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	60	60			
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	Зачет	Зачет			

4.Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. Очное	Практические занятия, час Очное	Занятия в интерактивной форме, час	Код компетенций
Пятый семестр				
Раздел 1. Концептуально-теоретические основы управления информационной безопасностью				
Тема 1. Базовые основы процессов и систем управления информационной безопасностью	4	8	2	ОПК-7; ПК-4,13
Тема 2. Политика информационной безопасности региона и отдельных региональных структур (объектов, процессов)	4	8	2	ОПК-7; ПК-4,13
Раздел 2. Прикладные аспекты управления информационной безопасностью				
Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью	4	8	2	ОПК-7; ПК-4,13
Тема 4. Основы оценки эффективности управления информационной безопасностью	4	8	3	ОПК-7; ПК-4,13
Итого:	**16**	**32**	**9**	

4.2. Содержание тем дисциплины

Раздел 1. Концептуально-теоретические основы управления информационной безопасностью

Тема 1. Базовые основы систем и процессов управления информационной безопасностью

Предмет и задачи курса. Значение и место курса в подготовке магистров по информационной безопасности. Взаимосвязь курса с другими дисциплинами.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения контрольных мероприятий. Формы проверки знаний. Состав и методика самостоятельной работы студентов по изучению дисциплины.

Знания и умения студентов, которые должны быть получены в результате изучения курса. Рекомендованная научная и учебная литература.

Характеристика базовой терминологии в области управления информационной безопасностью: сущность управления; управление как процесс; системный подход к управлению; процессный подход к управлению; циклическая модель улучшения процессов управления; системы управления информационной безопасностью.

Стандартизация систем и процессов управления информационной безопасностью: международные и российские стандарты; особенности стандартов банковской системы РФ.

Тема 2. Политика информационной безопасности отдельных региональных структур (объектов, процессов)

Понятие политики обеспечения информационной безопасности региона и политики информационной безопасности организаций (учреждений и предприятий). Причина выработки политики информационной безопасности. Основные требования и принципы, учитываемые при разработке и внедрении информационной безопасности. Содержание корпоративной и частных политик информационной безопасности.

Жизненный цикл политик информационной безопасности: разработка; внедрение; применение и аннулирование. Ответственность за исполнение политики информационной безопасности.

Раздел 2. Прикладные аспекты управления информационной безопасностью

Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью

Особенности организации управления информационной безопасностью региона: корпоративных структур, отдельных организаций и их информационно- телекоммуникационных технологий.

Организация реагирования на чрезвычайные ситуации (инциденты). Управления информационными рисками. Аудит (мониторинг)

состояния информационной безопасности региона. Стратегии построения и внедрения управленческих процессов и систем управления информационной безопасностью в целом.

Система управления информационной безопасностью: область действия; документальное обеспечение; политика системы управления и поддержка системы управления со стороны руководства. Основы кадрового обеспечения управления информационной безопасностью. Департамент информационной безопасности региона.

Технические аспекты управления информационной безопасностью. Администрирование информационных систем управления информационной безопасностью. Защита систем управления информационной безопасностью региона.

Страхование информационных рисков: основы методологии и рынок страховых услуг. Методические основы экономики информационной безопасности

Тема 4. Основы оценки эффективности управления информационной безопасностью

Нормативное обеспечение проверки и оценки деятельности по управлению информационной безопасностью: международные и российские стандарты.

Характеристики типовых процессов проверки систем управления информационной безопасности: виды проверок, мониторинг, самооценка, внутренний и внешний аудит, инструментальные средства.

Практическая оценка деятельности по управлению информационной безопасности: результативность (эффективность), метрики и измерения, модели зрелости процессов систем управления информационной безопасностью.

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 «Основы управления информационной безопасностью» 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 управления информационной безопасностью»

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 ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

(Приложение 1 к рабочей программе)

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

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

№ п/п	Индекс компе-тенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Тема:1,4	типовые шифры с открытыми ключами	основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры	навыками применения терминологии и процессорным подходом построения СУИБ
2.	ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	Тема:1,2,3	требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры;	основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры	навыками применения терминологии и процессорным подходом построения СУИБ
3.	ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Тема:3,7	научные и организационные основы защиты окружающей среды и ликвидации последствий аварий, катастроф, стихийных бедствий	основные задачи и понятия криптографии; требования к шифрам и основные характеристики шифров; типовые поточные и блочные шифры	навыками безопасного использования технических средств в профессиональной деятельности

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

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК-7	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-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.
ПК-13	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.

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 форме презентации:

1. Ведущие мировые разведки и их деятельность в России.

2. Основы обеспечения безопасности информации в компьютерных системах.
3. Информационная безопасность современной России: угрозы и их отражения.
4. Информационные войны в современном мире.
2. Компьютерная преступность в экономических областях.
3. Мир XXI века: информационное противоборство.
4. Компьютерные вирусы в современных информационных системах.
5. Информационные угрозы современным экономическим объектам.
6. Информатизация России и проблема защиты информации.
7. Безопасность информации в коммерческой деятельности.
8. Разведки России – исторический аспект.
9. Мировой информационный терроризм.
10. Этика защиты информации.
11. Становление и развитие промышленного шпионажа.

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

Формой контроля знаний по дисциплине «Основы управления информационной безопасностью» 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	ОПК-7 ПК-4 ПК-13	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	ОПК-7 ПК-4 ПК-13	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	Зачет	ОПК-7 ПК-4 ПК-13	3 вопроса	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета	Критерии оценки: **«Зачтено»:** – 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. **«Не зачтено»:** – 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. 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 зачет

1. Процессный подход к построению СУИБ и циклическая модель PDCA.
2. Цели и задачи, решаемые СУИБ.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Стратегии выбора области деятельности СУИБ.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.

7. Политика ИБ и политика СУИБ: сходства и различия.
8. Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Обучение и обеспечение осведомленности пользователей: цели и задачи процесса, роль процесса в рамках СУИБ.
16. Внедрение процессов управления ИБ: этапы и последовательность. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения
17. Правовые аспекты построения СУИБ организации.

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 ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

(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:

- Дать студентам концептуальные знания основ управления информационной безопасностью для региональных информационных объектов с учетом современных требований теории по защите информации;
- Выработать и закрепить у студентов базовые умения и навыки по практической организации и реализации современных технологий менеджмента информационной безопасности на 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

Раздел 1. Концептуально-теоретические основы управления информационной безопасностью

Тема 1. Базовые основы систем и процессов управления информационной безопасностью

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 – 8 ч.

Тема 2. Политика информационной безопасности отдельных структур (объектов, процессов)

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 – 8 ч.

Раздел 2. Прикладные аспекты управления информационной безопасностью

Тема 3. Организационно-кадровые и технические аспекты управления информационной безопасностью

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 – 8 ч.

Тема 4. Основы оценки эффективности управления информационной безопасностью

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 – 8 ч.

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	60
Вопросы, выносимые на самостоятельное изучение	24
Подготовка к практическим занятиям	12
Подготовка к лабораторным занятиям	-
Подготовка докладов	12
Выполнение практических заданий	12

Вопросы, выносимые на самостоятельное изучение:
для очной формы обучения:

1 Место информационной безопасности в системе национальной безопасности.

2. Современная концепция информационной безопасности.

3. Цели и концептуальные основы защиты информации.

4. Критерии, условия и принципы отнесения информации к защищаемой.

5. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.

6. Понятие и структура угроз защищаемой информации.

7. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.

8. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.

9. Виды уязвимости информации и формы ее проявления.

10. Каналы и методы несанкционированного доступа к конфиденциальной информации.

11. Модель нарушителя.

12. Модель угроз.

13. Критерии оценки безопасности информационных технологий.

14. Методы защиты информации от несанкционированного доступа.

15. Риски информационной безопасности.

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	24	Изучение открытых источников
2.	Подготовка к практическим занятиям	12	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	-	
4.	Тематика докладов	12	1. Внутренние аппаратные средства персонального компьютера 2. Внешние периферийные устройства персонального компьютера
5.	Выполнение практических	12	Разработка аппаратного средства

	заданий		вычислительной техники по заданным характеристикам

Примерные темы докладов

1. Вредоносные программы и антивирусные программные средства.
2. Методы программно-аппаратной защиты информации.
3. Аттестация объектов информатизации. 19. Виды защиты информации.
4. Системы защиты информации.
5. Модели разграничения доступа.
6. Криптографические стандарты и их использование в информационных системах.
7. Способы и средства защиты информации от утечки по техническим каналам.
8. Принципы организации информационных систем в соответствии с требованиями по защите информации.
9. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
10. Отечественные и зарубежные стандарты в области компьютерной безопасности.
11. Принципы и методы организационной защиты информации.
12. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях.
13. Лицензирование и сертификация в области защиты информации.
14. Комплексные системы защиты информации.

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 информационной безопасностью».