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

«БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

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 Воронов А.Н. Рабочая программа дисциплины: «Безопасность информационных технологий». – 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. Формирование у обучаемых специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, использовании организационно-правовых механизмов обеспечения конституционных прав и свобод граждан в информационной сфере, регламентирующих создание и использование средств защиты информации;

2. 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:

Общепрофессиональные компетенции:

- ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации;
- 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-2: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;
- ПК-8: способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов;
- ПК-15: способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Основными **задачами** дисциплины являются:

- ознакомление обучаемых с процессами анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества, разработка планов и программ проведения научных исследований и технических проектов, подготовка отдельных заданий для исполнителей и выполнение научных исследований по выбранной теме;
- формирование у обучаемых способности самостоятельно организовывать работу коллектива исполнителей, принятию управленческих решений в условиях спектра мнений, определению порядка выполнения работ;
- участие в работах по созданию, изготовлению, монтажу, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности, разработке проектов методических и нормативных документов, предложений и мероприятий по реализации разработанных проектов и программ;
- формирование обучаемыми предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

После завершения освоения данной дисциплины студент должен:

Знать:

- предполагаемые источники угроз информационной безопасности региона и порядок их выявления;
- возможные каналы утечки информации и предполагаемые информационные атаки на охраняемых объектах региона;
- методы и средства защиты информационных объектов, основные мероприятия по управлению информационной безопасностью в регионе;
- основные принципы организации технического, программного и информационного обеспечения защищенных информационных технологий региона;
- методы концептуального проектирования технологий обеспечения информационной безопасности региона;
- основные направления совершенствования безопасности объектов региона с помощью средств защиты;

Уметь:

- осуществлять классификацию охраняемых объектов, средств защиты и требований к системе информационной безопасности региона;
- проводить анализ защищённости объектов региона и определять классы защиты информации;
- использовать гипотетические модели защиты информации при выборе соответствующих способов и средств информационной безопасности региона;

- осуществлять выбор функциональной структуры системы обеспечения информационной безопасности региона;
- обосновывать принципы организации технического, программного и информационного обеспечения информационной безопасности региона;
- организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности региона;

Владеть навыками:

- выявления и анализа потенциально существующих угроз безопасности информации и охраняемым объектам региона;
- применения основных методов анализа и оценки рисков, методов определения размеров возможного ущерба защищаемым объектам региона;
- грамотного применения на практике основных методов и средств защищённых информационных технологий в регионе;
- применения методик организации и управления системой информационной безопасности в регионе.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Безопасность информационных технологий» относится к обязательным дисциплинам вариативной 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: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Системный анализ в области информационной безопасности», «Финансовое моделирование» и компетенциях: ОК-4,5,8, ОПК-2,3,4,5 и ПК-2,3,6,8,10,15.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Информационная безопасность кредитно-финансовых операций», «Защищенные электронные технологии банка», «Финансовые институты», «Основы расследования нарушений в финансовой сфере», 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 7**	**Семестр …**	**Семестр …**
Общая трудоемкость	108	108			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32	32			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	76	76			
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 с оценкой	Зачет с оценкой			

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
Тема 1. Информационные технологии предприятий, фирм как объекты информационной безопасности.	2	2	1	ОПК-4,7; ПК-2
Тема 2. Нормативно-правовые основы защиты	2	2	2	ОПК-4,7; ПК-2,

информационных технологий предприятий, фирм.				
Тема 3. Защищённые информационные технологии в государственном и муниципальном управлении.	4	4	2	ОПК-4,7; ПК-2,8
Тема 4. Защищённые информационные технологии в управлении коммерческими структурами.	4	4	2	ОПК-4,7; ПК-2,8,15
Тема 5. Организационно-технические методы защиты информационных технологий	4	4	2	ОПК-4,7; ПК-2,8,15
Итого	16	16	9	

4.2. Содержание тем дисциплины

Тема 1. Информационные технологии предприятий, фирм как объекты информационной безопасности.

Информационные технологии стратегического менеджмента на предприятии. Реализация задач стратегического менеджмента с использованием специализированных компьютерных систем экономического и финансового моделирования. Информационные технологии решения задач финансового менеджмента и их основные процедуры. Основные принципы построения информационных систем управления персоналом в условиях корпоративных организаций. Информационные технологии по использованию трудовых ресурсов и рабочего времени в корпоративных организациях.

Тема 2. Нормативно-правовые основы защиты информационных технологий предприятий, фирм.

Реализация теоретических и организационных принципов создания и функционирования информационных технологий в органах

государственного и муниципального управления. Информационно-вычислительные и ситуационные центры, их роль в государственном и муниципальном управлении. Информационное и технологическое обеспечение решения функциональных задач муниципального управления. Организация государственных информационных ресурсов России.

Тема 3. Защищённые информационные технологии в государственном и муниципальном управлении.

Необходимость обеспечения безопасности информационных технологий. Виды угроз безопасности информационных технологий и их характеристика. Формы атак на объекты информационных систем предприятия. Основные методы и средства защиты информации. Оценка безопасности информационных технологий, анализ угроз и каналов утечки информации. Анализ рисков и управление ими при использовании защищённых информационных технологий. Характеристика основных методов и средств построения систем информационной безопасности предприятия. Особенности защиты информации в корпоративных сетях.

Тема 4. Защищённые информационные технологии в управлении коммерческими структурами

Организационные способы противодействия телефонному пиратству. Ограничение доступа к телефонным линиям связи. Основные рекомендации абонентам в случае обнаружения самовольного подключения. Характеристика современных пассивных устройств технического противодействия телефонному пиратству. Специализированные анализаторы телефонных линий связи. Краткий обзор зарубежных приборов для контроля состояния телефонных линий. Особенности активных устройств технического противодействия телефонному пиратству. Критерии оценки систем закрытия речи. Основные тенденции развития систем закрытия речи. Характеристика современных методов противодействия утечке компьютерной и аудио видеоинформации.

Тема 5. Организационно-технические методы защиты информационных технологий

Решение задач безопасности речевой связи с помощью компьютерных информационных технологий. Представление речевых сигналов в виде графических образов. Компьютерные технологии безопасности связи на основе цифровой обработки изображений сонограмм. Технологии обеспечения безопасности на основе индивидуальных особенностей человека. Характеристика современных методов биометрической идентификации личности. Стеганографическая защита информации цифровыми водяными знаками. Характеристика современных систем цифровых водяных знаков. Обзор основных атак на системы цифровых водяных знаков.

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 «Безопасность информационных технологий» приведена в Приложении 1.

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

Основная литература:

1. Анисимов А.А. Менеджмент в сфере информационной безопасности. Учебное пособие. – М.: Интернет – Университет информационных технологий / БИНОМ. Лаборатория знаний, 2010.
2. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность. Учебное пособие. – М.: «ФОРУМ», 2011.
3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебное пособие для вузов. - М.: «Горячая линия – Телеком», 2012.

Дополнительная литература:

1. Ворона В.А., Тихонов В.А. Технические средства наблюдения в охране объектов. – М.: «Горячая Линия - Телеком», 2011.
2. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: «Горячая Линия - Телеком», 2010.
3. Титоренко Г. А. Информационные технологии управления. Учебное пособие. М.: Юнити-Дана, 2010.

Рекомендуемая литература:

1. Киселёв Г. М., Бочкова Р. В., Сафонов В. И. Информационные технологии в экономике и управлении. Учебное пособие. М.: Издательско-торговая корпорация «Дашков и К°», 2012.
2. Петраков А. В. Защитные информационные технологии аудиовидеоэлектросвязи. Учебное пособие. М.: Энергоатомиздат, 2010.
3. Тарасюк М. В. Защищённые информационные технологии. Проектирование и применение. Учебное пособие. М.: «Слон-пресс», 2004.
4. Ивасенко А. Г., Гридасов А. Ю., Павленко В. А. Информационные технологии в экономике и управлении. Учебное пособие. М.: КноРус, 2010.

Электронные книги:

1. 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

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.
2. Рабочая программа и методическое обеспечение по дисциплине: «Безопасность информационных технологий»

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

«ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

(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-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Тема:1,3,4	основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; характеристику основных отраслей российского права; правовые основы обеспечения национальной безопасности Российской Федерации	анализировать и составлять правовые акты и осуществлять правовую оценку информации, используемой в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
2.	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:1,2,4,5	основные методы управления информационной безопасностью; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах		
4.	ПК-2	способность применять программные средства	Тема:1,2,3,4,5	основы организационного и правового	реализовывать основные структуры данных и	навыками разработки технической документации в

		системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач		обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации;	базовые алгоритмы средствами языков программирования;	соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации
5.	ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Тема:3,4,5	основные угрозы безопасности информации и модели нарушителя в автоматизированных системах принципы формирования политики информационной безопасности в автоматизированных системах		навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации;
6.	ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Тема:4,5	основы организационного и правового обеспечения информационной безопасности, основные положения законодательства Российской Федерации в области защиты информации;	реализовывать основные структуры данных и базовые алгоритмы средствами языков программирования;	навыками разработки технической документации в соответствии с требованиями Единой системы конструкторской документации и Единой системы программной документации

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-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.
ОПК-7	Реферат	А) полностью сформирована – 5 баллов Б) частично сформирована – 3-4 балла В) не сформирована- менее 2 и менее баллов	Проводится в письменной форме Критерии оценки: 1.Соответствие содержания реферата заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке работы (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной работы (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в

			срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-2	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-8	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-15	Контрольная работа	А) полностью сформирована 5 баллов В) частично сформирована 3-4 балла С) не сформирована 2 балла	1. Проводится в форме письменной работы 2.Время, отведенное на процедуру – 90 мин. Неявка – 0. Критерии оценки: 1.Соответствие ответа уровню формирования компетенции (0-5 баллов). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – 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 / рефератов:

1. Характеристика защищённых технологий систем кабельного телевидения, понятие телеохраны в современном мире.
2. Основы защищённых технологий при обеспечении безопасности персонала и пользователей почтовой связи.
3. Защищённые технологии и особенности их применения в системах наблюдения дальнего действия.
4. Защищённые технологии читающих автоматов и особенности их использования в системе безопасности предприятий, фирм.
5. Характеристика современных технологий охраны объектов и основные направления их развития.
6. Основные проблемы применения защищённой технологии «речевая подпись» и пути их решения в современном мире.

7. Средства обнаружения и системы охранной сигнализации, применяемые в рамках защищённых информационных технологий предприятий и фирм.
8. Характеристика основных устройств противодействия съёму информации в муниципальных защищаемых помещениях.
9. Особенности применения защитных технологий читающе-опознающих автоматов в невидимых диапазонах электромагнитного спектра телевидения.
10. Защищённые технологии в системе обеспечения безопасности коммерческих объектов.
11. Новые возможности использования технологий стеганографии в системах цифрового телевидения.
12. Методы охраны и защиты конфиденциально ориентированного предприятия на основе применения нейро-сетевых технологий обработки информации.
13. Современные подходы в развитии биометрических технологий защиты и перспективы их развития.
14. Идентификация пользователей вычислительных систем на основе современных речевых технологий и методов искусственного интеллекта.

Примерная тематика заданий на контрольную работу:

1. Активные способы противодействия прослушиванию помещений по абонентским линиям связи.
2. Характеристика основных способов защиты абонентских телефонных линий связи от бесконтактного съёма информации.
3. Характеристика способов съёма акустической информации со стен и потолочных перекрытий охраняемых муниципальных объектов.
4. Характеристика способов съёма акустической информации с металлических труб и оконных стёкол охраняемых муниципальных объектов.
5. Характеристика способов съёма акустической информации в помещении по линии электросети охраняемых муниципальных объектов.
6. Характеристика пассивных способов противодействия прослушивания охраняемых помещений по абонентской линии связи.
7. Методика применения телефонолокационного способа съёма акустических сигналов в муниципальных защищаемых помещениях.
8. Характеристика основных устройств противодействия съёму информации в муниципальных защищаемых помещениях.
9. Основные компоненты охранной сигнализации при использовании различных датчиков.
10. Характеристика современных телевизионных средств охранной сигнализации.
11. Характеристика сетевых пассивных помехоподавляющих фильтров низких и высоких частот.
12. Методика обнаружения сигналов линейных сетевых закладок и особенности её применения.
13. Методика обнаружения оптических сигналов передатчиков ИК диапазона и

особенности её применения.

14. Методика обнаружения активных прослушивающих устройств с помощью индикатора электромагнитного поля.

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

Формой контроля знаний по дисциплине «Безопасность информационных технологий» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета с оценкой.

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-4 ОПК-7 ПК-2 ПК-8 ПК-15	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-4 ОПК-7 ПК-2 ПК-8 ПК-15	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 с оценкой	ОПК-4 ОПК-7 ПК-2 ПК-8 ПК-15	3 вопроса	Зачет с оценкой проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения зачета с оценкой	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 или несколько вариантов ответа.

1-е тестирование по дисциплине

1. Выберите устройства, входящие в систему сигнализации охраняемых объектов:

– устройство, обнаруживающее опасность;
– устройство, передающее сигнал к месту регистрации;
– устройство, размножения сигнала;
– устройство, регистрирующее сигнал;

2. На какие группы делятся извещатели по назначению?

– объектовые;
– точечные;
– линейные;
– периметровые.

3. Какие компоненты входят в устройство типового извещателя?

– передатчик (излучатель);
– приёмник;
– приёмо-контрольный прибор;
– блок обработки;

4. Выберите правильные критерии, по которым классифицируют извещатели:

– по принципу действия;
– по уровню маскировки;
– по важности;
– по степени конструктивной законченности.

5. Электро-магнитомеханические приборы относятся к одному из типов извещателей?

– да;
– нет;

6. Выберите приемлемые характеристики извещателей:

– адресность подключения;
– тактика применения;
– эффективность работы;
– дизайн исполнения;

7. Приёмо-контрольный прибор входит в систему сигнализации охраняемого объекта?

– да;
– нет;

8. Выберите основные показатели, от которых будет зависеть эффективность работы извещателей?

– вероятность обнаружения тревожной ситуации;
– частота ложных тревог;
– инерционность шлейфа;
– уязвимость к преодолению.

9. Коэффициент Стьюдента учитывается в формуле по расчёту вероятности обнаружения нарушителя отечественными разработчиками извещателей?

– да;
– нет;

10. Что понимается под когерентным источником излучений?

– это источники, формирующие волны с одинаковой частотой и фазой волны;
– это источники, формирующие колебания с разными частотами и разными фазами;
– это источники, формирующие волны с разными частотами и одинаковой фазой;
– это источники, формирующие колебания с одинаковой частотой и с постоянной по времени разностью фаз.

11. Что понимается под волновым фронтом?

– это отображение геометрического места точек, в которых совершаются колебания с одинаковой фазой;
– это отображение геометрического места точек, в которых совершаются колебания с одинаковой частотой;
– это отображение геометрического места точек, в которых совершаются колебания с одинаковой разностью фаз;
– это отображение геометрического места точек, в которых совершаются колебания с разной фазой и одинаковой частотой;

12. Что такое интерференция волн?

– это процесс огибания волнами предметов, размеры которых соизмеримы с длинной волны;
– это наложение волн от когерентных источников друг на друга;
– это отклонение распространения волн от прямой линии при прохождении их вблизи препятствий;

– это процесс затухания волн при их распространении в пространстве.

13. Как делятся радиоволновые извещатели в зависимости от контролируемого параметра электромагнитного поля и особенностей распространения электромагнитных волн?

– амплитудно-модуляционные;

– контактно-электризуемые;

– частотно-модуляционные;

– проводно-локационные.

14. Проводно-локационные извещатели относятся к типу амплитудно-модуляционных радиоволновых извещателей?

– да;

– нет.

15. В каких пределах измеряется длина волны для СВЧ - излучения?

– от 10 м. до 1 м;

– от 1 м. до 10 см;

– от 10 см. до 1 мм;

– менее 1 мм.

16. Выберите типы антенн, которые используются для передачи информации от извещателей?

– квадратурная;

– волноводно-щелевая;

– параболическая;

– рупорная.

17. Какой максимальный объём охраняемого пространства для одного приёмо-передающего тракта обеспечивает радиоволновой амплитудно-модуляционный объёмный извещатель «Конус»?

– 1000 $м^3$;

– 5000 $м^3$;

– 100 $м^3$;

– 50 $м^3$;

18. Из чего состоит чувствительный элемент радиоволнового амплитудно-модуляционного извещателя на принципе «вытекающей волны»?

– из трёх коаксиальных кабелей в экранированном слое с отверстиями;

– из одного специального коаксиального трибоэлектрического кабеля;

– из двух параллельно расположенных коаксиальных кабелей с перфорацией в экранированном слое;

– из двух параллельно расположенных одномодовых оптоволоконных кабелей.

19. Какую максимальную длину зоны обзора обеспечивает амплитуд- но-модуляционный проводно-радиоволновой извещатель типа «Газон»?

– 10 м;
– 50 м;
– 100 м;
– 150 м.

20. Скорость света используется в расчёте частоты отражённого сигнала от движущегося объекта на основе эффекта Доплера?

– да;
– нет;

21. Какие виды чувствительных элементов применяют в оптико-электронных извещателях?

– фотодиод;
– фотоконденсатор;
– фоторезистор;
– фототранзистор.

22. На основе каких элементов строится оптическая система оптико-электронного пассивного однопозиционного извещателя?

– на основе многосегментного зеркала;
– на основе многосегментированной линзы;
– на основе КМОП-матрицы;
– на основе линзы Френеля;

23. От каких величин зависит расчёт ёмкости в распределённой антенной системе ёмкостных извещателей?

– от заряда, накопленного проводником;
– от силы магнитного потока;
– от интервала времени;
– от приложенного напряжения.

24. Какие разновидности магнитометрических средств обнаружения применяют в системах сигнализации?

– с исползованием эффекта переизлучения сигнала;
– с использованием эффекта биения частоты;
– с использованием эффекта локального искажения магнитного поля Земли;
– с использованием трибоэлектрического эффекта.

25. На каких частотах располагаются акустические волны инфразвукового диапазона?

– до 16 Гц;
– от 16 Гц до 20 КГц;
– от 20 КГц до 10^{13} Гц;
– свыше 10^{13} Гц;

26. Инфразвуковые (барометрические) извещатели типа «Сирена» являются активными извещателями?

– да;
– нет.

27. Какие способы обработки звуковых сигналов используются в звуковых извещателях?

– технология “Time of Arrival Zone Processing”;
– технология Интервьюирования;
– алгоритм «анализа формы волны»;
– технология «КРАО».

28. Какие разновидности вибрационных извещателей применяют в системах сигнализации?

– пьезоэлектрические;
– барометрические;
– тензорезисторные;
– манометрические.

29. Какие материалы используются для монокристаллов в пьезоэлектрических извещателях?

– кварц;
– турмалин;
– сегнетовая соль;
– графит.

30. Какие физические процессы лежат в основе работы чувствительных элементов контактно-электризуемых извещателей?

– пьезоэффект;
– трибоэлектрический эффект;
– прецезионный эффект;
– контактная электризация;

2-е тестирование по дисциплине

1. Какие методы регистрации сигнала применяют в оптоволоконных извещателях?

– метод импульсной рефлектометрии;
– метод межмодовой интерференции;
– метод изменения интенсивности излучения;
– метод двухлучевой интерферометрии.

2. Схема «последовательного И» используется для обработки тревожных сообщений в комбинированных извещателях?

– да;
– нет;

3. Существуют ли радиолучевые виды средств сбора и обработки информации (ССОИ)?

– да;
– нет.

4. Выберите параметры, которыми характеризуют применение средств сбора и обработки информации (ССОИ)?

– инерционность шлейфа;
– асферика;
– нагрузочное сопротивление;
– функциональность.

5. Зона физического сдерживания входит в функциональные зоны охраны периметровой системы объектов?

– да;
– нет;

6. Какое максимальное время установки элементов охраны на местности позволяет отнести оборудование к быстроразвёртываемым охранным системам?

– не более 1 часа;
– не более 1,5 часов;
– не более 2 часов;
– не более 3,5 часов.

7. Выберите системы охраны зарубежного производства, которые можно отнести к быстроразвёртываемым?

– “TASS”;
– “MIDS”;
– “DEFENSOR”;
– “CLASSIC”.

8. Выберите основные компоненты, входящие в состав быстроразвёртываемой системы охраны “IREMBASS” (США)?

– комплекс датчиков;
– монитор - программатор;
– лёгкий радиотранслятор;
– поточный шифратор.

9. Что такое геофон?

– устройство для охраны объектов на основе пьезоэлектрического эффекта;
– устройство, обеспечивающее распознавание вторжения людей и транспорта на основе вибрационных и магнитных принципов;
– устройство для обнаружения нарушителей с помощью шланга из износостойкого материала, заполненного низкозамерзающей жидкостью или газом;
– устройство, для обнаружения нарушителя на основе принципа импульсной рефлектометрии.

10. Выберите быстроразвёртываемые системы охраны отечественного производства?

– «Витим»;
– «Мобиль-РЛД»;
– «Гюрза»;

– «Дрозд».

11. Выберите основные компоненты системы защиты персонального компьютера “HardLock”?

– электронный ключ;

– криптокарта;

– стриммер;

– специализированное программное обеспечение.

12. Электронный замок «Соболь» может применяться для автоматического уничтожения информации при попытке НСД?

– да;

– нет.

13. Выберите основные компоненты, входящие в считыватель “Parsec”?

– генератор;

– микропроцессор;

– антенна и контроллер;

– фотоэлемент.

14. Генерация ключей шифрования самим пользователем предусмотрена при использовании устройства “Secret Disk”?

– да;

– нет;

15. Какие средства разграничения доступа к информации используются в программно-аппаратном комплексе «Аккорд»?

– подсистема обнаружения нарушителя;

– подсистема управления доступом;

– подсистема регистрации и учёта;

– подсистема обеспечения целостности информации”.

16. Для чего предназначен кейс «Тень»?

– для криптографической защиты информации на электронных носителях;

– для транспортировки накопителей информации под охраной с возможностью автоматического уничтожения информации;

– для быстрого уничтожения информации на жёстких магнитных дисках;

– для записи аудиосигналов при ведении переговоров.

17. На какой длине волны работает инфракрасный извещатель комплекса «СПЭК-75»?

– 0,1 – 0,5 мкм;

– 0,8 – 0,9 мкм;

– 1 – 1,5 мкм;

– 8 – 9 мкм.

18. Выберите основные технологии, которые применяют для защиты инфракрасных систем защиты территории?

– технология антимаскинга;

– применение контактного датчика вскрытия;
– технология «КРАО»;
– использование специальных линз с зоной нечувствительности.

19. Для чего используют прецезионную оптику в инфракрасных системах?

– обеспечивает распознавание движения нарушителя;
– обеспечивает антибликовый режим работы объектива извещателя;
– обеспечивает цифровую обработку сигнала с помощью матрицы;
– обеспечивает равномерную чувствительность по всей диаграмме направленности излучателя.

20. Выберите формы зоны обнаружения, использующиеся в инфракрасных датчиках «Фотон»:

– объёмная трёхярусная зона;
– волновой фронт;
– сплошной занавес;
– лучевой барьер.

21. Отечественная ёмкостная система защиты территорий «Радиан-М» имеет грозозащиту?

– да;
– нет;

22. По каким характеристикам оценивается принятый сигнал в зарубежной ёмкостной охранной системе “E-Field” (США)?

– амплитуда сигнала;
– скорость изменения сигнала;
– продолжительность возмущения;
– частота сигнала.

23. Выберите современные периметровые отечественные охранные системы вибрационного типа:

– «Алмаз»
– «Арал»;
– «Дельфин-М»;
– «Дрозд».

24. Что такое майлара?

– гибкий магнитный полимер;
– изолирующий слой в кабельном проводнике;
– трубка с селиконовой смазкой;
– матрица с чувствительными элементами.

25. Сейсмомагнитометрическая система обнаружения «Дуплет» использует в своём составе геофоны?

– да;
– нет.

26. Выберите типы объективов и насадок, которыми оборудуются средства для скрытой фото- и видеосъёмки:

– миниатюрные;

– телескопические;
– стереофоническими;
– камуфляжными.

27. На каком принципе основывается работа классических приборов ночного видения?

– на основе использования микроканальной пластины с большим числом микроскопических каналов наблюдения;
– на основе усиления вторичной эмиссии электронов испускаемых катодом прибора;
– на основе применения фокальных матриц для наблюдения объектов;
– на преобразовании инфракрасного излучения, создаваемого на наблюдаемом объекте и естественного излучения фона в видимый свет.

28. В каком диапазоне волн работают современные тепловизоры?

– от 1 до 3 мкм;
– от 3 до 14 мкм;
– от 15 до 24 мкм;
– свыше 25 мкм.

29. Для чего предназначен монокуляр «Алмаз»?

– для лазерной телевизионной подсветки объектов наблюдения;
– для борьбы со скрытыми миникамерами всех видов и типов в помещениях;
– для маскирования видеоизображения при передаче его по проводным или радиоканалам;
– для наблюдения за теплоизлучающими объектами в условиях малой освещённости.

30. Выберите современные приборы ночного видения, применяемые для наблюдения на охраняемых объектах:

– «Дельфин-М»;
– «Ворон-3»;
– «Скорпион-2000»;
– «Дедал-200».

4.2. Типовые вопросы, выносимые на зачет с оценкой

1. Программное обеспечение финансовых решений на предприятиях в фирмах.
2. Информационные технологии решения задач финансового менеджмента и информационной безопасности на предприятиях.
3. Характеристика основных элементов управляющей подсистемы финансового менеджмента.
4. Комплекс задач моделирования и прогнозирования деятельности предприятий и их особенности, виды информации, использующиеся, при решении этих задач.
5. Классификация программных средств финансового менеджмента, какие

средства используются для решения задач фундаментального анализа деятельности предприятий?
6. Общие черты комплексных систем автоматизации управления финансово-хозяйственной деятельностью предприятий, как объектов информационной безопасности.
7. Особенности задач по оценке инвестиционных проектов и основные этапы их решения при комплексном анализе (диагностике) финансовой составляющей на предприятиях в фирмах.
8. Основные особенности программных продуктов «Project Expert» и «Альт-Инвест» для решения задач финансового анализа и прогнозирования.
9. Общие черты пакетов прикладных программ, применяемых для технического анализа деятельности предприятий, фирм и их характеристика.
10. Основные особенности программных продуктов, применяемых для статистического и математического анализа деятельности предприятий и их характеристика.
11. Технологии искусственного интеллекта, применяемые для решения задач финансового менеджмента, их классификация и характеристика, в чём отличие интеллектуальных систем от обычных программных продуктов.
12. Основная суть, особенности применения, достоинства и недостатки нейронных сетей для решения задач финансового менеджмента предприятий.
13. Основная суть, особенности применения, достоинства и недостатки генетических алгоритмов при решении задач финансового менеджмента предприятий.
14. Основная суть, особенности применения, достоинства и недостатки технологии нечёткой логики для решения задач финансового менеджмента предприятий.
15. Основная суть, особенности применения, достоинства и недостатки экспертных систем при решении задач финансового менеджмента предприятий.
16. Общие технологические принципы решения задач управления персоналом в корпоративных организациях и фирмах, суть кадровой политики государства и предприятия.

17. Основные подсистемы автоматизированной информационной системы управления персоналом, как объекта информационной безопасности и их характеристика.
18. Основные направления анализа информации в области управления персоналом, принципы построения информационных систем в корпоративных организациях.
19. Правовое обеспечение информационной поддержки принимаемых решений и обеспечения безопасности информационных систем (технологий) в нашем государстве.
20. Информационно-вычислительные и ситуационные центры в государственном и муниципальном управлении, как объекты информационной безопасности.

21. Информационные технологии решения функциональных задач в муниципальном управлении.
22. Государственные информационные ресурсы России, как объекты информационной безопасности и их характеристика.
23. Информационные ресурсы федеральных и муниципальных органов власти, как объекты защиты информации.
24. Информационные ресурсы и технологии в сфере финансов и внешнеэкономической деятельности страны.
25. Информационные ресурсы отраслей материального производства, государственной системы статистики и социальной сферы, их особенности.
26. Понятие информационной безопасности государства и предприятия, её составные части и направления.
27. Основные виды угроз безопасности информационных систем и технологий, их характеристика.
28. Основные формы атак на объекты информационных систем предприятий, фирм и их особенности.
29. Анализ основных угроз и каналов утечки информации на предприятиях в фирмах, их особенности проявления.
30. Характеристика современных методов и средств защиты информационных технологий на предприятиях в фирмах.
31. Основные методы и средства построения систем информационной безопасности предприятий, характеристика их структурных элементов.
32. Защита информации в корпоративных сетях управления.
33. Анализ возможных рисков деятельности предприятий с использованием информационных технологий и методология управления рисками.
34. Особенности стратегии защиты информации с использованием системного подхода, комплексных решений и принципа интеграции в защищённых информационных технологиях.
35. Организационные способы противодействия телефонному пиратству на предприятиях в фирмах.
36. Ограничение доступа к телефонным линиям связи и основные рекомендации абонентам в случае обнаружения самовольного подключения.
37. Характеристика современных пассивных устройств технического противодействия телефонному пиратству.
38. Специализированные анализаторы телефонных линий связи и их характеристика.
39. Обзор характеристик основных зарубежных приборов для контроля состояния телефонных линий.
40. Особенности активных устройств технического противодействия телефонному пиратству.
41. Основные критерии оценки систем закрытия речи и передовые тенденции развития этих систем.
42. Характеристика современных методов противодействия утечке компьютерной и аудиовидеоинформации.
43. Особенности современных сканирующих приёмников и индикаторов поля.

44. Характеристики и примеры многофункциональных поисковых систем и устройств защиты.
45. Основные характеристики и примеры выжигателей закладных устройств, обнаружителей и подавителей диктофонов, других высокочастотных электронных устройств.
46. Характеристики и примеры современных систем виброакустического зашумления помещений и сетей.
47. Организация защиты объектов от встроенных и узконаправленных микрофонов.
48. Организация защиты объектов от лазерных прослушивающих устройств.
49. Характеристика и особенности современных нелинейных радиолокаторов.
50. Решение задач безопасности речевой связи с помощью компьютерных информационных технологий.
51. Особенности представления речевых сигналов в виде графических образов.
52. Компьютерные технологии безопасности связи на основе цифровой обработки изображений сонограмм.
53. Технологии обеспечения безопасности на предприятиях в фирмах на основе индивидуальных особенностей человека.
54. Характеристика современных методов биометрической идентификации личности и их особенности.
55. Представление речевого сигнала сообщения в виде графических образов.
56. Реализация способов аудиомаркирования с помощью компьютерных технологий.
57. Основные рекомендации по практическому применению технологии «речевая подпись».
58. Стеганографическая защита информации цифровыми водяными знаками, история её появления и основные принципы применения.
59. Характеристика современных систем цифровых водяных знаков и их особенности использования.
60. Характеристика основных типов атак на системы цифровых водяных знаков и особенности их применения.
61. Особенности применения криптотехнологий в цифровом телевидении для защиты интеллектуальной собственности.
62. Основные рекомендации по практическому применению стеганографических технологий в цифровом телевидении.
63. Основные технологии маркирования и защиты интеллектуальной собственности в России.

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

(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 фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, в использовании организационно-правовых механизмов обеспечения конституционных прав и свобод граждан в информационной сфере, регламентирующих создание и применение защищённых информационных технологий, а также получение первичных навыков в применении защищённых технологий при обеспечении информационной безопасности различных объектов.

Задачи дисциплины:

- Теоретические основы подготовки студентов в области защиты информационных технологий;
- Формирование подходов к выполнению самостоятельных исследований студентами в области защиты информационных технологий и систем.

2. Указания по проведению практических занятий

Тема 1. Информационные технологии предприятий, фирм как объекты информационной безопасности.

Практическое занятие 1.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по защите информационных ресурсов и технологий предприятий, фирм и различных организаций.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Информационные ресурсы библиотечной сети России.
2. Ресурсы государственной системы экономической и научно-технической информации.
3. Российские ресурсы правовой информации.
4. Информационные ресурсы федеральных и муниципальных органов власти.

Учебное время: 2 часа.

Тема 2. Нормативно-правовые основы защиты информационных технологий предприятий, фирм.

Практическое занятие 2.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по применению основных нормативно-правовых актов защиты информационных технологий предприятий, фирм и организаций.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Информационные ресурсы в сфере финансов и внешнеэкономической деятельности государства.
2. Информационные ресурсы отраслей материального производства.
3. Информационные ресурсы государственной системы статистики.
4. Информационные ресурсы социальной сферы.

Учебное время: 2 часа.

Тема 3. Защищённые информационные технологии в государственном и муниципальном управлении

Практическое занятие 3.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по выявлению основных угроз безопасности для информационных объектов, определению возможных атак и каналов утечки информации.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Классификация угроз безопасности информационным объектам.
2. Основные формы атак на объекты информационных систем и технологий.
3. Анализ угроз и каналов утечки информации на информационных объектах.
4. Анализ рисков и управление ими при использовании защищённых инфомационных технологий.

Учебное время: 4 часа.

Тема 4. Защищённые информационные технологии в управлении коммерческими структурами

Практическое занятие 4.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по применению защищённых информационных технологий в управлении коммерческими структурами.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Создание системы защиты информации в корпоративной сети управления.
2. Основные этапы разработки систем защиты информационных систем и технологий и их характеристика.
3. Проблемы защиты интеллектуальной собственности на предприятиях, в фирмах.
4. Основные направления совершенствования защищённых информационных технологий.

Учебное время: 4 часа.

Тема 5. Организационно-технические методы защиты информационных технологий

Практическое занятие 5.

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

Тема и содержание практического занятия:

Цель работы: Получить знания и практические навыки по применению основных организационно-технических методов защиты информационных систем и технологий.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

Учебные вопросы:

1. Современные индикаторы поля и сканирующие приёмники.
2. Характеристика многофункциональных поисковых систем.
3. Выжигатели скрытых закладных устройств.
4. Обнаружители и подавители диктофонов и других высокочастотных электронных устройств.

Учебное время: 4 часа.

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

методов и средств безопасности информационных систем и технологий;

2) привить навыки самостоятельного решения нестандартных задач в области обеспечения безопасности информационных технологий.

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	**76**
Вопросы, выносимые на самостоятельное изучение	36
Подготовка к практическим занятиям	16
Подготовка к лабораторным занятиям	-
Подготовка докладов	8
Выполнение практических заданий	16

Вопросы, выносимые на самостоятельное изучение:

для очной формы обучения:

1. Характеристика современных методов биометрической идентификации личности и их особенности.
2. Представление речевого сигнала сообщения в виде графических образов.
3. Реализация способов аудиомаркирования с помощью компьютерных технологий.
4. Основные рекомендации по практическому применению технологии «речевая подпись».
5. Стеганографическая защита информации цифровыми водяными знаками.
6. Характеристика современных систем цифровых водяных знаков и их особенности.
7. Характеристика и особенности основных атак на системы цифровых водяных знаков.
8. Особенности применения крипто-технологий в цифровом телевидении.
9. Основные рекомендации по практическому применению стеганографической технологии в цифровом телевидении.
10. Маркирование и защита интеллектуальной собственности в России.
11. Организация и методика экспресс-поиска устройств несанкционированного съёма информации

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	-	
4.	Тематика докладов	8	1. Новые возможности использования технологий стеганографии в системах цифрового телевидения. 2. Основные проблемы применения защищённой технологии «речевая подпись» и пути их решения в современном мире.
5.	Выполнение практических заданий	16	Выявление проблем защиты интеллектуальной собственности на предприятиях, в фирмах.

Примерные темы докладов

1. Характеристика защищённых технологий систем кабельного телевидения, понятие телеохраны в современном мире.
2. Основы защищённых технологий при обеспечении безопасности персонала и пользователей почтовой связи.
3. Защищённые технологии и особенности их применения в системах наблюдения дальнего действия.
4. Защищённые технологии читающих автоматов и особенности их использования в системе безопасности предприятий, фирм.
5. Характеристика современных технологий охраны объектов и основные направления их развития.
6. Основные проблемы применения защищённой технологии «речевая подпись» и пути их решения в современном мире.
7. Средства обнаружения и системы охранной сигнализации, применяемые в рамках защищённых информационных технологий предприятий и фирм.
8. Характеристика основных устройств противодействия съёму информации в муниципальных защищаемых помещениях.
9. Особенности применения защитных технологий читающе опознающих автоматов в невидимых диапазонах электромагнитного спектра телевидения.

10. Защищённые технологии в системе обеспечения безопасности коммерческих объектов.
11. Новые возможности использования технологий стеганографии в системах цифрового телевидения.
12. Методы охраны и защиты конфиденциально ориентированного предприятия на основе применения нейросетевых технологий обработки информации.
13. Современные подходы в развитии биометрических технологий защиты и перспективы их развития.
14. Идентификация пользователей вычислительных систем на основе современных речевых технологий и методов искусственного интеллекта.

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. Анисимов А.А. Менеджмент в сфере информационной безопасности. Учебное пособие. – М.: Интернет – Университет информационных технологий / БИНОМ. Лаборатория знаний, 2010.

2. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность. Учебное пособие. – М.: «ФОРУМ», 2011.
3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации. Учебное пособие для вузов. - М.: «Горячая линия – Телеком», 2012.

Дополнительная литература:

1. Ворона В.А., Тихонов В.А. Технические средства наблюдения в охране объектов. – М.: «Горячая Линия - Телеком», 2011.
2. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: «Горячая Линия - Телеком», 2010.
3. Титоренко Г. А. Информационные технологии управления. Учебное пособие. М.: Юнити-Дана, 2010.

Рекомендуемая литература:

1. Киселёв Г. М., Бочкова Р. В., Сафонов В. И. Информационные технологии в экономике и управлении. Учебное пособие. М.: Издательско-торговая корпорация «Дашков и К°», 2012.
2. Петраков А. В. Защитные информационные технологии аудиовидео-электросвязи. Учебное пособие. М.: Энергоатомиздат, 2010.
3. Тарасюк М. В. Защищённые информационные технологии. Проектирование и применение. Учебное пособие. М.: «Слон-пресс», 2004.
4. Ивасенко А. Г., Гридасов А. Ю., Павленко В. А. Информационные технологии в экономике и управлении. Учебное пособие. М.: КноРус, 2010.

Электронные книги:

1. 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, PowerPoint.*

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ

2. Рабочая программа и методическое обеспечение по дисциплине «Безопасность информационных технологий».