Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич

Подписано цифровой подписью: Троицкий Александр Витальевич

УТВЕРЖДАЮ
И.о. проректора
А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки: 09.04.03 Прикладная информатика

Профиль: Моделирование и проектирование информационных систем

Уровень высшего образования: магистратура

Форма обучения: очная

Королев 2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Воронов А. Н. Рабочая программа дисциплины: Информационная безопасность – Королёв МО: «Технологический Университет», 2023

Рецензент: к.в.н. доцент Сухотерин А.И.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки магистров 09.04.03 «Прикладная информатика» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 г.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Сазонов С.Ю. к.т.н. доцент			
Год утверждения (переутверждения)	2023			
Номер и дата протокола заседания кафедры	№8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП _____ к.т.н., доцент Раев О.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023			
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

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

Целью изучения дисциплины является:
формирование у обучающихся специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества, в использовании организационно-технических механизмов обеспечения защиты информационных объектов, а также получение навыков в применении технологий обеспечения информационной безопасности для защищаемых объектов.

В процессе обучения обучающийся приобретает и совершенствует следующие компетенции:

профессиональные компетенции (ПК):

- Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС (ПК-5);
- Способность применять современные методы и инструментальные средства прикладной информатики для автоматизации решения прикладных задач различных классов и создания ИС (ПК-1).

Основными **задачами** дисциплины являются:

1. Ознакомление студентов с методологическими подходами применения и эксплуатации основных технических средств информационной безопасности защищаемых объектов, а также с основными методами определения параметров, характеристик и условий применения технических средств защиты на основе анализа возможных угроз информационной безопасности и потенциальных каналов утечки информации;
2. Формирование у студентов способности самостоятельно решать поставленные задачи в области информационной безопасности с помощью существующих принципов, методов и технологий в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам.

Показатель освоения компетенции отражают следующие индикаторы**:**

Необходимые знания:

- Понимает передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС
- Имеет понятие о методах и инструментальных средствах прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС.

Необходимые умения:

- Использует передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС

- Использует методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС.

Трудовые действия:

- Применяет передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС
- Применяет методы и инструментальные средства прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и создания ИС.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам по выбору части, формируемой участниками образовательных отношений основной профессиональной образовательной программы подготовки магистров по направлению подготовки 09.04.03 «Прикладная информатика».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на компетенциях, освоенных в курсе «Компьютерное моделирование бизнес процессов» (ПК-3, 6, 7), и служит основой изучения курса «Защищенные ИС».

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы обучения составляет 2 зачетных единицы, 72 часа.

Таблица 1

Виды занятий	Всего часов	Семестр …	Семестр 3	Семестр …	Семестр …
Общая трудоемкость	**72**		**72**		
Аудиторные занятия	**24**		**24**		
Лекции (Л)	8		8		
Практические занятия (ПЗ)	16		16		
Лабораторные работы (ЛР)	-		-		
Практическая подготовка					
Самостоятельная работа	**48**		**48**		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы					
Контрольная работа	+		+		
Текущий контроль знаний					
Вид итогового контроля	Экзамен		Экзамен		

4. Содержание дисциплины
4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час.	Практические занятия, час	Лабораторные занятия, час	Занятия в интерактивной форме, час	Практическая подготовка	Код компетенций
Тема 1. Концепция информационной безопасности.	1	2	-		-	ПК – 1,5
Тема 2. Основные направления обеспечения информационной безопасности.	1	2	-	1	-	ПК – 1,5
Тема 3. Основные способы защиты информации.	1	2	-	2	-	ПК – 1,5
Тема 4. Защита информации от утечки по техническим каналам связи.	1	2	-	2	-	ПК – 1,5
Тема 5. Способы противодействия несанкционированному доступу к источникам конфиденциальной информации.	1	2	-	2	-	ПК – 1,5
Тема 6. Особенности защиты информационных объектов с помощью технических средств.	1	2	-	2	-	ПК – 1,5
Тема 7. Защитные меры при работе с зарубежными партнёрами.	1	2	-	1	-	ПК – 1,5
Тема 8. Методика разработки системы защиты информации на предприятии.	1	2	-	2	-	ПК – 1,5
Итого:	**8**	**16**	**-**	**12**	-	

4.2. Содержание тем дисциплины

Тема 1. Концепция информационной безопасности.

Основные концептуальные положения системы информационной безопасности. Понятие информации и три подхода к определению информации. Определение системы информационной безопасности и требования к ней. Основные виды обеспечения информационной безопасности и системы защиты информации. Концептуальная модель информационной безопасности, её состав и особенности применения. Характеристика действий, приводящих к неправомерному овладению конфиденциальной информацией.

Тема 2. Основные направления обеспечения информационной безопасности.

Характеристика направлений информационной безопасности и перечень защитных действий. Особенности правовой защиты информации. Структура законодательства РФ в области информационной безопасности и защиты информации. Понятие конфиденциальной информации и виды тайн в Российском законодательстве. Основные определения, состав и особенности реализации организационной защиты информации. Предназначение, состав и основные задачи службы безопасности предприятия, фирмы. Предназначение, состав и особенности реализации инженерно-технической защиты информационных объектов.

Тема 3. Основные способы защиты информации.

Понятие способа защиты информации и состав основных организационных и технических мероприятий по её защите. Чем достигается обеспечение информационной безопасности, основные цели защиты информации. Каналы распространения информации и порядок реализации защитных действий от неправомерного овладения конфиденциальной информацией. Матрица, характеризующая взаимосвязь источников информации, целей защиты и механизмов защиты в процессе телекоммуникационного обмена сведениями.

Тема 4. Защита информации от утечки по техническим каналам связи.

Определение утечки информации и способы её классификации. Структура канала утечки информации и классификация технических каналов. Классификация и особенности проявления визуально-оптических каналов утечки информации и особенности защиты информации по ним. Классификация и особенности проявления акустических каналов утечки информации и особенности защиты информации по ним. Классификация и особенности проявления электромагнитных каналов утечки информации и особенности защиты информации по ним. Характеристика применяемых средств защиты информации от утечки по различным каналам.

Тема 5. Способы противодействия несанкционированному доступу к источникам конфиденциальной информации.

Характеристика основных способов несанкционированного доступа к информации. Состав обобщённой модели способов несанкционированного доступа к источникам конфиденциальной информации и их взаимосвязь друг с другом. Обзор и основные возможности технических средств несанкционированного доступа к информации. Порядок контроля и прослушивания телефонных каналов связи, методика непосредственного подключения к телефонной линии. Особенности перехвата компьютерной информации и несанкционированного внедрения в базы и банки данных. Применение скрытой фото- и видеосъёмки при помощи специальной оптики.

Тема 6. Особенности защиты информационных объектов с помощью технических средств.

Понятие, классификация и особенности применения акустических систем радиоподслушивания (радиозакладок), их параметры и характеристики. Обзор и классификация основных средств обнаружения радиосигналов. Предназначение, состав, основные характеристики и возможности индикаторов поля, панорамных радиоприёмников, сканеров и нелинейных радиолокаторов, порядок их применения и примеры. Понятие радиоэлектронных помех, их разновидности и порядок постановки. Методика обеспечения безопасности телефонных переговоров и противодействия лазерному подслушиванию с помощью специальных технических средств.

Тема 7. Защитные меры при работе с зарубежными партнёрами.

Основные направления взаимодействия с зарубежными партнёрами и порядок организации научно-технического сотрудничества с ними. Вопросы защиты интеллектуальной собственности в соглашениях и договорах о международном сотрудничестве. Технологический обмен результатами совместной деятельности и порядок его регулирования. Структура рынка по реализации новых технологий, характеристика основных путей технологического обмена между странами. Основные виды международных коммерческих операций и их характеристика. Анализ возможных условий разглашения сведений, составляющих коммерческую тайну и научно-техническая документация как источник конфиденциальной информации в международных сделках. Организация безопасной работы с зарубежными партнёрами.

Тема 8. Методика разработки системы защиты информации на предприятии.

Общепринятая методика проведения аудита выделенных помещений и её особенности. Возможности специального оборудования и технических средств, рекомендованных для проведения аудита. Состав итоговых документов по результатам аудита и их оценка. Порядок разработки системы защиты информации на предприятии, характеристика основных стадий разработки и этапов работы. Общий порядок действий по обеспечению информационной безопасности на основных этапах разработки системы. Полномочия специальной приёмной комиссии, её состав и итоговые документы по приёму разработанной или усовершенствованной системы защиты информационных объектов на предприятии.

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

«Методические указания для обучающихся по освоению дисциплины».

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

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Информационная безопасность» приведена в Приложении 1 к настоящей рабочей программе.

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

Основная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8.
   URL: http://znanium.com/go.php?id=491597
2. Малюк А. А., Горбатов В. С. и др**.** Введение в информационную безопасность: Учебное пособие / Малюк А. А.,Горбатов В.С. и др. ; под. ред. В.С. Горбатого. - М.: Телеком, 2011. - 288 с.: ил. - ISBN 978-5-9912-0160-5.
3. Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

1. Бирюков А. Информационная безопасность: защита и нападение [Текст] / А. Бирюков. - М.: ДМК Пресс, 2012. - 474 с.: ил.; 60х90 /16. - ISBN 978-5-94074-647-8.
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин Владимир Федорович. - Москва; Москва: Издательский Дом "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2014. - 416 с. - ДЛЯ УЧАЩИХСЯ ПТУ И СТУДЕНТОВ СРЕДНИХ СПЕЦИАЛЬНЫХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-8199-0331-5. URL: http://znanium.com/go.php?id=423927
3. Цирлов В. Л. Основы информационной безопасности [Текст]: краткий курс / В. Л. Цирлов. - Ростов н/Д.: Феникс, 2008. - 253 с. - (Профессиональное образование). - ISBN 978-5-222-13164-0.

Рекомендуемая литература:

1. Ворона В. А., Тихонов В. А. Инженерно-техническая и пожарная защита объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2012. - 512 с.: ил. - ISBN 978-5-9912-0179-7.
2. Ворона В. А., Тихонов В. А. Технические средства наблюдения в охране объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2011. - 184 с.: ил. - ISBN 978-5-9912-0143-8.
3. Зайцев А. П. и др**.** Технические средства и методы защиты информации [Текст]: учебное пособие для вуза / Зайцев А.П. и др.; под. ред. А. П. Зайцева, А. А. Шелупанова. - 4-е изд., испр. и доп. - М.: Горячая линия-Телеком, 2012. - 616 с.: ил. - ISBN 978-5-9912-0084-4.
4. Ярочкин В. И. Информационная безопасность / В. И. Ярочкин; В.И. Ярочкин. - 5-е изд. - Москва: Академический проект, 2008. - 544 с. - (Gaudeamus). - ISBN 978-5-8291-0987-5.
URL: http://biblioclub.ru/index.php?page=book&id=211164

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

Интернет-ресурсы:
http://www.znanium.com/ - электронно-библиотечная система
http://www.e.lanbook.com/ - ЭБС Издательства "ЛАНЬ"
http://www.rucont.ru/- электронно-библиотечная система
http://www.biblioclub.ru/ -университетская библиотека онлайн

9. Методические указания для обучающихся по освоению дисциплины

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

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

Перечень программного обеспечения: MS Office.
Информационные справочные системы:

1. Ресурсы информационно-образовательной среды Технологического университета.
2. Информационно – справочные (правовые) системы: «Консультант +».

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

Лекционные занятия:
- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций/слайдов.

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;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки: 09.04.03 Прикладная информатика

Профиль: Моделирование и проектирование информационных систем

Уровень высшего образования: магистратура

Форма обучения: очная

Королёв 2023

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

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся приобретает:		
				Необходимые знания	Необходимые умения	Трудовые действия
1.	ПК-5	Способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	Тема1-8.	Понимает передовые методы оценки качества, надежности и информационной безопасно-сти ИС в процессе эксплуата-ции прикладных ИС	Использует передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуата-ции прикладных ИС	Применяет передовые методы оценки качества, надежности и информационной безопасно-сти ИС в процессе эксплуата-ции прикладных ИС
2.	ПК-1	Способность применять современные методы и инструментальные средства прикладной информатики для автоматизации решения прикладных задач различных классов и создания ИС	Тема 1 - 8	Имеет понятие о методах и инструментальных средствах прикладной информатики для автоматизации и информатизации решения прикладных задач различных классов и со-здания ИС	Использует методы и инстру-ментальные средства прикла-клад-ной информатики для автома-тизации и информатизации решения прикладных задач различных классов и со-здания ИС	Применяет методы и инстру-ментальные средства прикладной информатики для автома-тизации и информатизации решения прикладных задач различных классов и со-здания ИС

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

Код компетенции	**Инструменты, оценивающие сформированность компетенции**	**Этапы и показатель оценивания компетенции**	**Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания**
ПК -1,5	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы

			аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК -1,5	Реферат	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	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 -1,5	Выполнение контрольной работы	А) **полностью сформирована** (компетенция освоена на высоком уровне) – 5 баллов Б) **частично сформирована**: •компетенция **освоена на продвинутом уровне** – 4 балла; •**компетенция освоена на базовом уровне** – 3 балла; В) **не сформирована** (компетенция не освоена) – 2 и менее баллов	При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида.

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

3.1 Примерная тематика докладов в презентационной форме:

1. Состав и основные характеристики современных средств охранной сигнализации.
2. Особенности применения современных средств охранной сигнализации в России и за рубежом.
3. Состав и основные характеристики современных систем и средств контроля и управления доступом.
4. Особенности применения современных систем и средств контроля и управления доступом в России и за рубежом.
5. Состав и основные характеристики современных радиоволновых однопозиционных средств охраны.
6. Особенности применения современных радиоволновых однопозиционных средств охраны в России и за рубежом.
7. Состав и основные характеристики современных радиоволновых двухпозиционных средств охраны.
8. Особенности применения современных радиоволновых двухпозиционных средств охраны в России и за рубежом.
9. Состав и основные характеристики современных проводноволновых средств охраны.
10. Особенности применения современных проводноволновых средств охраны в России и за рубежом.
11. Состав и основные характеристики современных вибрационных средств охраны.
12. Особенности применения современных вибрационных средств охраны в России и за рубежом.
13. Доктрина информационной безопасности РФ: современные информационные угрозы.
14. Доктрина информационной безопасности РФ: сущность и задачи.
15. Доктрина ИБ РФ: критически важные информационные объекты.
16. Доктрина ИБ РФ: направления обеспечения информационной безопасности.
17. Классификация защищаемого информационного ресурса.
18. Конфиденциальная информация и ее характеристика.
19. Секретная информация как объект информационной безопасности.
20. Организационное обеспечение информационной безопасности.
21. Техническое обеспечение информационной безопасности.
22. Правовое обеспечение информационной безопасности.
23. Организационная система обеспечения ИБ РФ.
24. Персональные данные как объект ИБ.
25. Понятие о теории защиты информации.

3.2 Примерная тематика реферата:

1. Состав и основные характеристики современных сейсмических средств охраны.
2. Особенности применения современных сейсмических средств охраны в России и за рубежом.
3. Состав и основные характеристики современных магнитометрических средств охраны.
4. Особенности применения современных магнитометрических средств охраны в России и за рубежом.
5. Состав и основные характеристики современных оптико-электронных однопозиционных средств охраны.
6. Особенности применения современных оптико-электронных однопозиционных средств охраны в России и за рубежом.
7. Состав и основные характеристики современных ёмкостных средств охраны.
8. Особенности применения современных ёмкостных средств охраны в России и за рубежом.
9. Состав и основные характеристики современных оптико-электронных двух позиционных средств охраны.
10. Особенности применения современных оптико-электронных двухпозиционных средств охраны в России и за рубежом.
11. Состав и основные характеристики современных звуковых средств охраны.
12. Особенности применения современных звуковых средств охраны в России и за рубежом.
13. Состав и характеристика основных компонентов понятия ИБ.
14. Сущность и содержание понятия защиты информации ограниченного доступа.
15. Сущность и содержание понятия защиты открытой информации.
16. Сущность и содержание понятия защиты объектов интеллектуальной собственности.
17. Сущность и содержание понятия защиты персональных данных.
18. Сущность и содержание понятия защиты личной тайны граждан.
19. Основы информационно-психологической безопасности персонала.
20. Энергоинформационная безопасность объектов информационной защиты.
21. Радиоэлектронная защита в системе информационной безопасности.
22. Радиоэлектронная разведка в системе информационной безопасности.
23. Рубежи и зоны защиты объектов ИБ.
24. Структурные подразделения типового предприятия по обеспечению ИБ.
25. Понятие технической защиты информации.

3.3 Примерная тематика контрольных работ:

1. Состав и основные характеристики современных электроконтактных средств охраны.
2. Особенности применения современных электро- контактных средств охраны в России и за рубежом.
3. Состав и основные характеристики современных быстро разворачиваемых мобильных сигнализационных комплексов.

4. Особенности применения современных быстро разворачиваемых мобильных сигнализационных комплексов в России и за рубежом.
5. Состав и основные характеристики современных электростатических пассивных средств охраны.
6. Особенности применения современных электростатических пассивных средств охраны в России и за рубежом.
7. Состав, основные характеристики современных гидроакустических средств охраны.
8. Особенности применения современных гидроакустических средств охраны в России и за рубежом.
9. Состав и основные характеристики современных пьезоэлектрических средств охраны.
10. Особенности применения современных пьезоэлектрических средств охраны в России и за рубежом.
11. Состав и основные характеристики современных манометрических средств охраны.
12. Особенности применения современных манометрических средств охраны в России и за рубежом.
13. Состав и основные характеристики современных приёмно-контрольных приборов.
14. Особенности применения современных приёмно-контрольных приборов в России и за рубежом.
15. Унифицированная концепция обеспечения ИБ.
16. Виды и способы обоснования стратегий по ИБ на типовом предприятии.
17. Характеристика и обоснование оборонительной стратегии в области ИБ.
18. Характеристика и обоснование наступательной стратегии в области ИБ.
19. Характеристика и обоснование упреждающей стратегии в области ИБ.
20. Кортеж принимаемых решений в области ИБ (понятие и состав).
21. Информационный ущерб и риски в области ИБ (понятия и различия).
22. Информационные угрозы и уязвимости для защищаемых объектов ИБ.
23. Различие понятий «служебная тайна» и «коммерческая тайна».
24. Виды и характеристика понятий «злоумышленник» и «нарушитель» в области ИБ.
25. Особенности защиты информации в локальных и корпоративных вычислительных сетях (объектах).

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

Формой контроля знаний по дисциплине «Информационная безопасность» является экзамен.

Неделя текущего кон-	Вид оценочного средства	Код компетенций, оценивающий знания, уме-	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов

троля		**ния, навыки**				
Проводится в сроки, установленные графиком учебного процесса	Экзамен	ПК -1,5	3 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: знание основных понятий предмета; умение использовать и применять полученные знания на практике; работа на практических занятиях; знание основных научных теорий, изучаемых предметов; ответ на вопросы билета. «**Хорошо**»: знание основных понятий предмета; умение использовать и применять полученные знания на практике; работа на практических занятиях; знание основных научных теорий, изучаемых предметов; ответы на большинство вопросов билета «У**довлетворительно**»: демонстрирует частичные знания по темам дисциплин; незнание неумение использовать и применять полученные знания на практике; не работал на практических занятиях; ответил не на все вопросы билета «**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 экзамен

1. Основные концептуальные положения системы информационной безопасности.
2. Понятие системы информационной безопасности и её основные отличия от системы защиты информации.
3. Общие и специфические требования к системе информационной безопасности и виды её обеспечения.
4. Концептуальная модель информационной безопасности и особенности её применения.
5. Характеристика угроз конфиденциальной информации и их классификация.
6. Особенности действий, приводящих к неправомерному овладению конфиденциальной информацией.
7. Направления обеспечения информационной безопасности и их характеристика.
8. Особенности правовой защиты информации, основные блоки правовых актов, касающихся информационной безопасности и защиты информации, их состав.
9. Понятие конфиденциальной информации и различные виды тайн, как объекты информационной безопасности.
10. Требования правовой обеспеченности информационной безопасности в уставах, учредительных и коллективных договорах и других организационных документах на предприятиях в фирмах.
11. Основные понятия и особенности организационной защиты информации.
12. Состав, основные задачи и особенности функционирования специальных штатных служб и ответственных лиц информационной безопасности на предприятиях в фирмах, организациях.
13. Особенности инженерно-технической защиты информационных объектов, как делятся средства инженерно-технической защиты?
14. Понятие физических средств и систем защиты информационных объектов, их классификация и особенности применения.
15. Особенности применения охранных телевизионных систем и охранного освещения на объектах.
16. Характеристика систем контроля доступа на охраняемые объекты и биометрических систем идентификации субъектов.
17. Особенности применения комплексных систем физической защиты и охраны объектов, как они делятся и что обеспечивают?
18. Предназначение, решаемые задачи, классификация и методика применения аппаратных средств защиты объектов, их примеры.

19. Характеристика программных средств защиты информации, их классификация и сферы применения.
20. Порядок защиты информации от несанкционированного доступа к ней, понятие идентификации и аутентификации объектов.
21. Порядок и особенности применения средств защиты от копирования и разрушения информации.
22. Методика применения криптографических средств защиты информации, общая технология шифрования данных.
23. Характеристика криптографических алгоритмов шифрования, понятие односторонней функции и её примеры, технология шифрования речи.
24. Понятие способа защиты информации, классификация основных защитных мероприятий и действий от неправомерного овладения конфиденциальной информацией.
25. Особенности применения организационных и технических мероприятий по защите информационных объектов, их классификация.
26. Основные каналы распространения информации, характеристика защитных действий и механизмов защиты объектов, их классификация.
27. Характеристика и особенности применения способов пресечения разглашения информации и каналов её бесконтрольного распространения.
28. Что понимается под техническим каналом утечки информации, его структура и разновидности, основные причины и условия возникновения технических каналов утечки информации.
29. Особенности проявления визуально-оптических каналов утечки информации, их классификация, порядок, средства и способы защиты от утечки сведений по визуально-оптическим каналам.
30. Особенности проявления акустических каналов утечки информации, их классификация, порядок, средства и способы защиты от утечки сведений по акустическим каналам.
31. Особенности проявления электромагнитных каналов утечки информации, их классификация, характеристика источников излучения, порядок, средства и способы защиты от утечки сведений по электромагнитным каналам.
32. Особенности проявления материально-вещественных каналов утечки информации, их классификация и порядок защиты от утечки сведений по материально-вещественным каналам.
33. Понятие микрофонного эффекта и основные аппаратные решения для подавления его, порядок проведения испытаний и исследований технических средств на наличие микрофонного эффекта.
34. Особенности защиты от утечки информации за счёт различных видов электромагнитного излучения средств связи и других технических устройств, основные возможности программно-аппаратного комплекса «Зарница».
35. Особенности защиты от утечки информации за счёт паразитной генерации излучений.
36. Особенности защиты от утечки информации по цепям электропитания и заземления устройств.

37. Особенности защиты от утечки информации за счёт взаимного влияния проводов, проводников и цепей в линиях связи, разновидности взаимного влияния между цепями.
38. Особенности защиты от утечки информации за счёт высокочастотного навязывания, характеристика источников навязываемого сигнала.
39. Особенности защиты от утечки информации в волоконно-оптических линиях и системах связи, понятие акустико-оптического эффекта и в чём он проявляется.
40. Характеристика способов несанкционированного доступа к информации, их взаимосвязь с источниками конфиденциальной информации и общие мероприятия по противодействию НСД.
41. Характеристика технических средств несанкционированного доступа к информации, особенности акустического контроля и прослушивания телефонных каналов связи.
42. Особенности перехвата компьютерной информации и несанкционированное внедрение в базы и банки данных, основные методы противодействия этим акциям.
43. Особенности скрытой фото- и видеосъёмки при помощи специальной оптики, основные меры защиты от наблюдения и фотографирования, состав частной модели фотографического контакта.
44. Организация защиты от подслушивания переговоров с помощью технических средств, противодействие подслушиванию посредством микрофонных систем, основные возможности стационарных и переносных обнаружителей диктофонов.
45. Предназначение, классификация и основные возможности средств радиоподслушивания (радиозакладок), их демаскирующие признаки.
46. Признаки классификации и основные возможности средств обнаружения радиосигналов, их параметры и характеристики.
47. Предназначение, состав, принцип работы и основные возможности индикаторов поля, их примеры.
48. Предназначение, состав, принцип работы и основные возможности панорамных радиоприёмников и сканеров, их примеры.
49. Предназначение, состав, принцип работы и основные возможности нелинейных радиолокаторов, их примеры.
50. Понятие радиоэлектронных помех, как они делятся, особенности их постановки, эффективные параметры, что понимается под коэффициентом подавления помех и как его определить?
51. Характеристика активных средств обеспечения безопасности телефонных переговоров и их разновидности, основные возможности, примеры.
52. Основные способы противодействия лазерному подслушиванию переговоров, основные разновидности и характеристики лазерных регистраторов, методика их обнаружения и противодействия.
53. Методика противодействия незаконному подключению к линиям связи, особенности противодействия контактному подключению, как определяют место и сам факт контактного подключения, основные возможности отечественной и зарубежной аппаратуры проверки проводных линий связи.

54. Особенности противодействия бесконтактному подключению к линиям связи, основные возможности специального поискового прибора и принцип его работы.
55. Определение и особенности радиоперехвата информации, основные меры защиты от него, сотав частной и параметрической модели информационного контакта средствами радиоразведки.
56. Как рассчитать возможность установления информационного контакта при перехвате и максимальную дальность действия для линии разведывательного контакта, от каких параметров они зависят?
57. Сущность и основные понятия научно-технического сотрудничества с зарубежными партнёрами, порядок составления соглашений (договоров) о сотрудничестве.
58. Организация технологического обмена и его регулирование в процессе совместной деятельности, составляющие рынка новых технологий.
59. Основные виды международных коммерческих операций и их характеристика.
60. Научно-техническая документация, как источник конфиденциальной информации, её состав, классификация, критерии достоверности и примеры.
61. Анализ возможных условий разглашения сведений, составляющих коммерческую тайну при международном сотрудничестве с зарубежными партнёрами.
62. Порядок организации работы с зарубежными партнёрами, особенности проведения переговоров и защиты информации при этом, оценка потенциальных партнёров.
63. Порядок проведения аудита выделенных помещений и его итоговые документы.
64. Порядок разработки системы защиты информации на предприятии и методика оценки её эффективности.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

Приложение 2

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление подготовки: 09.04.03 Прикладная информатика

Профиль: Моделирование и проектирование информационных систем

Уровень высшего образования: магистратура

Форма обучения: очная

Королев 2023

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-технических механизмов обеспечения защиты информационных объектов;

– выработать и закрепить у обучающихся базовые умения и навыки в применении технологий обеспечения информационной безопасности для защищаемых объектов.

Задачи дисциплины:

– ознакомление студентов с методологическими подходами применения и эксплуатации основных технических средств информационной безопасности защищаемых объектов;

– изучение основных методов определения параметров, характеристик и условий применения технических средств защиты на основе анализа возможных угроз информационной безопасности и потенциальных каналов утечки информации;

– формирование у студентов способности самостоятельно решать поставленные задачи в области информационной безопасности с помощью существующих принципов, методов и технологий в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам.

2. Указания по проведению практических занятий

Практическое занятие 1.

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

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 1. Концепция информационной безопасности.*

Цель работы: Получить знания и практические навыки по применению концептуальной модели информационной безопасности, её основным характеристикам и особенностям построения.

Основные положения темы занятия:

1. Определения и виды обеспечения системы информационной безопасности и основные требования к ней.

2. Характеристика действий, приводящих к неправомерному овладению конфиденциальной информацией.

Вопросы для обсуждения:

1. Определение и характеристика угроз конфиденциальной информации.

2. Порядок классификации угроз конфиденциальной информации по различным признакам.

3. Классификация и особенности действий, приводящих к неправомерному овладению конфиденциальной информацией.

4. Характеристика форм и методов недобросовестной конкуренции в современном мире.

Продолжительность занятия – 2 ч.

Практическое занятие 2.

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

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 2. Основные направления обеспечения информационной безопасности.*

Цель работы: Получить знания и практические навыки по основным направлениям информационной безопасности, как нормативно-правовым категориям, определяющим комплексные меры защиты информационных объектов на государственном уровне, а также на уровне предприятия, организации и отдельной личности.

Основные положения темы занятия:

1. Основные определения, состав и особенности реализации правовой и организационной защиты информационных объектов.

2. Предназначение, состав и особенности построения службы безопасности предприятия, фирмы, реализация инженерно-технической защиты информационных объектов.

Вопросы для обсуждения:

1. Состав, классификация и особенности применения физических средств защиты информационных объектов.

2. Основные задачи, состав, классификация и особенности применения аппаратных средств защиты персональных компьютеров и сетей.

3. Предназначение, состав, классификация и особенности применения программных средств защиты информации от чужого вторжения.

4. Особенности применения криптографических средств защиты информации в мире коммерческой деятельности.

Продолжительность занятия – 2 ч.

Практическое занятие 3.

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

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 3. Основные способы защиты информации.*

Цель работы: Получить знания и практические навыки по отдельным способам защиты информации, а также по составу и особенностям применения основных организационных и технических мероприятий по защите информационных объектов.

Основные положения темы занятия:

1. Характеристика каналов распространения информации и порядок реализации защитных действий от неправомерного овладения конфиденциальной информацией.

2. Взаимосвязь источников информации, целей защиты и механизмов защиты в процессе телекоммуникационного обмена сведениями.

Вопросы для обсуждения:

1. Анализ основных факторов и обстоятельств, приводящих к разглашению конфиденциальной информации.

2. Характеристика основных способов пресечения разглашения конфиденциальной информации.

3. Состав и классификация основных каналов распространения сведений, как средств обмена деловой и научной информацией.

4. Главные направления воспитательно- профилактической деятельности, как средств воздействия на чувства, волю и характер сотрудников в интересах формирования у них способности хранить тайну и соблюдать правила работы с закрытой информацией.

Продолжительность занятия – 2 ч.

Практическое занятие 4.

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

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 4. Защита информации от утечки по техническим каналам связи.*

Цель работы: Получить знания и практические навыки по применению защитных мер от утечки информации по техническим каналам связи

Основные положения темы занятия:

1. Структура канала утечки информации, классификация технических каналов и особенности их проявления.

2. Краткий обзор визуально-оптических, акустических и электромагнитных каналов утечки информации, особенности защиты информации по ним.

Вопросы для обсуждения:

1. Защита информации от утечки по цепям электропитания и заземления.

2. Защита информации от утечки за счёт взаимного влияния проводов и линий связи, в том числе в волоконно-оптических линиях связи.

3. Защита информации от утечки за счёт электромагнитного навязывания сигнала.

4. Защита информации от утечки по материально-вещественным каналам распространения информации.

Продолжительность занятия – 2 ч.

Практическое занятие 5.

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

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 5. Способы противодействия несанкционированному доступу к источникам конфиденциальной информации.*

Цель работы: Получить знания и практические навыки по основным способам противодействия несанкционированному доступу к источникам конфиденциальной информации.

Основные положения темы занятия:

1. Характеристика обобщённой модели способов несанкционированного доступа к источникам конфиденциальной информации и их взаимосвязь друг с другом.

2. Обзор технических средств несанкционированного доступа к информации и их основные возможности.

Вопросы для обсуждения:

1. Особенности защиты от наблюдения, съёмки и фотографирования, как способа ведения разведки с целью получения информации об объектах.

2. Особенности защиты от подслушивания переговоров, как способа ведения разведки и промышленного шпионажа.

3. Особенности формирования, состав и порядок применения частной модели фотографического контакта.

4. Методика организации противодействия подслушиванию переговоров посредством микрофонных систем.

Продолжительность занятия – 2 ч.

Практическое занятие 6.

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

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 6. Особенности защиты информационных объектов с помощью технических средств.*

Цель работы: Получить знания и практические навыки по методике защиты информационных объектов с помощью современных технических средств.

Основные положения темы занятия:

1. Предназначение, классификация и особенности применения акустических систем радиоподслушивания (радиозакладок), их параметры и основные характеристики.

2. Характеристика и классификация основных средств обнаружения радиосигналов, понятие радиоэлектронных помех, их разновидности и порядок постановки.

Вопросы для обсуждения:

1. Порядок организации противодействия контактному подключению к линиям связи, основные средства противодействия.

2. Порядок организации противодействия бесконтактному подключению к линиям связи, основные средства противодействия.

3. Организация защиты информации от радиоперехвата, обзор характеристик средств противодействия.

4. Состав, порядок построения и использования частной и параметрической моделей радиоперехвата.

Продолжительность занятия – 2 ч.

Практическое занятие 7.

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

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 7. Защитные меры при работе с зарубежными партнёрами.*

Цель работы: Получить знания и практические навыки по организации работы с зарубежными партнёрами с использованием защитных мероприятий и способов сохранения конфиденциальной информации, защиты коммерческой тайны и интеллектуальной собственности предприятия, фирмы, организации.

Основные положения темы занятия:

1. Характеристика основных направлений взаимодействия с зарубежными партнёрами и порядок организации научно-технического сотрудничества с ними.

2. Особенности технологического обмена результатами совместной деятельности и порядок его регулирования, анализ возможных условий разглашения сведений, составляющих коммерческую тайну в международных сделках.

Вопросы для обсуждения:

1. Основные формы и особенности защиты конфиденциальной информации при работе с зарубежными партнёрами по заключённым договорам и соглашениям.

2. Особенности подготовки и документального обеспечения визитов зарубежных организаций, основные режимные меры их сопровождения и взаимодействия с ними.

3. Порядок приёма зарубежных партнёров, организация деловых встреч и переговоров.

4. Порядок представления итоговых документов по результатам деловых встреч и совместной деятельности с зарубежными партнёрами, ответственность структурных подразделений и должностных лиц за сохранение конфиденциальной информации и других производственных секретов.

Продолжительность занятия – 2 ч.

Практическое занятие 8.

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

Образовательные технологии: *групповая дискуссия*

Тема и содержание практического занятия: *Тема 8. Методика разработки системы защиты информации на предприятии.*

Цель работы: Получить знания и практические навыки по основным этапам методики разработки или совершенствования системы защиты информации на предприятии.

Основные положения темы занятия:

1. Порядок разработки системы защиты информации на предприятии, характеристика основных стадий разработки и этапов работы.

2. Общий порядок действий по обеспечению информационной безопасности на основных этапах разработки системы защиты, методика проведения аудита выделенных помещений и её особенности.

Вопросы для обсуждения:

1. Методика оценки эффективности системы защиты информации на предприятии в соответствии с принципом комплексного подхода.

2. Понятия критериев и показателей эффективности системы защиты информации, их основные различия и порядок применения.

3. Определение важности защищаемых объектов на основании результатов оценки эффективности и грифов обрабатываемой информации на них.

4. Основные методы, способы и мероприятия по достижению конечных целей информационной безопасности предприятия на различных этапах её построения и эксплуатации.

Продолжительность занятия – 2 ч.

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом.

4. Указания по проведению самостоятельной работы обучающихся

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области информационной безопасности и существующих средств защиты информации;

2) привить навыки самостоятельного решения нестандартных задач в области применения защитных средств и технологий.

Тематическое содержание самостоятельной работы представлено в таблице:

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	12	1. Особенности шифрования данных псевдослучайными числами. 2. Основные методы шифрования информации и их характеристика. 3. Порядок применения поточных и блочных шифров, понятие криптографического протокола. 4. Криптографические системы с открытым ключом и их особенности применения. 5. Методы использования специальных свойств компьютерных форматов. 6. Философия использования электронной цифровой подписи и методы хеширования сообщений. 7. Методы использования избыточности аудио- и видеоин-

			формации в компьютерной стеганографии. 8. Характеристика современных распространённых методов биометрической идентификации личности и особенности их применения. 9. Реализация технологии речевой подписи (аудиомаркирования) сообщений с применением компьютерных технологий. 10. Практическое применение защитной технологии «речевая подпись» в современном мире.
2.	Тематика докладов	12	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. 15. Доктрина ИБ РФ: критически важные информационные объекты. 16. Доктрина ИБ РФ: направления обеспечения информационной безопасности. 17. Классификация защищаемого информационного ресурса. 18. Конфиденциальная информация и ее характеристика. 19. Секретная информация как объект информационной безопасности. 20. Организационное обеспечение информационной безопасности. 21. Техническое обеспечение информационной безопасности. 22. Правовое обеспечение информационной безопасности.

			23. Организационная система обеспечения ИБ РФ. 24. Персональные данные как объект ИБ. 25. Понятие о теории защиты информации.
3.	Выполнение практических заданий	8	1. Основные криптографические методы защиты электронной документации и данных. 2. Современные технологии обеспечения безопасности на основе индивидуальных особенностей человека.
4	Подготовка к экзамену	16	Проработка лекций, практик, изучение рекомендованной литературы. Консультации у преподавателя.

5. Указания по проведению контрольных работ для обучающихся очной формы обучения

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. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.
3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов.
4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).
5. Необходимо давать ссылки на используемую Вами литературу.
6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
7. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 10 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. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8.
URL: http://znanium.com/go.php?id=491597
2. Малюк А. А., Горбатов В. С. и др**.** Введение в информационную безопасность: Учебное пособие / Малюк А. А.,Горбатов В.С. и др. ; под. ред. В.С. Горбатого. - М.: Телеком, 2011. - 288 с.: ил. - ISBN 978-5-9912-0160-5.
3. Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

1. Бирюков А. Информационная безопасность: защита и нападение [Текст] / А. Бирюков. - М.: ДМК Пресс, 2012. - 474 с.: ил.; 60х90 /16. - ISBN 978-5-94074-647-8.
2. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин Владимир Федорович. - Москва; Москва: Издательский Дом "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2014. - 416 с. - ДЛЯ УЧАЩИХСЯ ПТУ И СТУДЕНТОВ СРЕДНИХ СПЕЦИАЛЬНЫХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-8199-0331-5. URL: http://znanium.com/go.php?id=423927
3. Цирлов В. Л. Основы информационной безопасности [Текст]: краткий курс / В. Л. Цирлов. - Ростов н/Д.: Феникс, 2008. - 253 с. - (Профессиональное образование). - ISBN 978-5-222-13164-0.

Рекомендуемая литература:

1. Ворона В. А., Тихонов В. А. Инженерно-техническая и пожарная защита объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2012. - 512 с.: ил. - ISBN 978-5-9912-0179-7.
2. Ворона В. А., Тихонов В. А. Технические средства наблюдения в охране объектов / Ворона В.А., Тихонов В.А. - М.: Горячая линия-Телеком, 2011. - 184 с.: ил. - ISBN 978-5-9912-0143-8.
3. Зайцев А. П. и др**.** Технические средства и методы защиты информации [Текст]: учебное пособие для вуза / Зайцев А.П. и др.; под. ред. А. П. Зайцева, А. А. Шелупанова. - 4-е изд., испр. и доп. - М.: Горячая линия-Телеком, 2012. - 616 с.: ил. - ISBN 978-5-9912-0084-4.
4. Ярочкин В. И. Информационная безопасность / В. И. Ярочкин; В.И. Ярочкин. - 5-е изд. - Москва: Академический проект, 2008. - 544 с. - (Gaudeamus). - ISBN 978-5-8291-0987-5. URL: http://biblioclub.ru/index.php?page=book&id=211164

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

Интернет-ресурсы:
http://www.znanium.com/ - электронно-библиотечная система
http://www.e.lanbook.com/ - ЭБС Издательства "ЛАНЬ"
http://www.rucont.ru/- электронно-библиотечная система
http://www.biblioclub.ru/ -университетская библиотека онлайн

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice.*
Информационные справочные системы:
1. Ресурсы информационно-образовательной среды Технологического университета
2. Информационно – справочные (правовые) системы: «Консультант +».