



Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



«УТВЕРЖДАЮ»

Проректор по учебно-методической работе

Н.В. Бабина

«28» апреля 2020 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

**ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ**

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Информационно-аналитические системы
финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

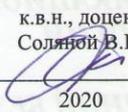
Королев
2020

Автор: к.в.н., доцент Соляной В.Н. Рабочая программа дисциплины: «Основы информационной безопасности». – Королев МО: «Технологический университет», 2020.

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

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н. 			
Год утверждения (переподтверждения)	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 (переподтверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

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

Целью изучения дисциплины является ознакомление и закрепление базовых положений по обеспечению информационной безопасности на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общекультурные компетенции:

- (ОК-5) - способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

Общепрофессиональные компетенции:

- (ОПК-4) - способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

Основными **задачами** дисциплины являются:

- раскрытие сущности, целей и содержание основ теории информационной безопасности и методологии защиты информации;
- определение методологических подходов построения систем защиты информации;
- освоение методических подходов установления состава защищаемой информации и выявления объектов защиты;
- выявление целесообразных методов определения актуальных информационных угроз и опасных нарушителей (злоумышленников);
- овладение методами оценки уязвимости защищаемой информации;
- определение методов выявления параметров и структуры систем защиты информации;
- освоение методов установления целесообразного состава мероприятий по защите информации;
- раскрытие методов управления системами защиты информации;

- определение методологических подходов оценки эффективности мер по защите информации и др.

После завершения освоения данной дисциплины студент должен:

Знать:

- базовый понятийный аппарат в области информационной безопасности и защиты информации;
- виды и состав угроз информационной безопасности;
- принципы и общие методы обеспечения информационной безопасности;
- основные положения государственной политики обеспечения информационной безопасности;
- критерии, условия и принципы отнесения информации к защищаемой;
- виды носителей защищаемой информации;
- виды и подвиды тайн конфиденциальной информации;
- виды уязвимости защищаемой информации и формы ее проявления;
- источники, виды и способы дестабилизирующего воздействия на защищаемую информацию;
- каналы и методы несанкционированного доступа к конфиденциальной информации;
- состав объектов защиты информации;
- классификацию видов, методов и средств защиты информации;
- состав кадрового, ресурсного и технологического обеспечения защиты информации и др.

Уметь:

- выявлять угрозы информационной безопасности применительно к объектам защиты;
- определять состав конфиденциальной информации применительно к видам тайны;
- выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия;
- выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации;
- определять направления и виды защиты информации с учетом характера информации и задач по ее защите;
- организовывать комплексный подход по защите информации и др.

Владеть навыками:

- письменной и публичной речи;
- нахождения необходимой литературы по вопросам информационной безопасности;
- определения требований и состава средств, методов и мероприятий по организации защиты информации;
- использования методов организации, планирования и контроля функционирования систем защиты информации;
- разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения систем защиты информации;
- проведения количественной и качественной оценки эффективности функционирования различных компонентов систем защиты информации и др.

2. Место дисциплины в структуре ОПОП ВО

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

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Информатика», «Введение в профессию», «Основы исследований информационной безопасности» и компетенциях: ОК-3, ОПК-2,4 и ПК-8,9,11,12.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации», «Основы управления информационной безопасностью», «Организация защиты персональных данных на предприятии», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

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

Таблица 1

Виды занятий	Всего часов	Семестр 2	Семестр 3	Семестр 4	Семестр ...
Общая трудоемкость	144	72	72		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	64	32	32		
Лекции (Л)	32	16	16		
Практические занятия (ПЗ)	32	16	16		
Лабораторные работы (ЛР)	-	-	-		
Самостоятельная работа	80	40	40		
КСР	-	-	-		
Курсовые работы (проекты)	-	-	-		
Расчетно-графические работы	-	-	-		
Контрольная работа, домашнее задание	+	+	+		
Текущий контроль знаний (7 - 8, 15 - 16 недели)	Тест	Тест	Тест		
Вид итогового контроля	Зачёт/Зачёт с оц.	Зачет	Зачёт с оц.		

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции		Практические занятия,		Занятия в интерактивной форме		Код компетенций
	Очное	очно-заочное	Очное	очно-заочное	Очное	очно-заочное	
2 семестр							
Раздел 1. Базовые положения по информационной безопасности							
Тема 1. Введение. Сущность и понятие информационной безопасности	1	-	1	-	1	-	ОК-5 ОПК-4

Тема 2. Значение информационной безопасности и ее место в системе национальной безопасности	1	-	1	-	1	-	ОК-5 ОПК-4
Тема 3. Доктрина информационной безопасности РФ	1		1		1		ОК-5 ОПК-4
Тема 4. Сущность понятия ЗИ	1		1				ОК-5 ОПК-4
Тема 5. Теоретико-концептуальные основы защиты информации	1	-	1	-	1	-	ОК-5 ОПК-4
Тема 6. Организационные основы и методологические принципы ЗИ	1		1		1		ОК-5 ОПК-4
Раздел 2. Характеристика защищаемой информации							
Тема 7. Критерии, условия и принципы отнесения информации к защищаемой	1		1		1		ОК-5 ОПК-4
Тема 8. Состав и классификация носителей ЗИ	1	-	1	-	1	-	ОК-5 ОПК-4
Тема 9. Классификация защищаемой информации	2		2				ОК-5 ОПК-4
Тема 10. Основы защиты государственной тайны	2		2				ОК-5 ОПК-4
Тема 11. Основы защиты коммерческой и служебной тайны	2	-	2	-	1	-	ОК-5 ОПК-4
Тема 12. Основы защиты личной и профессиональной тайны	2		2		1		ОК-5 ОПК-4
Итого: за семестр	16		16		9		
3 семестр							

Раздел 3. Условия, определяющие необходимость защиты информации							
Тема 13. Понятие и структура угроз защищаемой информации	1		1				ОК-5 ОПК-4
Тема 14. Дестабилизирующие воздействия на защищаемую информацию	1	-	1	-	1		ОК-5 ОПК-4
Тема 15. Каналы и методы несанкционированного доступа к защищаемой информации	1		1			-	ОК-5 ОПК-4
Тема 16. Характеристика деятельности разведывательных служб по несанкционированному доступу	1	-	1	-	1	-	ОК-5 ОПК-4
Тема 17. Объекты защиты информации	1		1		1		ОК-5 ОПК-4
Раздел 4. Характеристика основных мер по защите информации							
Тема 18. Виды и методы защиты информации	1		1				ОК-5 ОПК-4
Тема 19. Классификация и характеристика средств защиты информации	2	-	2	-		-	ОК-5 ОПК-4
Тема 20. Основные виды обеспечения защиты информации	2		2		1		ОК-5 ОПК-4
Тема 21. Системы защиты информации	2		2				ОК-5 ОПК-4
Тема 22. Основы управления защитой информации	2	-	2	-	1		ОК-5 ОПК-4
Тема 23. Методологические подходы оценки	2		2	-	1	-	ОК-5 ОПК-4

эффективности защиты информации							
Всего за 3 семестр	16	-	16	-	9	-	
Всего за год	32	-	32	-	18	-	

4.2. Содержание тем дисциплины 2 семестр

Раздел 1. Базовые положения по информационной безопасности

Тема 1. Введение. Сущность и понятие информационной безопасности

Предмет и задачи курса. Значение и место курса в подготовке специалистов по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами.

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

Анализ нормативных источников, научной и учебной литературы.

Знания и умения студентов, которые должны быть получены в результате изучения курса.

Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия.

Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности.

Тема 2. Значение информационной безопасности и ее место в системе национальной безопасности

Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации.

Понятие и современная концепция национальной безопасности.

Место информационной безопасности в системе национальной безопасности.

Тема 3. Доктрины информационной безопасности Российской Федерации

Общие положения о Доктрине информационной безопасности.

Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их достижения. Виды и состав угроз информационной безопасности.

Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.

Общие методы обеспечения информационной безопасности. Особенности обеспечения информационной безопасности в различных сферах общественной жизни и в международном сотрудничестве.

Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Организационная основа системы обеспечения информационной безопасности.

Тема 4. Сущность понятия защиты информации

Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части.

Методологическая основа раскрытия сущности и определения понятия защиты информации.

Формы выражения нарушения статуса информации. Обусловленность статуса информации и ее уязвимость. Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации.

Понятие "утечка информации". Соотношение форм и видов уязвимости информации

Содержательная часть понятия "защита информации". Способ реализации содержательной части защиты информации. Определение понятия "защита информации", его соотношение с понятием, сформулированным в ГОСТ Р 50922-96 "Защита информации. Основные термины и определения".

Цели и значение информации. Существующие подходы к определению целей защиты информации.

Понятие целей защиты информации, их отличие от задач защиты информации. Увязка целей защиты информации с защищаемой информацией и субъектами информационных отношений. Непосредственная цель защиты информации. Опосредованные (конечные) цели защиты информации.

Место защиты информации в системе национальной и информационной безопасности. Значение защиты информации для субъектов информационных отношений государства, общества, личности. Значение защиты информации в политической, военной, экономической и других областях деятельности. Социальные последствия защиты информации.

Тема 5. Теоретико-концептуальные основы защиты информации

Понятие и назначение теории защиты информации.

Основные положения теории защиты информации: объективная необходимость и общественная потребность в защите информации; включенность ее в систему общественных отношений; зависимость защиты информации от политико-правовых, социально-экономических, военно-

политических реальностей; увязка с проблемами информатизации общества; обеспечения баланса интересов личности, общества и государства.

Правовое регулирование и взаимный контроль субъектов информационных отношений в сфере защиты информации; содействие повышению эффективности соответствующей области деятельности.

Теоретические основы национальной политики в сфере защиты информации.

Понятие и назначение концепции защиты информации. Теория защиты информации как основа концепции защиты информации.

Содержание концепции защиты информации, ее значение для разработки стратегии, формирования целевых программ и практических мероприятий по защите информации. Уровни и виды концепции защиты информации.

Становление и развитие государственной концепции защиты информации.

Современная стратегия защиты информации.

Тема 6. Организационные основы и методологические принципы защиты информации

Организационные основы как необходимые условия для осуществления защиты информации. Основы, обеспечивающие технологию защиты информации. Основы, необходимые для обеспечения сохранности и конфиденциальности информации.

Значение методологических принципов защиты информации. Принципы, обусловленные принадлежностью, ценностью, конфиденциальностью, технологией защиты информации.

Современные факторы, влияющие на защиту информации:

факторы, обусловленные объективными тенденциями развития мирового сообщества, характер их влияния на защиту информации;

факторы, обусловленные современным состоянием России. Влияние политико-правовых и социально-экономических реальностей на защиту информации.

Раздел 2. Характеристика защищаемой информации

Тема 7. Критерии, условия и принципы отнесения информации к защищаемой

Современные подходы к определению состава защищаемой информации. Основа для отнесения информации к защищаемой, категории информации, подпадающие под эту основу.

Понятия "конфиденциальная информация", "секретная информация", "открытая информация", параметры их защиты. Понятие защищаемой информации.

Критерии отнесения открытой информации к защищаемой, их обусловленность необходимостью защиты информации от утраты.

Критерии отнесения конфиденциальной информации к защищаемой, их обусловленность необходимостью защиты информации от утраты и утечки.

Условия, необходимые для отнесения информации к защищаемой.

Правовые и организационные принципы отнесения информации к защищаемой.

Тема 8. Состав и классификация носителей защищаемой информации

Понятие "носитель защищаемой информации". Соотношение между носителем и источником информации.

Состав носителей защищаемой информации. Способы фиксирования информации в носителях. Виды отображения информации в носителях. Методы воспроизведения отображенной информации в носителях информации.

Носители письменной, видовой, излучаемой информации. Опосредованные носители защищаемой информации.

Свойства и значение типов носителей защищаемой информации.

Тема 9. Классификация защищаемой информации

Понятие "тайна информации".

Типовая классификация защищаемой информации.

Содержание понятия секретная и конфиденциальная информация.

Виды тайны конфиденциальной информации.

Показатели разделения конфиденциальной информации по видам тайн.

Степени и грифы конфиденциальности информации.

Тема 10. Основы защиты государственной тайны

Становление и современное определение понятия "государственная тайна". Основания и организационно-правовые формы отнесения информации к государственной тайне.

Функции должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне.

Перечень сведений, являющихся государственной тайной, их назначение и структура. Степени секретности сведений, отнесенных к государственной тайне. Критерии отнесения сведений к различным степеням секретности.

Грифы секретности носителей информации. Различия между степенью и грифом секретности. Основания для рассекречивания информации.

Тема 11. Основы защиты коммерческой и служебной тайны

Становление и современное определение коммерческой тайны. Место коммерческой тайны в системе предпринимательской деятельности.

Основания и методика отнесения сведений к коммерческой тайне. Степени конфиденциальности сведений, составляющих коммерческую тайну. Функции государства в сфере защиты коммерческой тайны. Тенденция и определяющие факторы развития коммерческой тайны.

Современные подходы к сущности служебной тайны. Понятие служебной тайны, границы и области ее действия. Распределение полномочий по отнесению сведений к служебной тайне.

Тема 12. Основы защиты личной и профессиональной тайны

Понятия "личная тайна", "защищаемая информация о гражданах (персональные данные)". Категории информации, отнесенной к персональным данным.

Разновидности личной тайны. Функции государства и граждан в сфере защиты личной тайны и персональных данных.

Понятие и особенности профессиональной тайны. Сфера действия профессиональной тайны. Соотношение между профессиональной и другими видами тайны. Разновидности профессиональной тайны.

Понятие интеллектуальной собственности.

Различие между правом собственности и авторским правом.

Объекты (предметы) интеллектуальной собственности как составная часть защищаемой информации.

3 семестр

Раздел 3. Условия, определяющие необходимость защиты информации

Тема 13. Понятие и структура угроз защищаемой информации

Современные подходы к понятию угрозы защищаемой информации.

Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации.

Структура явлений как сущностного выражения угрозы защищаемой информации.

Тема 14. Дестабилизирующие воздействия на защищаемую информацию

Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

Источники дестабилизирующего воздействия на защищаемую информацию как определяющая структурная часть угрозы.

Состав и характеристика источников дестабилизирующего воздействия на информацию.

Виды и способы дестабилизирующего воздействия на информацию со стороны различных источников.

Соотношение видов дестабилизирующего воздействия на защищаемую информацию с формами проявления уязвимости информации.

Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на информацию, их обусловленность источниками и видами воздействия.

Причины, вызывающие преднамеренное и непреднамеренное дестабилизирующее воздействие на информацию со стороны людей.

Обстоятельства (предпосылки), способствующие появлению этих причин.

Условия, создающие возможность для дестабилизирующего воздействия на информацию.

Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны других источников воздействия.

Тема 15. Каналы и методы несанкционированного доступа к защищаемой информации

Канал несанкционированного доступа к защищаемой информации как составная часть угрозы информации.

Современные подходы к понятию канала несанкционированного доступа к информации. Соотношение между каналами несанкционированного доступа и каналами утечки информации, их сущность и понятия.

Состав и характеристика каналов несанкционированного доступа к конфиденциальной информации. Специально создаваемые и потенциально существующие каналы несанкционированного доступа.

Методы несанкционированного доступа к защищаемой информации.

Зависимость методов и форм их использования от целей и возможностей соперника.

Существующая классификация каналов и ее недостатки.

Тема 16. Характеристика деятельности разведывательных служб по несанкционированному доступу

Структура государственных разведывательных органов ведущих зарубежных стран. Органы политической, военной и радиотехнической разведки.

Структура разведывательных служб частных объединений.

Направления и виды разведывательной деятельности, их соотношение и взаимосвязь.

Особенности деятельности разведывательных органов, их сочетание при добывании информации.

Тема 17. Объекты защиты информации

Понятие объекта защиты. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты.

Состав и характеристика объектов хранения письменных и видовых носителей информации, подлежащих защите.

Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации. Другие объекты защиты информации.

Виды и способы дестабилизирующего воздействия на объекты защиты.

Раздел 4. Характеристика основных мер по защите информации

Тема 18. Виды и методы защиты информации

Виды защиты информации, сферы их действия.

Классификация методов защиты информации.

Универсальные методы защиты информации, область их применения.

Области применения организационных, криптографических и инженерно-технических методов защиты информации.

Тема 19. Классификация и характеристика средств защиты информации

Понятие «средства защиты информации».

Классификация средств защиты информации.

Назначение и общая характеристика программных средств защиты.

Назначение и общая характеристика криптографических средств защиты.

Назначение и общая характеристика технических средств защиты.

Тема 20. Основные виды обеспечения защиты информации

Значение и состав кадрового обеспечения защиты информации. Полномочия руководства предприятия в области защиты информации. Полномочия специальных комиссий по защите информации. Полномочия службы защиты информации. Полномочия пользователей защищаемой информации.

Состав и назначение ресурсного обеспечения защиты информации. Характеристика основных видов ресурсного обеспечения защиты информации: финансовое; материальное; техническое; энергетическое; информационное; временное; пространственное. Значение ресурсного обеспечения для организации эффективной защиты информации.

Понятие и назначение технологического обеспечения защиты информации. Классификация организационно-технологических документов по

защите информации. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий.

Понятие о процессе проектирования и внедрения целесообразных мер по защите информации. Виды проектирования и их особенности. Характеристика основных этапов проектирования. Разрабатываемые документы в ходе проектирования и внедрения мер по защите.

Тема 21. Системы защиты информации

Понятие "система защиты информации". Назначение систем защиты информации. Классификация систем защиты информации, сферы их действия. Структура систем защиты информации.

Общая характеристика типовых подсистем защиты информации (программно-аппаратной, криптографической, физической, организационной, управления, инженерно-технической и др.).

Сущность и значение комплексной системы защиты информации как основная форма организации деятельности по защите информации.

Структура комплексной системы защиты информации, назначение составных частей системы.

Требования к подсистемам защиты информации и, в целом, к комплексной системе защите информации.

Тема 22. Основы управления защитой информации

Сущность и значение управления защитой информацией в современных условиях.

Виды управления защитой информацией.

Органы и средства управления защитой информацией.

Типовые функции управления защитой информации.

Документы, обрабатываемые в ходе управления защитой информацией.

Тема 23. Методологические подходы оценки эффективности защиты информации

Понятие об эффективности защиты информации в целом и отдельных ее процессов.

Основы моделирования эффективности защиты информации.

Функциональная и экономическая оценка эффективности защиты информации.

Качественные и количественные показатели и критерии эффективности защиты информации. Понятия об ущербах и информационных рисках. Виды ожидаемых ущербов.

Существующие проблемы при оценке эффективности защиты информации.

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 приведена в Приложении 1.

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

Основная литература:

1. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации : учебное пособие. - М. : Форум, 2011 г;
2. Малюк А.А. Теория защиты информации. Научное издание.- М.: Горячая линия-телеком, 2013 г.;
3. Зайцев, А.П. и др. Технические средства и методы защиты информации: учебное пособие для вуза / под. ред. А. П. Зайцева, А. А. Шелупанова. - 4-е изд., испр. и доп. - М. : Горячая линия-Телеком, 2012 г.;
4. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах : учебное пособие для вузов. - 4-е изд., стереотип. - М. : Горячая линия - Телеком, 2011 г.

Дополнительная литература:

1. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие. - М. : ИД "ФОРУМ" : ИНФРА-М, 2013 г.;
2. Мельников, Д.А. Информационная безопасность открытых систем: учебник. - М.: ФЛИНТА, 2013 г.;
3. Грибунин, В.Г. Комплексная система защиты информации на предприятии : учеб. пособие. - М.: Академия ИЦ, 2009 г.;
4. Ворона В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. - М.: Горячая линия-Телеком, 2013 г.;
5. Чипига, А.Ф. Информационная безопасность автоматизированных систем : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности - М. : Гелиос АРВ, 2010 г.;
6. Васильков А.В., Васильков А.А., Васильков И.А. Информационные

системы и их безопасность: учебное пособие. - М.: ФОРУМ, 2013 г.

Рекомендуемая литература:

1. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000.
2. Волокитин А.В. Информационная безопасность государственных организаций и коммерческих фирм. - М: ИНФО, 2002.
3. Девянин П.Н. и др. Теоретические основы компьютерной безопасности / - М.: Радио и связь, 2000.
4. Домарев В.В. Безопасность ИТ. Системный подход. – К.: ООО «ТИД «ДС»», 2004.
5. Байбурин В.Б. и др. Введение в защиту информации. Учебное пособие для вузов - М: ИНФРА-М, 2004.
6. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов.– М.: Горячая линия-Телеком, 2004.
7. Сидак А.А. Формирование требований безопасности современных сетевых информационных технологий. - М.: МГУЛ, 2001.
8. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - 2-е изд. - М.: Радио и связь, 2001.
9. Общие критерии оценки безопасности информационных технологий: Учеб. пособие/ Пер. с англ. Е.А. Сидак. - М.: ЦБИ, 2001.
10. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. - СПб.: БХВ-Петербург, 2000.

Электронные книги:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013 г.
<http://znanium.com/bookread.php?book=405000>
2. Жук А. П.Жук Е ПЛепешкин О МТимошкин А И. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура).
<http://znanium.com/bookread.php?book=474838>
3. Бабаш А В., Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013 г.
<http://znanium.com/bookread.php?book=405000>

4. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013 г.
<http://znanium.com/bookread.php?book=415501>

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

Интернет-ресурсы:

1. <http://eup.ru> – научно - образовательный портал.
2. <http://znanium.com> – образовательный портал
3. <http://www.academy.it> – академия АЙТИ

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: MSOffice, PowerPoint.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды;
2. Рабочая программа и методическое обеспечение по дисциплине: «Основы информационной безопасности».

Ресурсы информационно-образовательной среды Технологический университет:

Рабочая программа и методическое обеспечение по курсу «Основы информационной безопасности».

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 лекции в форме слайд-презентации, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже Windows 7, офисные программы MSOffice;

- рабочее место преподавателя, оснащенное компьютером с доступом в глобальную сеть Интернет ;

- рабочие места студентов, оснащенные компьютерами с доступом в глобальную сеть Интернет.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

***ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО
ДИСЦИПЛИНЕ**

**«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
(Приложение 1 к рабочей программе)**

Направление подготовки: 10.03.01 «Информационная безопасность»

**Профиль: Информационно-аналитические системы
финансового мониторинга**

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

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

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				знать	уметь	владеть
1	ОК-5	Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Введение. Сущность и понятие информационной безопасности; Значение информационной безопасности и ее место в системе национальной безопасности; Доктрина информационной безопасности РФ; Сущность понятия ЗИ; Состав и классификация носителей ЗИ; Основы защиты государственной тайны; Понятие и структура угроз защищаемой информации; Виды и методы защиты информации; Основные виды обеспечение защиты информации; Методологические подходы оценки эффективности защиты информации.	Базовый понятийный аппарат в области информационной безопасности и защиты информации; виды и состав угроз информационной безопасности	Выявлять угрозы информационной безопасности применительно к объектам защиты	Навыками письменной и публичной речи.

2.	ОПК -4	Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Значение информационной безопасности и ее место в системе национальной безопасности; Теоретико-концептуальные основы защиты информации; Критерии, условия и принципы отнесения информации к защищаемой; Состав и классификация носителей ЗИ; Основы защиты коммерческой и служебной тайны; Понятие и структура угроз защищаемой информации; Дестабилизирующие воздействия на защищаемую информацию; Основы управления защитой информации; Методологические подходы оценки эффективности защиты информации	Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию; состав объектов защиты информации; Классификацию видов, методов и средств защиты информации; Состав кадрового, ресурсного и технологического обеспечения защиты информации.	Выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников в воздействии; Определять направления и виды защиты информации с учетом характера информации и задач по ее защите	Навыками разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения систем защиты информации
----	-------------------	--	---	--	--	---

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

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОК-5	Доклад в форме презентации	<p>А) компетенция не сформирована</p> <p>В) сформирована частично</p> <p>С) сформирована полностью</p>	<p>Проводится устно с использованием мультимедийных систем, а также с использованием технических средств</p> <p>Время, отведенное на процедуру – 10 - 15 мин.</p> <p>Неявка – 0.</p> <p>Критерии оценки:</p> <p>1.Соответствие представленной презентации заявленной тематике (1 балл).</p> <p>2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл).</p> <p>3.Владение информацией и способность отвечать на вопросы аудитории (1 балл).</p> <p>4.Качество самой представленной презентации (1 балл).</p> <p>5.Оригинальность подхода и всестороннее раскрытие выбранной тематике (1 балл).</p> <p>Максимальная сумма баллов - 5 баллов.</p> <p>Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.</p>
ОПК-4	Реферат	<p>А) компетенция не сформирована</p> <p>В) сформирована частично</p> <p>С)</p>	<p>Проводится в письменной форме</p> <p>Критерии оценки:</p> <p>1.Соответствие содержания реферата заявленной тематике (1 балл).</p> <p>2.Качество источников и их количество при подготовке</p>

		сформирована полностью	<p>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.</p> <p>Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.</p>
--	--	------------------------	--

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

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

14. Становление и развитие промышленного шпионажа.

Примерная тематика реферата:

1. Безопасность сети Интернет.
2. Информационное общество и проблема его безопасности.
3. Российская экономика и ее информационная безопасность.
4. Стандартизация информации и ее роль в информационной безопасности.
5. Защита информации в деятельности государственного предприятия.
6. Развитие информационной безопасности в России.
7. Правовая основа защиты информации в России.
8. Банки в электронную эпоху и их информационная безопасность.
9. Организационные мероприятия по информационной безопасности.
10. Информационная безопасность в ведущих зарубежных странах.
11. Инженерно – техническая защита информации как базовое направление обеспечения информационной безопасности.
12. Криптографическая защита информации в современных информационных технологиях.
13. Современная доктрина информационной безопасности России.
14. Современные информационные системы и технологии управления и обеспечение их безопасности.
15. Система безопасности предприятия и роль службы защиты информации.
16. Безопасность электронного бизнеса.

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

Формой контроля знаний по дисциплине «Основы информационной безопасности» являются две текущие аттестации в виде тестов и одна промежуточная аттестация в виде зачета и зачёта с оценкой в устной форме.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оцениваемых знаний, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ОК-5; ОПК-4	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% Хорошо - от 70%. Отлично – от 90%.
Согласно учебному плану	тестирование	ОК-5; ОПК-4	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% Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно	Зачёт/Зачёт	ОК-5;	3 вопроса	Зачёт/Зачёт	Результат	Критерии оценки:

сно учебному плану	т с оценкой	ОПК-4		с оценкой проводится в устной форме, путем ответа на вопросы. Время отведенное на процедуру – 4 часа.	бы предоставлены в день проведения зачета/зачёта с оценкой	<p>«Зачтено»:</p> <ul style="list-style-type: none"> • 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. <p>«Не зачтено»:</p> <ul style="list-style-type: none"> • 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. <p>Критерии оценки:</p> <p>«Отлично»:</p> <ul style="list-style-type: none"> • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на семинарских занятиях;
--------------------	-------------	-------	--	---	--	--

				<ul style="list-style-type: none"> • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. <p>«Хорошо»:</p> <ul style="list-style-type: none"> • умение использовать и применять полученные знания на практике; • работа на семинарских занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. <p>«Удовлетворительно»:</p> <ul style="list-style-type: none"> • ответ на вопросы билета. • работа на семинарских занятиях; <p>«Неудовлетворительно»:</p> <ul style="list-style-type: none"> • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на семинарских занятиях; • не отвечает
--	--	--	--	--

Типовые вопросы, выносимые на зачет:**Вопросы к зачёту 2 семестра**

1. Сущность понятия «теория информационной безопасности»: определение, цели и задачи.
2. Сущность понятия «методология защиты информации»: определение, методы, задачи.
3. Современное понятие «информационной безопасности»: узкий и широкий подход, их содержание.
4. Сущность и структура классических понятий «информационной безопасности» и «защиты информации».
5. Объекты и компоненты информационной безопасности.
6. Роль информационной безопасности в информационной сфере общества: международный и внутригосударственный уровень.
7. Связь понятий информационная безопасность и безопасность информации.
8. Понятие Концепции национальной безопасности РФ и место в ней информационной безопасности.
9. Сущность Доктрины информационной безопасности и основные источники угроз информационной сферы.
10. Состояние и основные задачи обеспечения информационной безопасности РФ (требования Доктрины ИБ РФ).
11. Методы обеспечения информационной безопасности РФ (по доктрине ИБ РФ).
12. Государственная политика обеспечения информационной безопасности РФ (по Доктрине ИБ РФ).
13. Организационная основа системы обеспечения информационной

безопасности РФ (по Доктрине РФ).

14. Основные федеральные законы РФ в области ИБ (ЗИ).
15. Существующие подходы к понятию «защита информации» и их содержание.
16. Понятие «уязвимости» информации в теории защиты информации.
17. Понятие «утечки» информации в теории защиты информации.
18. Цели, функции и задачи защиты информации.
19. Кортеж концептуальных решений по защите информации: понятие и основные этапы.
20. Роль защиты информации в различных сферах деятельности.
21. Защита информации и проблема информационной войны.
22. Понятие «защита от негативной информации» в теории защиты информации.
23. Понятие, задачи и составные части теории защиты информации.
24. Научно-методологическая основа теории защиты информации: понятие и состав.
25. Общеметодологические (общетеоретические и теоретико-прикладные) принципы формирования теории защиты информации.
26. Инструментально-методологический базис теории защиты информации: понятие и характеристика методов.
27. Понятие о Концепции защиты информации.
28. Виды стратегий защиты информации как основа построения Концепции защиты информации.
29. Сущность и структура Унифицированной концепции защиты информации.
30. Организационные основы защиты информации: технологические и

правовые составляющие.

31. Международные факторы, влияющие на защиту информации в РФ.
32. Факторы, обуславливающие современное состояние РФ и их влияние на защиту информации.
33. Определение и классификация защищаемого информационного ресурса (информации).
34. Отличительные признаки защищаемой информации.
35. Критерии отнесения информации к защищаемой.
36. Модель (условия и принципы) отнесения информации к защищаемой.
37. Понятие и состав носителей защищаемой информации.
38. Прямые и косвенные носители защищаемой информации.
39. Понятие и виды тайн конфиденциальной информации.
40. Определение «государственной тайны» и порядок отнесения к ней сведений.
41. Степени и грифы сведений, отнесенных к государственной тайне.
42. Порядок рассекречивания сведений, отнесенных к государственной тайне.
43. Определение «коммерческой тайны» и порядок отнесения к ней сведений.
44. Степени конфиденциальности, составляющих коммерческую тайну.
45. Сущность понятия «служебной тайны», границы и области ее действий.
46. Понятие и сферы действий профессиональной тайны.
47. Соотношения между профессиональной тайной и другими видами тайн, разновидности профессиональной тайны.
48. Понятия «личная тайна» и «персональные данные» (защищаемая информация о гражданах).
49. Разновидности личной тайны (персональных данных).
50. Понятие и характер форм собственности на защищаемую информацию.

51. Понятия «собственники» и «владельцы» защищаемой информации.
52. Понятия «обладатели» и «конфиденты» защищаемой информации.
53. Основные субъекты профессиональной тайны: собственник, доверитель, держатель и пользователь.
54. Понятие и характеристика «интеллектуальной собственности».
55. Общепринятые методы защиты интеллектуальной собственности.
56. Различия между правом интеллектуальной собственности и авторским правом.
57. Понятие «патент» как общепринятый подход к защите интеллектуальной собственности.
58. Понятие «авторское право» с позиций защиты интеллектуальной собственности.
59. Первичные объекты интеллектуальной собственности, подлежащие защите.
60. Вторичные объекты интеллектуальной собственности, подлежащие защите и перечень произведений, не являющихся объектами авторского права.

Вопросы к зачёту с оценкой 3 семестра

1. Сущность понятия «теория информационной безопасности»: определение, цели и задачи.
2. Сущность понятия «методология защиты информации»: определение, методы, задачи.
3. Объекты и компоненты информационной безопасности.
4. Роль информационной безопасности в информационной сфере общества: международный и внутригосударственный уровень.
5. Понятие Концепции национальной безопасности РФ и место в ней информационной безопасности.

6. Сущность Доктрины информационной безопасности и основные источники угроз информационной сферы.
7. Состояние и основные задачи обеспечения информационной безопасности РФ (требования Доктрины ИБ РФ).
8. Государственная политика обеспечения информационной безопасности РФ (по Доктрине ИБ РФ).
9. Организационная основа системы обеспечения информационной безопасности РФ (по Доктрине ИБ РФ).
10. Основные федеральные законы РФ в области ИБ (ЗИ).
11. Понятие «уязвимости» информации в теории защиты информации.
12. Понятие «утечки» информации в теории защиты информации.
13. Цели, функции и задачи защиты информации.
14. Кортеж концептуальных решений по защите информации: понятие и основные этапы.
15. Защита информации и проблема информационной войны.
16. Понятие «защита от негативной информации» в теории защиты информации.
17. Понятие, задачи и составные части теории защиты информации.
18. Научно-методологическая основа теории защиты информации: понятие и состав.
19. Общеметодологические (общетеоретические и теоретико-прикладные) принципы формирования теории ЗИ.
20. Инструментально-методологический базис теории защиты информации: понятие и характеристика методов.
21. Понятие о Концепции защиты информации.
22. Виды стратегий защиты информации как основа построения Концепции защиты информации.

23. Сущность и структура Унифицированной концепции защиты информации.
24. Международные факторы, влияющие на защиту информации в РФ.
25. Факторы, обуславливающие современное состояние РФ и их влияние на защиту информации.
26. Определение и классификация защищаемого информационного ресурса (информации).
27. Отличительные признаки защищаемой информации.
28. Критерии отнесения информации к защищаемой.
29. Понятие и состав носителей защищаемой информации.
30. Прямые и косвенные носители защищаемой информации.
31. Понятие и виды тайн конфиденциальной информации.
32. Определение «государственной тайны» и порядок отнесения к ней сведений.
33. Определение «коммерческой тайны» и порядок отнесения к ней сведений.
34. Сущность понятия «служебной тайны», границы и области ее действий.
35. Понятие и сферы действий профессиональной тайны.
36. Понятия «личная тайна» и «персональные данные» (защищаемая информация о гражданах).
37. Понятие и характер форм собственности на защищаемую информацию.
38. Общепринятые методы защиты интеллектуальной собственности.
39. Объекты интеллектуальной собственности, подлежащие защите.
40. Понятие и структура угроз защищаемой информации.
41. Понятие, состав и характеристика источников воздействия на защищаемую информацию.
42. Виды и способы воздействия различных источников на защищаемую

информацию.

43. Понятие канала несанкционированного доступа (НСД) и его соотношение с каналом утечки информации.
44. Классификация каналов НСД и их характеристика.
45. Характеристика существующих организационных структур разведок зарубежных стран (государственных и частных объединений).
46. Понятия объекта защиты информации и носителей информации.
47. Виды защиты информации и их сферы действия.
48. Классификация методов защиты информации и их характеристика.
49. Характеристика организационных, криптографических и инженерно-технических методов защиты информации.
50. Определение и классификация средств защиты информации.
51. Назначение программных, криптографических и технических средств защиты.
52. Характеристика (понятие, назначение и состав) кадрового обеспечения защиты информации.
53. Полномочия представителей предприятий и организаций (руководства, специальных комиссий и пользователей) в области защиты информации.
54. Характеристика (понятие, назначение и состав) ресурсного обеспечения защиты информации.
55. Характеристика (понятие, назначение и состав) технологического обеспечения защиты информации.
56. Классификация организационно-технологических документов по ЗИ.
57. Виды и характеристика контрольных мероприятий по ЗИ.
58. Понятие и назначение систем защиты информации.
59. Структура и состав систем защиты информации, требования к ним.

60. Характеристика (сущность и значение) комплексной системы защиты информации как форма деятельности организаций (предприятий).

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

***ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ
И ТЕХНОЛОГИЙ***

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО
ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
(Приложение 2 к рабочей программе)**

Направление подготовки: 10.03.01 «Информационная безопасность»

**Профиль: Информационно-аналитические системы
финансового мониторинга**

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Общие положения

Целью изучения дисциплины является ознакомление и закрепление базовых положений по обеспечению информационной безопасности на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан.

Основными **задачами** дисциплины являются:

- раскрытие сущности, целей и содержание основ теории информационной безопасности и методологии защиты информации;
- определение методологических подходов построения систем защиты информации;
- освоение методических подходов установления состава защищаемой информации и выявления объектов защиты;
- выявление целесообразных методов определения актуальных информационных угроз и опасных нарушителей (злоумышленников);
- овладение методами оценки уязвимости защищаемой информации;
- определение методов выявления параметров и структуры систем защиты информации;
- освоение методов установления целесообразного состава мероприятий по защите информации;
- раскрытие методов управления системами защиты информации;
- определение методологических подходов оценки эффективности мер по защите информации и др.

2. Указания по проведению практических (семинарских) занятий

2 семестр

Практическое занятие 1.

Введение. Сущность и понятие информационной безопасности

Учебные вопросы

Предмет и задачи курса. Значение и место курса в подготовке специалистов по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами.

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

Анализ нормативных источников, научной и учебной литературы.

Знания и умения студентов, которые должны быть получены в результате изучения курса.

Становление и развитие понятия "информационная безопасность".
Современные подходы к определению понятия.

Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности.

Продолжительность занятия – 2 ч.

Практическое занятие 2

Значение информационной безопасности и ее место в системе национальной безопасности

Учебные вопросы

Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации.

Понятие и современная концепция национальной безопасности.
Место информационной безопасности в системе национальной безопасности.

Продолжительность занятия – 1 ч.

Практическое занятие 3

Доктрины информационной безопасности Российской Федерации

Учебные вопросы

Общие положения о Доктрине информационной безопасности.

Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их достижения. Виды и состав угроз информационной безопасности.

Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.

Общие методы обеспечения информационной безопасности. Особенности обеспечения информационной безопасности в различных сферах общественной жизни и в международном сотрудничестве.

Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Организационная основа системы обеспечения информационной безопасности.

Продолжительность занятия – 1 ч.

Практическое занятие 4

Сущность понятия защиты информации

Учебные вопросы

Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части.

Методологическая основа раскрытия сущности и определения понятия защиты информации.

Формы выражения нарушения статуса информации. Обусловленность статуса информации и ее уязвимость. Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации.

Понятие "утечка информации". Соотношение форм и видов уязвимости информации

Содержательная часть понятия "защита информации". Способ реализации содержательной части защиты информации. Определение понятия "защита информации", его соотношение с понятием, сформулированным в ГОСТ Р 50922-96 "Защита информации. Основные термины и определения".

Цели и значение информации. Существующие подходы к определению целей защиты информации.

Понятие целей защиты информации, их отличие от задач защиты информации. Увязка целей защиты информации с защищаемой информацией и субъектами информационных отношений. Непосредственная цель защиты информации. Опосредованные (конечные) цели защиты информации.

Место защиты информации в системе национальной и информационной безопасности. Значение защиты информации для субъектов информационных отношений государства, общества, личности. Значение защиты информации в политической, военной, экономической и других областях деятельности. Социальные последствия защиты информации.

Продолжительность занятия – 1 ч.

Практическое занятие 5

Теоретико-концептуальные основы защиты информации

Учебные вопросы

Понятие и назначение теории защиты информации.

Основные положения теории защиты информации: объективная необходимость и общественная потребность в защите информации; включенность ее в систему общественных отношений; зависимость защиты информации от политико-правовых, социально-экономических, военно-политических реальностей; увязка с проблемами информатизации общества; обеспечения баланса интересов личности, общества и государства.

Правовое регулирование и взаимный контроль субъектов информационных отношений в сфере защиты информации; содействие повышению эффективности соответствующей области деятельности.

Теоретические основы национальной политики в сфере защиты информации.

Понятие и назначение концепции защиты информации. Теория защиты информации как основа концепции защиты информации.

Содержание концепции защиты информации, ее значение для разработки стратегии, формирования целевых программ и практических мероприятий по защите информации. Уровни и виды концепции защиты информации.

Становление и развитие государственной концепции защиты информации.

Современная стратегия защиты информации.

Продолжительность занятия – 1 ч.

Практическое занятие 6.

Организационные основы и методологические принципы защиты информации

Учебные вопросы

Организационные основы как необходимые условия для осуществления защиты информации. Основы, обеспечивающие технологию защиты информации. Основы, необходимые для обеспечения сохранности и конфиденциальности информации.

Значение методологических принципов защиты информации. Принципы, обусловленные принадлежностью, ценностью, конфиденциальностью, технологией защиты информации.

Современные факторы, влияющие на защиту информации:

Факторы, обусловленные объективными тенденциями развития мирового сообщества, характер их влияния на защиту информации;

Факторы, обусловленные современным состоянием России. Влияние политико-правовых и социально-экономических реальностей на защиту информации.

Продолжительность занятия – 1 ч.

Практическое занятие 7

Критерии, условия и принципы отнесения информации к защищаемой

Учебные вопросы

Современные подходы к определению состава защищаемой информации. Основа для отнесения информации к защищаемой, категории информации, подпадающие под эту основу.

Понятия "конфиденциальная информация", "секретная информация", "открытая информация", параметры их защиты. Понятие защищаемой информации.

Критерии отнесения открытой информации к защищаемой, их обусловленность необходимостью защиты информации от утраты.

Критерии отнесения конфиденциальной информации к защищаемой, их обусловленность необходимостью защиты информации от утраты и утечки.

Условия, необходимые для отнесения информации к защищаемой.

Правовые и организационные принципы отнесения информации к защищаемой.

Продолжительность занятия – 1 ч.

Практическое занятие 8

Состав и классификация носителей защищаемой информации

Учебные вопросы

Понятие "носитель защищаемой информации". Соотношение между носителем и источником информации.

Состав носителей защищаемой информации. Способы фиксирования информации в носителях. Виды отображения информации в носителях. Методы воспроизведения отображенной информации в носителях информации.

Носители письменной, видовой, излучаемой информации. Опосредованные носители защищаемой информации.

Свойства и значение типов носителей защищаемой информации.

Продолжительность занятия – 1 ч.

Практическое занятие 9

Классификация защищаемой информации

Учебные вопросы

Понятие "тайна информации".

Типовая классификация защищаемой информации.

Содержание понятия секретная и конфиденциальная информация.

Виды тайны конфиденциальной информации.

Показатели разделения конфиденциальной информации по видам тайн.

Степени и грифы конфиденциальности информации.

Продолжительность занятия – 2 ч.

Практическое занятие 10

Основы защиты государственной тайны

Учебные вопросы

Становление и современное определение понятия "государственная тайна". Основания и организационно-правовые формы отнесения информации к государственной тайне.

Функции должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне.

Перечень сведений, являющихся государственной тайной, их назначение и структура. Степени секретности сведений, отнесенных к государственной тайне. Критерии отнесения сведений к различным степеням секретности.

Гриффы секретности носителей информации. Различия между степенью и грифом секретности. Основания для рассекречивания информации.

Продолжительность занятия – 2 ч.

Практическое занятие 11

Основы защиты коммерческой и служебной тайны

Учебные вопросы

Становление и современное определение коммерческой тайны. Место коммерческой тайны в системе предпринимательской деятельности.

Основания и методика отнесения сведений к коммерческой тайне. Степени конфиденциальности сведений, составляющих коммерческую тайну. Функции государства в сфере защиты коммерческой тайны. Тенденция и определяющие факторы развития коммерческой тайны.

Современные подходы к сущности служебной тайны. Понятие служебной тайны, границы и области ее действия. Распределение полномочий по отнесению сведений к служебной тайне.

Продолжительность занятия – 2 ч.

Практическое занятие 12

Основы защиты личной и профессиональной тайны

Учебные вопросы

Понятия "личная тайна", "защищаемая информация о гражданах (персональные данные)". Категории информации, отнесенной к персональным данным.

Разновидности личной тайны. Функции государства и граждан в сфере защиты личной тайны и персональных данных.

Понятие и особенности профессиональной тайны. Сфера действия профессиональной тайны. Соотношение между профессиональной и другими видами тайны. Разновидности профессиональной тайны.

Понятие интеллектуальной собственности.

Различие между правом собственности и авторским правом.

Объекты (предметы) интеллектуальной собственности как составная часть защищаемой информации.

Продолжительность занятия – 2 ч.

3 семестр

Практическое занятие 13

Понятие и структура угроз защищаемой информации

Учебные вопросы

Современные подходы к понятию угрозы защищаемой информации.

Связь угрозы защищаемой информации с уязвимостью информации.
Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации.

Структура явлений как сущностного выражения угрозы защищаемой информации.

Продолжительность занятия – 1 ч.

Практическое занятие 14

Дестабилизирующие воздействия на защищаемую информацию

Учебные вопросы

Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

Источники дестабилизирующего воздействия на защищаемую информацию как определяющая структурная часть угрозы.

Состав и характеристика источников дестабилизирующего воздействия на информацию.

Виды и способы дестабилизирующего воздействия на информацию со стороны различных источников.

Соотношение видов дестабилизирующего воздействия на защищаемую информацию с формами проявления уязвимости информации.

Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на информацию, их обусловленность источниками и видами воздействия.

Причины, вызывающие преднамеренное и непреднамеренное дестабилизирующее воздействие на информацию со стороны людей.

Обстоятельства (предпосылки), способствующие появлению этих причин.

Условия, создающие возможность для дестабилизирующего воздействия на информацию.

Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны других источников воздействия.

Продолжительность занятия – 1 ч.

Практическое занятие 15

Каналы и методы несанкционированного доступа к защищаемой информации

Учебные вопросы

Канал несанкционированного доступа к защищаемой информации как составная часть угрозы информации.

Современные подходы к понятию канала несанкционированного доступа к информации. Соотношение между каналами несанкционированного доступа и каналами утечки информации, их сущность и понятия.

Состав и характеристика каналов несанкционированного доступа к конфиденциальной информации. Специально создаваемые и потенциально существующие каналы несанкционированного доступа.

Методы несанкционированного доступа к защищаемой информации.

Зависимость методов и форм их использования от целей и возможностей соперника.

Существующая классификация каналов и ее недостатки.

Продолжительность занятия – 1 ч.

Практическое занятие 16

Каналы и методы несанкционированного доступа к защищаемой информации

Учебные вопросы

Структура государственных разведывательных органов ведущих зарубежных стран. Органы политической, военной и радиотехнической разведки.

Структура разведывательных служб частных объединений.

Направления и виды разведывательной деятельности, их соотношение и взаимосвязь.

Особенности деятельности разведывательных органов, их сочетание при добывании информации.

Продолжительность занятия – 1 ч.

Практическое занятие 17

Объекты защиты информации

Учебные вопросы

Понятие объекта защиты. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты.

Состав и характеристика объектов хранения письменных и видовых носителей информации, подлежащих защите.

Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации. Другие объекты защиты информации.

Виды и способы дестабилизирующего воздействия на объекты защиты.

Продолжительность занятия – 1 ч.

Практическое занятие 18

Виды и методы защиты информации

Учебные вопросы

Виды защиты информации, сферы их действия.

Классификация методов защиты информации.

Универсальные методы защиты информации, область их применения.

Области применения организационных, криптографических и инженерно-технических методов защиты информации.

Продолжительность занятия – 1 ч.

Практическое занятие 19

Классификация и характеристика средств защиты информации

Учебные вопросы

Понятие «средства защиты информации».

Классификация средств защиты информации.

Назначение и общая характеристика программных средств защиты.

Назначение и общая характеристика криптографических средств защиты.

Назначение и общая характеристика технических средств защиты.

Продолжительность занятия – 1 ч.

Практическое занятие 20

Основные виды обеспечения защиты информации

Учебные вопросы

Значение и состав кадрового обеспечения защиты информации.

Полномочия руководства предприятия в области защиты информации.

Полномочия специальных комиссий по защите информации.

Полномочия службы защиты информации. Полномочия пользователей защищаемой информации.

Состав и назначение ресурсного обеспечения защиты информации. Характеристика основных видов ресурсного обеспечения защиты информации: финансовое; материальное; техническое; энергетическое; информационное; временное; пространственное. Значение ресурсного обеспечения для организации эффективной защиты информации.

Понятие и назначение технологического обеспечения защиты информации. Классификация организационно-технологических документов по защите информации. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий.

Понятие о процессе проектирования и внедрения целесообразных мер по защите информации. Виды проектирования и их особенности. Характеристика основных этапов проектирования. Разрабатываемые документы в ходе проектирования и внедрения мер по защите.

Продолжительность занятия – 2 ч.

Практическое занятие 21

Системы защиты информации

Учебные вопросы

Понятие "система защиты информации". Назначение систем защиты информации. Классификация систем защиты информации, сферы их действия. Структура систем защиты информации.

Общая характеристика типовых подсистем защиты информации (программно-аппаратной, криптографической, физической, организационной, управления, инженерно-технической и др.).

Сущность и значение комплексной системы защиты информации как основная форма организации деятельности по защите информации.

Структура комплексной системы защиты информации, назначение составных частей системы.

Требования к подсистемам защиты информации и, в целом, к комплексной системе защите информации.

Продолжительность занятия – 2 ч.

Практическое занятие 22

Основы управления защитой информации

Учебные вопросы

Сущность и значение управления защитой информацией в современных условиях.

Виды управления защитой информацией.

Органы и средства управления защитой информацией.

Типовые функции управления защитой информации.

Документы, отрабатываемые в ходе управления защитой информацией.

Продолжительность занятия – 2 ч.

Практическое занятие 23

Методологические подходы оценки эффективности защиты информации

Учебные вопросы

Понятие об эффективности защиты информации в целом и отдельных ее процессов.

Основы моделирования эффективности защиты информации.

Функциональная и экономическая оценка эффективности защиты информации.

Качественные и количественные показатели и критерии эффективности защиты информации. Понятия об ущербах и информационных рисках. Виды ожидаемых ущербов.

Существующие проблемы при оценке эффективности защиты информации.

Продолжительность занятия – 2 ч.

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Сущность и понятие информационной безопасности	Подготовка докладов по темам: 1. Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия. 2. Сущность информационной безопасности. Объекты информационной безопасности. 3. Связь информационной безопасности с информатизацией общества. 4. Структура информационной безопасности
2.	Значение информационной безопасности и ее место в системе национальной безопасности	Подготовка докладов по темам: 1. Значение информационной безопасности для субъектов информационных отношений. 2. Связь между информационной безопасностью и безопасностью информации.

		<p>3. Понятие и современная концепция национальной безопасности.</p> <p>4. Место информационной безопасности в системе национальной безопасности.</p>
3	Доктрина информационной безопасности Российской Федерации	<p><i>Подготовка докладов по темам:</i></p> <p>1. Общие положения о Доктрине информационной безопасности.</p> <p>2. Интересы личности, общества и государства в информационной сфере.</p> <p>3. Составляющие национальных интересов в информационной сфере, пути их достижения.</p> <p>4. Виды и состав угроз информационной безопасности.</p> <p>5. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.</p> <p>6. Общие методы обеспечения информационной безопасности. Особенности обеспечения информационной безопасности в различных сферах общественной жизни и в международном сотрудничестве.</p> <p>7. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.</p> <p>8. Организационная основа системы обеспечения информационной безопасности.</p>
4	Сущность понятия защиты информации	<p><i>Подготовка докладов по темам:</i></p> <p>1. Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части.</p> <p>2. Методологическая основа раскрытия сущности и определения понятия защиты информации.</p> <p>3. Понятие уязвимости информации. Формы проявления</p>

		<p>уязвимости информации. Виды уязвимости информации.</p> <p>4. Содержательная часть понятия "защита информации". Существующие подходы к определению целей защиты информации.</p> <p>5. Место защиты информации в системе национальной и информационной безопасности.</p> <p>6. Значение защиты информации для субъектов информационных отношений государства, общества, личности.</p> <p>7. Значение защиты информации в политической, военной, экономической и других областях деятельности.</p>
5	Теоретико-концептуальные основы защиты информации	<p>Презентации по темам:</p> <p>1. Понятие и назначение теории защиты информации.</p> <p>2. Основные положения теории защиты информации: объективная необходимость и общественная потребность в защите информации; включенность ее в систему общественных отношений.</p> <p>3. Зависимость защиты информации от политико-правовых, социально-экономических, военно-политических реальностей; увязка с проблемами информатизации общества; обеспечения баланса интересов личности, общества и государства.</p> <p>4. Правовое регулирование и взаимный контроль субъектов информационных отношений в сфере защиты информации; содействие повышению эффективности соответствующей области деятельности.</p> <p>5. Понятие и назначение концепции защиты информации. Теория защиты информации как основа концепции защиты информации.</p> <p>6. Содержание концепции защиты информации, ее</p>

		<p>значение для разработки стратегии, формирования целевых программ и практических мероприятий по защите информации.</p> <p>7. Уровни и виды концепции защиты информации.</p> <p>8. Становление и развитие государственной концепции защиты информации.</p> <p>9. Современная стратегия защиты информации.</p>
6	<p>Организационные основы и методологические принципы защиты информации</p>	<p>Презентации по темам:</p> <p>1. Организационные основы как необходимые условия для осуществления защиты информации.</p> <p>2. Основы, обеспечивающие технологию защиты информации.</p> <p>3. Основы, необходимые для обеспечения сохранности и конфиденциальности информации.</p> <p>4. Значение методологических принципов защиты информации. Принципы, обусловленные принадлежностью, ценностью, конфиденциальностью, технологией защиты информации.</p> <p>5. Факторы, обусловленные объективными тенденциями развития мирового сообщества, характер их влияния на защиту информации.</p> <p>6. Факторы, обусловленные современным состоянием России.</p> <p>7. Влияние политико-правовых и социально-экономических реальностей на защиту информации.</p>
7	<p>Критерии, условия и принципы отнесения информации к защищаемой</p>	<p>Презентации по темам:</p> <p>1. Современные подходы к определению состава защищаемой информации. Основа для отнесения информации к защищаемой, категории информации, подпадающие под эту основу.</p> <p>2. Понятия "конфиденциальная информация", "секретная</p>

		<p>информация", "открытая информация", параметры их защиты. Понятие защищаемой информации.</p> <p>3. Критерии отнесения открытой информации к защищаемой, их обусловленность необходимостью защиты информации от утраты.</p> <p>4. Критерии отнесения конфиденциальной информации к защищаемой, их обусловленность необходимостью защиты информации от утраты и утечки.</p> <p>5. Условия, необходимые для отнесения информации к защищаемой.</p> <p>6. Правовые и организационные принципы отнесения информации к защищаемой.</p>
8	Состав и классификация носителей защищаемой информации	<p>Презентации по темам:</p> <p>1. Понятие "носитель защищаемой информации". Соотношение между носителем и источником информации.</p> <p>2. Состав носителей защищаемой информации. Способы фиксирования информации в носителях. Виды отображения информации в носителях. Методы воспроизведения отображенной информации в носителях информации.</p> <p>3. Носители письменной, видовой, излучаемой информации. Опосредованные носители защищаемой информации.</p> <p>4. Свойства и значение типов носителей защищаемой информации.</p>
9	Классификация защищаемой информации	<p>Презентации по темам:</p> <p>1. Понятие "тайна информации".</p> <p>2. Типовая классификация защищаемой информации.</p> <p>3. Содержание понятия секретная и конфиденциальная</p>

		<p>информация.</p> <p>4. Виды тайны конфиденциальной информации.</p> <p>5. Показатели разделения конфиденциальной информации на виды тайны.</p> <p>6. Степени и грифы конфиденциальности информации.</p>
10	Основы защиты государственной тайны	<p>Подготовка рефератов по темам:</p> <p>1. Становление и современное определение понятия "государственная тайна". Основания и организационно-правовые формы отнесения информации к государственной тайне.</p> <p>2. Функции должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне.</p> <p>3. Перечень сведений, являющихся государственной тайной, их назначение и структура. Степени секретности сведений, отнесенных к государственной тайне. Критерии отнесения сведений к различным степеням секретности.</p> <p>4. Грифы секретности носителей информации. Различия между степенью и грифом секретности. Основания для рассекречивания информации.</p>
11	Основы защиты коммерческой и служебной тайны	<p>Подготовка рефератов по темам:</p> <p>1. Становление и современное определение коммерческой тайны. Место коммерческой тайны в системе предпринимательской деятельности.</p> <p>2. Основания и методика отнесения сведений к коммерческой тайне.</p> <p>3. Степени конфиденциальности сведений, составляющих коммерческую тайну.</p> <p>4. Функции государства в сфере защиты коммерческой тайны. Тенденция и определяющие факторы развития коммерческой тайны.</p>

		<p>5. Современные подходы к сущности служебной тайны. Понятие служебной тайны, границы и области ее действия.</p> <p>6. Распределение полномочий по отнесению сведений к служебной тайне.</p> <p>7.</p>
12	Основы защиты личной и профессиональной тайны	<p>Подготовка рефератов по темам:</p> <p>1. Понятия "личная тайна", "защищаемая информация о гражданах (персональные данные)".</p> <p>2. Категории информации, отнесенной к персональным данным.</p> <p>3. Разновидности личной тайны. Функции государства и граждан в сфере защиты личной тайны и персональных данных.</p> <p>4. Понятие и особенности профессиональной тайны. Сфера действия профессиональной тайны.</p> <p>5. Соотношение между профессиональной и другими видами тайны.</p> <p>6. Разновидности профессиональной тайны.</p> <p>7. Понятие интеллектуальной собственности.</p> <p>8. Различие между правом собственности и авторским правом.</p> <p>9. Объекты (предметы) интеллектуальной собственности как составная часть защищаемой информации.</p>
13	Понятие и структура угроз защищаемой информации	<p>Подготовка рефератов по темам:</p> <p>1. Современные подходы к понятию угрозы защищаемой информации.</p> <p>2. Связь угрозы защищаемой информации с уязвимостью информации.</p> <p>3. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации.</p>

		4. Структура явлений как сущностного выражения угрозы защищаемой информации.
14	Дестабилизирующие воздействия на защищаемую информацию	<p>Подготовка рефератов по темам:</p> <ol style="list-style-type: none"> 1. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию. 2. Состав и характеристика источников дестабилизирующего воздействия на информацию. 3. Виды и способы дестабилизирующего воздействия на информацию со стороны различных источников. 4. Причины, вызывающие преднамеренное и непреднамеренное дестабилизирующее воздействие на информацию со стороны людей. 5. Обстоятельства (предпосылки), способствующие появлению этих причин. 6. Условия, создающие возможность для дестабилизирующего воздействия на информацию. 7. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны других источников воздействия.
15	Каналы и методы несанкционированного доступа к защищаемой информации	<p>Подготовка рефератов по темам:</p> <ol style="list-style-type: none"> 1. Канал несанкционированного доступа к защищаемой информации как составная часть угрозы информации. 2. Современные подходы к понятию канала несанкционированного доступа к информации. Соотношение между каналами несанкционированного доступа и каналами утечки информации, их сущность и понятия. 3. Состав и характеристика каналов несанкционированного доступа к конфиденциальной информации. Специально создаваемые и потенциально существующие каналы

		<p>несанкционированного доступа.</p> <p>4. Методы несанкционированного доступа к защищаемой информации. Зависимость методов и форм их использования от целей и возможностей соперника.</p> <p>5. Существующая классификация каналов и ее недостатки.</p>
16	Характеристика деятельности разведывательных служб по несанкционированному доступу	<p>Подготовка рефератов по темам:</p> <p>1. Структура государственных разведывательных органов ведущих зарубежных стран.</p> <p>2. Органы политической, военной и радиотехнической разведки.</p> <p>3. Структура разведывательных служб частных объединений.</p> <p>4. Направления и виды разведывательной деятельности, их соотношение и взаимосвязь.</p> <p>5. Особенности деятельности разведывательных органов, их сочетание при добывании информации.</p>
17	Объекты защиты информации	<p>Подготовка рефератов по темам:</p> <p>1. Понятие объекта защиты.</p> <p>2. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты.</p> <p>3. Состав и характеристика объектов хранения письменных и видовых носителей информации, подлежащих защите.</p> <p>4. Состав, подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации.</p> <p>5. Виды и способы дестабилизирующего воздействия на</p>

		объекты защиты.
18	Виды и методы защиты информации	<p>Подготовка рефератов по темам:</p> <p>Виды защиты информации, сферы их действия.</p> <p>Классификация методов защиты информации.</p> <p>Универсальные методы защиты информации, область их применения.</p> <p>Области применения организационных, криптографических и инженерно-технических методов защиты информации.</p>
19	Классификация и характеристика средств защиты информации	<p>Подготовка рефератов по темам:</p> <p>Понятие «средства защиты информации».</p> <p>Классификация средств защиты информации.</p> <p>Назначение и общая характеристика программных средств защиты.</p> <p>Назначение и общая характеристика криптографических средств защиты.</p> <p>Назначение и общая характеристика технических средств защиты.</p>
20	Основные виды обеспечения защиты информации	<p>Подготовка рефератов по темам:</p> <p>Значение и состав кадрового обеспечения защиты информации. Полномочия руководства предприятия в области защиты информации. Полномочия специальных комиссий по защите информации. Полномочия службы защиты информации. Полномочия пользователей защищаемой информации.</p> <p>Состав и назначение ресурсного обеспечения защиты информации. Характеристика основных видов ресурсного обеспечения защиты информации: финансовое; материальное; техническое; энергетическое; информационное; временное; пространственное.</p> <p>Значение ресурсного обеспечения для организации эффективной защиты информации.</p>

		<p>Понятие и назначение технологического обеспечения защиты информации. Классификация организационно-технологических документов по защите информации. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий.</p> <p>Понятие о процессе проектирования и внедрения целесообразных мер по защите информации. Виды проектирования и их особенности. Характеристика основных этапов проектирования. Разрабатываемые документы в ходе проектирования и внедрения мер по защите.</p>
21	Системы защиты информации	<p>Подготовка рефератов по темам:</p> <p>Понятие "система защиты информации". Назначение систем защиты информации. Классификация систем защиты информации, сферы их действия. Структура систем защиты информации.</p> <p>Общая характеристика типовых подсистем защиты информации (программно-аппаратной, криптографической, физической, организационной, управления, инженерно-технической и др.).</p> <p>Сущность и значение комплексной системы защиты информации как основная форма организации деятельности по защите информации.</p> <p>Структура комплексной системы защиты информации, назначение составных частей системы.</p> <p>Требования к подсистемам защиты информации и, в целом, к комплексной системе защите информации.</p>
22	Основы управления защитой информации	<p>Подготовка рефератов по темам:</p> <p>Сущность и значение управления защитой информацией в современных условиях.</p> <p>Виды управления защитой информацией.</p> <p>Органы и средства управления защитой</p>

		<p>информацией.</p> <p>Типовые функции управления защитой информации.</p> <p>Документы, обрабатываемые в ходе управления защитой информацией.</p>
23	<p>Методологические подходы оценки эффективности защиты информации</p>	<p>Подготовка рефератов по темам:</p> <p>Понятие об эффективности защиты информации в целом и отдельных ее процессов.</p> <p>Основы моделирования эффективности защиты информации.</p> <p>Функциональная и экономическая оценка эффективности защиты информации.</p> <p>Качественные и количественные показатели и критерии эффективности защиты информации. Понятия об ущербах и информационных рисках. Виды ожидаемых ущербов.</p> <p>Существующие проблемы при оценке эффективности защиты информации.</p>

5. Указания по проведению контрольных работ для студентов факультета заочного обучения

Не предусмотрены учебным планом.

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

Основная литература:

1. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации : учебное пособие. - М. : Форум, 2011 г;
2. Малюк А.А. Теория защиты информации. Научное издание.- М.: Горячая линия-телеком, 2013 г.;
3. Зайцев, А.П. и др. Технические средства и методы защиты информации: учебное пособие для вуза / под. ред. А. П. Зайцева, А. А. Шелупанова. - 4-е

изд., испр. и доп. - М. : Горячая линия-Телеком, 2012 г.;

4. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах : учебное пособие для вузов. - 4-е изд., стереотип. - М. : Горячая линия - Телеком, 2011 г.

Дополнительная литература:

1. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах : учеб. пособие. - М. : ИД "ФОРУМ" : ИНФРА-М, 2013 г.;
2. Мельников, Д.А. Информационная безопасность открытых систем: учебник. - М.: ФЛИНТА, 2013 г.;
3. Грибунин, В.Г. Комплексная система защиты информации на предприятии : учеб. пособие. - М.: Академия ИЦ, 2009 г.;
4. Ворона В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. - М.: Горячая линия-Телеком, 2013 г.;
5. Чипига, А.Ф. Информационная безопасность автоматизированных систем : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности - М. : Гелиос АРВ, 2010 г.;
6. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность: учебное пособие. - М.: ФОРУМ, 2013 г.

Рекомендуемая литература:

1. Анин Б.Ю. Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000.
2. Волокитин А.В. Информационная безопасность государственных организаций и коммерческих фирм. - М: ИНФО, 2002.
3. Девянин П.Н. и др. Теоретические основы компьютерной безопасности / - М.: Радио и связь, 2000.
4. Домарев В.В. Безопасность ИТ. Системный подход. – К.: ООО «ТИД «ДС»», 2004.
5. Байбурин В.Б. и др. Введение в защиту информации. Учебное пособие для вузов - М: ИНФРА-М, 2004.
6. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов.– М.: Горячая линия-Телеком, 2004.
7. Сидак А.А. Формирование требований безопасности современных сетевых информационных технологий. - М.: МГУЛ, 2001.
8. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - 2-е изд. - М.: Радио и связь, 2001.

9. Общие критерии оценки безопасности информационных технологий: Учеб. пособие/ Пер. с англ. Е.А. Сидак. - М.: ЦБИ, 2001.
10. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. - СПб.: БХВ-Петербург, 2000.

Электронные книги:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013 г.
<http://znanium.com/bookread.php?book=405000>
2. Жук А. П.Жук Е ПЛепешкин О МТимошкин А И. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура).
<http://znanium.com/bookread.php?book=474838>
3. Бабаш А В., Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013 г.
<http://znanium.com/bookread.php?book=405000>
4. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013 г.
<http://znanium.com/bookread.php?book=415501>

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

Интернет-ресурсы:

1. <http://eup.ru> – научно - образовательный портал.
2. <http://znanium.com> – образовательный портал
3. <http://www.academy.it> – академия АЙТИ

8. 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: MSOffice, PowerPoint.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды;
2. Рабочая программа и методическая обеспечение по дисциплине: «Основы информационной безопасности».

Ресурсы информационно-образовательной среды МГОТУ:

Рабочая программа и методическое обеспечение по курсу «Основы информационной безопасности».