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

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

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Специальность: 38.05.01 «Экономическая безопасность»
Специализация: «Экономико-правовое обеспечение экономической безопасности»
Уровень высшего образования: специалитет
Квалификация (степень) выпускника: экономист
Форма обучения: очная, заочная

Королев
2023

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

Автор: преподаватель Ульянов Д.В. Рабочая программа дисциплины: «Основы информационной безопасности». – Королев МО: «Технологический университет», 2023.

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

Программа составлена в соответствии с требованиями федерального Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 «Экономическая безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол **№ 9 от 11 апреля 2023 г.**

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Сапунов В.К., к.в.н., доцент				
Год утверждения (переутверждения)	2023	2024	2025	2026	2027
Номер и дата протокола заседания кафедры	№ 8 от 29.03.2023 г.				

Рабочая программа согласована:
Руководитель ОПОП_____ к.э.н., доцент Коба Е.Е.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026	2027
Номер и дата протокола заседания УМС	№ 5 от 11.04.2023 г.				

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**:**

- УК-1: способность осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;
- ПК-4: способность создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационному обеспечению системы стратегического управления рисками.

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:

- методические материалы, регламентирующие работу по защите информации;
- технологии защиты информации, безопасной системы внутренней и

внешней коммуникации и отчетности;
- положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности;
- принципы и требования обеспечения сохранения государственной и коммерческой тайны и конфиденциальной информации;
- действующее российское законодательство в сфере защиты государственной и коммерческой тайны и конфиденциальной информации;
- методику проведения анализа проблемной ситуации как системы, ее составляющие и связи между ними.

Уметь:
- разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации;
- осуществлять выбор средств и технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности;
- использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности;
- решать поставленные задачи в области системных и прикладных вопросов защиты информации в системах электронного документооборота на основе действующего российского законодательства с помощью современных принципов, методов и средств в различных организационных структурах, по базовым направлениям защиты государственной и коммерческой тайны и конфиденциальной информации;
- проводить анализ проблемной ситуации как системы, выявляя ее составляющие и связи между ними.

2. Место дисциплины в структуре ОПОП

Дисциплина относится к вариативной части дисциплин по выбору Блока 1 основной образовательной программы подготовки специалиста по направлению подготовки 38.05.01 «Экономическая безопасность».

Дисциплина базируется на ранее изученной дисциплине: «Введение в специальность».

Знания и компетенции, полученные при освоении дисциплины, являются базовыми при изучении дисциплин: «Экономическая безопасность», «Национальная безопасность», «Безопасность банковских и платежных ИС», «Информационная аналитическая деятельность по обеспечению информационной безопасности» и выполнении выпускной квалификационной работы специалиста.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и заочной формы обучения составляет 3 зачетных единицы, 108 академических часов.

Виды занятий	**Всего часов**	**Семестр** 2	**Семестр** 3	**Семестр** …	**Семестр** …
Общая трудоемкость	**108**		**108**		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**48**		**48**		
Лекции (Л)	**16**		**16**		
Практические занятия (ПЗ)	**32**		**32**		
Лабораторные работы (ЛР)					
Самостоятельная работа	**60**		**60**		
КСР	-		-		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+ -		+ -		
Текущий контроль знаний	**Тесты**		**Тесты**		
Вид итогового контроля	**Экзамен**		**Экзамен**		
ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**12**		**12**		
Лекции (Л)	**4**		**4**		
Практические занятия (ПЗ)	**8**		**8**		
Лабораторные работы (ЛР)					
Самостоятельная работа	**96**		**96**		
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+ -	+ -			
Вид итогового контроля	**Экзамен**	**Экзамен**			

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Наименование тем	Лекции, час. очное/заочное	Лабораторная работа, час.	Практические занятия, час	Занятия в интерактивной форме,	Код компетенций

		очное/заочное	очное/заочное	час очное/заочное	
Раздел 1. Базовые положения по информационной безопасности					
Тема 1. Сущность и понятие информационной безопасности	1/0.25		3/0.5	2/0.5	УК-1, ПК-4
Тема 2. Значение информационной безопасности и ее место в системе национальной безопасности. Доктрина информационной безопасности РФ	1/0.25		3/0.5	2/0.5	УК-1, ПК-4
Тема 3. Сущность и теоретико-концептуальные основы защиты информации	2/0.25		3/1	2/1	УК-1, ПК-4
Раздел 2. Характеристика защищаемой информации					
Тема 4. Критерии, условия и принципы отнесения информации к защищаемой. Состав и классификация ЗИ и их носителей	2/0.25		3/1	3/1	УК-1, ПК-4
Тема 5. Основы защиты государственной, коммерческой, служебной, личной и профессиональной тайн	2/0.5		4/1	3/1	УК-1, ПК-4
Раздел 3. Условия, определяющие необходимость защиты информации					
Тема 6. Дестабилизирующие воздействия на защищаемый информационный ресурс. Каналы и методы противоправных действий в информационной безопасности	2/0.5		4/1	3/1	УК-1, ПК-4
Тема 7. Характеристика	2/0.5		4/1	3/1	УК-1, ПК-4

деятельности разведывательных служб по несанкционированному доступу к защищаемому информационному ресурсу					
Раздел 4. Характеристика основных мер по защите информации					
Тема 8. Основные виды обеспечение, системы и средства защиты информации (информационной безопасности)	2/0.5		4/1	3/1	УК-1, ПК-4
Тема 9. Основы управления и оценки эффективности защиты информации	2/1		4/1	3/1	УК-1, ПК-4
Итого:	16/4		32/8	24/8	

4.2. Содержание тем дисциплины

Раздел 1. Базовые положения по информационной безопасности

Тема 1. 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. Доктрины информационной безопасности Российской Федерации

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.

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 3. Сущность и теоретико-концептуальные основы 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.

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.

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 4. Критерии, условия и принципы отнесения информации к защищаемой. Состав и классификация защищаемой информации и их носителей

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.

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.

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 5. Основы защиты государственной, коммерческой, служебной, личной и профессиональной тайн

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.

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.

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.

Раздел 3. Условия, определяющие необходимость защиты информации

Тема 6. Дестабилизирующие воздействия на защищаемый информационный ресурс. Каналы и методы противоправных действий в информационной безопасности

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.

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.

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 противоправных действий с защищаемой информацией.

Тема 7. Характеристика деятельности разведывательных служб по несанкционированному доступу к защищаемому информационному ресурсу

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.

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 8. Основные виды обеспечение, системы и средства защиты информации (информационной безопасности)

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.

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.

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.

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 9. Основы управления и оценки эффективности защиты 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, отрабатываемые в ходе управления защитой информацией.

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. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 3-е изд., доп. - М.: Форум , 2016. - 240 с.: ил.; 60x90 1/16. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-00091-007-8http://znanium.com/bookread2.php?book=491597

2. Моргунов А.В. Информационная безопасность: учебно - методическое пособие, Новосибирский государственный технический университет, Новосибирск, 2019.

3. Информационная безопасность: учебное пособие под общ. редакцией проф. Ясенева В.Н.; Министерство образования и науки Российской Федерации, Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского - Нижний Новгород, 2017. - 198 с. : УДК

311(075.8) ББК У051; [Электронный ресурс]:
http://www.iee.unn.ru/wp-content/uploads/sites/9/2014/09/Uchebnoe-posobie-po-IB-pod-redaktsiej-YAseneva-V.N.-2017.pdf

Дополнительная литература:

1. Балдин К.В., Информационные системы в экономике: учебник; Дашков и Ко; М. 2021;
2. Е.В. Вострецова, Основы информационной безопасности; Учебное пособие; Министерство образования и науки Российской Федерации, Уральский федеральный университет, Екатеринбург, Издательство Уральского университета 2019; 204 с., ISBN 978-5-7996-2677-8, https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
3. Безопасность объектов критической информационной инфраструктуры организации. Общие рекомендации (версия 1.0); АРСИБ, Москва 2019, http://aciso.ru/news/3948/
4. А. Першин, Безопасность мобильных технологий в корпоративном секторе. Общие рекомендации (версия 2.0); АРСИБ, Москва 2016, http://aciso.ru/news/3901/

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

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 методическая обеспечение по дисциплине: «Основы информационной безопасности».

Ресурсы информационно-образовательной среды МГОТУ:

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

2. 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.

Приложение 1

ИНСТИТУТ 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)

Специальность: 38.05.01 Экономическая безопасность

Специализация: экономико-правовое обеспечение экономической безопасности

Квалификация (степень) выпускника: экономист

Форма обучения: очная, заочная

Королев
2023

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.	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Тема1. - 4.	Методики проведения анализа проблемной ситуации как системы, ее составляющих и связи между ними; Знать методику разработки стратегий решения проблемных ситуаций на основе системного и междисциплинарных подходов	Проводить анализ проблемной ситуации как системы, выявляя ее составляющие и связи между ними; Уметь разрабатывать и аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов	Анализировать проблемную ситуацию как систему, выявляя ее составляющие и связи между ними; Разрабатывать и содержательно аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.
2.	ПК-4	Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-	Тема 5. - 9.	Знать методические материалы, регламентирующие работу по защите информации Знать технологии защиты информации, безопасной системы внутренней и внешней коммуникац	Уметь разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации и осуществлять выбор средств и	Разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации, предлагать технологии защиты информации, безопасную систему внутренней и внешней

		информационному обеспечению системы стратегического управления рисками		ии и отчетности	технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности	коммуникации и отчетности

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**	**Шкала и критерии оценки**
УК-1	Доклад в форме презентации	A) компетенция не сформирована B) сформирована частично C) сформирована полностью	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-4	Реферат	A) компетенция не сформирована B) сформирована частично C) сформирована полностью	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-4	Доклад в форме презентации	A) компетенция не сформирована B) сформирована частично C) сформирована полностью	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-4	Контрольная работа	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	1. Проводится устно в форме защиты отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-4	Реферат	А) компетенция не сформирована В) сформирована частично С)	Проводится в письменной форме Критерии оценки: 1.Соответствие содержания реферата заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке

		сформирована полностью	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.

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

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.

Тематика рефератов:

1. Программы компьютерного слежения и радиоэлектронной разведки в США, Великобритании, КНР и других странах.
2. Информационное общество и проблема его безопасности.
3. Российская экономика и ее информационная безопасность.
4. ФСТЭК и ФСБ как регуляторы деятельности в области информационной безопасности.
5. Защита информации в деятельности государственного предприятия.
6. Вопросы информационной безопасности в критической информационной инфраструктуре (КИИ) - нормативные документы, терминология и технологические решения.
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.
17. Квантовые компьютеры. Разработки, перспективы применения и влияние на тематику информационной безопасности.
18. Технология «блокчейн». Состояние на настоящее время и перспективы ее использования.

Тематика эссе:

1. Понятие национальной безопасности РФ и место в ней информационной безопасности.
2. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
3. Правовая база обеспечения информационной безопасности личности (общества, государства) в РФ.
4. Понятие и общая характеристика основ теории информационной безопасности.
5. Виды защищаемой информации.
6. Общеметодологические принципы теории информационной безопасности.
7. Интересы личности, общества и государства в информационной

сфере.

8. Угрозы информационной безопасности Российской Федерации.

9. Внешние и внутренние источники угроз информационной безопасности государства.

10. Проблемы региональной информационной безопасности.

11. Информационное оружие, его классификация и возможности.

12. Методы нарушения конфиденциальности, целостности и доступности информации.

13. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.

14. Обеспечение информационной безопасности компьютерных систем.

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 экзамена.

Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов

Тестирование (Т1)	УК-1 ПК-4	30 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 45 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Тестирование(Т2)	УК-1 ПК-4	30 вопросов	Компьютерное тестирование; время отведенное на процедуру – 45 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Экзамен	УК-1 ПК-4	2 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время отведенное на процедуру – 4 часа.	Результаты предоставляются в день проведения зачета	Критерии оценки: **«Отлично»:** • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на семинарских занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета.

					«Хорошо»: • умение использовать и применять полученные знания на практике; • работа на семинарских занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. **«Удовлетворительно»:** • ответ на вопросы билета. • работа на семинарских занятиях; **«Неудовлетворительно»**: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на семинарских занятиях; • не отвечает на вопросы.

Типовые вопросы, выносимые на тестирование

1. Технология VPN может обеспечивать

Целостность, аутентификацию и конфиденциальность передаваемых сообщений

Устойчивую связь на каналах плохого качества

Помехозащищенность передаваемых сообщений

Все перечисленное выше.

2. Внедрение СКУД и современных «интеллектуальных» систем видеонаблюдения позволяет

Повысить капитализацию и инвестиционную привлекательность предприятия

Построить один из «рубежей» комплексной системы информационной безопасности объекта

Эффективно осваивать бюджет СЭБ предприятия

3. Увеличение отношения «сигнал/шум» обеспечивает

надежность передачи сигнала в канале связи

снижение вероятности перехвата опасных сигналов на границе контролируемой зоны

качество воспроизведения сигнала в системах звукоусиления

4. Какой фрагмент шифртекста при шифровании «по Шеннону» соответствует фрагменту 001011010010101 открытого текста при использовании фрагмента ключа шифрования 101101001011000

001011011010011

100110011001101

101100101010110

Правильный фрагмент отсутствует

5. Для активной защиты от утечки речевого сигнала лучше использовать

«Белый шум» в частотном диапазоне от 150 Гц до 8 кГц

«Розовый шум» в частотном диапазоне от 300 Гц до 3.4 кГц

Гармонические сигналы в частотном диапазоне от 20 Гц до 20 кГц

6. Какое утверждение относительно технологии блокчейн вы считаете наиболее верным, полным и объективным

Технология блокчейн обеспечивает анонимность платежей криптовалютами для использования в «теневой экономике» и иных противоправных целях

Блокчейн позволяет создавать криптовалютные «финансовые пирамиды»

Блокчейн - основанная на децентрализованном шифровании с «открытым ключом» технология с перспективами применения в самых разных сферах

Блокчейн - способ зарабатывания биткоинов для майнеров

7. Условием абсолютной стойкости шифра по Шеннону является

Однократное использование ключа шифрования

Использование в «открытом тексте» только цифр и символов латинского алфавита

Статистическая надежность ключа шифрования

Длина ключа шифрования должна быть больше или равна длине исходного сообщения

8. Какие критерии используются для принятия решений в условиях неопределенности

Фурье и Лагранжа

Вальда, Сэвиджа и Гурвица

Бойля и Мариотта

9. TEMPEST это

Принятый в США руководящий документ по противодействию средствам и методам РЭБ в Вооруженных силах блока НАТО

Действующий в США и ряде стран Западной Европы набор стандартов, определяющих защищенность технических средств и объектов от утечки информации по каналу ПЭМИН

Протокол шифрования данных, используемый в системе управления средствами ПВО США

10. Информационная безопасность крупного корпоративного центра обработки данных (ЦОД) обеспечивается

Резервированием каналов связи

Использованием ИБП и резервного электропитания

Системой защиты от НСД к объекту размещения ЦОД, его отдельным серверам и иным компонентам

Внедрением межсетевых экранов, антивирусной защиты и системы DLP

Криптографической защитой передаваемой по каналам связи информации

Всеми перечисленными методами

11. Как определяется понятие «информация» в 149-ФЗ от 27.07.06

Универсальный товар в период развития цифровой экономики

Сведения, сообщения, данные, независимо от формы их представления

Объективное содержание связи между взаимодействующими материальными объектами, проявляющееся в изменении состояния этих объектов

Любые данные, содержащиеся в электронных и печатных документах, имеющих все необходимые реквизиты

12. Какие каналы утечки речевой конфиденциальной информации принято выделять при ведении переговоров в типовом офисном помещении

Акустический и виброакустический

Визуальный

Акустоэлектрический

Все перечисленные выше

13. Что означает сокращение ФСТЭК

Фонд Содружества Технологических и Электротехнических Комиссий

Федеральная Служба по Техническому и Экспортному Контролю

Федеральная Система Технической и Экономической Координации

14. Понятие «Red Equipment» стандарта TEMPEST соответствует

BTCC

OTCC

Измерительному оборудованию, используемому для оценки защищенности от утечек по каналу ПЭМИН

15. Какие меры противодействия доступу к конфиденциальной информации с использованием СТС могут быть реализованы коммерческим предприятием

Введение особого порядка допуска на территорию и в выделенные помещения

Получение статуса субъекта ОРД и реализация «встречных мер» в отношении конкурентов

Периодическое проведение спецобследований выделенных помещений - собственными силами или с привлечением имеющих лицензии фирм

Подавление СТС техническими средствами в период проведения конфиденциальных мероприятий

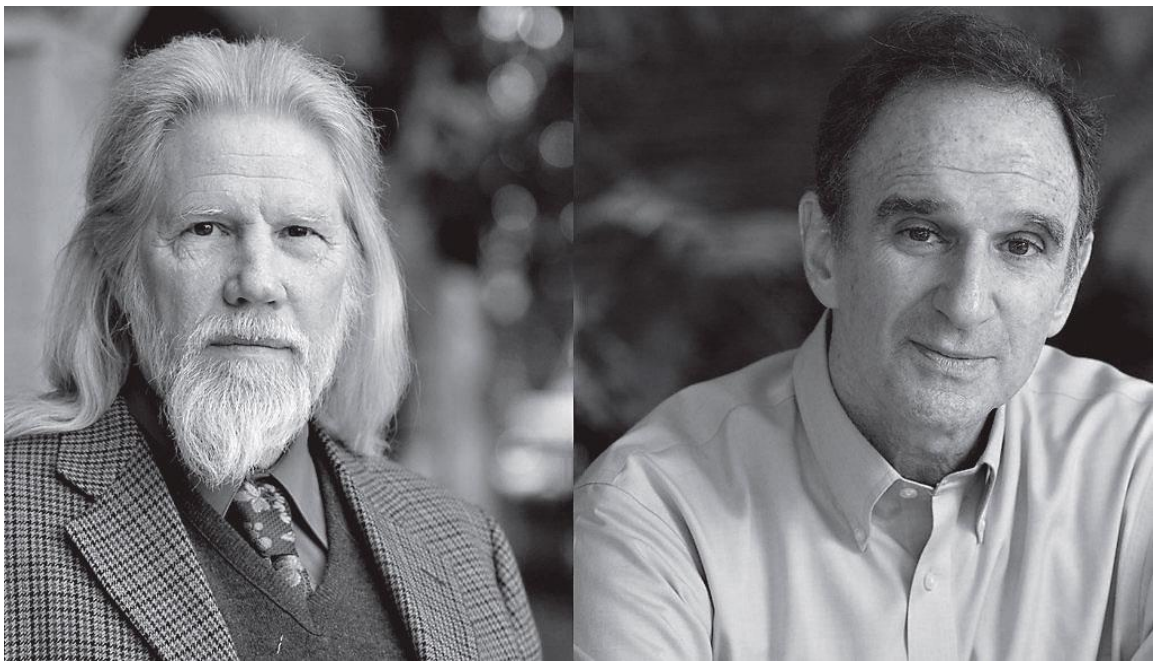
16. Наиболее точные результаты СИ достигаются в условиях

Проведения исследований на объекте, где эксплуатируются технические средства

Специализированной лаборатории с использованием аттестованной безэховой экранированной камеры

Полигона с минимальными индустриальными помехами

17. На фотографиях изображены



У. Диффи и М. Хеллман

Р. Ривест и А. Шамир

Д. Леннон и П. Маккартни

18. Какие органы государственной власти относятся к «Регуляторам» деятельности в области информационной безопасности

Роскомнадзор и Министерство цифрового развития, связи и массовых коммуникаций

ФСТЭК и ФСБ

Совет безопасности Российской Федерации и Администрация Президента Российской Федерации

19. Кто из перечисленных ученых - академиков внес значительный вклад в развитие информационной безопасности в СССР

И.В. Курчатов и А.Д. Сахаров

Н.Г. Басов и А.М. Прохоров

В.А. Котельников и А.Н. Колмогоров

20. К субъектам КИИ относятся

Предприятия ВПК

Системообразующие сетевые предприятия розничной торговли

Предприятия ТЭК и отрасли связи

Предприятия финансового сектора

Крупнейшие строительные компании

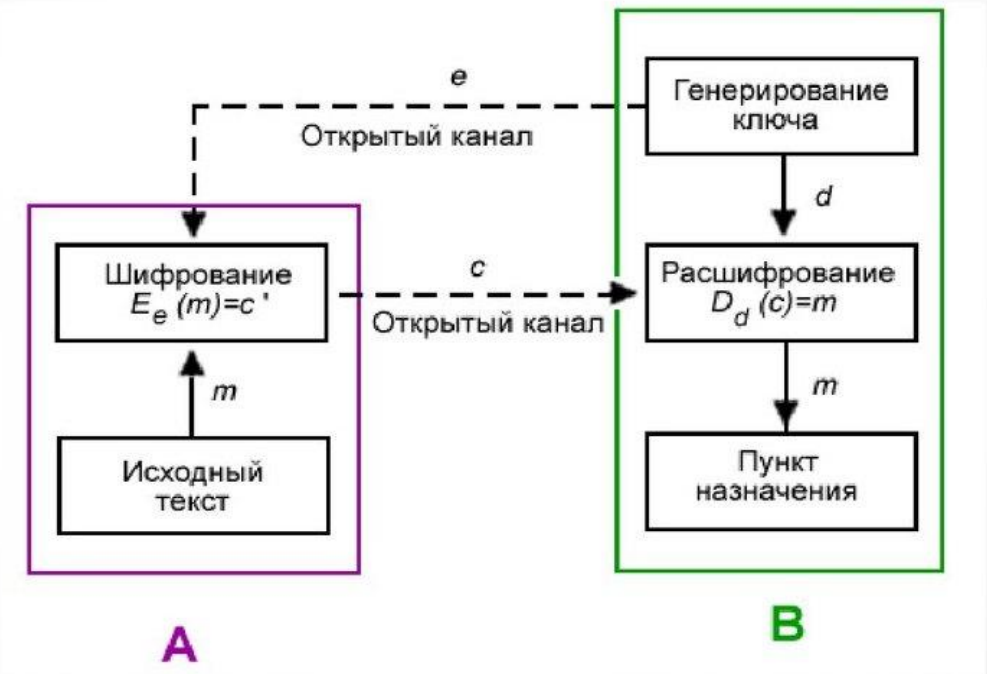
21. Какой алгоритм реализует программа PGP

Шифрования с симметричным ключом

Шифрования с «открытым» ключом

Стеганографического преобразования информации

22. На рисунке изображена структурная схема



Обработки почты при конфиденциальном делопроизводстве

Помехозащищенного кодирования

Шифрования с «открытым» ключом

Шифрования по Шеннону

23. Защита информации от утечки по каналу ПЭМИН обеспечивается

Использованием специализированных электронных компонентов и схемотехнических решений

Применением экранирования электромагнитных полей и фильтрацией в цепях распространения сигналов

Зашумлением объекта защиты с использованием сертифицированных генераторов электромагнитных помех

Всеми перечисленными методами

24. Triple DES это

Разработанный и применяемый в США стандарт симметричного шифрования

Модификация DES, обеспечивающая лучшую криптографическую стойкость

Национальный Японский стандарт шифрования с «открытым» ключом

25. Безопасность информации обеспечивается при сохранении ее

Конфиденциальности

Целостности

Доступности

Выполнении всех трех перечисленных выше условий

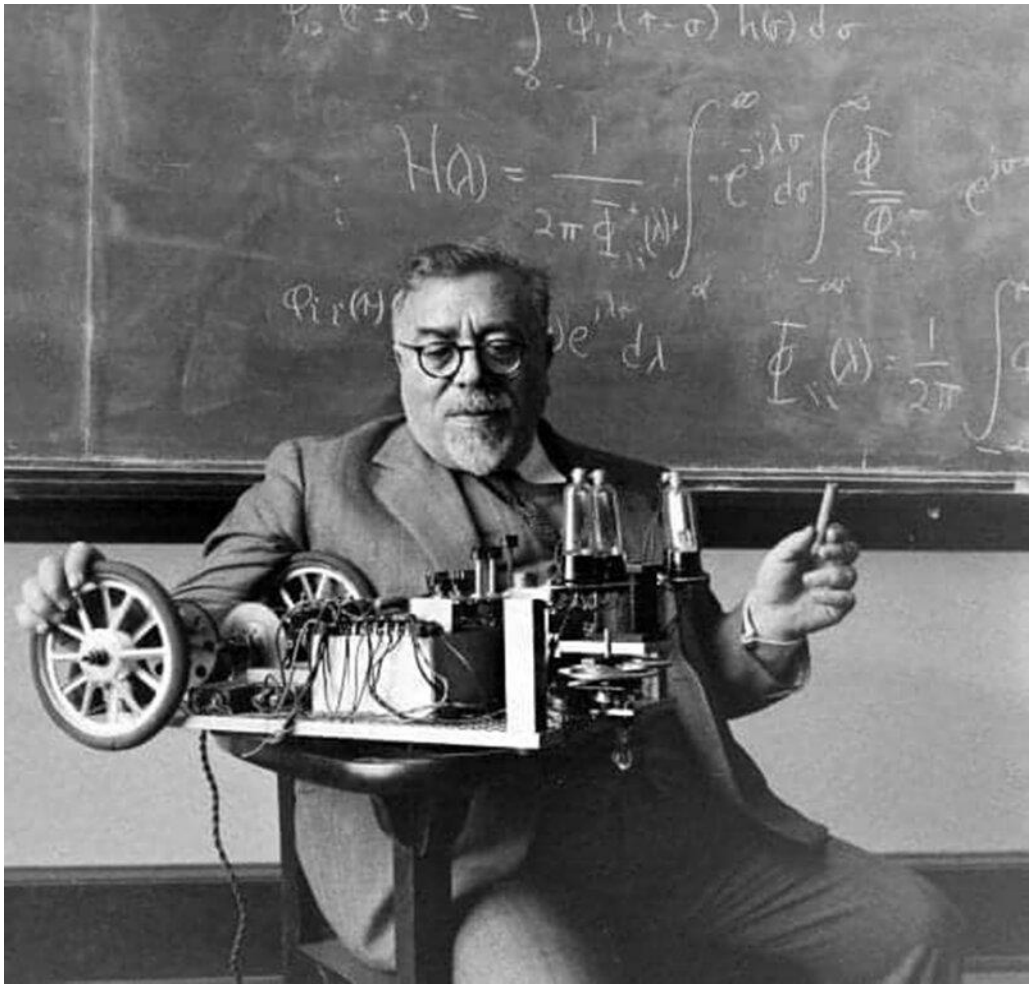
26. Стандартный протокол шифрования А5, применяемый в сетях сотовой подвижной связи GSM-900, обеспечивает защиту передаваемой информации

Во всем тракте передачи информации – от абонентского устройства до абонентского устройства

От базовой станции до Центра коммутации оператора связи

Только в радиоканале от абонентского устройства до работающей с ним базовой станции

27. Выберите из представленных изображений фотографию академика В.А. Котельникова



28. Стеганография это

Разновидность методов блочного шифрования

Метод защиты информации, в котором используется сокрытие самого факта наличия информации

Система помехоустойчивого кодирования с применением векторной графики

29. Пассивная защита от утечки информации по виброакустическому каналу обеспечивается

Применением демпфирующих вставок на трубах систем отопления и водоснабжения и ослабляющих звук экранов перед элементами данных систем

Применением подключаемых к генератору шума вибродатчиков, устанавливаемых на трубах систем отопления и водоснабжения, оконных рамах и стеклах

Специальной конструкцией стеклопакетов и крепления оконных рам в стенах здания

30. Инциденты информационной безопасности, связанные с нарушением доступности, могут вызываться

DDoS атакой на информационную инфраструктуру

Аварийным отключением электропитания оборудования ЦОД

Разрушением или блокированием каналов связи

Деструктивным компьютерным вирусом, заразившим серверное оборудование или ПК и блокирующим их работу

Всеми указанными выше причинами.

Типовые задания к проверочным работам

Вариант 1

1. Критерии обеспеченности информационной безопасности. Примеры нарушений по каждому критерию.
2. ПЭМИН как канал утечки информации. Причины возникновения и меры противодействия.

Вариант 2

1. Комплексный подход к вопросам защиты информации. Примеры инцидентов (не менее двух) при отсутствии комплексного системного подхода к защите.
2. Каналы утечки речевой конфиденциальной информации. Типовые меры защиты.

Типовые вопросы к экзамену

1. Понятие Концепции национальной безопасности РФ и место в ней информационной безопасности.
2. Общая характеристика организационных структур разведок развитых зарубежных стран.
3. Сущность Доктрины информационной безопасности РФ. Источники угроз в информационной сфере.
4. Основные задачи обеспечения ИБ РФ (по Доктрине ИБ).
5. Государственная политика обеспечения ИБ РФ (по Доктрине ИБ).
6. Организационная основа системы обеспечения ИБ РФ (по Доктрине ИБ).
7. Основные федеральные законы РФ в области ИБ.
8. Цели, функции и задачи защиты информации.
9. Защита информации и проблема «информационной войны».
10. Понятие о Концепции и стратегиях защиты информации.
11. Критерии отнесения информации к защищаемой.
12. Понятие носителей защищаемой информации, их состав.
13. Определение «государственной тайны» и порядок отнесения к ней сведений.
14. Определение «коммерческой тайны» и порядок отнесения к ней сведений.
15. Понятие «служебной тайны», границы и области ее действия.
16. Организация взаимодействия сторон, связанного с передачей конфиденциальной информации. Понятие о NDA.
17. Понятие «персональные данные», правовые требования по их защите.
18. Понятие критической информационной инфраструктуры (КИИ). Правовые требования по ее защите.

19. Понятие и структура угроз защищаемой информации.
20. Понятие, состав и характеристика источников воздействия на защищаемую информацию.
21. Классификация методов защиты информации и их характеристика.
22. Понятие, назначение и состав кадрового обеспечения защиты информации.
23. Понятие, назначение и состав ресурсного обеспечения защиты информации.
24. Понятие, назначение и состав технологического обеспечения защиты информации.
25. Основные организационные и технологические документы по защите информации.
26. Контрольные мероприятия по защите информации. Их виды и характеристики.
27. Роль науки в деятельности, связанной с информационной безопасностью.
28. Конфиденциальность, доступность и целостность как критерии информационной безопасности.
29. Инциденты информационной безопасности, связанные с нарушением доступности и целостности. Примеры.
30. Требование комплексности при защите информации.
31. Понятия «модели угроз» и «модели нарушителя» в информационной безопасности.
32. Основные факторы и причины утечки информации.
33. Правовые и организационные методы защиты информации.
34. Основные технические каналы утечки информации.
35. Криптографическая защита информации. Основные понятия.
36. Стеганографические методы защиты информации.
37. Математические основы криптографии и криптоанализа.
38. «Классическая» криптография Шеннона.
39. Криптография с открытым ключом.
40. Физические основы информационной безопасности. Отношение сигнал/шум
41. Программа и стандарты TEMPEST, основные подходы.
42. Понятие «специальные исследования».
43. Понятие «специальные проверки».
44. Понятие «специальные обследования».
45. Понятие «основные технические средства и системы».
46. Понятие «вспомогательные технические средства и системы».
47. Основные этапы аттестации объектов информатизации на соответствие требованиям безопасности.
48. Методы защиты от утечки информации по каналу ПЭМИН.
49. Методы защиты речевой информации от утечки по акустическому и виброакустическому каналам.
50. Комплаенс в информационной безопасности.
51. Кибербезопасность как составляющая информационной безопасности.
52. Основные элементы комплексной информационной безопасности распределенной корпоративной ИТ - системы.

Приложение 2

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

(Приложение 2 к рабочей программе)

Специальность: 38.05.01 «Экономическая безопасность»

Специализация: «Экономико-правовое обеспечение экономической безопасности»

Квалификация (степень) выпускника: экономист

Форма обучения: очная, заочная

Королев
2023

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.

1. Указания по проведению практических (семинарских) занятий

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: 4/1 часов

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.

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:4/1 часов

Практическое занятие 3

Сущность и теоретико- концептуальные основы 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.

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:4/1 часов

Практическое занятие 4**.**

Критерии, условия и принципы отнесения информации к защищаемой. Состав и классификация ЗИ и их носителей

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.

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.

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:4/1 часов

Практическое занятие 5

Основы защиты государственной, коммерческой, служебной, личной и профессиональной тайн

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.

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

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.

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:4/1 часов

Практическое занятие 6

Дестабилизирующие воздействия на защищаемый информационный ресурс. Каналы и методы противоправных действий в информационной безопасности

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.

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.

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 противоправных действий в области информационной безопасности.

Продолжительность занятия:4/1 часов

Практическое занятие 7

Характеристика деятельности разведывательных служб по несанкционированному доступу к защищаемому информационному ресурсу

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.

Понятие объекта информационной 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.

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.

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.

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.

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:4/1 часов

Практическое занятие 8.

Основные виды обеспечение, системы и средства защиты информации (информационной безопасности)

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.

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:4/1 часов

2. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

1) расширить представление в области существующих современных аппаратных средств вычислительной техники;

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

Объем времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения/заочная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	60/96
Вопросы, выносимые на самостоятельное изучение	15/24
Подготовка к практическим занятиям	15/24
Подготовка докладов	15/24
Выполнение практических заданий	15/24

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

1. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
2. Информационная безопасность модели Интернет - банкинга.
3. Информационная безопасность расчетов банковскими картами в Интернете.
4. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
5. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
6. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
7. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
8. Режим счетчика (counter). Функция хеширования и ассиметричные алгоритмы.
9. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
10. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
11. Информационная безопасность при составление и направление ЭД участником – отправителем.
12. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
13. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

для заочной формы обучения:

1. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
2. Информационная безопасность модели Интернет - банкинга.
3. Информационная безопасность расчетов банковскими картами в Интернете.
4. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
5. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
6. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
7. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
8. Режим счетчика (counter). Функция хеширования и ассиметричные алгоритмы.
9. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
10. Информационная безопасность электронных платежей с помощью цифровых денег.
11. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.
12. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.
13. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
14. Информационная безопасность при составлении и направление ЭД участником – отправителем.
15. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
16. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	15/24	Изучение открытых источников

2.	Подготовка к практическим занятиям	15/24	Изучение открытых источников при подготовке доклада на выбранную тему.
4.	Тематика докладов	15/24	1. Внутренние аппаратные средства персонального компьютера 2. Внешние периферийные устройства персонального компьютера
5.	Выполнение практических заданий	15/24	Разработка аппаратного средства вычислительной техники по заданным характеристикам

Примерные темы докладов

1. Предмет, цель и задачи криптографии.
2. История криптографии.
3. Краткие сведения о криптоанализе.
4. Простейшие шифры и их свойства.
5. Системы шифрования с открытыми ключами.
6. Виртуальные частные сети.
7. Электронные цифровые подписи (электронные подписи).
8. Основные подходы к реализации PKI.
9. Компоненты и сервисы инфраструктуры открытых ключей.
10. Архитектура и топология PKI.
11. Стандарты в области PKI 50.
12. Стандарты Internet X.509 PKI (PKIX).
13. Сертификаты открытых ключей X.509.
14. Списки аннулированных сертификатов. Атрибутные сертификаты.
15. Основные требования к политике PKI.
16. Политика применения сертификатов и регламент.
17. Краткая характеристика политики PKI.
18. Набор положений политики PKI.
19. Проблемы формирования политики PKI.
20. Симметричные криптосистемы.
21. Основы теории К. Шеннона.
22. Симметричные методы шифрования.
23. Алгоритмы блочного шифрования.
24. Асимметричные системы шифрования.
25. Применение асимметричных алгоритмов.
26. Стеганография как метод защиты информации. Исторические примеры и современное состояние.
27. Хранилище сертификатов ОС MS Windows.

№ п/п	Наименование раздела дисциплины	Виды СРС
1.	Сущность и понятие информационной безопасности Значение информационной безопасности и ее место в системе национальной 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 5. Значение информационной безопасности для субъектов информационных отношений. 6. Связь между информационной безопасностью и безопасностью информации. 7. Понятие и современная концепция национальной безопасности. 8. Место информационной безопасности в системе национальной безопасности.
2	Доктрина информационной безопасности Российской Федерации	Подготовка докладов по темам: 1. Общие положения о Доктрине информационной безопасности. 2. Интересы личности, общества и государства в информационной сфере. 3. Составляющие национальных интересов в информационной сфере, пути их достижения. 4. Виды и состав угроз информационной безопасности. 5. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. 6. Общие методы обеспечения информационной безопасности. Особенности обеспечения

		информационной безопасности в различных сферах общественной жизни и в международном сотрудничестве. 7. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. 8. Организационная основа системы обеспечения информационной безопасности.
3	Сущность понятия защиты информации Теоретико-концептуальные основы защиты информации	Подготовка докладов по темам: 1. Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части. 2. Методологическая основа раскрытия сущности и определения понятия защиты информации. 3. Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. 4. Содержательная часть понятия "защита информации". Существующие подходы к определению целей защиты информации. 5. Место защиты информации в системе национальной и информационной безопасности. 6. Значение защиты информации для субъектов информационных отношений государства, общества, личности. 7. Значение защиты информации в политической, военной, экономической и других областях деятельности.

		Презентации по темам: 1. Понятие и назначение теории защиты информации. 2. Основные положения теории защиты информации: объективная необходимость и общественная потребность в защите информации; включенность ее в систему общественных отношений. 3. Зависимость защиты информации от политико-правовых, социально-экономических, военно-политических реальностей; увязка с проблемами информатизации общества; обеспечения баланса интересов личности, общества и государства. 4. Правовое регулирование и взаимный контроль субъектов информационных отношений в сфере защиты информации; содействие повышению эффективности соответствующей области деятельности. 5. Понятие и назначение концепции защиты информации. Теория защиты информации как основа концепции защиты информации. 6. Содержание концепции защиты информации, ее значение для разработки стратегии, формирования целевых программ и практических мероприятий по защите информации. 7. Уровни и виды концепции защиты информации. 8. Становление и развитие государственной концепции защиты информации. 9. Современная стратегия защиты информации.
	Организационные основы и методологические принципы защиты информации	Презентации по темам: 1. Организационные основы как необходимые условия для осуществления защиты информации. 2. Основы, обеспечивающие технологию защиты информации. 3. Основы, необходимые для обеспечения сохранности и конфиденциальности информации. 4. Значение методологических принципов защиты информации. Принципы, обусловленные

		принадлежностью, ценностью, конфиденциальностью, технологией защиты информации. 5. Факторы, обусловленные объективными тенденциями развития мирового сообщества, характер их влияния на защиту информации. 6. Факторы, обусловленные современным состоянием России. 7. Влияние политико-правовых и социально-экономических реальностей на защиту информации.
4	Критерии, условия и принципы отнесения информации к защищаемой Состав и классификация носителей защищаемой информации	Презентации по темам: 1. Современные подходы к определению состава защищаемой информации. Основа для отнесения информации к защищаемой, категории информации, подпадающие под эту основу. 2. Понятия "конфиденциальная информация", "секретная информация", "открытая информация", параметры их защиты. Понятие защищаемой информации. 3. Критерии отнесения открытой информации к защищаемой, их обусловленность необходимостью защиты информации от утраты. 4. Критерии отнесения конфиденциальной информации к защищаемой, их обусловленность необходимостью защиты информации от утраты и утечки. 5. Условия, необходимые для отнесения информации к защищаемой. 6. Правовые и организационные принципы отнесения информации к защищаемой.
		Презентации по темам: 1. Понятие "носитель защищаемой информации". Соотношение между носителем и источником информации. 2. Состав носителей защищаемой информации. Способы фиксирования информации в носителях. Виды отображения информации в носителях. Методы воспроизведения отображенной информации в носителях информации. 3. Носители письменной, видовой, излучаемой информации. Опосредованные носители защищаемой информации. 4. Свойства и значение типов носителей защищаемой информации.

5	Классификация защищаемой информации Основы защиты государственной тайны	Презентации по темам: 1. Понятие "тайна информации". 2. Типовая классификация защищаемой информации. 3. Содержание понятия секретная и конфиденциальная информация. 4. Виды тайны конфиденциальной информации. 5. Показатели разделения конфиденциальной информации на виды тайны. 6. Степени и грифы конфиденциальности информации.
		Подготовка рефератов по темам: 7. Становление и современное определение понятия "государственная тайна". Основания и организационно-правовые формы отнесения информации к государственной тайне. 8. Функции должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне. 9. Перечень сведений, являющихся государственной тайной, их назначение и структура. Степени секретности сведений, отнесенных к государственной тайне. Критерии отнесения сведений к различным степеням секретности. 10. Грифы секретности носителей информации. Различия между степенью и грифом секретности. Основания для рассекречивания информации.
	Основы защиты коммерческой и служебной тайны	Подготовка рефератов по темам: 1. Становление и современное определение коммерческой тайны. Место коммерческой тайны в системе предпринимательской деятельности. 2. Основания и методика отнесения сведений к коммерческой тайне. 3. Степени конфиденциальности сведений, составляющих коммерческую тайну. 4. Функции государства в сфере защиты коммерческой тайны. Тенденция и определяющие факторы развития коммерческой тайны. 5. Современные подходы к сущности служебной тайны. Понятие служебной тайны, границы и области ее действия. 6. Распределение полномочий по отнесению сведений к служебной тайне.
	Основы защиты личной и профессиональной тайны	Подготовка рефератов по темам: 1. Понятия "личная тайна", "защищаемая информация о гражданах (персональные данные)". 2. Категории информации, отнесенной к персональным

		данным. 3. Разновидности личной тайны. Функции государства и граждан в сфере защиты личной тайны и персональных данных. 4. Понятие и особенности профессиональной тайны. Сфера действия профессиональной тайны. 5. Соотношение между профессиональной и другими видами тайны. 6. Разновидности профессиональной тайны. 7. Понятие интеллектуальной собственности. 8. Различие между правом собственности и авторским правом. 9. Объекты (предметы) интеллектуальной собственности как составная часть защищаемой информации.

6	Понятие и структура угроз защищаемой информации Дестабилизирующие воздействия на защищаемую информацию	Подготовка рефератов по темам: 1. Современные подходы к понятию угрозы защищаемой информации. 2. Связь угрозы защищаемой информации с уязвимостью информации. 3. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации. 4. Структура явлений как сущностного выражения угрозы защищаемой информации. 5. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию. 6. Состав и характеристика источников дестабилизирующего воздействия на информацию. 7. Виды и способы дестабилизирующего воздействия на информацию со стороны различных источников. 8. Причины, вызывающие преднамеренное и непреднамеренное дестабилизирующее воздействие на информацию со стороны людей. 9. Обстоятельства (предпосылки), способствующие появлению этих причин. 10. Условия, создающие возможность для дестабилизирующего воздействия на информацию. 11. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны других источников воздействия.
	Каналы и методы несанкционированного доступа к защищаемой информации	Подготовка рефератов по темам: 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 несанкционированного доступа. 4. Методы несанкционированного доступа к защищаемой информации. Зависимость методов и форм их использования от целей и возможностей соперника. 5. Существующая классификация каналов и ее недостатки.
7	Характеристика деятельности разведывательных служб по несанкционированному доступу	Подготовка рефератов по темам: 1. Структура государственных разведывательных органов ведущих зарубежных стран. 2. Органы политической, военной и радиотехнической разведки. 3. Структура разведывательных служб частных объединений. 4. Направления и виды разведывательной деятельности, их соотношение и взаимосвязь. 5. Особенности деятельности разведывательных органов, их сочетание при добывании информации.
	Объекты защиты информации	Подготовка рефератов по темам: 1. Понятие объекта защиты. 2. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты. 3. Состав и характеристика объектов хранения письменных и видовых носителей информации, подлежащих защите. 4. Состав, подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации. 5. Виды и способы дестабилизирующего воздействия на объекты защиты.
8	Виды и методы защиты информации	Подготовка рефератов по темам: 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.
	Классификация и	Подготовка рефератов по темам:

	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.
	Основные виды обеспечение защиты информации	Подготовка рефератов по темам: 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.
	Системы защиты информации	Подготовка рефератов по темам: 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.
9	Основы управления защитой информации	Подготовка рефератов по темам: 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.
	Методологические подходы оценки эффективности защиты информации	Подготовка рефератов по темам: 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.

Указания по проведению контрольных работ для студентов факультета заочного обучения

Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.
3. В процессе изложения материала необходимо давать ссылки на используемую литературу.
4. Заключение должно содержать сделанные автором работы выводы,

итоги исследования.

5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

Рекомендуемая тематика

1. Сущность и понятие информационной безопасности
2. Значение информационной безопасности и ее место в системе национальной безопасности. Доктрина информационной безопасности РФ
3. Сущность и теоретико-концептуальные основы защиты информации
4. Характеристика защищаемой информации
5. Критерии, условия и принципы отнесения информации к защищаемой.
6. Состав и классификация ЗИ и их носителей
7. Основы защиты коммерческой тайны
8. Основы защиты государственной тайны
9. Основы защиты личной тайны
10. Основы защиты профессиональной тайны
11. Условия, определяющие необходимость защиты информации
12. Дестабилизирующие воздействия на защищаемый информационный ресурс.
13. Каналы противоправных действий в информационной безопасности
14. Методы противоправных действий в информационной безопасности
15. Характеристика деятельности разведывательных служб по несанкционированному доступу к защищаемому информационному ресурсу
16. Общая характеристика основных мер по защите информации (информационной безопасности)
17. Основные виды обеспечение, системы и средства защиты информации (информационной безопасности)
18. Основные виды обеспечение защиты информации (информационной безопасности)
19. Основные виды системы защиты информации (информационной безопасности)
20. Классификация средств защиты информации (информационной безопасности)
21. Основы управления информационной безопасности
22. Основы оценки эффективности защиты информации

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; 60х90

1/16. - (Высшее образование: Бакалавриат). (обложка) ISBN 978-5-00091-007-8http://znanium.com/bookread2.php?book=491597

2. Информационная безопасность: учебное пособие под общ. редакцией проф. Ясенева В.Н.; Министерство образования и науки Российской Федерации, Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского - Нижний Новгород, 2017. - 198 с. : УДК 311(075.8) ББК У051; [Электронный ресурс]: http://www.iee.unn.ru/wp-content/uploads/sites/9/2014/09/Uchebnoe-posobie-po-IB-pod-redaktsiej-YAseneva-V.N.-2017.pdf

Дополнительная литература:

1. Е.В. Вострецова Основы информационной безопасности; Учебное пособие; Министерство образования и науки Российской Федерации, Уральский федеральный университет, Екатеринбург, Издательство Уральского университета 2019; 204 с., ISBN 978-5-7996-2677-8, https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf

2. Безопасность объектов критической информационной инфраструктуры организации. Общие рекомендации (версия 1.0); АРСИБ, Москва 2019, http://aciso.ru/news/3948/

3. А. Першин, Безопасность мобильных технологий в корпоративном секторе. Общие рекомендации (версия 2.0); АРСИБ, Москва 2016, http://aciso.ru/news/3901/

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

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

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
2. **http://informika.ru/** – образовательный портал.
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. –

Публикации, статьи.

4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
6. **http://www.academy.it.ru/** - академия АЙТИ.
7. **http://www.minfin.ru/** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации.
9. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

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