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

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ»

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: Пономаренко Г.В. Рабочая программа дисциплины: «Информационная безопасность предприятия». – Королев МО: «Технологический университет», 2023.

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

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)	Соляной 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 _____ Коба Е.Е., к.э.н., доцент

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 предприятия на всех уровнях функционирования: международном, государственном, ведомственном и отдельных граждан.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Универсальные компетенции:

- УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Общепрофессиональные компетенции:

- ОПК-7: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

Профессиональные компетенции:

- ПК-4: Способен 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.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

УК-1. И-1. Анализирует проблемную ситуацию как систему, выявляя

ее составляющие и связи между ними.

УК-1. И-2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению.

УК-1. И-3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников.

УК-1. И-4. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.

УК-1. И-5. Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области.

ОПК-7. И-1. Имеет представление, понимает принципы работы современных информационных технологий в экономике, программных средств для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач.

ОПК-7. И-2. Ставит задачу для решения экономических задач, понимая специфику применения информационных технологий.

ОПК-7. И-3. Понимает алгоритмы работы разных поисковых систем и особенности составления запросов при поиске информации в сети Интернет и базах данных.

ПК-4. И-1. Создает организационно-управленческую и информационную структуру интегральной системы управления рисками, разрабатывает проекты нормативных и методических материалов, регламентирующих работу по защите информации, предлагает технологии защиты информации, безопасную систему внутренней и внешней коммуникации и отчетности.

ПК-4. И-2. Координирует работы по технико-информационному обеспечению системы стратегического управления рисками, анализирует информацию об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, оценивает ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками.

ПК-4. И-3. Использует современные принципы, методы и технологии работы с информацией, принципы и методы управления проектами, положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности.

ПК-4. И-4. Применяет в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками, работает с различными информационными ресурсами и технологиями, использует программные обеспечения для работы с информацией (текстовые,

графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя.

ПК-4. И-5. Использует в профессиональной деятельности основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, компьютерную технику, оснащенную альтернативными устройствами ввода-вывода информации, адаптивные технические средства для людей с ограниченными возможностями здоровья.

ПК-4. И-6. Решает 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.

Необходимые умения:

УК-1. И-1. У-1. Умеет проводить анализ проблемной ситуации как системы, выявляя ее составляющие и связи между ними.

УК-1. И-2. У-1. Умеет определять пробелы в информации, необходимой для решения проблемной ситуации.

УК-1. И-2. У-2. Умеет проектировать процессы по устранению пробелов в информации.

УК-1. И-3. У-1. Умеет критически оценивать надежность источников информации, работать с противоречивой информацией из разных источников.

УК-1. И-4. У-1. Умеет разрабатывать и аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.

УК-1. И-5. У-1. Умеет использовать логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области.

ОПК-7. И-1. У-1. Умеет осуществлять поиск, аккумулирование, хранение, обработку, анализ, планирование, оценку и передачу данных при решении профессиональных задач с использованием современных информационных технологий.

ОПК-7. И-2. У-1. Умеет интегрировать и перерабатывать цифровой контент для постановки и решения задачи путем анализа закрытых и открытых баз данных.

ОПК-7. И-3. У-1. Умеет составлять запрос и проанализировать извлеченные данные.

ПК-4. И-1. У-1. Умеет создавать организационно-управленческую и информационную структуру интегральной системы управления рисками.

ПК-4. И-1. У-2. Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации.

ПК-4. И-1. У-3. Умеет осуществлять выбор средств и технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности.

ПК-4. И-2. У-1. Умеет координировать работы по технико-информационному обеспечению системы стратегического управления рисками.

ПК-4. И-2. У-2. Умеет проводить анализ информации об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации.

ПК-4. И-2. У-3. Умеет оценивать ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками.

ПК-4. И-3. У-1. Умеет использовать современные принципы, методы и технологии работы с информацией.

ПК-4. И-3. У-2. Умеет применять принципы и методы управления проектами.

ПК-4. И-3. У-3. Умеет использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности.

ПК-4. И-4. У-1. Умеет применять в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками.

ПК-4. И-4. У-2. Умеет работать с различными информационными ресурсами и технологиями, программными обеспечениями для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя.

ПК-4. И-5. У-1. Умеет использовать в профессиональной деятельности основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, компьютерную технику, оснащенную альтернативными устройствами ввода-вывода информации, адаптивные технические средства для людей с ограниченными возможностями здоровья.

ПК-4. И-6. У-1. Умеет 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.

Необходимые знания:

УК-1. И-1. З-1. Знает методику проведения анализа проблемной

ситуации как системы, знает ее составляющие и связи между ними.

УК-1. И-2. З-1. Знает способы определения пробелов в информации, необходимой для решения проблемной ситуации.

УК-1. И-2. З-2. Знает алгоритм проектирования процессов по устранению пробелов в информации, необходимой для решения проблемной ситуации.

УК-1. И-3. З-1. Знает методы оценки надежности источников информации, порядок работы с противоречивой информацией из различных источников.

УК-1. И-4. З-1. Знает методику разработки стратегий решения проблемных ситуаций на основе системного и междисциплинарных подходов.

УК-1. И-5. З-1. Знает современные концепции философского и социального характера в своей предметной области, методологический инструментарий для их критической оценки.

ОПК-7. И-1. З-1. Знает принципы работы современных информационных технологий в экономике и программных средств.

ОПК-7. И-2. З-1 Знает принципы классификации экономических задач в зависимости от типа экономических данных.

ОПК-7. И-3. З-1. Знает принципы работы и формирования запросов методом парсинга, используя базовые знания программирования.

ПК-4. И-1. З-1. Знает принципы создания организационно-управленческой и информационной структуры интегральной системы управления рисками.

ПК-4. И-1. З-2. Знает методические материалы, регламентирующие работу по защите информации.

ПК-4. И-1. З-3. Знает технологии защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности.

ПК-4. И-2. З-1. Знает требования к технико-информационному обеспечению управления рисками.

ПК-4. И-2. З-2. Знает современные информационные технологии, применяемые в управлении рисками.

ПК-4. И-2. З-3. Знает бюджет организации на внедрение и поддержание технико-информационного обеспечения системы управления рисками.

ПК-4. И-3. З-1. Знает современные принципы, методы и технологии работы с информацией.

ПК-4. И-3. З-2. Знает принципы и методы управления проектами.

ПК-4. И-3. З-3. Знает положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности.

ПК-4. И-4. З-1. Знает различные информационные ресурсы и технологии, программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных).

ПК-4. И-5. З-1. Знает основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации.

ПК-4. И-5. З-2. Знает принципы работы с компьютерной техникой, оснащенной альтернативными устройствами ввода-вывода информации, адаптивными техническими средствами для людей с ограниченными возможностями здоровья.

ПК-4. И-6. З-1. Знает принципы и требования обеспечения сохранения государственной и коммерческой тайны и конфиденциальной информации.

ПК-4. И-6. З-2. Знает принципы работы в системах электронного документооборота.

ПК-4. И-6. З-3. Знает действующее российское законодательство в сфере защиты государственной и коммерческой тайны и конфиденциальной информации.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность предприятия» относится к дисциплинам специальной подготовки базовой части Блока 1 модуля «Информационные технологии и экономическая безопасность» основной профессиональной образовательной программы подготовки специалистов по направлению 38.05.01 «Экономическая безопасность». Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информационная безопасность операционных систем и баз данных», «Информационные системы в экономике», «Информационно-аналитическая деятельность по обеспечению комплексной информационной безопасности», «Безопасность электронного документооборота» и компетенциях УК-1; ОПК-6; ОПК-7; ПК-4.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для выполнения выпускной квалификационной работы.

3. Объем дисциплины и виды учебной работы

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

Виды занятий	**Всего часов**	**Семестр 6**	**Семестр 7**	**Семестр 8**	**Семестр 9**
Общая трудоемкость	**108**	**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	**Зачёт**	**Зачёт**			
ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**16**				**16**
Лекции (Л)	**8**				**8**
Практические занятия (ПЗ)	**8**				**8**
Лабораторные работы (ЛР)					
Самостоятельная работа	**92**				**92**
Курсовые работы (проекты)	**-**				**-**
Расчетно-графические работы	**-**				**-**
Контрольная работа, домашнее задание	+ -				+ -
Вид итогового контроля	**Зачёт**				**Зачёт**

4. Содержание дисциплины

4.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. очное/заочное	Лабораторная работа, час. очное/заочное	Практические занятия, час очное/заочное	Занятия в интерактивной форме, час очное/заочное	Код компетенций
Раздел 1. Базовые положения по информационной безопасности					
Тема 1. Сущность и понятие информационной безопасности	2/1	-	4/1	3/1	УК-1, ОПК-7
Тема 2. Значение информационной безопасности и её место в системе национальной безопасности.	2/1	-	4/1	3/1	УК-1, ОПК-7

Тема 3. Сущность и теоретико-концептуальные основы защиты информации	2/1	-	4/1	3/1	УК-1, ОПК-7
Раздел 2. Характеристика защищаемой информации					
Тема 4. Критерии, условия и принципы отнесения информации к защищаемой. Состав и классификация ЗИ и их носителей	2/1	-	4/1	4/1	УК-1, ОПК-7
Тема 5. Основы защиты государственной, коммерческой, служебной, личной и профессиональной тайн	2/1	-	4/1	3/1	УК-1, ОПК-7
Раздел 3. Условия, определяющие необходимость защиты информации					
Тема 6. Дестабилизирующие воздействия на защищаемый информационный ресурс предприятия. Каналы и методы противоправных действий в информационной безопасности	2/1	-	4/1	4/1	УК-1, ОПК-7, ПК-4
Тема 7. Характеристика деятельности разведывательных служб по несанкционированному доступу к защищаемому информационному ресурсу	2/1	-	4/1	4/1	УК-1, ОПК-7, ПК-4
Раздел 4. Характеристика основных мер по защите информации					
Тема 8. Основные виды обеспечения информационной	2/1	-	4/1	4/1	УК-1, ОПК-7, ПК-4

безопасности предприятия, системы и средства защиты информации					
Итого:	16/8	-	32/8	28/8	

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 её место в системе национальной безопасности.

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

Понятие и современная концепция национальной безопасности.

Место информационной безопасности в системе национальной безопасности.

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 предприятия. 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 обеспечения информационной безопасности предприятия, системы и средства защиты информации

Виды защиты информации, сферы их действия. Классификация методов защиты информации. Универсальные методы защиты информации, область их применения. Области применения организационных, криптографических и инженерно-технических методов защиты информации. 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.

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. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726 (дата обращения: 04.10.2022). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный

2. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Наталия Васильевна. – 2 ; доп. – М.: Издательство «ФОРУМ» : ООО «Научно-издательский центр ИНФРА-М», 2016. – 240 с. – ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=544554

Дополнительная литература:

1. 1.Балдин, К. В. Информационные системы в экономике : учебник / К. В. Балдин, В. Б. Уткин. – 9-е изд., стер. – Москва : Дашков и К°, 2021. – 395 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=684194 (дата обращения: 04.10.2022). – Библиогр. в кн. – ISBN 978-5-394-04038-2. – Текст : электронный.

2. Мошак Н.Н. Защищенные информационные системы [Электронный ресурс]: учебное пособие / Мошак Н.Н., Птицына Л.К. - Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2020. - 216 с. URL: https://e.lanbook.com/book/180099

Рекомендуемая литература

1. Гладких, Т. В. Информационные системы учета и контроля ресурсов предприятия : учебное пособие : [16+] / Т. В. Гладких, Л. А. Коробова, М. Н. Ивлиев ; науч. ред. Д. С. Сайко ; Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2020. – 89 с. : ил., табл., схем., граф. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612378 (дата обращения: 04.10.2022). – Библиогр. в кн. – ISBN 978-5-00032-475-2. – Текст : электронный.

2. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL://biblioclub.ru/index.php?page=book&id=362895

3. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=363040

4. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.: 60x90 1/16. - (Профессиональное образование) (Обложка) ISBN 978-5-00091-079-5,http://znanium.com/bookread2.php?book=508381

5. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 416 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт 7БЦ) ISBN 978-5-8199-0331-5http://znanium.com/bookread2.php?book=549989

Электронные книги:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013 г.

   http://znanium.com/bookread.php?book=405000

2. Жук А. П.Жук Е ПЛепешкин О МТимошкин А И. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура).

   http://znanium.com/bookread.php?book=474838

3. Бабаш А В., Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013 г.

http://znanium.com/bookread.php?book=405000

4. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013 г.

http://znanium.com/bookread.php?book=415501

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

Интернет-ресурсы:

Интернет-ресурсы:

9. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
10. **http://informika.ru/** – образовательный портал.
11. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
12. **www.biblioclub.ru** - Универсальная библиотека онлайн.
13. **www.rucont.ru** - ЭБС «Руконт».
14. **http://www.academy.it.ru/** - академия АЙТИ.
15. **http://www.minfin.ru/** - Официальный сайт Министерства финансов Российской Федерации
16. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации.
17. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности
18. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

19. 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: «Информационная безопасность предприятия».

Ресурсы информационно-образовательной среды ФГБОУВОТУ:

Рабочая программа и методическое обеспечение по курсу «Информационная безопасность предприятия».

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, оснащённое компьютером с доступом в глобальную сеть Интернет ;
- рабочие места студентов, оснащённые 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 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ»

Специальность: 38.05.01 Экономическая безопасность

Специализация: «Экономико-правовое обеспечение экономической безопасности»

Квалификация (степень) выпускника: экономист

Форма обучения: очная, заочная

Королев
2023

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

№ п/п	Индекс компетенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Тема 1-8	УК-1. И-1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними; УК-1. И-2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению; УК-1. И-3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников; УК-1. И-4. Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов; УК-1. И-5. Использует логико-методологический инструментарий для критической оценки современных концепций философского и социального характера в своей предметной области.	УК-1. И-1. У-1 Умеет проводить анализ проблемной ситуации как системы, выявляя ее составляющие и связи между ними; УК-1. И-2. У-1 Умеет определять пробелы в информации, необходимой для решения проблемной ситуации; УК-1. И-2. У-2 Умеет проектировать процессы по устранению пробелов в информации; УК-1. И-3. У-1 Умеет критически оценивать надежность источников информации, работать с противоречивой информацией из разных источников; УК-1. И-4. У-1 Умеет разрабатывать и аргументировать стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов; УК-1. И-5. У-1 Умеет использовать логико-методологический инструментарий для критической оценки современных концепций философского и социального	УК-1. И-1. З-1 Знает методику проведения анализа проблемной ситуации как системы, знает ее составляющие и связи между ними; УК-1. И-2. З-1 Знает способы определения пробелов в информации, необходимой для решения проблемной ситуации; УК-1. И-2. З-2 Знает алгоритм проектирования процессов по устранению пробелов в информации, необходимой для решения проблемной ситуации; УК-1. И-3. З-1 Знает методы оценки надежности источников информации, порядок работы с противоречивой информацией из различных источников; УК-1. И-4. З-1 Знает методику разработки стратегий решения проблемных ситуаций на основе системного и междисциплинарных подходов; УК-1. И-5. З-1 Знает современные концепции философского и социального характера в своей предметной области, методологический инструментарий для их критической оценки.

					характера в своей предметной области.	
2	ОПК-7	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.	Тема 1-8	ОПК-7. И-1 Имеет представление, понимает принципы работы современных информационных технологий в экономике, программных средств для поиска, аккумулирования, хранения, обработки, анализа, планирования, оценки и передачи данных при решении профессиональных задач; ОПК-7. И-2 Ставит задачу для решения экономических задач, понимая специфику применения информационных технологий; ОПК-7. И-3 Понимает алгоритмы работы разных поисковых систем и особенности составления запросов при поиске информации в сети Интернет и базах данных.	ОПК-7. И-1. У-1 Умеет осуществлять поиск, аккумулирование, хранение, обработку, анализ, планирование, оценку и передачу данных при решении профессиональных задач с использованием современных информационных технологий; ОПК-7. И-2. У-1 Умеет интегрировать и перерабатывать цифровой контент для постановки и решения задачи путем анализа закрытых и открытых баз данных; ОПК-7. И-3. У-1 Умеет составлять запрос и проанализировать извлеченные данные.	ОПК-7. И-1. З-1 Знает принципы работы современных информационных технологий в экономике и программных средств; ОПК-7. И-2. З-1 Знает принципы классификации экономических задач в зависимости от типа экономических данных; ОПК-7. И-3. З-1 Знает принципы работы и формирования запросов методом парсинга, используя базовые знания программирования.
3	ПК-4	Способен создавать организационно-управленческую и информационную структуру интегральной системы управления рисками, осуществлять координацию работ по технико-информационно	Тема 6-8	ПК-4. И-1 Создает организационно-управленческую и информационную структуру интегральной системы управления рисками, разрабатывает проекты нормативных и методических материалов, регламентирующих работу по защите информации, предлагает технологии защиты информации, безопасную систему внутренней и внешней коммуникации и отчетности. ПК-4. И-2 Координирует работы по технико-информационному обеспечению системы стратегического управления	ПК-4. И-1. У-1 Умеет создавать организационно-управленческую и информационную структуру интегральной системы управления рисками; ПК-4. И-1. У-2 Умеет разрабатывать проекты нормативных и методических материалов, регламентирующих работу по защите информации, ПК-4. И-1. У-3 Умеет осуществлять выбор средств и технологий защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности; ПК-4. И-2. У-1 Умеет координировать работы по технико-информационному	ПК-4. И-1. З-1 Знает принципы создания организационно-управленческой и информационной структуры интегральной системы управления рисками; ПК-4. И-1. З-2 Знает методические материалы, регламентирующие работу по защите информации; ПК-4. И-1. З-3 Знает технологии защиты информации, безопасной системы внутренней и внешней коммуникации и отчетности; ПК-4. И-2. З-1 Знает требования к технико-информационному обеспечению управления рисками; ПК-4. И-2. З-2

		му обеспечению системы стратегического управления рисками.		рисками, анализирует информацию об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, оценивает ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками; ПК-4. И-3 Использует современные принципы, методы и технологии работы с информацией, принципы и методы управления проектами, положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной; безопасности; ПК-4. И-4 Применяет в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками, работает с различными информационными ресурсами и технологиями, использует программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя; ПК-4. И-5 Использует в профессиональной деятельности основные методы,	обеспечению системы стратегического управления рисками; ПК-4. И-2. У-2 Умеет проводить анализ информации об уровне и тенденциях развития технико-информационного обеспечения системы управления рисками в отрасли и в организации, ПК-4. И-2. У-3 Умеет оценивать ресурсные затраты на внедрение и функционирование технико-информационной составляющей и эффективность внедрения автоматизированных информационных систем, управляет проектами технико-информационного обеспечения системы управления рисками; ПК-4. И-3. У-1 Умеет использовать современные принципы, методы и технологии работы с информацией; ПК-4. И-3. У-2 Умеет применять принципы и методы управления проектами; ПК-4. И-3. У-3 Умеет использовать положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности; ПК-4. И-4. У-1 Умеет применять в профессиональной деятельности современные информационные технологии, используемые в сфере управления рисками; ПК-4. И-4. У-2 Умеет работать с различными информационными ресурсами и	Знает современные информационные технологии, применяемые в управлении рисками ПК-4. И-2. З-3 Знает бюджет организации на внедрение и поддержание технико-информационного обеспечения системы управления рисками; ПК-4. И-3. З-1 Знает современные принципы, методы и технологии работы с информацией; ПК-4.И-3. З-2 Знает принципы и методы управления проектами; ПК-4. И-3. З-3 Знает положения национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасности; ПК-4. И-4. З-1 Знает различные информационные ресурсы и технологии, программные обеспечения для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных); ПК-4. И-5. З-1 Знает основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, ПК-4. И-5. З-2 Знает принципы работы с компьютерной техникой, оснащенной альтернативными устройствами ввода-вывода информации, адаптивными техническими средствами для

				способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, компьютерную технику, оснащенную альтернативными устройствами ввода-вывода информации, адаптивные технические средства для людей с ограниченными возможностями здоровья; ПК-4. И-6 Решает 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.	технологиями, программными обеспечениями для работы с информацией (текстовые, графические, табличные и аналитические приложения, приложения для визуального представления данных) на уровне опытного пользователя; ПК-4. И-5. У-1 Умеет использовать в профессиональной деятельности основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации, компьютерную технику, оснащенную альтернативными устройствами ввода-вывода информации, адаптивные технические средства для людей с ограниченными возможностями здоровья; ПК-4. И-6. У-1 Умеет 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.	людей с ограниченными возможностями здоровья; ПК-4. И-6. З-1 Знает принципы и требования обеспечения сохранения государственной и коммерческой тайны и конфиденциальной информации; ПК-4. И-6. З-2 Знает принципы работы в системах электронного документооборота; ПК-4. И-6. З-3 Знает действующее российское законодательство в сфере защиты государственной и коммерческой тайны и конфиденциальной информации.

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

Код компетенции	**Инструменты, оценивающие сформированность компетенции**	**Этапы и показатель оценивания компетенции**	**Шкала и критерии оценки**
УК-1, ОПК-7, 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.
УК-1, ОПК-7, ПК-4	Реферат	A) компетенция не сформирована B) сформирована частично C) сформирована	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).

		полностью	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.
УК-1, ОПК-7, 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.

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

Тематика докладов в презентационной форме:

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

Тематика рефератов:

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

Тематика контрольных работ:

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.

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

Формой контроля знаний по дисциплине «Информационная безопасность предприятия» являются две текущие аттестации в виде тестов и одна промежуточная аттестация в виде зачета.

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, ОПК-7	20 вопросов	Компьютерное тестирование; время, отведенное на процедуру -30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%

Тестирование(Т2)	УК-1, ОПК-7, ПК-4	20 вопросов	Компьютерное тестирование; время, отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка -0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Зачёт	УК-1, ОПК-7, ПК-4	2 вопроса	Зачет проводится в устной форме, путем ответа на вопросы. Время отведенное на процедуру – 2 часа.	Результаты предоставляются в день проведения зачета	Критерии оценки: «**Зачтено**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Незачтено**»: • демонстрирует частичные знания по темам дисциплин или незнание основных понятий; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся, согласно приказу «О внедрении новой балльно-рейтинговой системы контроля и оценивания

уровня знаний и внеучебной созидательной активности обучающихся» № 01-04/428 от 25 сентября 2020 г.

Тестовые задания

1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...

(?) политическая разведка;
(!) промышленный шпионаж;
(?) добросовестная конкуренция;
(?) конфиденциальная информация;
(?) правильного ответа нет.

2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?

(?) любая информация;
(?) только открытая информация;
(!) запатентованная информация;
(?) закрываемая собственником информация;
(?) коммерческая тайна.

3. Кто может быть владельцем защищаемой информации?

(?) только государство и его структуры;
(?) только предприятия, акционерные общества, фирмы;
(?) только общественные организации;
(!) все вышеперечисленные организационные структуры;
(?) кто угодно.

4. Какие сведения на территории РФ могут составлять коммерческую тайну?

(?) учредительные документы и устав предприятия;
(?) сведенья о численности работающих, их заработной плате и условиях труда;
(!) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
(?) другие;
(?) любые.

5. Какие закрытые сведения входят в понятие «коммерческая тайна»?

(?) только связанные с производством;
(?) только связанные с планированием производства и сбытом продукции;
(?) только технические и технологические решения предприятия;
(?) только 1 и 2 вариант ответа;
(!) три первых варианта ответа.

6. Что называют источником конфиденциальной информации?

(!) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников;

(?) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе;

(?) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники;

(?) это защищаемые предприятием сведения в области производства и коммерческой деятельности;

(?) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.

7. Как называют процессы обмена информацией с помощью официальных, деловых документов?

(?) непосредственные**;**

(?) межличностные;

(?) формальные**;**

(?) неформальные**;**

(!) конфиденциальные.

8. Какое наиболее распространенное действие владельца конфиденциальной информации, приводит к неправомерному овладению ею при минимальных усилиях со стороны злоумышленника?

(?) хищение носителей информации;

(?) использование технических средств для перехвата электромагнитных ПЭВМ;

(!) разглашение;

(?) копирование программой информации с носителей;

(?) другое.

9. Каким образом происходит разглашение конфиденциальной информации?

(?) утеря документов и других материалов, или пересылка их посредством почты, посыльного, курьера;

(?) опубликование материалов в печати;

(?) сообщение, передача, предоставление в ходе информационного обмена;

(!) все вышеперечисленные способы;

(?) правильного варианта ответа нет.

10. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?

(?) получить, изменить, а затем передать ее конкурентам;

(?) размножить или уничтожить ее;

(!) получить, изменить или уничтожить;

(?) изменить и уничтожить ее;

(?) изменить, повредить или ее уничтожить.

11. Какой самый прямой и эффективный способ склонения к сотрудничеству?

(?) психическое давление;

(!) подкуп;

(?) преследование;

(?) шантаж;

(?) угрозы.

12. Наиболее сложный и дорогостоящий процесс несанкционированного доступа к источникам конфиденциальной информации?

(?) инициативное сотрудничество;

(?) выпытывание;

(?) наблюдение;

(!) хищение;

(?) копирование.

13. Какое из утверждений неверно?

(?) подкуп — сложный процесс, требует долгой и кропотливой работы;

(?) выпытывание — это стремление путем внешне наивных вопросов получить определенные сведения;

(!) процесс наблюдения не сложен, так как не требует затрат сил и средств;

(?) под незаконным подключением понимают контактное или бесконтактное подсоединение к линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них;

(?) негласное ознакомление — способ получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность кое-что узнать.

14. Завершающим этапом любого сбора конфиденциальной информации является

(?) копирование;

(?) подделка;

(!) аналитическая обработка;

(?) фотографирование;

(?) наблюдение.

15. Как называются реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации?

(?) ненадежность;

(!) угроза;

(?) несчастный случай;

(?) авария;

(?) правильного ответа среди перечисленных нет.

16. Что в скором времени будет являться главной причиной информационных потерь?

(?) материальный ущерб, связанный с несчастными случаями;

(?) кража и преднамеренная порча материальных средств;

(!) информационные инфекции;

(?) аварии и выход из строя аппаратуры, программ и баз данных;

(?) ошибки эксплуатации.

17. В каком варианте ответа инфекции расположены от более простого к более сложному, по возрастанию?

(?) логические бомбы, троянский конь, червь, вирус;

(?) червь, вирус, логические бомбы, троянский конь;

(?) червь, логические бомбы, вирус, троянский конь;

(?) логические бомбы, вирус, троянский конь, червь;

(!) вирус, логические бомбы, троянский конь, червь.

18. Причины, связанные с информационным обменом приносящие наибольшие убытки?

(?) остановка или выход из строя информационных систем;

(?) потери информации;

(?) неискренность;

(?) проникновение в информационную систему;

(!) перехват информации.

19. Какие цели преследуются при активном вторжении в линии связи?

(?) анализ информации (содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;

(?) воздействие на поток сообщений (модификация, удаление и посылка ложных сообщений) или воспрепятствие передаче сообщений;

(?) инициализация ложных соединений;

(!) варианты 1 и 2;

(?) варианты 2 и 3.

20. Что определяет модель нарушителя?

(?) категории лиц, в числе которых может оказаться нарушитель;

(?) возможные цели нарушителя и их градации по степени важности и опасности;

(?) предположения о его квалификации и оценка его технической вооруженности;

(?) ограничения и предположения о характере его действий;

(!) все выше перечисленные.

21. Выберите наиболее полный список мотивов, которые преследуют компьютерные пираты (хакеры), пытаясь получить несанкционированный доступ к информационной системе или вычислительной сети.

(?) ознакомление с информационной системой или вычислительной сетью;

(?) похитить программу или иную информацию;
(?) оставить записку, выполнить, уничтожить или изменить программу;
(?) вариант 2 и 3;
(!) вариант 1, 2 и 3.

22. Какое из утверждений неверно?

(?) наблюдается тенденция к стремительному росту попыток получить несанкционированный доступ к информационным системам или вычислительным сетям;
(?) недовольный руководителем служащий создает одну из самых больших угроз вычислительным системам коллективного пользования;
(?) считается, что компьютерные преступления, более легкий путь добывания денег, чем ограбление банков;
(!) очень малое число фирм могут пострадать от хакеров;
(?) к категории хакеров-профессионалов обычно относят: преступные группировки, преследующие политические цели.

23. Какое из утверждений неверно?

(?) хакеры могут почерпнуть много полезной информации из газеты и других периодических изданий;
(?) хакерами часто используется завязывание знакомств для получения информации о вычислительной системе или выявления служебных паролей;
(?) один из наиболее эффективных и наименее рискованных путей получения конфиденциальной информации и доступа к ЭВМ — просто изучая черновые распечатки;
(!) о перехвате сообщений в каналах связи речь может идти лишь в связи с деятельностью военных или секретных служб;
(?) после получения необходимого объема предварительной информации, компьютерный хакер-профессионал осуществляет непосредственное вторжение в систему.

24. Какое из утверждений неверно?

(!) наибольшие убытки (в среднем) приносит саботаж в нематериальной сфере;
(?) убытки, связанные с забастовками не превышают убытков, связанных с аварией оборудования;
(?) уход ведущих специалистов опасен для малых центров;
(?) хищения, в первую очередь осуществляются сотрудниками предприятия или пользователями;
(?) аварии оборудования или основных элементов системы являются мало распространенными и определяются надежностью аппаратуры.

25. Метод скрытие — это...

(?) максимальное ограничение числа секретов, из-за допускаемых к ним лиц;
(!) максимального ограничения числа лиц, допускаемых к секретам;
(?) уменьшение числа секретов неизвестных большинству сотрудников;
(?) выбор правильного места, для утаивания секретов от конкурентов;

(?) поиск максимального числа лиц, допущенных к секретам.

26. Что включает в себя ранжирование как метод защиты информации?

(?) регламентацию допуска и разграничение доступа к защищаемой информации**;**

(?) деление засекречиваемой информации по степени секретности;

(?) наделять полномочиями назначать вышестоящими нижестоящих на соответствующие посты;

(!) вариант ответа 1 и 2;

(?) вариант ответа 1, 2 и 3.

27. К какому методу относятся следующие действия: имитация или искажение признаков и свойств отдельных элементов объектов защиты, создания ложных объектов?

(!) скрытие;

(?) дезинформация;

(?) дробление;

(?) кодирование;

(?) шифрование.

28. Что в себя включают морально-нравственные методы защиты информации?

(?) воспитание у сотрудника, допущенного к секретам, определенных качеств, взглядов и убеждений;

(?) контроль работы сотрудников, допущенных к работе с секретной информацией;

(?) обучение сотрудника, допущенного к секретам, правилам и методам защиты информации, и навыкам работы с ней;

(?) вариант ответа 1 и 3;

(!) вариант ответа 1, 2 и 3.

29. Какое из выражений не верно?

(?) страхование — как метод защиты информации пока еще не получил признания;

(?) кодирование — это метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации;

(?) шифрование может быть предварительное и линейное;

(!) дирекция очень часто не может понять необходимость финансирования безопасности;

(?) безопасность предприятия — не стабильное состояние предприятия, не поддающееся прогнозированию во времени.

30. Что является одним из основных признаков защищаемой информации?

(!) ограничения, вводимые собственником информации на ее распространение и использование

(?) в каком виде эта информация представлена (электронном, печатном, письменном и т.д.)

(?) все вышеперечисленное

31. Какой должна быть защита информации с позиции системного подхода?

(?) безопасной для сотрудников;

(?) активной;

(?) универсальной;

(!) надежной;

(?) непрерывной.

32. Что такое «служба информационной безопасности»?

(?) система внештатных формирований, предназначенных для обеспечения безопасности объекта;

(?) структурное подразделение, предназначенное для охраны помещений и территорий предприятия;

(!) система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности и защиты конфиденциальной информации;

(?) структурное подразделение, предназначенное для хранения и выдачи документов, носителей конфиденциальной информации;

(?) структурное подразделение, задача которого: подбор персонала и работа с сотрудниками.

33. Кому непосредственно подчиняется служба информационной безопасности?

(?) владельцу предприятия;

(?) владельцу предприятия и лицу которому тот подчиняется;

(?) руководителю предприятия, либо лицу, которому тот делегировал свои права по руководству ее деятельностью;

(?) заместителю руководителя предприятия по организационным вопросам;

(!) начальнику службы безопасности.

34. Какие задачи не входят в круг обязанностей службы информационной безопасности?

(!) внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической безопасности предприятия;

(?) определение участков сосредоточения сведений, составляющих коммерческую тайну;

(?) определение на предприятии технологического оборудования, выход из строя которого может привести к большим экономическим потерям;

(?) ограничение круга сторонних предприятий, работающих с данным предприятием, на которых возможен выход из-под контроля сведений составляющих коммерческую тайну предприятия;

(?) определение круга сведений, составляющих коммерческую тайну.

35. Какие средства использует инженерно-техническая защита (по функциональному назначению)?

(?) программные, аппаратные, криптографические, технические;

(?) программные, физические, шифровальные, криптографические;

(?) программные, аппаратные, криптографические, физические;

(?) физические, аппаратные, материальные, криптографические;

(!) аппаратные, физические, программные, материальные.

36. В каком нормативном акте говорится о формировании и защите информационных ресурсов как национального достояния?

(?) в Конституции РФ;

(?) в Законе об оперативно розыскной деятельности;

(?) в Законе об частной охране и детективной деятельности;

(!) в Законе об информации, информационных технологиях и защите информации;

(?) в Указе Президента РФ № 170 от 20 января 1994 г. «Об основах государственной политики в сфере информатизации».

37. Владельцами (собственниками) защищаемой информации могут быть…

(?) государство и его структуры; предприятия, товарищества, акционерные общества;

(?) общественные организации; граждане государства: их права (тайна переписки, телефонных и телеграфных разговоров, врачебная тайна и др.)

(!) все вышеперечисленное

38. На каком уровне защиты информации создаются комплексные системы защиты информации?

(?) на организационно-правовом;

(?) на социально-политическом;

(?) на тактическом;

(?) на инженерно-техническом;

(!) на всех вышеперечисленных.

39. Какие существуют наиболее общие задачи защиты информации на предприятии?

(?) снабжение всех служб, подразделений и должностных лиц необходимой информацией, как засекреченной, так и несекретной;

(?) предотвращение утечки защищаемой информации и предупреждение любого несанкционированного доступа к носителям засекреченной информации;

(?) документирование процессов защиты информации, с целью получения соответствующих доказательств в случае обращения в правоохранительные органы;

(?) создание условий и возможностей для коммерческого использования секретной и конфиденциальной информации предприятия;

(!) все вышеперечисленные.

40. Какие меры и методы защиты секретной или конфиденциальной информации в памяти людей не являются основными?

(?) воспитание понимания важности сохранения в тайне доверенных им секретных или конфиденциальных сведений;

(?) подбор людей, допускаемых к секретным работам;

(?) обучение лиц, допущенных к секретам, правилам их сохранения;

(!) добровольное согласие на запрет работы по совместительству у конкурентов;

(?) стимулирование заинтересованности работы с засекреченной информацией и сохранения этих сведений в тайне.

41. В каком документе содержаться основные требования к безопасности информационных систем в США?

(?) в красной книге;

(?) в желтой прессе;

(!) в оранжевой книге;

(?) в черном списке;

(?) в красном блокноте.

42. Какое определение соответствует термину «Аутентификация»?

(?) набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации в данной организации;

(?) распознавание имени объекта;

(!) подтверждение того, что предъявленное имя соответствует объекту;

(?) регистрация событий, позволяющая восстановить и доказать факт происшествия событий;

(?) правильного определения нет.

43. Какое требование относится к термину «Подотчетность»?

(?) субъекты индивидуально должны быть идентифицированы;

(?) гарантированно защищенные механизмы, реализующие указанные базовые требования, должны быть постоянно защищены от "взламывания";

(?) необходимо иметь явную и хорошо определенную политику обеспечения безопасности;

(?) аудиторская информация должна храниться и защищаться так, чтобы имелась возможность отслеживать действия, влияющие на безопасность;

(!) метки, управляющие доступом, должны быть установлены и связаны с объектами.

44. Какой уровень безопасности системы соответствует низшему?

(?) A;

(?) B;

(?) C;

(?) D;
(!) E.

45. Какой класс присваивается системам которые не прошли испытания?
(?) A1;
(?) B2:
(?) B3;
(?) C4;
(!) D.

46. Что включают в себя технические мероприятия по защите информации?
(?) поиск и уничтожение технических средств разведки;
(?) кодирование информации или передаваемого сигнала;
(?) подавление технических средств постановкой помехи;
(?) применение детекторов лжи;
(!) все вышеперечисленное.

47. Какие устройства поиска технических средств разведки не относятся к устройствам поиска пассивного типа?
(!) металлоискатели;
(?) тепловизоры;
(?) устройства и системы поиска по электромагнитному излучению;
(?) детекторы записывающей аппаратуры

48. Какие устройства не относятся к устройствам поиска по электромагнитному излучению?
(?) частотомер;
(?) шумомер;
(?) сканер;
(!) нелинейный локатор;
(?) анализатор спектра.

49. С какого расстояния можно считать информацию с монитора компьютера?
(?) 200 м.
(!) менее 200 м.
(?) 500 м.
(?) 750 м.
(?) 1 км.

50. Какие материалы не применяются при экранировании помещения?
(?) листовая сталь;
(?) медная сетка;
(?) алюминиевая фольга;
(!) фтористая сетка.

51. Какое устройство позволяет обеспечивать защищенность от разного рода сигналов, генерируемых устройствами, которые могут служить источником утечки информации?

(?) приемник-сканер;

(?) телефонный адаптер;

(?) скремблер;

(!) сетевой фильтр;

(?) все вышеперечисленные.

52. Какие основные направления в защите персональных компьютеров от несанкционированного доступа Вы знаете?

(?) недопущение нарушителя к вычислительной среде;

(?) защита вычислительной среды;

(?) использование специальных средств защиты информации ПК от несанкционированного доступа;

(!) все вышеперечисленные;

(?) правильного ответа нет.

53. Какие средства защиты информации в ПК наиболее распространены?

(?) применение различных средств шифрования, не зависящих от контекста информации;

(?) средства защиты от копирования коммерческих программных продуктов;

(?) средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя;

(?) средства защита от компьютерных вирусов и создание архивов;

(!) все вышеперечисленные.

54. Какое утверждение неверно?

(?) чтобы уменьшить потери по эксплуатационным причинам, следует иметь архивные копии используемых файлов и систематически обновлять копии изменяемых файлов;

(?) программы-архиваторы позволяют не только сэкономить место на архивных дискетах, но и объединять группы совместно используемых файлов в один архивный файл, что заметно облегчает ведение архивов:

(?) информация на жестком диске может разрушиться только вследствие действия компьютерного вируса или злого умысла вашего недоброжелателя;

(?) единственно надежным способом уберечь информацию от любых разрушительных случайностей является четкая, неукоснительно соблюдаемая система резервного копирования;

(!) одним из основных симптомов, возникновения серьезных дефектов на диске, является замедление работы дисковода.

55. Кто является собственником защищаемой информации?

(?) юридическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией

(!) юридическое или физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией

(?) физическое лицо, которое по своему усмотрению владеет, пользуется и распоряжается принадлежащей ему информацией

56. На какие группы делятся информационные ресурсы государства?

(!) информация открытая, информация запатентованная и информация, «закрываемая» ее собственником, владельцем и защищаемая им с помощью отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны

(?) информация открытая и информация запатентованная

(?) информация запатентованная и информация, «закрываемая» ее собственником, владельцем и защищаемая им с помощью отработанных механизмов защиты государственной, коммерческой или другой охраняемой тайны

57. Что такое запатентованная информация?

(?) на распространение и использование которой не имеется никаких ограничений

(!) охраняется внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности;

(?) информация, которая принадлежит одному единственному собственнику

58. К защищаемой информации относят…

(?) секретную информацию и конфиденциальную информацию

(?) личную тайну

(!) все вышеперечисленное

59. Применительно к органам государственной власти и управления под тайной понимается…

(!) то, что скрывается от других, что известно строго определенному кругу людей

(?) секретная переписка

(?) секретные переговоры

60. Какие из ниже перечисленных сведений, согласно Постановлению Правительства РФ от 5 декабря 1991 г. № 35, не могут составлять коммерческую тайну?

(?) учредительные документы и устав предприятия; документы, дающие право заниматься предпринимательской деятельностью; сведения по установленным формам отчетности о финансово-хозяйственной деятельности, необходимые для проверки уплаты налогов; документы о платежеспособности

(?) сведения о численности, заработной плате и условиях труда, о наличии свободных рабочих мест; документы об уплате налогов; сведения о загрязнении

окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасности условий труда, а также других нарушениях законодательства РФ

(!) все вышеперечисленное

Вопросы к зачёту:

1. Сущность понятия «теория информационной безопасности»: определение, цели и задачи.
2. Сущность понятия «методология защиты информации»: определение, методы, задачи.
3. Современное понятие «информационной безопасности»: узкий и широкий подход, их содержание.
4. Сущность и структура классических понятий «информационной безопасности» и «защиты информации».
5. Объекты и компоненты информационной безопасности.
6. Роль информационной безопасности в информационной сфере общества: международный и внутригосударственный уровень.
7. Связь понятий информационная безопасность и безопасность информации.
8. Понятие Концепции национальной безопасности РФ и место в ней информационной безопасности.
9. Сущность Доктрины информационной безопасности и основные источники угроз информационной сферы.
10. Основные федеральные законы РФ в области ИБ (ЗИ).
11. Существующие подходы к понятию «защита информации" и их содержание.
12. Понятие «уязвимости» информации в теории защиты информации.
13. Понятие «утечки» информации в теории защиты информации.
14. Цели, функции и задачи защиты информации.
15. Роль защиты информации в различных сферах деятельности.
16. Защита информации и проблема информационных войн.
17. Понятие «защита от негативной информации» в теории защиты информации.
18. Понятие, задачи и составные части теории защиты информации.
19. Научно-методологическая основа теории защиты информации: понятие и состав.
20. Общеметодологические (общетеоретические и теоретико-прикладные) принципы формирования теории защиты информации.
21. Инструментально-методологический базис теории защиты информации: понятие и характеристика методов.
22. Понятие о Концепции защиты информации.
23. Виды стратегий защиты информации как основа построения Концепции защиты информации.
24. Сущность и структура Унифицированной концепции защиты информации.
25. Организационные основы защиты информации: технологические и

правовые составляющие.

26. Международные факторы, влияющие на защиту информации в РФ.
27. Факторы, обуславливающие современное состояние РФ и их влияние на защиту информации.
28. Определение и классификация защищаемого информационного ресурса (информации).
29. Отличительные признаки защищаемой информации.
30. Критерии отнесения информации к защищаемой.
31. Модель (условия и принципы) отнесения информации к защищаемой.
32. Понятие и состав носителей защищаемой информации.
33. Прямые и косвенные носители защищаемой информации.
34. Понятие и виды тайн конфиденциальной информации.
35. Определение «государственной тайны» и порядок отнесения к ней сведений.
36. Степени и грифы сведений, отнесенных к государственной тайне.
37. Порядок рассекречивания сведений, отнесенных к государственной тайне.
38. Определение «коммерческой тайны» и порядок отнесения к ней сведений.
39. Степени конфиденциальности, составляющих коммерческую тайну.
40. Сущность понятия «служебной тайны», границы и области ее действий.
41. Понятие и сферы действий профессиональной тайны.
42. Соотношения между профессиональной тайной и другими видами тайн, разновидности профессиональной тайны.
43. Понятия «личная тайна» и «персональные данные» (защищаемая информация о гражданах).
44. Разновидности личной тайны (персональных данных).
45. Понятие и характер форм собственности на защищаемую информацию.
46. Понятия «собственники» и «владельцы» защищаемой информации.
47. Основные субъекты профессиональной тайны: собственник, доверитель, держатель и пользователь.
48. Понятие и характеристика «интеллектуальной собственности».
49. Общепринятые методы защиты интеллектуальной собственности.
50. Различия между правом интеллектуальной собственности и авторским правом.
51. Понятие «патент» как общепринятый подход к защите интеллектуальной собственности.
52. Понятие «авторское право» с позиций защиты интеллектуальной собственности.
53. Первичные объекты интеллектуальной собственности, подлежащие защите.
54. Вторичные объекты интеллектуальной собственности, подлежащие защите и перечень произведений, не являющихся объектами авторского права.
55. Сущность понятия «теория информационной безопасности»: определение, цели и задачи.
56. Сущность понятия «методология защиты информации»: определение,

методы, задачи.

57. Объекты и компоненты информационной безопасности.
58. Роль информационной безопасности в информационной сфере общества: международный и внутригосударственный уровень.
59. Понятие и структура угроз защищаемой информации.
60. Понятие, состав и характеристика источников воздействия на защищаемую информацию.
61. Виды и способы воздействия различных источников на защищаемую информацию.
62. Понятие канала несанкционированного доступа (НСД) и его соотношение с каналом утечки информации.
63. Классификация каналов НСД и их характеристика.
64. Характеристика существующих организационных структур разведок зарубежных стран (государственных и частных объединений).
65. Классификация методов защиты информации и их характеристика.
66. Характеристика организационных, криптографических и инженерно-технических методов защиты информации.
67. Определение и классификация средств защиты информации.
68. Назначение программных, криптографических и технических средств защиты.
69. Классификация организационно-технологических документов по ЗИ.
70. Виды и характеристика контрольных мероприятий по ЗИ.
71. Характеристика (сущность и значение) комплексной системы защиты информации как форма деятельности организаций (предприятий).

Приложение 2

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ»

(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.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

ОПК-7 - Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

ПК-4 - Способен 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.

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 час

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 час

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 час

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 час

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 час

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 час

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 час

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 час

3. Указания по проведению лабораторного практикума

Лабораторные работы не предусмотрены учебным планом дисциплины.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить студентов к самостоятельному научному творчеству.

Задачи самостоятельной работы:

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

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

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

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения/заочная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	60/92
Вопросы, выносимые на самостоятельное изучение	12/18
Подготовка к практическим занятиям	16/18
Подготовка к лабораторным занятиям	12/18
Подготовка докладов	12/18
Выполнение практических заданий	12/20

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 представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	12/18	Изучение открытых источников
2.	Подготовка к практическим занятиям	12/18	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Подготовка к лабораторным занятиям	12/18	Изучение открытых источников
4.	Тематика докладов	12/18	1. Внутренние аппаратные средства персонального компьютера 2. Внешние периферийные устройства персонального компьютера
5.	Выполнение практических заданий	12/20	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. 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	1. Подготовка докладов по темам: 2. Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия. 3. Сущность информационной безопасности. Объекты информационной безопасности. 4. Связь информационной безопасности с информатизацией общества. 5. Структура информационной безопасности 6. Значение информационной безопасности для субъектов информационных отношений. 7. Связь между информационной безопасностью и безопасностью информации. 8. Понятие и современная концепция национальной безопасности. 9. 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.
4	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.
5	Критерии, условия и принципы отнесения информации к защищаемой Состав и классификация	***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.

	носителей 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.
6	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.
7	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.
8	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.

9	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.
10	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.
11	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.
12	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.
13	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.
14	Классификация и характеристика средств защиты информации	***Подготовка рефератов по темам:*** 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.
15	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.
16	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.
17	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.

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

5.1. Требования к структуре

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

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

3. В процессе изложения материала необходимо давать ссылки на используемую

литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

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

5.3. Требования к оформлению

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

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

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

Основная литература:

1. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=576726 (дата обращения: 04.10.2022). – Библиогр.: с. 64. – ISBN 978-5-7782-3918-0. – Текст : электронный

2. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие / Наталия Васильевна. – 2 ; доп. – М.: Издательство «ФОРУМ» : ООО «Научно-издательский центр ИНФРА-М», 2016. – 240 с. – ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=544554

Дополнительная литература:

1. 1.Балдин, К. В. Информационные системы в экономике : учебник / К. В. Балдин, В. Б. Уткин. – 9-е изд., стер. – Москва : Дашков и К°, 2021. – 395 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=684194 (дата обращения: 04.10.2022). – Библиогр. в кн. – ISBN 978-5-394-04038-2. – Текст : электронный.

2. Мошак Н.Н. Защищенные информационные системы [Электронный ресурс]: учебное пособие / Мошак Н.Н., Птицына Л.К. - Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2020. - 216 с. URL: https://e.lanbook.com/book/180099

Рекомендуемая литература

1. Гладких, Т. В. Информационные системы учета и контроля ресурсов предприятия : учебное пособие : [16+] / Т. В. Гладких, Л. А. Коробова, М. Н. Ивлиев ; науч. ред. Д. С. Сайко ; Воронежский государственный университет инженерных технологий. – Воронеж : Воронежский государственный университет инженерных технологий, 2020. – 89 с. : ил., табл., схем., граф. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612378 (дата обращения: 04.10.2022). – Библиогр. в кн. – ISBN 978-5-00032-475-2. – Текст : электронный.

2. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 105 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4 ; То же [Электронный ресурс]. - URL://biblioclub.ru/index.php?page=book&id=362895

3. Нестеров, С.А. Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=363040

4. Основные положения информационной безопасности: Учебное пособие/В.Я.Ищейнов, М.В.Мецатунян - М.: Форум, НИЦ ИНФРА-М, 2015. - 208 с.:

60x90 1/16. - (Профессиональное образование) (Обложка) ISBN 978-5-00091-079-5,http://znanium.com/bookread2.php?book=508381

5. Информационная безопасность компьютерных систем и сетей: Учебное пособие / Шаньгин В. Ф. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 416 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт 7БЦ) ISBN 978-5-8199-0331-5http://znanium.com/bookread2.php?book=549989

Электронные книги:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013 г.

http://znanium.com/bookread.php?book=405000

2. Жук А. П.Жук Е ПЛепешкин О МТимошкин А И. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура).

http://znanium.com/bookread.php?book=474838

3. Бабаш А В., Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013 г.

http://znanium.com/bookread.php?book=405000

4. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013 г.

http://znanium.com/bookread.php?book=415501

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

Интернет-ресурсы:

1. **http://eup.ru/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

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

Перечень программного обеспечения: MSOffice, PowerPoint.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды ФГБОУВОТУ;
2. Рабочая программа и методическая обеспечение по дисциплине: «Информационная безопасность предприятия».