МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра информационной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 09.03.03 «Прикладная информатика»
Направленность (профиль): Информационно-коммуникационные технологии цифровой трансформации
Уровень высшего образования: бакалавриат

Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

Информационная безопасность
Рабочая программа дисциплины
Составитель
канд. ист. наук, доц., доц. *И.А. Русецкая*
Ответственный редактор
канд. ист. наук, доц., директор ИИНТБ *Г.А. Шевцова*

УТВЕРЖДЕНО
Протокол заседания кафедры
информационной безопасности
№ 11 от 18.03.2024

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины - формирование знаний о совокупности проблем в сфере науки, техники и технологий, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере, понимания основных принципов, направлений и методов обеспечения информационной безопасности.

Задачи дисциплины: изучить теорию и методологию обеспечения защищенности объектов в условиях существования угроз в информационной сфере с целью научить владению понятийным аппаратом в области информационной безопасности, сформировать способности к осуществлению подбора, изучения и обобщения научно-технической литературы, нормативных материалов по вопросам обеспечения информационной безопасности и их использованию в практической деятельности.

1.2. Перечень планируемых результатов обучения по дисциплине (*модулю*), соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ОПК-3 Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*ОПК-3.*1Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*Знать:* цели и принципы защиты информации; основные понятия в области информационной безопасности и защиты информации; современную доктрину информационной безопасности РФ.
	ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*Уметь:* раскрывать назначения, сущности и структуры систем защиты информации; ставить цели и выбирать пути эффективного решения задач в области информационной безопасности.
	ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	*Владеть:* умением анализировать существующие угрозы информационной безопасности и пути их нейтрализации и устранения; подходами к использованию информационных технологий для создания мер по защите информации.
ОПК-4 Способность участвовать в разработке стандартов, норм и правил, а также технической	*ОПК-4.1* Знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	*Знать:* базовые содержательные положения в области информационной безопасности и защиты информации; виды и методы обеспечения информационной безопасности; понятие и структуру комплексных систем обеспечения информационной

документации, связанной с профессиональной деятельностью		безопасности
	ОПК-4.2 Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	*Уметь:* устанавливать структуры угроз ИТ-инфраструктуры; выявлять факторы, влияющие на защиту информации; устанавливать и раскрывать сущности компонентов защиты информации
	ОПК-4.3 Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы	*Владеть:* принципами и методами управления информационной безопасностью.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к обязательной части блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Информационные технологии», «Информационно-коммуникационные технологии».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: «Разработка и внедрение информационных систем», «Управление информационными системами».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	**16**
3	Практические работы	**26**
	Всего:	**42**

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет _66_ академических часов.

3. Содержание дисциплины

Введение. Сущность и понятие информационной безопасности, безопасности информации и защиты информации.

Значение и место курса в подготовке специалистов по защите информации. Связь с другими дисциплинами учебного плана.

Структура курса.

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.

Методологическая основа для раскрытия сущности и определения понятия защиты информации.

Существующие подходы к содержательной части понятия “защиты информации” и способы реализации содержательной части.

Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие “утечка информации”. Соотношение форм и видов уязвимости информации.

Понятие безопасности информации.

Сущность информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия “информационная безопасность”.

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.

Значение защиты информации применительно к областям деятельности. Значение защиты информации в области внешней политики, экономики, в военной области и в социальной сфере.

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.

Современная нормативная база в области информационной безопасности. Базовые законы в области информационной безопасности.

Понятие и назначение Доктрины информационной безопасности РФ. Интересы личности, общества и государства в информационной сфере. Виды и состав угроз информационной безопасности РФ. Состояние информационной безопасности Российской Федерации. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Особенности обеспечения информационной безопасности в различных сферах общественной жизни. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.

Полномочия органов государственной власти, специальных федеральных органов и предприятий в области обеспечения информационной безопасности. Полномочия органов законодательной власти, Президента, Правительства, органов исполнительной и судебной власти в области обеспечения информационной безопасности. Полномочия Совета Безопасности и Межведомственной комиссии по защите государственной тайны. Полномочия Федеральной службы безопасности, Федеральной службы по техническому и экспортному контролю, Министерства обороны, Службы внешней разведки в области защиты информации. Полномочия предприятий, учреждений и организаций в области защиты информации.

Понятие защищаемой информации и подходы к составу защищаемой информации.

Критерии отнесения открытой 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 различных типов носителей защищаемой информации.

Классификация конфиденциальной информации по видам тайн

Виды тайн. Показатели разделения конфиденциальной информации на виды тайны.

Определение понятия «государственная тайна». Правовое регулирование защиты информации, относимой к государственной тайне. Основания отнесения информации к государственной тайне. Перечни 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.

Понятие коммерческой тайны. Правовое регулирование защиты коммерческой тайны. Основания и методика отнесения сведений к коммерческой тайне.

Подходы к сущности служебной тайны. Понятие служебной тайны, границы и области ее действия.

Понятия «личная тайна» и «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 и структура угроз защищаемой информации. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации.

Подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия.

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 конфиденциальной информации как составная часть угрозы информации.

Подходы к понятию канала несанкционированного доступа к информации. Соотношение между каналами несанкционированного доступа и каналами утечки информации.

Классификация и характеристика каналов несанкционированного доступа к конфиденциальной информации.

Методы несанкционированного доступа к конфиденциальной информации, применяемые при использовании каждого канала. Зависимость методов и форм их использования от целей и возможностей соперника.

Направления и виды разведывательной деятельности, их соотношение и взаимосвязь.

Агентурная разведка. Техническая разведка. Легальная разведка. Промышленный шпионаж.

Особенности деятельности разведывательных органов при добывании информации.

Внешняя разведка РФ. Сферы деятельности органов внешней разведки РФ. Правовое регулирование деятельности органов внешней разведки России.

Классификация видов, методов и средств защиты информации. Объекты защиты информации. Назначение и структура систем 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 и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты.

Понятие объекта защиты.

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

Хранилища 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.

Понятие «система защиты информации». Назначение систем.

Классификация систем защиты информации, сферы их действия.

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

Структура системы защиты информации, назначение составных частей системы. Требования к системам защиты информации.

Кадровое, ресурсное и технологическое обеспечение систем защиты информации.

4. Образовательные технологии

Для проведения учебных занятий по дисциплине используются различные образовательные технологии. Для организации учебного процесса может быть использовано электронное обучение и (или) дистанционные образовательные технологии.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Максимальное количество баллов
Текущий контроль: - опрос (устный или письменный) - участие в дискуссии на семинаре - контрольная работа - тестирование - реферат	25 баллов (5 письменных заданий по 5 баллов каждое) 5 баллов 10 баллов 10 баллов 10 баллов
Промежуточная аттестация (зачет с оценкой)	40 баллов
Итого за семестр	100 баллов

Текущий контроль (опрос, в том числе в виде выполнения интерактивных заданий, участие в дискуссии, тестирование) проводится в устном или письменном виде; контрольная работа, реферат — в письменном виде.

Промежуточная аттестация (зачет с оценкой) проводится в форме коллоквиума в устном виде.

Система текущего и промежуточного контроля знаний студентов по дисциплине предусматривает проверку сформированности компетенций ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-4.1; ОПК-4.2; ОПК-4.3.

Полученный совокупный результат (максимум 100 баллов) конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

<table>
<tr><td>100-балльная шкала</td><td colspan="2">Традиционная шкала</td><td>Шкала ECTS</td></tr>
<tr><td>95 – 100</td><td rowspan="2">отлично</td><td rowspan="5">зачтено</td><td>A</td></tr>
<tr><td>83 – 94</td><td>B</td></tr>
<tr><td>68 – 82</td><td>хорошо</td><td>C</td></tr>
<tr><td>56 – 67</td><td rowspan="2">удовлетворительно</td><td>D</td></tr>
<tr><td>50 – 55</td><td>E</td></tr>
<tr><td>20 – 49</td><td rowspan="2">неудовлетворительно</td><td rowspan="2">не зачтено</td><td>FX</td></tr>
<tr><td>0 – 19</td><td>F</td></tr>
</table>

5.2.Критерии выставления оценки по дисциплине

Общим критерием оценки служит освоение студентом фактических данных, основных терминов и понятий, а также способность ориентироваться в концептуальных подходах в области методологии и теории информационной безопасности и защиты информации.

Оценка результатов устных, письменных **опросов** (в том числе при выполнении интерактивных заданий) **и участия в дискуссии** на семинаре предполагает использование следующих критериев оценки:

- 5 баллов: проблема освещена полностью с использованием элементов творческого подхода;
- 4 балла: проблемы освещена грамотно, но имеется ряд недостатков;

- 3 балла: проблема освещена в целом;
- 2 балла: низкий уровень освоения материала, требуется дополнительная работа;
- 1 балл: работа выполнена, но либо уровень освоения материала неприемлемо низкий, либо работа является полностью списанной.

Оценка **реферата** предполагает использование следующих критериев:

- 11-15 баллов: тема реферата раскрыта полностью с использованием элементов творческого подхода, соблюдены общие требования к содержанию, качеству, стилю изложения и оформлению реферата, студент продемонстрировал знакомство с основной и дополнительной литературой по теме реферата, возможны незначительные недостатки;
- 6-10 баллов: тема реферата раскрыта достаточно полно, в целом соблюдены общие требования к содержанию, качеству, стилю изложения и оформлению реферата, студент продемонстрировал знакомство с основной литературой по теме реферата, однако работа содержит ряд недостатков;
- 0-5 баллов: тема реферата раскрыта не полностью, не в полной мере соблюдены общие требования к содержанию, качеству, стилю изложения и оформлению реферата, студент продемонстрировал знакомство с основной литературой по теме реферата, работа содержит ряд значительных недостатков.

Критерии оценки **контрольных работ**:

- 9-10 баллов - проблема освещена полностью с использованием элементов творческого подхода;
- 6-8 баллов - проблема освещена грамотно, но имеется ряд недостатков;
- 3-5 баллов - проблема освещена в целом;
- 0-2 балла - неприемлемый уровень освоения материала, требуется дополнительная работа.

Критерии оценки **тестов** (каждый тест содержит 40 вопросов):

- 10 баллов - правильно отвечено на 40 вопросов теста;
- 9 баллов - правильно отвечено на 36-39 вопросов теста;
- 8 баллов - правильно отвечено на 32-35 вопросов теста;
- 7 баллов - правильно отвечено на 28-31 вопросов теста;
- 6 баллов - правильно отвечено на 24-27 вопросов теста;
- 5 баллов - правильно отвечено на 20-23 вопросов теста;
- 4 балла - правильно отвечено на 16-19 вопросов теста;
- 3 балла - правильно отвечено на 12-15 вопросов теста;
- 2 балла - правильно отвечено на 8-11 вопросов теста;
- 1 балл - правильно отвечено на 4-7 вопросов теста.

Промежуточная аттестация (зачет с оценкой в форме коллоквиума)

Оценка **коллоквиума** проводится с учетом следующих критериев:

30-40 баллов выставляется студенту, который полно и всесторонне освоил материал, предусмотренный программой, в достаточной мере ознакомился с основной и дополнительной литературой по курсу при условии правильного ответа на вопросы, заданные преподавателем в ходе коллоквиума и дополнительные вопросы.

20-29 баллов ставится студенту, который показал достаточно полное знание материала, ответил на большую часть вопросов, заданных преподавателем в ходе коллоквиума, однако допустил в ходе ответа на вопросы ряд неточностей и недочетов.

10-19 баллов выставляется студенту, который продемонстрировал знание основного материала и знакомство с основной литературой по дисциплине, но допустил ряд существенных ошибок при участии в коллоквиуме.

0-9 баллов ставится студенту, который не усвоил предусмотренный программой материал, допустил принципиальные ошибки при ответе на вопросы коллоквиума.

Оценка за зачет ставится также путем суммирования баллов за текущий контроль и

промежуточную аттестацию и переводом итоговой суммы в традиционную шкалу (см. таблицу выше).

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Текущий контроль ***(проверка сформированности компетенций ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-4.1; ОПК-4.2; ОПК-4.3)***

Примерная тематика **контрольных работ**:

1. Анализ современных подходов к определению понятий «защита информации», «безопасность информации», «информационная безопасность», «утечка информации», «уязвимость информации».
2. Значение защиты информации для субъектов информационных отношений в сферах их деятельности.
3. Соотношение источников, видов и способов дестабилизирующего воздействия на информацию с видами носителей и формами проявления уязвимости информации.
4. Источники, виды, способы и результаты дестабилизирующего воздействия на объекты защиты информации (кроме носителей).
5. Соотношение между видами и универсальными методами защиты информации и объектами защиты.

Темы **рефератов**:

1. Понятие, сущность, цели и значение защиты информации.
2. Виды и состав угроз информационной безопасности.
3. Задачи, принципы и методы обеспечения информационной безопасности.
4. Критерии, условия, принципы и формы отнесения информации к защищаемой.
5. Анализ существующих подходов к классификации конфиденциальной информации по видам тайны.
6. Виды и характеристика носителей защищаемой информации.
7. Структура и характеристика угроз защищаемой информации.
8. Соотношение угроз защищаемой информации с видами носителей и формами проявления уязвимости информации.
9. Соотношение видов разведывательной деятельности с каналами и методами несанкционированного доступа к конфиденциальной информации.
10. Классификация и характеристика объектов защиты информации.
11. Классификация и характеристика видов, методов и средств защиты информации и их соотношение с объектами защиты.
12. Сущность, назначение и структура систем защиты информации.

Примерные вопросы для **тестирования**:

1. Официальные определения понятия "информационная безопасность" сформулированы в следующих нормативных актах:
    a) закон "О государственной тайне" и Гражданский кодекс РФ
    b) Доктрина информационной безопасности РФ
    c) закон "Об информации, информационных технологиях и защите информации" и Конституция РФ
2. Чтобы быть достаточной для принятия необходимых решений, информация должна:
    a) отвечать требованиям полноты, своевременности, достоверности
    b) быть надежно защищенной от несанкционированного доступа

c) передаваться по современным сетям передачи данных

3. К формам проявления уязвимости информации относятся:
   a) хищение, несанкционированное уничтожение информации (или ее носителя), несанкционированная модификация, блокирование, разглашение информации, потеря носителя информации
   b) утечка и утрата информации
   c) несанкционированное размножение, перехват, фальсификация, распространение информации
4. Принципы отнесения информации к защищаемой делятся на:
   a) Зафиксированные в законах или нормативных документах отдельного предприятия
   b) Правовые и организационные
   c) Первоочередные и второстепенные
5. Безопасность информации – это состояние защищенности информации от:
   a) внутренних и внешних угроз
   b) случайных или преднамеренных несанкционированных воздействий или ее несанкционированного получения
   c) воздействий, нарушающих ее статус
6. К безопасности информации непосредственное отношение имеет следующий вид угроз информационной безопасности:
   a) угрозы безопасности информационных и телекоммуникационных средств и систем
   b) угрозы информационному обеспечению государственной политики РФ
   c) угрозы развитию российской индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи
7. Информационная безопасность РФ и национальная безопасность РФ связаны между собой следующим образом:
   a) информационная безопасность – самостоятельный вид национальной безопасности
   b) информационная безопасность – отдельная составляющая национальной безопасности, а также аспект безопасности в других сферах общественной жизни
   c) эти понятия не взаимосвязаны
8. Адвокатская тайна – это разновидность:
   a) государственной тайны
   b) профессиональной тайны
   c) служебной тайны
9. Информация в виде символов может отображаться в:
   a) бумажных, магнитных, оптических носителях
   b) физических полях, выпускаемой продукции и технологических процессах производства
   c) в носителях любого вида
10. К утрате информации приводят:
   a) разглашение информации
   b) хищение информации при сохранности ее носителя у владельца
   c) несанкционированное уничтожение информации
11. Утечка и разглашение информации связаны между собой следующим образом:
   a) утечка приводит к разглашению информации
   b) разглашение информации приводит к ее утечке
   c) это одно и то же
12. Основным критерием отнесения информации к конфиденциальной является:
   a) возможность получения преимуществ от использования информации за счет неизвестности ее третьим лицам

b) необходимость информации для финансовой деятельности
c) наличие технических возможностей для защиты носителей информации

13. Является ли информация, составляющая государственную тайну, конфиденциальной?
a) да
b) нет
c) только информация с грифом "секретно"

14. Личная тайна – это вид тайны, включающий в себя:
a) устанавливаемую гражданином и (или) законодательством информацию ограниченного доступа о частной жизни гражданина, которая защищается гражданином и (или) уполномоченными на то юридическими и физическими лицами в интересах гражданина
b) защищаемую физическим лицом информацию личного характера, распространение которой может нанести моральный или материальный ущерб отдельному физическому лицу
c) информацию, составляющую тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, врачебную тайну и т.п.

15. Как соотносятся между собой причины и обстоятельства дестабилизирующего воздействия на информацию?
a) обстоятельства предопределяют возникновение причин
b) обстоятельства возникают в силу существующих причин дестабилизирующего воздействия
c) причины и обстоятельства в данном случае означают одно понятие

16. Поломка (разрушение) технических средств обработки информации, в том числе разрыв (повреждение) кабельных линий связи – это вид воздействия со стороны:
a) природных явлений
b) людей
c) людей и природных явлений

17. В рамках легальной разведки может использоваться такой канал несанкционированного доступа как:
a) Вербовка или внедрение агентов
b) Изучение доступных источников информации
c) Организация физического проникновения к носителям конфиденциальной информации

18. В законе "О государственной тайне" содержится:
a) Перечень сведений, составляющих государственную тайну
b) Перечень сведений, отнесенных к государственной тайне
c) Перечень сведений, подлежащих засекречиванию

19. Формами проявления уязвимости информации являются:
a) разглашение, потеря, хищение
b) несанкционированная модификация, блокирование, уничтожение
c) все вышеперечисленные формы

20. В чем заключаются различия между личной тайной и персональными данными?
a) Нет различий
b) Информацию, составляющую личную тайну создает само это лицо, а персональные данные формируются без его участия
c) Личная тайна – это разновидность профессиональной тайны, а персональные данные – служебной

21. Информация в виде технических решений может отображаться в:
a) бумажных и магнитных носителях
b) выпускаемой продукции и технологических процессах производства
c) такого вида отображения информации не существует

22. Относятся ли средства транспортировки носителей защищаемой информации к

объектам защиты?

a) Да
b) Нет
c) Да, но только если это носители информации, составляющей государственную тайну

23. К опосредованным носителям защищаемой информации относятся:
    a) физические лица
    b) носители на фотоэмульсионной основе
    c) геометрические формы, размеры и архитектурные особенности строений
24. К факторам, как составляющей угрозы защищаемой информации, относятся:
    a) источники виды и способы дестабилизирующего воздействия
    b) причины и обстоятельства дестабилизирующего воздействия
    c) причины и обстоятельства дестабилизирующего воздействия и каналы несанкционированного доступа к конфиденциальной информации
25. Системы обеспечения функционирования технических средств обработки информации включают в себя:
    a) системы электроснабжения, водоснабжения, теплоснабжения, кондиционирования
    b) вспомогательные электрические и радиоэлектронные средства (электрические часы, бытовые магнитофоны, радиоприемники, телевизоры и др.)
    c) все перечисленные в пунктах а) и б) системы и средства
26. По каким критериям можно классифицировать системы защиты информации?
    a) по видам тайны, категориям защищаемой информации, объектам защиты
    b) по видам угроз защищаемой информации
    c) по уровню затрат на построение системы
27. Самым опасным источником дестабилизирующего воздействия являются:
    a) люди
    b) технические средства обработки информации
    c) природные явления
28. Одним из видов дестабилизирующего воздействия со стороны технических средств обработки информации является:
    a) несанкционированное распространение конфиденциальной информации
    b) создание электромагнитных излучений
    c) непосредственное воздействие на носители защищаемой информации
29. Выход из строя технических средств обработки информации как вид дестабилизирующего воздействия приводит к:
    a) искажению и уничтожению информации
    b) разглашению и блокированию информации
    c) искажению, уничтожению и блокированию информации
30. К причинам, вызывающим преднамеренное дестабилизирующее воздействие со стороны людей, относятся:
    a) стремление получить материальную выгоду, продвинуться по службе, обезопасить себя от угроз, шантажа
    b) тяжелое материальное положение, алчность, недовольство служебным положением, зависть, тщеславие
    c) плохие взаимоотношения между сотрудниками, недостаточный контроль и внимание со стороны администрации вопросам защиты информации
31. Канал несанкционированного доступа и канал утечки информации…
    a) Одно и то же
    b) Различаются соотношением с формами уязвимости информации и направлением воздействия
    c) Различаются количеством и составом каналов
32. К видам разведывательной деятельности относятся:

a) агентурная, техническая, легальная разведка
b) политическая, экономическая, военная разведка
c) внешняя и внутренняя разведка

33. Главным органом внешней разведки РФ является:
a) Министерство обороны
b) Федеральная служба безопасности
c) Служба внешней разведки

34. На уровне частных объединений разведывательные органы преимущественно существуют в виде:
a) Разведывательных служб в составе подразделений безопасности
b) Самостоятельных разведывательных подразделений в составе предприятия
c) Специализированных разведывательных служб, являющихся самостоятельными предприятиями

35. К объектам хранения письменных и визуальных носителей информации относятся:
a) Помещения службы защиты информации, а также помещения, в которых ведется работа сотрудников с защищаемой информацией
b) Технические средства обработки, получения, хранения и передачи информации
c) Здания предприятия и прилегающая к ним территория

36. К видам защиты информации относятся:
a) Правовая, организационная,
b) программно-аппаратная, инженерно-техническая, криптографическая
c) все, перечисленные в пунктах а) и б) виды

37. Какая группа методов относится к криптографическим:
a) Принуждение и побуждение
b) Учет и регламентация
c) Шифрование и кодирование

38. Ответственность за организацию защиты информации на предприятии несет:
a) Каждый сотрудник предприятия
b) Руководитель предприятия
c) Начальник службы безопасности

39. Комплексность системы защиты информации:
a) Обеспечивает необходимые составляющие защиты и устанавливает связи между ними
b) Требует полноты этих составляющих, всеохватности защиты информации
c) Обеспечивает руководство и управление системой

40. Какие из этих требований предъявляются к системам защиты информации?
a) Целостность и всеохватность
b) Привязанность к задачам защиты информации на конкретном предприятии и достаточность для решения этих задач
c) Обе группы требований.

Промежуточная аттестация (зачет с оценкой) ***(проверка сформированности компетенций ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-4.1; ОПК-4.2; ОПК-4.3)***

Примерные контрольные вопросы к **коллоквиуму:**

1. Сущность и понятие информационной безопасности и защиты информации.
2. Место информационной безопасности в системе национальной безопасности.
3. Структура угроз информационной безопасности.
4. Принципы обеспечения информационной безопасности.
5. Место защиты информации в системе информационной безопасности.

6. Организационные основы системы обеспечения информационной безопасности РФ.
7. Основные положения государственной политики обеспечения информационной безопасности РФ.
8. Виды угроз информационной безопасности РФ.
9. Цели и значение защиты информации.
10. Соотношение защиты информации с уязвимостью информации.
11. Каналы и методы несанкционированного доступа к защищаемой информации.
12. Формы и виды проявления уязвимости информации.
13. Причины, обстоятельства и условия дестабилизирующего воздействия на информацию.
14. Виды и способы дестабилизирующего воздействия на информацию.
15. Источники дестабилизирующего воздействия на информацию.
16. Критерии, условия и принципы отнесения информации к защищаемой.
17. Соотношение между носителем и источником защищаемой информации.
18. Носители письменной, видовой, излучаемой информации.
19. Опосредованные носители защищаемой информации.
20. Классификация защищаемой информации по видам тайн.
21. Методологические подходы к определению понятий различных видов тайны.
22. Методика отнесения сведений к государственной тайне.
23. Классификация сведений, составляющих государственную тайну, по степеням и грифам секретности.
24. Методика отнесения сведений к коммерческой тайне.
25. Отличительные особенности служебной тайны.
26. Особенности и разновидности профессиональной тайны.
27. Общее и различия между личной тайной и персональными данными.
28. Защита персональных данных в РФ.
29. Виды и методы разведывательной деятельности.
30. Основные методы легальной разведки и промышленного шпионажа.
31. Понятие и виды объектов защиты информации.
32. Органы защиты государственной тайны в РФ.
33. Правовое обеспечение информационной безопасности в РФ.
34. Классификация видов и методов защиты информации.
35. Основные методы правовой защиты информации.
36. Организационная защита информации: понятие и основные принципы.
37. Универсальные и локальные методы защиты информации.
38. Методы и средства программно-аппаратной, инженерно-технической и криптографической защиты информации.
39. Состав кадрового, ресурсного и технологического обеспечения защиты информации.
40. Понятие и назначение систем защиты информации.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Основные источники

1. Федеральный закон «О безопасности» от 28.12.2010 №390-ФЗ http://www.consultant.ru/document/cons_doc_LAW_108546/

2. Федеральный закон «О государственной тайне» от 21.07.1993 N 5485-1 (ред. от 08.11.2011) http://www.consultant.ru/document/cons_doc_LAW_2481

3. Федеральный закон «Об информации, информационных технологиях и о защите

информации» от 27.07.2006 № 149-ФЗ http://www.consultant.ru/document/cons_doc_LAW_61798

4. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ http://www.consultant.ru/document/cons_doc_LAW_48699

5. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (ред. от 25.07.2011) http://www.consultant.ru/document/cons_doc_LAW_61801/

6. ГОСТ 50922-2006. Защита информации. Основные термины и определения. http://docs.cntd.ru/document/1200058320

7. Доктрина информационной безопасности Российской Федерации (утв. Президентом Рос. Федерации 05.12.2016 № Пр-646) http://ivo.garant.ru/#/document/71556224/paragraph/1:1

Основная литература

8. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1912987

9. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. - 2-е изд. - Москва : ДМК Пресс, 2023. - 594 с. - ISBN 978-5-89818-506-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/2107178

10. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие. - 2 ; доп. - Москва ; Москва : Издательство "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2017. - 239 с. - ISBN 978-5-00091-007-8. -Режим доступа: https://new.znanium.com/catalog/document?id=343811.

11.Криптографическая защита информации : учебное пособие / С.О. Крамаров, О.Ю. Митясова, С.В. Соколов [и др.] ; под ред. С.О. Крамарова. — Москва : РИОР : ИНФРА-М, 2023. — 321 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1716-6. - ISBN 978-5-369-01716-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1899016

Дополнительная литература

11. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Москва: РИОР : Инфра-М, 2019. - 336 с. - ВО - Бакалавриат. - ISBN 978-5-369-01761-6. -Режим доступа: https://new.znanium.com/catalog/document?id=336219.

12. Словарь терминов и определений по информационной безопасности и защите информации [Электронный ресурс] : учебно-справочное пособие : для бакалавриата по направлению 090900.62 "Информационная безопасность" / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информ. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. информац. безопасности ; [сост.: Ищейнов В. Я., Мецатунян М. В.]. - Москва : РГГУ, 2014. - 117 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009502. - ISBN 978-5-7281-1836-7

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

- http://www.consultant.ru/
- http://base.garant.ru/

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины «Информационная безопасность» необходима академическая аудитория для проведения лекционных и семинарских занятий, оборудованная необходимыми техническими средствами (доска, компьютер, проектор). Для трансляции презентаций при проведении семинаров необходимо приложение MS Office - Power Point.

Перечень программного обеспечения (ПО):

№п/п	Наименование ПО	Производитель	Способ распространения
1	Windows 10 Pro	Microsoft	лицензионное
2	Kaspersky Endpoint Security	Kaspersky	лицензионное
3	Microsoft Office 2016	Microsoft	лицензионное
4	Платформа ZOOM	Zoom	лицензионное

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

· для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

· для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

· для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.
При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.
Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.
Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:
· для слепых и слабовидящих:
- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.
· для глухих и слабослышащих:
- в печатной форме;
- в форме электронного документа.
· для обучающихся с нарушениями опорно-двигательного аппарата:
- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.
Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:
· для слепых и слабовидящих:
- устройством для сканирования и чтения с камерой SARA CE;
- дисплеем Брайля PAC Mate 20;
- принтером Брайля EmBraille ViewPlus;
· для глухих и слабослышащих:
- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;
· для обучающихся с нарушениями опорно-двигательного аппарата:
- передвижными, регулируемыми эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий

Практическое занятие № 1. Сущность и понятие информационной безопасности, безопасности информации и защиты информации (2 часа) (*проверка сформированности компетенций - ОПК-3.1, ОПК-3.2, ОПК-4.1).*

Практические задания:

1. Составить схему, отражающую связи между понятиями «защита информации», «безопасность информации», «информационная безопасность».
2. Составить таблицу, раскрывающую названия и примеры форм проявления уязвимости информации, результатом которых может являться:
   а) утечка информации;
   б) утрата информации.

Контрольные вопросы:

1. Сходство и различие понятий «безопасность информации» и «информационная

безопасность».

2. Сходство и различие понятий «защита информации» и «безопасность информации».

Список источников и литературы:

https://new.znanium.com/catalog/document?id=336219.-C.32-92.

Практическое занятие № 2. Цели и задачи защиты информации (2 часа) (*проверка сформированности компетенций - ОПК-3.1, ОПК 3.3, ОПК-4.1)*

Практическое задание:

Составить таблицу, содержащую примеры, указывающие на значение защиты информации в экономической, политической, военной, научной и социальной областях деятельности.

Контрольные вопросы:

1. Различия между целями и задачами защиты информации.
2. Оценка современных подходов к выявлению значения защиты информации в различных областях деятельности.

Практическое занятие № 3. Значение информационной безопасности в рамках национальной безопасности России и современная система защиты информации в РФ (2 часа) (*проверка сформированности компетенций - ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.3).*

Практическое задание (выполняется письменно в текстовом виде или в табличной форме):

На основе анализа Доктрины информационной безопасности России определить основные положения государственной политики обеспечения информационной безопасности, выделить первоочередные мероприятия по обеспечению информационной безопасности РФ и дать им характеристику.

Контрольные вопросы:

1. Основные угрозы информационной безопасности России согласно Доктрине информационной безопасности России.
2. Цели и значение Доктрины информационной безопасности России.

Практическое занятие № 4. Состав и классификация носителей защищаемой информации (2 часа) (*проверка сформированности компетенций - ОПК-3.2, ОПК-4.1, ОПК-4.3).*

Занятие проводится в форме дискуссии.

Цель занятия: развитие способности логически верно, аргументировано и ясно строить устную речь, публично представлять собственные и известные научные выводы на примере анализа состава и классификации носителей защищаемой информации.

Правила проведения: дискуссия проводится после изучения материалов лекции по соответствующей теме, анализа литературы в ходе самостоятельной работы студентов с привлечением максимального числа участников — студентов группы.

Функции и схемы взаимодействия участников: студенты участвуют в устной дискуссии, помогающей раскрыть следующие вопросы:

1. Анализ сущности и соотношения понятий «носитель информации» и «источник информации».
2. Подходы к классификации носителей защищаемой информации.
3. Анализ свойств и значения носителей защищаемой информации.
4. Анализ достоинств и недостатков человека как носителя защищаемой информации.
5. Анализ достоинств и недостатков письменных носителей на бумажной основе.
6. Изучение особенностей электронных носителей информации.
7. Анализ сферы, методов использования и особенностей видовых носителей защищаемой информации.
8. Опосредованные носители защищаемой информации: особенности применения, достоинства и недостатки.

Система оценки: см. раздел «Принципы оценки форм текущего контроля и промежуточной аттестации. Текущий контроль».

Практическое занятие № 5. Классификация конфиденциальной информации по видам тайн (2 часа) (*проверка сформированности компетенций - ОПК-3.1, ОПК-3.2, ОПК-3.3, ОПК-4.1, ОПК-4.3).*

Практическое задание: Составить таблицу, в которой для каждого из рассмотренных видов тайны указаны:

а) основные законодательные акты, регулирующие защиту того или иного вида тайны;

б) основные особенности защиты того или иного вида тайны;

в) грифы или пометки ограничения доступа;

г) обладатель информации, составляющей тот или иной вид тайны.

Контрольные вопросы:

1. Определить сущность и понятие государственной тайны.
2. Перечислить основные законодательные акты, регулирующие защиту государственной тайны в РФ.
3. Дать определения понятиям «коммерческая тайна», «профессиональная тайна», «служебная тайна», «личная тайна».
4. Перечислить и охарактеризовать разновидности профессиональной тайны.
5. Выявить сходства и различия понятий «личная тайна» и «персональные данные».
6. Описать методику отнесения сведений к коммерческой тайне.

Практическое занятие № 6. Понятие и структура угроз защищаемой информации (2 часа) (*проверка сформированности компетенций - ОПК-3.1, ОПК-4.2).*

Практическое задание (выполняется по вариантам):

Определить основные составляющие угрозы защищаемой информации для следующих объектов защиты:

- пластиковая банковская карта;
- веб-сервер;
- компьютер, стоящий в отделе кадров;
- мобильный телефон;
- комната для переговоров в охраняемом здании;
- кабинет руководителя;
- компьютер, на котором обрабатываются и хранятся сведения, составляющие коммерческую тайну организации;
- компьютер, на котором обрабатываются и хранятся сведения о работниках организации;
- территория, окружающая предприятие;
- здание предприятия с окружающей его территорией;
- телефонная сеть;
- поликлиника;
- университет;
- отделение банка;
- работник организации, допущенный к конфиденциальной информации.

Контрольные вопросы:

1. Дать определение источника дестабилизирующего воздействия на защищаемую информацию.
2. Привести классификацию источников дестабилизирующего воздействия на защищаемую информацию.
3. Привести классификацию и дать характеристику видов и способов

дестабилизирующего воздействия на информацию.

4. Привести определение и классификацию каналов несанкционированного доступа к информации.
5. Привести определение и классификацию методов несанкционированного доступа к информации по каждому каналу.

Практическое занятие № 7. Направления, виды разведки и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации (2 часа) (*проверка сформированности компетенций - ОПК-3.1, ОПК-4.2).*

Занятие проводится в форме выполнения проблемно-ориентированного задания с использованием кейс-метода.

Цель занятия: осмысление практической ситуации, актуализирующей комплекс знаний, который необходимо усвоить при решении данной проблемы и который включает в себя изучение возможностей реализации угроз конфиденциальной информации при несанкционированном доступе к ней.

Правила проведения: группу разбивают на подгруппы и передают информацию в виде фактов, основывающихся на реальной ситуации и просят обсудить проблемы, проанализировать вопросы и дать рекомендации.

Функции и схемы взаимодействия участников:

1. Подготовительный этап.

1. Подготовительный этап.

Определение места занятия в изучении данной дисциплины, цели и задачи занятия.

2. Ознакомительный этап.

На данном этапе происходит вовлечение студентов в решение профессиональной ситуации.

Описание ситуации: в качестве объекта защиты выступает факультет защиты информации в составе всех своих подразделений, расположенный по адресу: Кировоградская улица, дом 25, корпус 1.

Постановка задачи: выявить возможные источники дестабилизирующего воздействия на защищаемую информацию, виды и способы воздействия, каналы и методы несанкционированного доступа к защищаемой информации, а также возможные действия злоумышленников по добыванию информации.

Определение информационного материала: конспекты лекций, источники и литература, изученные в ходе самостоятельной работы студентов.

3. Основной (аналитический) этап.

- распределение студентов по группам (4-5 человек в каждой);
- организация работы групп: краткое изложение членами групп изученных материалов и их обсуждение; выявление проблемных моментов; определение докладчиков.
- первый раунд дискуссии - обсуждение проблемных моментов в малых группах, поиск аргументов и решений.
- второй раунд дискуссии - представление результатов анализа, общегрупповая дискуссия, подведение итогов дискуссии и найденных решений.

4. Итоговый этап.

Заключительная презентация результатов аналитической работы (студенты могут узнать и сравнить несколько подходов к проблеме); обобщающее выступление преподавателя – анализ ситуации; оценка полученных знаний.

Система оценки: см. раздел «Принципы оценки форм текущего контроля и промежуточной аттестации. Текущий контроль».

Практическое занятие № 8. Классификация видов, методов и средств защиты информации защиты информации (2 часа) (*проверка сформированности компетенций* -

ОПК-3, ОПК-4).
Занятие проводится в форме дискуссии.
Цель занятия: развитие способности логически верно, аргументировано и ясно строить устную речь, публично представлять собственные и известные научные выводы на примере анализа состава и классификации носителей защищаемой информации.
Правила проведения: дискуссия проводится после изучения материалов лекции по соответствующей теме, анализа литературы в ходе самостоятельной работы студентов с привлечением максимального числа участников — студентов группы.
Функции и схемы взаимодействия участников: студенты участвуют в устной дискуссии, помогающей раскрыть следующие вопросы:

1. Классификация и характеристика универсальных и локальных методов защиты информации.
2. Изучение областей и особенностей применения организационных, криптографических и инженерно-технических методов защиты информации.
3. Оценка современных подходов в области классификации средств защиты информации.
4. Изучение состава и характеристик средств защиты информации.

Система оценки: см. раздел «Принципы оценки форм текущего контроля и промежуточной аттестации. Текущий контроль».

Практическое занятие № 9. Объекты защиты информации (2 часа) (*проверка сформированности компетенций - ОПК-3.3, ОПК-4.2, ОПК-4.3).*
Занятие проводится в форме выполнения проблемно-ориентированного задания с использованием кейс-метода.
Цель занятия: осмысление практической ситуации, актуализирующей комплекс знаний, который необходимо усвоить при решении данной проблемы и который включает в себя изучение возможностей реализации угроз конфиденциальной информации при несанкционированном доступе к ней.
Правила проведения: группу разбивают на подгруппы и передают информацию в виде фактов, основывающихся на реальной ситуации и просят обсудить проблемы, проанализировать вопросы и дать рекомендации.
Функции и схемы взаимодействия участников:
1. Подготовительный этап.
Определение места занятия в изучении данной дисциплины, цели и задачи занятия.
2. Ознакомительный этап.
На данном этапе происходит вовлечение студентов в решение профессиональной ситуации.
Описание ситуации: в качестве объекта исследования выступает факультет защиты информации в составе всех своих подразделений, расположенный по адресу: Кировоградская улица, дом 25, корпус 1.
Постановка задач:

- выявление и анализ видов защищаемой информации, циркулирующей на факультете;
- выявление и анализ достоинств и недостатков существующей системы защиты информации по объектам защиты информации;
- предложение мер совершенствования защиты информации на факультете по объектам защиты.

Определение информационного материала: конспекты лекций, источники и литература, изученные в ходе самостоятельной работы студентов.
3. Основной (аналитический) этап.

- распределение студентов по группам (4-5 человек в каждой);
- организация работы групп: краткое изложение членами групп изученных

материалов и их обсуждение; выявление проблемных моментов; определение докладчиков.
- первый раунд дискуссии - обсуждение проблемных моментов в малых группах, поиск аргументов и решений.
- второй раунд дискуссии - представление результатов анализа, общегрупповая дискуссия, подведение итогов дискуссии и найденных решений.

4. Итоговый этап.
Заключительная презентация результатов аналитической работы (студенты могут узнать и сравнить несколько подходов к проблеме);
обобщающее выступление преподавателя – анализ ситуации;
оценка полученных знаний.
Система оценки: см. раздел «Принципы оценки форм текущего контроля и промежуточной аттестации. Текущий контроль».

Практическое занятие № 10. Назначение и структура систем защиты информации (2 часа) (*проверка сформированности компетенций - ОПК-3.1, ОПК-3.3, ОПК-4.3).*
Практическое задание:
Составить таблицу, раскрывающую для различных видов систем защиты информации:
- структуру систем;
- основные требования к построению;
- состав кадрового, ресурсного и технологического обеспечения систем защиты информации.

Контрольные вопросы: см. вопросы для контрольной работы и тестирования.

9.2. Методические рекомендации по подготовке письменных работ

Требования к рефератам

Рефераты являются составной частью самостоятельной учебно-исследовательской работы студента и предназначены для углубленного изучения дисциплины, развития индивидуальных творческих способностей студента.
Задачами работы студента над рефератом работами являются:
· углубленное изучение выбранной темы;
· приобретение умения вести поиск необходимого фактического материала, его анализа и систематизации, формулирования научных целей и выводов;
· развития навыков грамотного и логически доказательного изложения текста;
· получение опыта правильного оформления научной работы.
Основными элементами реферата являются:
· титульный лист;
· содержание;
· введение;
· основная (содержательная) часть;
· заключение;
· список использованных источников и литературы;
· приложения.
Во введении содержатся:
· научное и практическое обоснование значения и актуальности выбранной темы и вытекающие из этого цели и задачи работы;
· анализ использованных, при написании работы, источников:
– опубликованных - документов органов государственной власти (законов, указов, постановлений и т.п.), документов органов государственного управления (постановлений, решений, стандартов, инструкций, правил и т.п.), отраслевых нормативных документов;
– неопубликованных - архивных фондов, рабочих инструкций, положений, правил, методик и

других документов, полученных из текущего делопроизводства или архивных фондов;
· анализ степени разработанности темы в научной литературе и обзор использованных при написании работы отечественной и зарубежной литературы (монографий, сборников статей, учебников, учебных пособий), дипломных и курсовых работ, текстов лекций и т.п.
· обоснование выбранной структуры письменной работы, состав и содержание глав (разделов) и подразделов, особенности размещения и изложения материала, наличие приложений, схем, графиков и таблиц.
Анализ источников и научной литературы должен быть конкретным и критическим, т.е. давать представление об их роли в раскрытии данной темы. При анализе источников и литературы их целесообразно группировать по отдельным проблемам или направлениям темы. Анализируемые источники и научная литература должны обязательно иметь подстрочные ссылки по тексту работы.
По объему введение не должно быть больше какой-либо главы (раздела) основной части работы.
Введение реферата должно иметь 1-2 листа печатного текста.
Основная (содержательная) часть работы строится в соответствии с разработанным по конкретной теме планом, позволяющим последовательно, логично и доказательно изложить материал и сделать вытекающие из него теоретические и практические выводы.
Основная часть реферата, как правило, подразделов не имеет, так как отражает исследование одного, достаточно узкого вопроса. Заголовком основной части реферата является заглавие темы.
Объем содержательной части реферата составляет 5-10 листов.
Выводы должны начинаться со слов «следовательно», «таким образом» и т.п. Не следует изложение выводов начинать с заголовка «выводы». Выводы не нумеруются, их можно излагать в виде абзацев или перечисления, начиная каждый вывод на новой строке с дефиса (–).
В заключении к работе даются общие итоги проведенного исследования, обобщаются результаты и выводы, содержится авторская оценка результатов с точки зрения соответствия их поставленным целям и задачам исследования, могут быть указаны перспективы и направления дальнейшей разработки темы.
Заключение реферата должно иметь от 0,5 до 1 листа печатного текста.
Общий объем реферата – от 7 до 13 листов печатного текста.
Текст письменной работы следует размещать соблюдая следующие размеры полей: левое – 30 мм, правое – 15 мм, верхнее и нижнее – 20 мм. Стандартная страница печатного текста должна иметь 30 строк по 70 знаков, включая пробелы.
Разрешается использовать компьютерные возможности для акцентирования внимания на отдельных терминах, формулах и т.п., применяя шрифты различной гарнитуры.
Иллюстрации могут быть выполнены в цветном исполнении.
В отпечатанной работе линии, буквы, цифры и знаки должны быть четкие, полностью пропечатанные.
Возможные опечатки (ошибки) должны быть закрашены корректирующей краской белого цвета, поверх которой наносится черной пастой (рукописным способом) правильный текст.
Повреждение листов и помарки на них не допускаются.
Каждая письменная работа должна иметь титульный лист. Реквизиты титульного листа печатаются через один интервал.
За титульным листом размещается содержание работы.
В содержании последовательно перечисляются все составные части работы. С правой стороны указываются номера страниц, с которых начинают излагаться разделы (подразделы). Номер страницы окончания главы (раздела) или подраздела не указывается. Буквы «Стр.» или «С» над номерами страниц не проставляются. Промежуток от окончания названия до номера страницы заполняют точками.
Слова «СОДЕРЖАНИЕ», «ВВЕДЕНИЕ», «ЗАКЛЮЧЕНИЕ», «СПИСОК

ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ печатаются заглавными буквами, как в содержании, так и по тексту работы.

Содержание печатается через один интервал; перед названием глав (разделов), словами «ЗАКЛЮЧЕНИЕ», «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ» оставляется по одной свободной строке (пробел).

Текст письменной работы должен быть написан грамотно, научным языком, тщательно отредактирован и проверен после распечатки.

Материал излагается от третьего лица, например: «нами установлено», «автором работы предложено» и т.д. Слова «я», «мною» и т.п. не применяются.

На каждой странице (листе) письменной работы ставится его порядковый номер (кроме титульного листа). Номер страницы ставится на верхнем поле в центре листа без каких-либо знаков препинания. Отсчет страниц начинается с титульного листа и заканчивается последним листом приложений. Шрифт номеров страниц может быть меньше шрифта текста (но не менее шрифта 12). Страницы нумеруются по порядку без пропусков и литерных добавлений.

Содержание, введение, заключение, список использованных источников и литературы, начинаются с нового листа.

Точки в конце заголовков не ставятся.

Все заголовки печатаются с абзаца, через один интервал, без выделения шрифтом.

Включаемые в текст реферата таблицы, схемы, графический материал и т.п. оформляются, как правило, непосредственно по тексту работы или на отдельных листах, помещаемых сразу за листом текста, к которому относятся.

Таблицу, рисунок и чертеж, размеры которого больше размеров формата А4, учитывают как одну страницу и складывают по размерам формата работы.

Таблицы применяются при изложении цифровой и словесной информации о нескольких объектах по ряду признаков, а также для лучшей наглядности или сравнения показателей.

Таблицы имеют два уровня размещения текста: вертикальный – графы и горизонтальный – строки. Если таблица располагается более чем на одной странице, или по тексту работы идут неоднократные ссылки на графы, то графы таблицы должны быть пронумерованы; на последующих страницах повторяются только номера граф (без заголовков).

Заголовки и подзаголовки граф и строк должны быть выражены именем существительным в именительном падеже единственного числа. В заголовках и подзаголовках строк и граф таблицы могут употребляться только общепринятые сокращения и условные обозначения. Заголовки граф центруются.

Перед каждой таблицей указывается слово «Таблица» и ее заголовок; если таблиц несколько, то их нумеруют в нарастающем порядке арабскими цифрами в пределах всей работы, например:

Таблица 2. Критерии оценки показателей качества СЗИ

Графы «№ п/п» в таблицу включать не следует.

При переносе таблицы на следующую страницу её заголовок не повторяют, а указывают (над продолжением таблицы, с левой стороны), что это продолжение, например «Продолжение таблицы 2».

В таблице разрешается применять шрифт меньший, чем используется в самой работе (но не менее шрифта 10).

Иллюстративный материал (чертежи, схемы, диаграммы, рисунки и т.п.) помещают в работе с целью установления свойств и характеристик объекта исследования или для лучшего понимания текста. Иллюстративный материал, несущий полезную информацию, должен располагаться непосредственно после текста, в котором о нем упоминается впервые, или на следующей странице, а в случае констатации факта – в приложении.

Под графическим материалом, при необходимости, помещают поясняющие данные (подрисуночный текст).

Помещаемые в работе чертежи, схемы, рисунки, диаграммы и т.д. должны выполняться в

соответствии с требованиями государственных стандартов.

Иллюстративный материал должен иметь название, которое помещают под ним, и нумероваться в нарастающем порядке арабскими цифрами в пределах всей работы, например:

«Схема 4. Оперограмма движения конфиденциального приказа».

Если в работе имеется только один чертеж (рисунок), схема, диаграмма и т.д., то его не нумеруют.

При внесении в текст формул и уравнений их следует выделять из текста в отдельную строку. Выше и ниже каждой формулы (уравнения) должно быть оставлено по одной свободной строке (пробел).

Если по тексту работы даются ссылки на формулы, то формулы нумеруют в нарастающем порядке арабскими цифрами в пределах всей работы в круглых скобках, в крайнем правом положении на строке.

Ссылки в тексте на порядковые номера формул также дают в скобках.

Пример расположения текста с формулой:

«Весомость оцениваемых направлений работ определялась по коэффициенту Zi,, вычисляемому по формуле (10):

$$Zi = \frac{(mn - Si)}{0{,}5\, mn\, (n - 1)}, \quad (10)$$

где m – число экспертов;

n - число направлений работы;

Si - сумма рангов по i–му направлению работы».

Если формула не умещается в одну строку, она может быть перенесена после знака равенства (=) или знаков действия (+, -, х, :); на новой строке знак равенства или действия повторяется.

Листы реферата должны быть сброшюрованы. (Скреплять листы канцелярской скрепкой не допускается).

При использовании в работе сокращений, их необходимо оформлять отдельным приложением. Список сокращений печатается через один интервал, без абзацев. Между названиями делается пропуск в один интервал (пробел).

Особое внимание следует обращать на правильное оформление ссылок на использованные в исследовании источники и научную литературу.

Список использованных источников и литературы должен включать все источники и литературу, с которыми автор знакомился при подготовке письменной работы.

Наименования источников и научной литературы печатаются через один интервал, с абзаца. Между названиями работ делается пропуск в один интервал (пробел). Включаемые в список источники и литература, как правило, не нумеруются.

На последнем листе списка источников и литературы ставятся подпись, фамилия и инициалы студента (автора работы), а также дата.

Приложение 1

АННОТАЦИЯ ДИСЦИПЛИНЫ

Целью курса является формирование знаний о совокупности проблем в сфере науки, техники и технологий, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере, понимания основных принципов, направлений и методов обеспечения информационной безопасности.

Задачи: анализ вопросов, связанных с сущностью и значением информационной безопасности, её местом в системе национальной безопасности, определением теоретических, концептуальных, методологических и организационных основ обеспечения безопасности объектов информатизации, анализом методов и средств защиты информации.

В результате освоения дисциплины обучающийся должен:

Знать основные понятия в области информационной безопасности и защиты информации; базовые содержательные положения в области информационной безопасности и защиты информации; современную доктрину информационной безопасности; цели и принципы защиты информации;

Уметь выявлять факторы, влияющие на защиту информации; устанавливать структуры угроз защищаемой информации; устанавливать и раскрывать сущности компонентов защиты информации; раскрывать назначения, сущности и структуры систем защиты информации; ставить цели и выбирать пути эффективного решения задач в области информационной безопасности;

Владеть классификацией защищаемой информации по видам тайны; умению анализировать существующие угрозы информационной безопасности и пути их нейтрализации и устранения; подходами к созданию комплекса мер по защите информации предприятия; навыками подбора, изучения и обобщения научно-технической литературы, нормативных материалов по вопросам обеспечения информационной безопасности.