Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт Информационных технологий и радиоэлектроники

УТВЕРЖДАЮ:
Директор института
_____Галкин А.А
«__26__» ___августа___ 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы информационной безопасности
(наименование дисциплины)

направление подготовки / специальность

10.05.04 «Информационно-аналитические системы безопасности»
(код и наименование направления подготовки (специальности)

направленность (профиль) подготовки

Автоматизация информационно-аналитической деятельности
(направленность (профиль) подготовки))

г. Владимир

2021 год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины *Основы информационной безопасности* является обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО и учебного плана по специальности 10.05.04 «Информационно-аналитические системы безопасности», формирование у студентов знаний и навыков в предметной области. Предмет курса - понятийный аппарат, а также сущность, теоретические, концептуальные, методологические аспекты и структура ИБ.

Профессиональные цели курса — раскрытие сущности и значения ИБ, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения информационной безопасности, классификация и характеристика составляющих ИБ, установление взаимосвязи и логической организации входящих в них компонентов.

Образовательные цели курса — раскрытие значения ИБ для субъектов информационных отношений (личности, общества, государства), роли защиты информации в обеспечении прав граждан, ее места в политической, экономической, военной и других областях деятельности, в безопасности функционирования различных хозяйственных и управленческих структур.

Задачами изучения дисциплины являются:

- изучение понятийного аппарата в области ИБ;
- раскрытие базовых содержательных положений в области ИБ;
- изучение современной доктрины информационной безопасности;
- установление факторов, влияющих на ИБ;
- изучение методов определения состава защищаемой информации, классификация ее по видам тайны, материальным носителям, собственникам и владельцам;
- установление структуры угроз защищаемой информации;
- изучение направлений, видов, методов и особенностей деятельности разведывательных органов по добыванию конфиденциальной информации;
- раскрытие сущности компонентов защиты информации;
- определение назначения, сущности и структуры комплексных систем защиты информации.
- определение места ИБ в системе информационных отношений;
- определение направлений и областей деятельности субъектов информационных отношений, составной частью которых является обеспечение ИБ;
- раскрытие взаимосвязи между информационной безопасностью и удовлетворением информационных потребностей субъектов информационных отношений;
- определение значения обеспечения ИБ для предотвращения негативного информационного воздействия на субъекты информационных отношений.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина *Основы информационной безопасности* относится к обязательной части Блока 1 (код Б1.О.19). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и самостоятельной работы студентов. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции	Результаты обучения по дисциплине	
ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1.1	Знать понятия информации и информационной безопасности	Тестовые вопросы
	ОПК-1.1.2	Знать место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики	
	ОПК-1.1.3	Знать источники и классификацию угроз информационной безопасности	
	ОПК-1.1.4	Знать основные понятия, связанные с обеспечением информационно-психологической безопасности личности, общества и государства, понятия информационного противоборства, информационной войны и формы их проявлений в современном мире	
	ОПК-1.2.1	Уметь классифицировать и оценивать общие угрозы информационной безопасности для личности, общества и государства	
	ОПК-1.2.2	Уметь определять состав конфиденциальной информации применительно к видам тайны	
	ОПК-1.2.3	Уметь выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия	
	ОПК-1.2.4	Уметь выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к конфиденциальной информации	
	ОПК-1.2.5	Уметь определять направления и виды защиты информации с учетом характера информации и задач по ее защите	
	ОПК-1.3.1	Владеть основными системными подходами к определению целей, задач обеспечения информационной безопасности в автоматизированных системах	
	ОПК-1.3.2	Владеть основными навыками поиска информации о современных и перспективных методах обеспечения информационной безопасности в автоматизированных системах и поиска источников специальной информации, необходимой в профессиональной деятельности	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	Введение	1	1-2	2				6	
2	Характеристика защищаемой информации	1	3-4	2				6	
3	Значение ИБ и ее место в системе национальной безопасности	1	5-6	2				6	Рейтинг-контроль №1
4	Доктрина ИБ	1	7-8	2				6	
5	Основные понятия и определения в области ИБ и защиты информации	1	9-10	2				6	
6	Цели и значение защиты информации	1	11-12	2				6	Рейтинг-контроль №2
7	Критерии, условия и принципы отнесения информации к защищаемой	1	13-14	2				6	
8	Состав и классификация носителей защищаемой информации	1	15-16	2				6	
9	Классификация конфиденциальной информации	1	17-18	2				6	Рейтинг-контроль №3
Всего за 1 семестр:		**72**		**18**				**54**	**зачет**
10	Служебная, личная и профессиональная тайна	2	1-2	2				2	
11	Концептуальная модель системы информационной безопасности	2	3-4	2				2	
12	Действия, приводящие к незаконному овладению конфиденциальной информацией	2	5-6	2				2	Рейтинг-контроль №1
13	Угрозы конфиденциальной информации	2	7-8	2				2	
14	Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию.	2	9-10	2				2	
15	Угрозы доступности, целостности, конфиденциальности информации,	2	11-12	2				2	Рейтинг-контроль №2
16	Способы защиты информации	2	13-14	2				2	
17	Основные защитные действия и мероприятия	2	15-16	2				2	
18	Уровни информационной безопасности	2	17-18	2				2	Рейтинг-контроль №3
Всего за 2 семестр:		**72**		**18**				**18**	**Экзамен (36)**
Итого по дисциплине		**144**		**36**				**72**	**Зачет Экзамен (36)**

Содержание лекционных занятий по дисциплине
1 Семестр

Раздел 1. Введение. Предмет и задачи курса. Значение и место курса в подготовке специалистов по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами. 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. Знания и умения студентов, которые должны быть получены в результате изучения курса.

Раздел 2. Характеристика защищаемой информации. Признаковая структура объекта. Предметом защиты. Признаковая информация. Демаскирующие признаки объектов. Информативность демаскирующего признака. Свойства информации как предмета защиты. Основные носители признаковой информации. «Источник конфиденциальной информации».

Раздел 3. Значение ИБ и ее место в системе национальной безопасности. 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. Определение понятия "информационная безопасность". Значение информационной безопасности для субъектов информационных отношений. Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе национальной безопасности.

Раздел 4. Доктрина информационной безопасности. Понятие и назначение доктрины 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. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.

Раздел 5. Основные понятия и определения в области информационной безопасности и защиты информации. Значение раскрытия сущности и определения понятия защиты информации. Существующие подходы к содержательной части понятия "защита информации" и способам реализации содержательной части. Методологическая основа для раскрытия сущности и определения понятия защиты информации. Формы выражения нарушения статуса информации. Обусловленность статуса информации ее уязвимостью. 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".

Раздел 6. Цели и значение защиты 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

Раздел 7. Критерии, условия и принципы отнесения информации к защищаемой. Современные подходы к составу 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.

Раздел 8. Состав и классификация носителей защищаемой информации. Понятие "носитель защищаемой информации". Соотношение между носителем и источником информации. Состав носителей защищаемой информации. Способы фиксирования информации в носителях. Виды отображения информации в носителях. Методы воспроизведения отображенной информации в носителях информации. Носители письменной, видовой, излучаемой информации. Опосредованные носители защищаемой информации. Свойства и значение типов носителей защищаемой информации.

Раздел 9. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности. Понятие "тайна информации". Виды тайны конфиденциальной информации. Показатели разделения конфиденциальной информации на виды тайны. Становление и современное определение понятия "государственная тайна". Основания и организационно-правовые формы отнесения информации к государственной тайне. Функции должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне. 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. 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.

2 Семестр

Раздел 10. Служебная, личная и профессиональная тайна. 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.

Раздел 11. Концептуальная модель системы информационной безопасности. Понятие и назначение теории защиты информации. Основные положения теории защиты информации: объективная необходимость и общественная потребность в защите информации, включенность ее в систему общественных отношений, зависимость защиты информации от политико-правовых, социально-экономических, военно-политических реальностей, увязка с проблемами информатизации общества, обеспечения баланса интересов личности, общества и государства, правовое регулирование и взаимный контроль субъектов информационных отношений в сфере защиты информации, содействие повышению эффективности соответствующей области деятельности. Теоретические основы национальной политики в сфере защиты информации. Понятие и назначение концепции защиты информации. Теория защиты информации как основа концепции защиты информации. Содержание концепции защиты информации, ее значение для разработки стратегии, формирования целевых программ

и практических мероприятий по защите информации. Уровни и виды концепции защиты информации. Становление и развитие государственной концепции защиты информации. Современная стратегия защиты информации.

Раздел 12. Действия, приводящие к незаконному овладению конфиденциальной информацией. Основные способы несанкционированного доступа к конфиденциальной информации. Обобщенная модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации. Утечка конфиденциальной информации. «Разглашение» конфиденциальной информации.

Раздел 13. Угрозы конфиденциальной информации. Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации. Структура явлений как сущностного выражения угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

Раздел 14. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию. 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.

Раздел 15. Угрозы доступности, целостности, конфиденциальности информации, характерные для информационных систем. Угрозы доступности. Непреднамеренные ошибки. Внутренний отказ ИС. Отказ поддерживающей инфраструктуры. Повреждение разрушение оборудования (в том числе носителей данных). Программные атаки на доступность. Вредоносное программное обеспечение. Основные угрозы целостности. Нарушения статической целостности. Угрозы динамической целостности. Основные угрозы конфиденциальности. Перехват данных. Кражи. Методы морально-психологического воздействия

Раздел 16. Способы защиты информации. Способ предупреждения возможных угроз. Основные действия способа выявления угроз. Способ обнаружения угроз. Способ пресечения или локализации угроз. Основные действия способа ликвидации последствий. Основные защитные действия при реализации способов ЗИ. Защита от разглашения. Защитные действия от утечки и от НСД к конфиденциальной информации. Мероприятия по технической защите информации.

Раздел 17. Основные защитные действия и мероприятия. Защита от разглашения. Защита от утечки конфиденциальной информации. Защита от НСД к конфиденциальной информации. Мероприятия по технической защите информации. Организационные мероприятия. Территориальные ограничения Пространственные ограничения. Временные ограничения. Организационно-технические мероприятия. Пространственные меры. Режимные меры. Энергетические меры. Технические мероприятия. Скрытие Подавление. Дезинформация

Раздел 18. Уровни информационной безопасности. Организационные основы как необходимые условия осуществления защиты информации. Условия, необходимые для обеспечения технологии защиты информации, а также сохранности и конфиденциальности информации. Значение методологических принципов защиты информации. Принципы, обусловленные принадлежностью, ценностью, конфиденциальностью, технологией защиты информации. Основные меры и архитектурные принципы обеспечения обслуживаемости ИС. Сервисы безопасности. Понятие и назначение технологического обеспечения защиты информации. Классификация организационно-технологических документов по защите информации.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Семестр 1:

Вопросы рейтинг-контроля №1

1. Что такое признаковая структура объекта?
2. Что понимают под полученной объектом информацией?
3. Какая информация является предметом защиты?
4. Что такое признаковая информация?
5. Почему семантическая информация по отношению к признаковой является вторичной?
6. Какие признаки объектов являются демаскирующими?
7. Приведите классификацию демаскирующих признаков объектов защиты.
8. Опишите опознавательные демаскирующие признаки объектов защиты.
9. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
10. Что такое информативность демаскирующего признака?
11. Перечислите основные свойства информации как предмета защиты.
12. Почему информацию можно рассматривать как товар?
13. Изменяется ли цена информации во времени? Если да, то аргументируйте свой ответ.
14. Какой аналитической зависимостью можно аппроксимировать характер старения информации?
15. Что понимается под временем жизни информации?
16. Что такое количество информации?
17. Что такое тезаурус?
18. Почему информация способна случайным образом «растекаться» в пространстве?
19. Почему при копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а ее цена снижается?
20. Перечислите основные носители признаковой информации.

Вопросы рейтинг-контроля №2:

21. Что такое «источник конфиденциальной информации»?
22. Перечислите основные источники конфиденциальной информации.
23. В чем отличие прямых источников семантической информации от косвенных?
24. Охарактеризуйте людей (сотрудники, обслуживающий персонал, продавцы, клиенты и др.) в качестве источника конфиденциальной информации.
25. Охарактеризуйте документы как источники конфиденциальной информации.
26. В чем специфика публикаций, докладов, статей, интервью, проспектов, книг и т.д. в качестве источников конфиденциальной информации?
27. Охарактеризуйте технические носители информации и документов как источники конфиденциальной информации.
28. Охарактеризуйте технические средства обработки информации - автоматизированные средства обработки информации и средства обеспечения производственной и трудовой деятельности, в том числе и средства связи в качестве источника конфиденциальной информации.
29. Охарактеризуйте выпускаемую продукцию как источник конфиденциальной информации.
30. Охарактеризуйте производственные и промышленные отходы как источник конфиденциальной информации
31. Как в Доктрине информационной безопасности Российской Федерации определяется термин «информационная безопасность»?

32. Как в Законе РФ "Об участии в международном информационном обмене" определяется термин «информационная безопасность»?
33. Дайте определение информационной безопасности, прокомментируйте его составляющие.
34. Что такое защита информации?
35. Перечислите основные категории информационной безопасности и дайте им определения.
36. Охарактеризуйте понятие доступности.
37. Охарактеризуйте понятие целостности.
38. Охарактеризуйте понятие конфиденциальности.
39. Приведите убедительные доводы того, что информационная безопасность – одна из важнейших проблем современной жизни.
40. Дайте определение национальной безопасности согласно Концепции национальной безопасности РФ.
41. В чем заключаются национальные интересы России?
42. Чем обеспечиваются национальные интересы России?
43. В чем заключаются национальные интересы России в информационной сфере?
44. Что такое государственная информационная политика?
45. Перечислите и прокомментируйте основные составляющие информационной безопасности РФ.
46. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.
47. Что такое угроза в контексте ИБ России?

Вопросы рейтинг-контроля №3:

48. Классифицируйте угрозы ИБ РФ по общей направленности.
49. В чем состоят угрозы ИБ для личности?
50. В чем состоят угрозы ИБ для общества?
51. В чем состоят угрозы ИБ для государства?
52. Классифицируйте угрозы ИБ РФ по происхождению и прокомментируйте их.
53. Перечислите основные принципы ИБ России согласно Доктрине.
54. Каковы функции государственной системы по обеспечению ИБ?
55. Охарактеризуйте государственную структуру органов, обеспечивающая информационную безопасность.
56. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
57. В чем специфика деятельности Федеральной службой по техническому и экспортному контролю (ФСТЭК России)?
58. Перечислите основные задачи в области обеспечения информационной безопасности для ФСТЭК России.
59. В чем специфика деятельности Федеральной службы безо¬пасности?
60. Прокомментируйте основные права ФСБ в части задач информационной безопасности.
61. В чем специфика деятельности службы внешней разведки РФ в отношении ИБ?
62. В чем специфика деятельности Минобороны России в отношении проблем ИБ?
63. В чем специфика деятельности органов государственного управления (министерств, ведомств) в обеспечении ИБ?
64. Какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
65. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
66. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
67. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.

Семестр 2:

Вопросы рейтинг-контроля №1

1. Какую информацию относят к защищаемой?
2. Дайте определение защищаемой информации.
3. Охарактеризуйте основные признаки защищаемой информации.
4. Перечислите и охарактеризуйте основных собственников защищаемой информации.
5. Что такое государственная тайна?
6. Приведите формальную модель определения государственных секретов
7. Перечислите сведения, которые могут быть отнесены к государственной тайне.
8. Какую информацию нельзя засекречивать как имеющую статус государст¬венной тайны?
9. Что характеризует политический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
10. Что характеризует экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
11. Что характеризует моральный ущерб, наносимый при утечке сведений, составляющих государственную тайну?
12. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
13. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
14. Перечислите основные объекты банковской тайны.
15. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне? Перечислите и охарактеризуйте основные объекты профессиональной тайны.
16. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
17. Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
18. Перечислите основные объекты интеллектуальной собственности.
19. Что понимается под системой безопасности?

Вопросы рейтинг-контроля №2:

20. Перечислите основные компоненты концептуальной модели ИБ.
21. Что такое объекты угроз ИБ и в чем они выражаются?
22. Каковы основные источники угроз защищаемой информации?
23. Каковы цели угроз информации со стороны злоумышленников?
24. Перечислите основные источники конфиденциальной информации.
25. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
26. Перечислите базовые способы защиты информации.
27. Изобразите графически схему концептуальной модели системы ИБ.
28. Приведите возможный перечень способов получения информации.
29. Дайте определение способа несанкционированного доступа к источникам конфиденциальной информации.
30. Перечислите основные способы несанкционированного доступа к конфиденциальной информации.
31. Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
32. Что такое утечка конфиденциальной информации?
33. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?

Вопросы рейтинг-контроля №3:

1. Дайте определение угрозы конфиденциальной информации.
2. Что такое атака?
3. Что такое окно опасности?
4. Что такое угрозы воздействия на источник информации?
5. Что такое угрозы утечки информации?
6. Какие угрозы называются преднамеренными, а какие случайными?
7. Что такое канал несанкционированного доступа?
8. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
9. Что такое наблюдение в теории информационной безопасности?
10. Что такое подслушивание в теории информационной безопасности?
11. Что такое перехват в теории информационной безопасности?
12. Что такое технический канал утечки информации?
13. Охарактеризуйте случайный и организованный канал утечки информации.
14. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
15. Какие организации формируют структуру разведывательного сообщества США?
16. Прокомментируйте наиболее распространенные угрозы доступности.
17. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
18. Что такое отказ пользователей? Какое отношение данное понятие имеет к угрозам доступности?
19. Охарактеризуйте программные атаки на доступность.
20. Что такое вредоносное программное обеспечение?
21. Дайте определение «бомбы», «червя», «вируса».
22. Охарактеризуйте основные угрозы целостности конфиденциальной информации.
23. Прокомментируйте понятия «кража» и «подлог» в качестве угрозы целостности.
24. Перечислите основные угрозы конфиденциальности информации
25. Что в ИБ понимают под маскарадом?
26. Дайте определение способа защиты информации.
27. Охарактеризуйте способ предупреждения возможных угроз.
28. Прокомментируйте основные действия способа выявления угроз
29. Охарактеризуйте способ обнаружения угроз.
30. Охарактеризуйте способ пресечения или локализации угроз.
31. Прокомментируйте основные действия способа ликвидации последствий.
32. Перечислите основные защитные действия при реализации способов ЗИ,
33. Что такое защита от разглашения?
34. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
35. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
36. Назовите три группы мероприятий по технической защите информации.
37. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
38. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
39. Прокомментируйте основные технические мероприятия по технической защите информации.
40. Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.
41. В чем заключается специфика управления, как сервиса безопасности?

5.2. Промежуточная аттестация по итогам освоения дисциплины

Примерный перечень вопросов к зачету 1 семестр

1. Приведите классификацию демаскирующих признаков объектов защиты.
2. Опишите опознавательные демаскирующие признаки объектов защиты.
3. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
4. Почему при копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а ее цена снижается?
5. Перечислите основные носители признаковой информации.
6. Что такое «источник конфиденциальной информации»?
7. Перечислите основные источники конфиденциальной информации.
8. В чем отличие прямых источников семантической информации от косвенных?
9. Перечислите основные категории информационной безопасности и дайте им определения.
10. Охарактеризуйте понятие доступности, целостности, конфиденциальности.
11. Дайте определение национальной безопасности согласно Концепции национальной безопасности РФ.
12. В чем заключаются и чем обеспечиваются национальные интересы России в информационной сфере?
13. Что такое государственная информационная политика?
14. Перечислите и прокомментируйте основные составляющие информационной безопасности РФ.
15. Перечислите важнейшие задачи обеспечения информационной безопасности РФ.
16. Классифицируйте угрозы ИБ РФ по общей направленности.
17. В чем состоят угрозы ИБ для личности?
18. В чем состоят угрозы ИБ для общества?
19. В чем состоят угрозы ИБ для государства?
20. Перечислите основные принципы ИБ России согласно Доктрине.
21. Охарактеризуйте государственную структуру органов, обеспечивающая информационную безопасность.
22. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
23. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
24. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.
25. Охарактеризуйте основные признаки защищаемой информации.
26. Перечислите и охарактеризуйте основных собственников защищаемой информации.
27. Что такое государственная тайна?
28. Перечислите сведения, которые могут быть отнесены к государственной тайне.
29. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
30. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
31. Перечислите основные объекты банковской тайны.
32. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне? Перечислите и охарактеризуйте основные объекты профессиональной тайны.
33. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к служебной тайне? Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
34. Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?

35. Перечислите основные объекты интеллектуальной собственности.
36. Перечислите основные компоненты концептуальной модели ИБ.
37. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).

Примерный перечень вопросов к экзамену 2 семестр

1. Перечислите базовые способы защиты информации.
2. Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
3. Что такое утечка конфиденциальной информации?
4. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
5. Как осуществляется утечка конфиденциальной информации?
6. Дайте определение угрозы конфиденциальной информации.
7. Какие угрозы называются преднамеренными, а какие случайными?
8. Что такое канал несанкционированного доступа?
9. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
10. Что такое наблюдение в теории информационной безопасности?
11. Что такое подслушивание в теории информационной безопасности?
12. Что такое перехват в теории информационной безопасности?
13. Что такое технический канал утечки информации?
14. Охарактеризуйте случайный и организованный канал утечки информации.
15. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
16. Прокомментируйте наиболее распространенные угрозы доступности.
17. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
18. Что такое отказ пользователей? Какое отношение данное понятие имеет к угрозам доступности?
19. Охарактеризуйте программные атаки на доступность.
20. Что такое вредоносное программное обеспечение?
21. Дайте определение способа защиты информации.
22. Охарактеризуйте способ предупреждения возможных угроз.
23. Прокомментируйте основные действия способа выявления угроз
24. Охарактеризуйте способ обнаружения угроз.
25. Охарактеризуйте способ пресечения или локализации угроз.
26. Прокомментируйте основные действия способа ликвидации последствий.
27. Перечислите основные защитные действия при реализации способов ЗИ,
28. Что такое защита от разглашения?
29. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
30. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
31. Назовите три группы мероприятий по технической защите информации.
32. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
33. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
34. Прокомментируйте основные технические мероприятия по технической защите информации.

5.3. Самостоятельная работа обучающегося.

Примерные вопросы и задания для самостоятельной работы студентов
1 Семестр

- Какие признаки объектов являются демаскирующими?
- Приведите классификацию демаскирующих признаков объектов защиты.
- Опишите опознавательные демаскирующие признаки объектов защиты.
- Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
- Что такое информативность демаскирующего признака?
- Что такое тезаурус?
- Перечислите основные носители признаковой информации.
- Перечислите основные источники конфиденциальной информации.
- В чем отличие прямых источников семантической информации от косвенных?
- Охарактеризуйте производственные и промышленные отходы как источник конфиденциальной информации
- В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
- Перечислите основные задачи в области обеспечения информационной безопасности для ФСТЭК России.
- В чем специфика деятельности Федеральной службы безопасности?
- Прокомментируйте основные права ФСБ в части задач информационной безопасности.
- В чем специфика деятельности службы внешней разведки РФ в отношении ИБ?
- В чем специфика деятельности Минобороны России в отношении проблем ИБ?
- В чем специфика деятельности органов государственного управления (министерств, ведомств) в обеспечении ИБ?
- Какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
- Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
- Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
- Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.
- Как в Доктрине информационной безопасности Российской Федерации определяется термин «информационная безопасность»?
- Как в Законе РФ "Об участии в международном информационном обмене" определяется термин «информационная безопасность»?
- Дайте определение информационной безопасности, прокомментируйте его составляющие.
- Что такое защита информации?
- Приведите убедительные доводы того, что информационная безопасность – одна из важнейших проблем современной жизни.
- Какую информацию нельзя засекречивать как имеющую статус государственной тайны?
- Что характеризует политический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
- Что характеризует экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
- Что характеризует моральный ущерб, наносимый при утечке сведений, составляющих государственную тайну?
- Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
- Какая информация не может быть отнесена к коммерческой тайне?
- Перечислите основные объекты банковской тайны.

- Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
- Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
- Перечислите основные объекты интеллектуальной собственности.

2 Семестр

- Что такое объекты угроз ИБ и в чем они выражаются?
- Каковы основные источники угроз защищаемой информации?
- Каковы цели угроз информации со стороны злоумышленников?
- Перечислите основные источники конфиденциальной информации.
- Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
- Перечислите базовые способы защиты информации.
- Изобразите графически схему концептуальной модели системы ИБ.
- Перечислите основные способы несанкционированного доступа к конфиденциальной информации.
- Охарактеризуйте обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
- Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
- Как осуществляется утечка конфиденциальной информации?
- Каким образом непреднамеренное разглашение информации может привести к ее утечке?
- Что такое наблюдение в теории информационной безопасности?
- Что такое подслушивание в теории информационной безопасности?
- Что такое перехват в теории информационной безопасности?
- Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
- Какие организации формируют структуру разведывательного сообщества США?
- Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
- Охарактеризуйте программные атаки на доступность.
- Приведите примеры «бомбы», «червя», «вируса».
- Прокомментируйте понятия «кража» и «подлог» в качестве угрозы целостности.
- Что в ИБ понимают под маскарадом?
- Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
- Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
- Назовите три группы мероприятий по технической защите информации.
- Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
- Прокомментируйте основные организационно-технические мероприятия по ЗИ.
- Прокомментируйте основные технические мероприятия по технической защите информации.
- Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.
- В чем заключается специфика управления, как сервиса безопасности?

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература		
Основы информационной безопасности: учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев; Академия Следственного комитета Российской Федерации. – Москва: Юнити-Дана: Закон и право, 2018. – 287 с. – ISBN 978-5-238-02857-6	2018	https://biblioclub.ru/index.php?page=book&id=562348 (дата обращения: 18.09.2021)
Гультяева, Т. А. Основы информационной безопасности: учебное пособие: [16+] / Т. А. Гультяева. – Новосибирск: Новосибирский государственный технический университет, 2018. – 79 с.– ISBN 978-5-7782-3640-0	2018	https://biblioclub.ru/index.php?page=book&id=574729 (дата обращения: 18.09.2021)
Загинайлов, Ю. Н. Основы информационной безопасности: курс визуальных лекций / Ю. Н. Загинайлов. – Москва; Берлин: Директ-Медиа, 2015. – 105 с. – ISBN 978-5-4475-3947-4	2015	https://biblioclub.ru/index.php?page=book&id=362895 (дата обращения: 18.09.2021)
Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: [16+] / В. Я. Ищейнов. – Москва; Берлин: Директ-Медиа, 2020. – 271 с.– ISBN 978-5-4499-0496-6. – DOI 10.23681/571485	2020	https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 18.09.2021)
Ковалев, Д. В. Информационная безопасность: учебное пособие: [16+] / Д. В. Ковалев, Е. А. Богданова; Южный федеральный университет. – Ростов-на-Дону, 2016. – 74с.– ISBN 978-5-9275-2364-1	2016	https://biblioclub.ru/index.php?page=book&id=493175 (дата обращения: 18.09.2021)
Дополнительная литература		
Прохорова, О. В. Информационная безопасность и защита информации: учебник: [16+] / О. В. Прохорова ; Самарский государственный архитектурно-строительный университет. – Самара, 2014. – 113с. – ISBN 978-5-9585-0603-3	2014	https://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 18.09.2021)
Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю. Н. Загинайлов. – Москва; Берлин: Директ-Медиа, 2015. – 253 с. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557	2015	https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 18.09.2021)
Технологии обеспечения безопасности информационных систем: учебное пособие: [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва; Берлин: Директ-Медиа, 2021. – 210 с. – ISBN 978-5-4499-1671-6. – DOI 10.23681/598988	2021	https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 18.09.2021)
Козьминых, С. И. Обеспечение комплексной защиты объектов информатизации: учебное пособие / С. И. Козьминых; Финансовый университет при Правительстве Российской Федерации. – Москва: Юнити-Дана, 2020. – 544 с. – ISBN 978-5-238-03200-9	2020	https://biblioclub.ru/index.php?page=book&id=615695 (дата обращения: 18.09.2021)

6.2. Периодические издания

1. Отраслевой lifestyle-журнал по теме безопасности «Рубеж». Режим доступа: http://ru-bezh.ru/;

2. Журнал «Защита информации. Инсайд» ISSN 2413-3582, Режим доступа: http://inside-zi.ru/pages/about.html;

3. Журнал "Алгоритм безопасности» – Режим доступа: http://www.algoritm.org/index.php;

4. Электронный научный журнал «Проблемы безопасности» – Режим доступа: http://www.pb.littera-n.ru/

6.3. Интернет-ресурсы

1.Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru

2.Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru

3.Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/

4.ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил: заведующий кафедрой ИЗИ
д.т.н. Монахов М.Ю._____

Рецензент: Заместитель руководителя РАЦ ООО
«ИнфоЦентр» к.т.н. Вертилевский Н.В_____

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 26.08.21 года
Заведующий кафедрой д.т.н., профессор_____/М.Ю. Монахов/____

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии специальности 10.05.04 «Информационно-аналитические системы безопасности»

Протокол № 1 от 26.08.21 года
Председатель комиссии д.т.н., профессор_____/М.Ю. Монахов/____

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20 22 / 20 23 учебный год

Протокол заседания кафедры № 14 от 28.06.22 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/__
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/__
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/__
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/__
(ФИО, подпись)

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

Основы информационной безопасности

образовательной программы специальности

10.05.04 «Информационно-аналитические системы безопасности»

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____/М.Ю. Монахов/

Подпись *ФИО*