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
_____ А.А. Галкин
«31» 05 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки/ специальность
27.03.04 – Управление в технических системах

Направленность (профиль подготовки)
Управление и информатика в технических системах

г. Владимир

2021

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины *Информационная безопасность* является обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 27.03.04 «Управление в технических системах»; формирование у бакалавров 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.

Задачи:

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

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина *Информационная безопасность* относится к обязательной части Блока 1. Код Б1.О.23.

В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций и практических занятий.

Дисциплина изучается на 3 курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по дисциплине «Информатика» за курс средней школы.

Курс тесно взаимосвязан с другими дисциплинами. Он является полезным для изучения таких дисциплин как «Управление информационными ресурсами», «Администрирование информационных систем».

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесённые 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-3 Способен использовать фундаментальные знания для решения базовых задач управления в технических системах с целью совершенствования в профессиональной деятельности	ОПК-3.1 ОПК-3.2 ОПК-3.3	Знает устройство основных типовых средств управления информационной безопасностью; Умеет выполнять проект системы защиты информации на предприятии; Владеет навыками обеспечения информационной безопасности технических систем	Тестовые вопросы
ОПК-6. Способен разрабатывать и использовать алгоритмы и программы, современные информационные технологии, методы и средства контроля, диагностики и управления, пригодные для практического применения в сфере своей профессиональной деятельности	ОПК-6.1 ОПК-6.2	Умеет использовать информационно-коммуникационные технологии для практического применения в обеспечении информационной безопасности; Умеет разрабатывать алгоритмы организационного обеспечения защиты данных.	Тестовые вопросы

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоёмкость дисциплины составляет 3 зачётных единицы, 108 часов.

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[1]	Лабораторные работы	*в форме практической подготовки*[2]		
1	Введение. Характеристика защищаемой информации	5	1-2	2				8	Рейтинг-контроль №1
2	Значение ИБ и ее место в системе национальной безопасности	5	3-4	2				8	
3	Основные понятия и определения в области информационной безопасности и защиты информации	5	5-6	2				8	
4	Категории защищаемой информации	5	7-8	2				8	Рейтинг-контроль №2
5	Концептуальная модель системы информационной безопасности	5	9-10	2		4		8	
6	Действия, приводящие к незаконному овладению конфиденциальной информацией	5	11-12	2		4		8	
7	Угрозы конфиденциальной информации	5	13-14	2		4		8	Рейтинг-контроль №3
8	Способы защиты информации	5	15-16	2		4		8	
9	Уровни информационной безопасности	5	17-18	2		2		8	
Всего за 5 семестр:		108		18		18		72	Зачёт
Итого по дисциплине		108		18		18		72	Зачёт

Содержание лекционных занятий по дисциплине

Тема 1. Введение. Характеристика защищаемой информации

Научная и учебная взаимосвязь курса с другими дисциплинами. Структура курса. Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения семинарских занятий.

Формы проверки знаний. Знания и умения студентов, которые должны быть получены в результате изучения курса. Признаковая структура объекта. Предметом защиты. Признаковая

1 Распределение общего числа часов, указанных на практические занятия в УП, с учётом часов на КП/КР

[2] Данный пункт включается в рабочую программу только при формировании профессиональных компетенций.

информация. Демаскирующие признаки объектов. Информативность демаскирующего признака. Свойства информации как предмета защиты. Основные носители признаковой информации. «Источник конфиденциальной информации».

Тема 2. Значение ИБ и её место в системе национальной безопасности

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.

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.

Тема 3. Основные понятия и определения в области информационной безопасности и защиты информации

Основные признаки защищаемой информации. Собственники защищаемой информации.

Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.

Тема 4. Категории защищаемой информации

Политический и экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну.

Коммерческая тайна. Банковская тайна. Основные объекты профессиональной тайны. Основные объекты интеллектуальной собственности.

Тема 5. Концептуальная модель системы информационной безопасности

Основные компоненты концептуальной модели ИБ. Объекты угроз ИБ. Источники угроз
.

Основные способы неправомерного овладения конфиденциальной информацией (способы доступа). Базовые способы защиты информации. Схема концептуальной модели системы ИБ.

Тема 6. Действия, приводящие к незаконному овладению конфиденциальной информацией

Обобщённая модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации. «Разглашение» конфиденциальной информации.

Тема 7. Угрозы конфиденциальной информации

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

Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

Тема 8. Способы защиты информации

Основные действия способа выявления угроз. Способ пресечения или локализации угроз. Основные действия способа ликвидации последствий. Основные защитные действия при реализации способов ЗИ. Защита от разглашения.

Мероприятия по технической защите информации.

Тема 9. Уровни информационной безопасности

Условия, необходимые для обеспечения технологии защиты информации, а также сохранности и конфиденциальности информации. Значение методологических принципов защиты информации.

Основные меры и архитектурные принципы обеспечения обслуживаемости ИС. Сервисы безопасности. Понятие и назначение технологического обеспечения защиты информации.

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

Темы лабораторных работ по дисциплине

Лабораторная работа №1. Антивирусный программы.
Лабораторная работа №2. Антивирусный программы.
Лабораторная работа №3. Управление учётными записями MS Windows.

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

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 её цена снижается?
20. Перечислите основные носители признаковой информации.
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 к контексте ИБ России?

Вопросы рейтинг-контроля №2:

1. Классифицируйте угрозы ИБ РФ по общей направленности.
2. В чем состоят угрозы ИБ для личности?
3. В чем состоят угрозы ИБ для общества?
4. В чем состоят угрозы ИБ для государства?
5. Классифицируйте угрозы ИБ РФ по происхождению и прокомментируйте их.
6. Перечислите основные принципы ИБ России согласно Доктрине.
7. Каковы функции государственной системы по обеспечению ИБ?
8. Охарактеризуйте государственную структуру органов, обеспечивающая информационную безопасность.
9. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?

10. В чем специфика деятельности Федеральной службой по техническому и экспортному контролю (ФСТЭК России)?
11. Перечислите основные задачи в области обеспечения информационной безопасности для ФСТЭК России.
12. В чем специфика деятельности Федеральной службы безо¬пасности?
13. Прокомментируйте основные права ФСБ в части задач информационной безопасности.
14. В чем специфика деятельности службы внешней разведки РФ в отношении ИБ?
15. В чем специфика деятельности Минобороны России в отношении проблем ИБ?
16. В чем специфика деятельности органов государственного управления (министерств, ведомств) в обеспечении ИБ?
17. Какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
18. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
19. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.
20. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.
21. Какую информацию относят к защищаемой?
22. Дайте определение защищаемой информации.
23. Охарактеризуйте основные признаки защищаемой информации.
24. Перечислите и охарактеризуйте основных собственников защищаемой информации.
25. Что такое государственная тайна?
26. Приведите формальную модель определения государственных секретов
27. Перечислите сведения, которые могут быть отнесены к государственной тайне.
28. Какую информацию нельзя засекречивать как имеющую статус государст¬венной тайны?
29. Что характеризует политический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
30. Что характеризует экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
31. Что характеризует моральный ущерб, наносимый при утечке сведений, составляющих государственную тайну?
32. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
33. Каким требованиям должна отвечать коммерческая тайна? Охарактеризуйте основные субъекты права на коммерческую тайну. Какая информация не может быть отнесена к коммерческой тайне?
34. Перечислите основные объекты банковской тайны.
35. Каким требованиям должна удовлетворять информация, чтобы ее можно было бы отнести к профессиональной тайне? Перечислите и охарактеризуйте основные объекты профессиональной тайны.
36. 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).
37. Дайте определение персональных данных. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
38. Перечислите основные объекты интеллектуальной собственности.
39. Что понимается под системой безопасности?

Вопросы рейтинг-контроля №3:

1. Перечислите основные компоненты концептуальной модели ИБ.
2. Что такое объекты угроз ИБ и в чем они выражаются?
3. Каковы основные источники угроз защищаемой информации?

4. Каковы цели угроз информации со стороны злоумышленников?
5. Перечислите основные источники конфиденциальной информации.
6. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
7. Перечислите базовые способы защиты информации.
8. Изобразите графически схему концептуальной модели системы ИБ.
9. Приведите возможный перечень способов получения информации.
10. Дайте определение способа несанкционированного доступа к источникам конфиденциальной информации.
11. Перечислите основные способы несанкционированного доступа к конфиденциальной информации.
12. Охарактеризуйте обобщённую модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
13. Что такое утечка конфиденциальной информации?
14. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
15. Как осуществляется утечка конфиденциальной информации?
16. Дайте определение угрозы конфиденциальной информации.
17. Что такое атака?
18. Что такое окно опасности?
19. Что такое угрозы воздействия на источник информации?
20. Что такое угрозы утечки информации?
21. Какие угрозы называются преднамеренными, а какие случайными?
22. Что такое канал несанкционированного доступа?
23. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
24. Что такое наблюдение в теории информационной безопасности?
25. Что такое подслушивание в теории информационной безопасности?
26. Что такое перехват в теории информационной безопасности?
27. Что такое технический канал утечки информации?
28. Охарактеризуйте случайный и организованный канал утечки информации.
29. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
30. Какие организации формируют структуру разведывательного сообщества США?
31. Прокомментируйте наиболее распространённые угрозы доступности.
32. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
33. Что такое отказ пользователей? Какое отношение данное понятие имеет к угрозам доступности?
34. Охарактеризуйте программные атаки на доступность.
35. Что такое вредоносное программное обеспечение?
36. Дайте определение «бомбы», «червя», «вируса».
37. Охарактеризуйте основные угрозы целостности конфиденциальной информации.
38. Прокомментируйте понятия «кража» и «подлог» в качестве угрозы целостности.
39. Перечислите основные угрозы конфиденциальности информации
40. Что в ИБ понимают под маскарадом?
41. Дайте определение способа защиты информации.
42. Охарактеризуйте способ предупреждения возможных угроз.
43. Прокомментируйте основные действия способа выявления угроз
44. Охарактеризуйте способ обнаружения угроз.
45. Охарактеризуйте способ пресечения или локализации угроз.
46. Прокомментируйте основные действия способа ликвидации последствий.
47. Перечислите основные защитные действия при реализации способов ЗИ,
48. Что такое защита от разглашения?

49. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
50. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
51. Назовите три группы мероприятий по технической защите информации.
52. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
53. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
54. Прокомментируйте основные технические мероприятия по технической защите информации.
55. Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.
56. В чем заключается специфика управления, как сервиса безопасности?

5.2. Промежуточная аттестация по итогам освоения дисциплины

Перечень вопросов к зачёту:

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 её 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).

5.3. Самостоятельная работа обучающегося.

Вопросы и задания для самостоятельной работы студентов:

Тема 1

1. Какие признаки объектов являются демаскирующими?
2. Приведите классификацию демаскирующих признаков объектов защиты.
3. Опишите опознавательные демаскирующие признаки объектов защиты.
4. Охарактеризуйте признаки деятельности как демаскирующие признаки объектов защиты.
5. Что такое информативность демаскирующего признака?
6. Что такое тезаурус?
7. Перечислите основные носители признаковой информации.
8. Перечислите основные источники конфиденциальной информации.
9. В чем отличие прямых источников семантической информации от косвенных?
10. Охарактеризуйте производственные и промышленные отходы как источник конфиденциальной информации

Тема 2

1. В чем специфика деятельности Межведомственной комиссии по защите государственной тайны?
2. Перечислите основные задачи в области обеспечения информационной безопасности для ФСТЭК России.
3. В чем специфика деятельности Федеральной службы безопасности?
4. Прокомментируйте основные права ФСБ в части задач информационной безопасности.
5. В чем специфика деятельности службы внешней разведки РФ в отношении ИБ?
6. В чем специфика деятельности Минобороны России в отношении проблем ИБ?
7. В чем специфика деятельности органов государственного управления (министерств, ведомств) в обеспечении ИБ?
8. Какие ключевые проблемы необходимо решить безотлагательно, чтобы обеспечить достаточный уровень ИБ в России?
9. Раскройте содержание политических факторов, влияющих на состояние информационной безопасности РФ.
10. Раскройте содержание экономических факторов, влияющих на состояние информационной безопасности РФ.

11. Раскройте содержание организационно-технических факторов, влияющих на состояние информационной безопасности РФ.

Тема 3

1. Как в Доктрине информационной безопасности Российской Федерации определяется термин «информационная безопасность»?
2. Как в Законе РФ "Об участии в международном информационном обмене" определяется термин «информационная безопасность»?
3. Дайте определение информационной безопасности, прокомментируйте его составляющие.
4. Что такое защита информации?
5. Приведите убедительные доводы того, что информационная безопасность – одна из важнейших проблем современной жизни.

Тема 4

1. Какую информацию нельзя засекречивать как имеющую статус государственной тайны?
2. Что характеризует политический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
3. Что характеризует экономический ущерб, наносимый при утечке сведений, составляющих государственную тайну?
4. Что характеризует моральный ущерб, наносимый при утечке сведений, составляющих государственную тайну?
5. Перечислите основные виды конфиденциальной информации, нуждающейся в защите.
6. Какая информация не может быть отнесена к коммерческой тайне?
7. Перечислите основные объекты банковской тайны.
8. Приведите перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения (согласно законодательству).
9. Какие сведения могут быть отнесены к персональным данным? Кто является держателем персональных данных?
10. Перечислите основные объекты интеллектуальной собственности.

Тема 5

1. Что такое объекты угроз ИБ и в чем они выражаются?
2. Каковы основные источники угроз защищаемой информации?
3. Каковы цели угроз информации со стороны злоумышленников?
4. Перечислите основные источники конфиденциальной информации.
5. Назовите основные способы неправомерного овладения конфиденциальной информацией (способы доступа).
6. Перечислите базовые способы защиты информации.
7. Изобразите графически схему концептуальной модели системы ИБ.

Тема 6

1. Перечислите основные способы несанкционированного доступа к конфиденциальной информации.
2. Охарактеризуйте обобщённую модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации.
3. Определите понятие «разглашение» конфиденциальной информации, в чем оно выражается?
4. Как осуществляется утечка конфиденциальной информации?

Тема 7

1. Каким образом непреднамеренное разглашение информации может привести к ее утечке?
2. Что такое наблюдение в теории информационной безопасности?

3. Что такое подслушивание в теории информационной безопасности?
4. Что такое перехват в теории информационной безопасности?
5. Что такое источник угроз безопасности информации? Назовите основные источники преднамеренных угроз.
6. Какие организации формируют структуру разведывательного сообщества США?
7. Охарактеризуйте непреднамеренные ошибки в качестве угрозы доступности.
8. Охарактеризуйте программные атаки на доступность.
9. Приведите примеры «бомбы», «червя», «вируса».
10. Прокомментируйте понятия «кража» и «подлог» в качестве угрозы целостности.
11. Что в ИБ понимают под маскарадом?

Тема 8

1. Перечислите и прокомментируйте защитные действия от утечки конфиденциальной информации
2. Перечислите и охарактеризуйте защитные действия от НСД к конфиденциальной информации
3. Назовите три группы мероприятий по технической защите информации.
4. Прокомментируйте основные организационные мероприятия по технической защите информации. В каких ограничительных мерах они выражаются?
5. Прокомментируйте основные организационно-технические мероприятия по ЗИ.
6. Прокомментируйте основные технические мероприятия по технической защите информации.

Тема 9

1. Назовите основные меры и архитектурные принципы обеспечения обслуживаемости ИС.
2. В чем заключается специфика управления, как сервиса безопасности?

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*		
1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. – Москва : ИНФРА-М, 2021. – 201 с. – (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1191479	2021	https://znanium.com/catalog/product/1191479
2. Бирюков, А. А. Информационная безопасность: защита и нападение / А.А. Бирюков. - 2-е изд., перераб. и доп. - Москва : ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1028060	2017	https://znanium.com/catalog/product/1028060
3. Международная информационная безопасность: теория и практика : в трех томах. Том 1 : учебник / под общ. ред А. В. Крутских. - 2-е изд., доп. - Москва : Издательство «Аспект Пресс», 2021. - 384 с. - ISBN 978-5-7567-1098-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1241985	2021	https://znanium.com/catalog/product/1241985
Дополнительная литература		
1. Бахаров, Л. Е. Информационная безопасность и защита информации : сборник тестов / Л. Е. Бахаров. -	2015	https://znanium.com/catalog/product/1232263

Москва : Изд. Дом МИСиС, 2015. - 43 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232263		
2. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс	2012	http://www.studentlibrary.ru/book/ISBN9785940746478.html
3. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с. ISBN 978-5-00091-007-8.	2015	http://znanium.com/catalog.php?bookinfo=491597

6.2. Периодические издания

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

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м^2, 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 м^2, 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 м^2, 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: доц. каф. ИЗИ к.т.н. Полянский Д.А.

Рецензент: зав. каф. УОи НБ „Вл. инст. развития образования им. А.И. Кобяшовой Шишов Д.В.

Программа рассмотрена и одобрена на заседании кафедры «Вычислительная техника и системы управления»
Протокол № 1 от 31.08.2021 года
Заведующий кафедрой В.Н.Ланцов

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 27.03.04 «Управление в технических системах»
Протокол № 1 от 31.08.2021 года
Председатель комиссии А.Б.Градусов