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)**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационно-аналитические системы безопасности

(наименование дисциплины)

Направление подготовки 10.04.01 "Информационная безопасность "

Программа подготовки

Уровень высшего образования магистратура

Форма обучения очная

Семестр	Трудоемкость зач. ед./ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
1	7/252	18		36	153	Экзамен (45ч)
2	5/180	18		36	81	Экзамен (45ч), КР
Итого	12/432	36		72	234	Экзамен (45ч), экзамен (45ч), КР

Владимир 2018

Целями освоения дисциплины «Информационно-аналитические системы безопасности» являются обеспечение профессиональной подготовки магистров в соответствии с требованиями ФГОС ВО и учебного плана направления подготовки 10.04.01 «Информационная безопасность формирование у студентов обобщенного представления по следующим вопросам: -изучение методологических и законодательных основ организации системы защиты информации на предприятии, а также основных аспектов практической деятельности по ее созданию, обеспечению функционирования и контролю и эффективности. Сущность и задачи дисциплины «Комплексная система защиты информации на предприятии»: -принципы организации и этапы разработки СЗИ; -факторы, влияющие на организацию СЗИ; -определение и нормативное закрепление состава защищаемой информации; -определение объектов защиты; -анализ и оценка угроз безопасности информации; - выявление и оценка источников, способов и результатов дестабилизирующего воздействия на информацию; -определение потенциальных каналов и методов несанкционированного доступа к информации; -определение возможностей несанкционированного доступа к защищаемой информации. Кроме того, изучаются вопросы: -технологическое и организационное построение СЗИ; - кадровое обеспечение функционирования СЗИ; -материально-техническое и нормативно-методическое обеспечение функционирования СЗИ; -принципы и методы планирования функционирования СЗИ; - сущность и содержание контроля функционирования СЗИ; управление.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО СПЕЦИАЛИТЕТА

Данная дисциплина относится к базовой части Блока Б1 (код Б1.В.ДВ.01.01). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и практических занятий. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

Дисциплина изучается на четвертом курсе, требования к «входным» знаниям, умениям и готовностям (пререквизитам) обучающегося определяются требованиями к уровню подготовки по курсам «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности», «Техническая защита информации» по направлению подготовки 10.04.01 «Информационная безопасность», квалификации - магистр.

Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими профессиональными компетенциями:

ПК-1 – способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты;

ПК-2– способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

ПК-3 – способностью проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов;

ПК-9 – способностью проводить аудит информационной безопасности информационных систем и объектов информатизации.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) **Знать:** - цели, задачи и принципы построения системы защиты информации; - требования, предъявляемые к системе защиты информации; - этапы разработки комплексной системы защиты информации; - первоочередные мероприятия по обеспечению безопасности информационных ресурсов организации; - перечень вопросов ЗИ, требующих документационного закрепления; - виды контроля функционирования системы защиты информации на предприятии (ПК-1; ПК-2; ПК-3; ПК-9);

2) **Уметь:** - определять состав защищаемой информации предприятия; - синтезировать структуру комплексной системы защиты информации; - оценивать эффективность системы защиты информации (ПК-1; ПК-2; ПК-3; ПК-9);

3) **Владеть***:* - информацией о факторах, определяющие необходимость защиты территории и здания предприятия; -информацией о взаимодействии между субъектами, защищающими и использующими информацию ограниченного доступа; - информацией о структуре технического задания на создание комплексной системы защиты информации на предприятии; - методикой выявления и оценки источников, способов и результатов дестабилизирующего воздействия на информацию; - методикой определения возможностей несанкционированного доступа к защищаемой информации; -методикой разработке модели комплексной системы защиты информации (ПК-1; ПК-2; ПК-3; ПК-9).

У обучаемых в процессе изучения дисциплины должны вырабатываться дополнительные компетенции, с учетом требований работодателей:

- способность осуществлять комплексный подход к организации системы защиты на предприятии с учетом экономической эффективности СЗИ и требований нормативнотехнических документов.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 12 зачетных единиц, 432 часа.

№ п/п	Раздел (тема) дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Объем учебной работы, с применением интерактивных методов (в часах/ %)	Формы текущего контроля успеваемости *(по неделям семестра)* , форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	Контрольные работы.	СРС	КП / КР		
1	Основные руководящие документы и показатели эффективности системы ЗИ	1	1-2	2		4		17		2 (33%)	
2	Методика выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них	1	3-4	2		4		17		2 (33%)	
3	Формирование концепции обеспечения ИБ.	1	5-6	2		4		17		2 (33%)	Рейтингконтроль №1
4	Решения по ЗИ и оценка их качества.	1	7-8	2		4		17		2 (33%)	
5	Угрозы ИБ и оценка вероятности их реализации.	1	9-10	2		4		17		2 (33%)	
6	Формирование облика нарушителя	1	11-12	2		4		17		2 (33%)	Рейтингконтроль №2
7	Алгоритм проведения анализа информационного риска на предприятии	1	13-14	2		4		17		2 (33%)	
8	Аналитические технологии управления ИБ.	1	15-16	2		4		17		2 (33%)	
9	План обеспечения ИБ предприятия	1	17-18	2		4		17		2 (33%)	Рейтингконтроль №3
Всего по 1 семестру:				18		36		153		18 (33%)	Экзамен (45ч)
1	Цель, задачи, содержание и структура дисциплины.	2	1-2	2		4		7	2	2 (33%)	
2	Служба защиты информации как орган управления защитой информации и составная часть системы защиты.	2	3-4	2		4		7	2	2 (33%)	
3	Виды и типы организационных структур службы защиты информации.	2	5-6	2		4		7	2	2 (33%)	Рейтингконтроль №1
4	Порядок создания службы защиты информации.	2	7-8	2		4		7	2	2 (33%)	
5	Принципы организации и деятельности службы защиты информации.	2	9-10	2		4		7	2	2 (33%)	

6	Условия и факторы, влияющие на организацию службы защиты информации.	2	11-12	2		4		7	2	2 (33%)	Рейтингконтроль №2
7	Организация взаимодействия службы защиты информации и подразделений и внешних служб защиты информации.	2	13-14	2		4		7	2	2 (33%)	
8	Технология управления службой защиты информации.	2	15-16	2		4		7	2	2 (33%)	
9	Цели планирования. Виды планирования и их назначение	2	17-18	2		4		7	2	2 (33%)	Рейтингконтроль №3
Всего по 2 семестру:				18		36		63	18	18(33%)	Экзамен (45ч)
ИТОГО:				36		72		216	18	36 (33%)	Экзамен (45ч), экзамен (45ч)

Содержание дисциплины «Информационно-аналитические системы безопасности »:

Раздел 1. Введение. Основные руководящие документы и показатели эффективности системы ЗИ Комплексный подход к обеспечению ИБ объекта

Раздел 2. Методика выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них **Раздел**

3. Формирование концепции обеспечения ИБ.

Раздел 4. Решения по ЗИ и оценка их качества. Анализ риска. Общие положения и характеристика атаки на АС.

Раздел 5. Угрозы ИБ и оценка вероятности их реализации.

Раздел 6. Формирование облика нарушителя

Раздел 7. Алгоритм проведения анализа информационного риска на предприятии

Раздел 8. Аналитические технологии управления ИБ. Обеспечение ИБ в чрезвычайных ситуациях

Раздел 9. План обеспечения ИБ предприятия

Раздел 10. Цель, задачи, содержание и структура дисциплины.

Раздел 11. Служба защиты информации как орган управления защитой информации и составная часть системы защиты.

Раздел 12. Виды и типы организационных структур службы защиты информации.

Раздел 13. Порядок создания службы защиты информации.

Раздел 14. Принципы организации и деятельности службы защиты информации.

Раздел 15. Условия и факторы, влияющие на организацию службы защиты информации.

Раздел 16. Организация взаимодействия службы защиты информации и подразделений и внешних служб защиты информации.

Раздел 17. Технология управления службой защиты информации. **Раздел**

18. Цели планирования. Виды планирования и их назначение

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления магистра по направлению подготовки 10.04.01 «Информационная безопасность».

Для реализации компетентностного подхода предлагается интегрировать в учебный процесс интерактивные образовательные технологии, включая информационные и коммуникационные технологии (ИКТ), при осуществлении различных видов учебной работы:

 учебную дискуссию;

 электронные средства обучения (слайд-лекции, электронные тренажеры, компьютерные тесты); дистанционные (сетевые) технологии.

Как традиционные, так и лекции инновационного характера могут сопровождаться компьютерными слайдами или слайд-лекциями. Основное требование к слайд-лекции – применение динамических эффектов (анимированных объектов), функциональным назначением которых является наглядно-образное представление информации, сложной для понимания и осмысления студентами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП направления подготовки 10.04.01 «Информационная безопасность» особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом, в учебном процессе, они составляют не менее 30 процентов аудиторных занятий.

Занятия лекционного типа для соответствующих групп студентов согласно требованиям стандарта высшего образования не могут составлять более 55 процентов аудиторных занятий. Программа дисциплины соответствует данным требованиям.

Таким образом, применение интерактивных образовательных технологий придает инновационный характер практически всем видам учебных занятий, включая лекционные. При этом делается акцент на развитие самостоятельного, продуктивного мышления, основанного на диалогических дидактических приемах, субъектной позиции обучающегося в образовательном процессе. Тем самым создаются условия для реализации компетентностного подхода при изучении данной дисциплины.

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

Для текущего контроля успеваемости предлагается использование рейтинговой системы оценки, которая носит интегрированный характер и учитывает успешность студента в различных видах учебной деятельности, степень сформированности у студента общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг-контроля №1 семестр 1:

1. Дать определение СЗИ.
2. Что такое информационная безопасность?
3. Цели информационной безопасности.
4. Основные требования к комплексной системе защиты информации
5. Задачи системы компьютерной безопасности
6. Основные принципы организации СЗИ
7. В чём заключается принцип системности?
8. В чём заключается принцип комплексности?
9. В чём заключается принцип непрерывности защиты?
10. В чём заключается принцип разумной достаточности?
11. В чём заключается гибкость системы защиты?
12. Принцип простоты применения средств защиты
13. Этап работ по созданию СЗИ.

Вопросы рейтинг-контроля №2 семестр 2:

1. Что включает в себя обследование организации?
2. Факторы, влияющие на организацию СЗИ.

3. Определение состава защищаемой информации
4. Нормативное закрепление состава защищаемой информации
5. Виды информации.
6. Необходимые свойства защищаемой информации
7. Категорирование защищаемой информации.
8. Определение объектов защиты.
9. Что называется объектом защиты.
10. Основные объекты защиты.
11. Основные виды угроз информационной безопасности:
12. Классификация угроз безопасности
13. Неформальная модель нарушителя в АС .
14. Что определяются при разработке модели нарушителя.

Вопросы рейтинг-контроля №3 семестр 2:

1. Причины совершения компьютерных преступлений
2. Потенциальные каналы несанкционированного доступа к защищаемой информации 3. Потенциальные методы несанкционированного доступа к защищаемой информации. 4. Классификация каналов проникновения в систему и утечки информации
5. Физические каналы.
6. Электромагнитные каналы.
7. Информационные каналы
8. Общая модель комплексной системы защиты информации.
9. Средства защиты, используемые для создания системы защиты.
10. Типы моделей управления доступом.
11. Организационное направление работ по созданию СЗИ.
12. Технология построения СЗИ
13. Кадровое обеспечение функционирования СЗИ.
14. Организационная структура, основные функции службы компьютерной безопасности.
15. Концепция (политика) безопасности.

Вопросы рейтинг контроля №1 семестр 2:

1. Требования, предъявляемые к специалисту по защите информации.
2. Нормативные акты правового регулирования вопросов информатизации и защиты информации в Российской Федерации.
3. Основные принципы организации службы защиты информации на предприятии.
4. Структура и основные функции государственной системы защиты информации.
5. Организация и координация работ по защите информации в оборонной сфере.
6. Организация и координация работ по защите информации в экономической деятельности.
7. Перечень видов деятельности, на осуществление которых требуется лицензия.
8. Органы, уполномоченные на ведение лицензионной деятельности.
9. Основные нормативно-техническим документам по вопросам обеспечения безопасности информации.
10. Что устанавливает государственная система аттестации объектов информатизации.
11. Основные принципы, организационная структура и порядок проведения аттестации.
12. Какие объекты информатизации подлежат о*бязательной аттестации.*
13. Что такое безопасность информационных технологий.
14. Основные свойства информации и система ее обработки.
15. Что понимается под защитой информации.
16. Назовите основные элементы типовой системы защиты информации.
17. Назначение службы защиты информации.

18. Типовая организационно-штатная структура службы защиты информации.
19. Организационные и технологические задачи службы защиты информации. 20. Координационные задачи и функции службы защиты информации.

Вопросы рейтинг контроля №2 семестр 2:

1. Основное содержание положения о службе защиты информации.
2. Распределение обязанностей между сотрудниками службы защиты информации.
3. Порядок распределения обязанностей между сотрудниками службы защиты информации.
4. Основные принципы организации деятельности службы защиты информации.
5. Факторы, влияющие на создание службы защиты информации.
6. Основные направления организации работы службы защиты информации на предприятии.
7. Порядок установления взаимодействия службы защиты информации и подразделений внешних служб защиты информации.
8. Условия и порядок подбора кадров для службы защиты информации.
9. Требования, предъявляемые к сотрудникам службы защиты информации.
10. Что относится к конфиденциальной информации.
11. Виды ответственности в сфере безопасности информации.
12. Место информационной безопасности в общей системе безопасности РФ.
13. Основные задачи государственной системы защиты информации.
14. Организационная структура государственной системы защиты информации.
15. Функциональная структура государственной системы защиты информации.
16. Классификация технических средств негласного съема информации.
17. Основные характеристики технических средств негласного съема информации.
18. Какую информации необходимо защищать на объекте.
19. К каким последствиям может привести утрата конфиденциальной информации. 20. От кого Вы защищаете конфиденциальную информацию.

Вопросы рейтинг контроля №3 семестр 2:

1. Основы технологического процесса по управлению службой защиты информации.
2. Значение управленческих функций службы защиты информации.
3. Виды планирования и их назначение.
4. Основные методы контроля выполнения планов.
5. Основные формы контроля выполнения планов.
6. Цели и основные принципы планирования деятельности службой защиты информации.
7. Принципы управления службой защиты информации.
8. Применяемая система методов управления службой защиты информации.
9. Установление персональной ответственности за сохранность носителей информации.
10. Структура должностных инструкций сотрудников службы защиты информации.
11. Краткое содержание должностных инструкций сотрудников службы защиты информации.
12. Административно-правовые методы управления.
13. Экономические методы управления.
14. Социально-психологические методы управления.
15. Критерии оценки эффективности службы защиты информации.
16. Порядок оценки качества организации службы защиты информации.

Перечень вопросов к экзамену 1 семестр (промежуточной аттестации по итогам освоения дисциплины):

1. Дать определение СЗИ.

2. Что такое информационная безопасность?
3. Цели информационной безопасности.
4. Основные требования к комплексной системе защиты информации
5. Задачи системы компьютерной безопасности
6. Основные принципы организации СЗИ
7. В чём заключается принцип системности?
8. В чём заключается принцип комплексности?
9. В чём заключается принцип непрерывности защиты?
10. В чём заключается принцип разумной достаточности?
11. В чём заключается гибкость системы защиты?
12. Принцип простоты применения средств защиты
13. Этап работ по созданию СЗИ.
14. Что включает в себя обследование организации?
15. Факторы, влияющие на организацию СЗИ.
16. Определение состава защищаемой информации
17. Нормативное закрепление состава защищаемой информации
18. Виды информации.
19. Необходимые свойства защищаемой информации
20. Категорирование защищаемой информации.
21. Определение объектов защиты.
22. Что называется объектом защиты.
23. Основные объекты защиты.
24. Основные виды угроз информационной безопасности:
25. Классификация угроз безопасности
26. Неформальная модель нарушителя в АС .
27. Что определяются при разработке модели нарушителя.
28. Причины совершения компьютерных преступлений
29. Потенциальные каналы несанкционированного доступа к защищаемой информации 30. Потенциальные методы несанкционированного доступа к защищаемой информации. 31. Классификация каналов проникновения в систему и утечки информации
32. Физические каналы.
33. Электромагнитные каналы.
34. Информационные каналы
35. Общая модель комплексной системы защиты информации.
36. Средства защиты, используемые для создания системы защиты.
37. Типы моделей управления доступом.
38. Организационное направление работ по созданию СЗИ.
39. Технология построения СЗИ
40. Кадровое обеспечение функционирования СЗИ.
41. Организационная структура, основные функции службы компьютерной безопасности. 42. Концепция (политика) безопасности.

Перечень вопросов к экзамену 2 семестр (промежуточной аттестации по итогам освоения дисциплины):

1. Требования, предъявляемые к специалисту по защите информации.
2. Нормативные акты правового регулирования вопросов информатизации и защиты информации в Российской Федерации.
3. Основные принципы организации службы защиты информации на предприятии.
4. Структура и основные функции государственной системы защиты информации.
5. Организация и координация работ по защите информации в оборонной сфере.

6. Организация и координация работ по защите информации в экономической деятельности.
7. Перечень видов деятельности, на осуществление которых требуется лицензия.
8. Органы, уполномоченные на ведение лицензионной деятельности.
9. Основные нормативно-техническим документам по вопросам обеспечения безопасности информации.
10. Что устанавливает государственная система аттестации объектов информатизации.
11. Основные принципы, организационная структура и порядок проведения аттестации.
12. Какие объекты информатизации подлежат обязательной аттестации.
13. Что такое безопасность информационных технологий.
14. Основные свойства информации и система ее обработки.
15. Что понимается под защитой информации.
16. Назовите основные элементы типовой системы защиты информации.
17. Назначение службы защиты информации.
18. Типовая организационно-штатная структура службы защиты информации.
19. Организационные и технологические задачи службы защиты информации.
20. Координационные задачи и функции службы защиты информации.
21. Основное содержание положения о службе защиты информации.
22. Распределение обязанностей между сотрудниками службы защиты информации. 23. Порядок распределения обязанностей между сотрудниками службы защиты информации.
24. Основные принципы организации деятельности службы защиты информации.
25. Факторы, влияющие на создание службы защиты информации.
26. Основные направления организации работы службы защиты информации на предприятии.
27. Порядок установления взаимодействия службы защиты информации и подразделений внешних служб защиты информации.
28. Условия и порядок подбора кадров для службы защиты информации.
29. Требования, предъявляемые к сотрудникам службы защиты информации.
30. Что относится к конфиденциальной информации.
31. Виды ответственности в сфере безопасности информации.
32. Место информационной безопасности в общей системе безопасности РФ.
33. Основные задачи государственной системы защиты информации.
34. Организационная структура государственной системы защиты информации.
35. Функциональная структура государственной системы защиты информации.
36. Классификация технических средств негласного съема информации.
37. Основные характеристики технических средств негласного съема информации.
38. Какую информации необходимо защищать на объекте.
39. К каким последствиям может привести утрата конфиденциальной информации.
40. От кого Вы защищаете конфиденциальную информацию.
41. Основы технологического процесса по управлению службой защиты информации.
42. Значение управленческих функций службы защиты информации.
43. Виды планирования и их назначение.
44. Основные методы контроля выполнения планов.
45. Основные формы контроля выполнения планов.
46. Цели и основные принципы планирования деятельности службой защиты информации.
47. Принципы управления службой защиты информации.
48. Применяемая система методов управления службой защиты информации.
49. Установление персональной ответственности за сохранность носителей информации.
50. Структура должностных инструкций сотрудников службы защиты информации. 51. Краткое содержание должностных инструкций сотрудников службы защиты информации.
52. Административно-правовые методы управления.

53. Экономические методы управления.
54. Социально-психологические методы управления.
55. Критерии оценки эффективности службы защиты информации.
56. Порядок оценки качества организации службы защиты информации.

Темы лабораторных работ 1 семестр:

1. Построение описания объекта информатизации. Общее описание объекта и его планировка.
2. Построение описания объекта информатизации. Организационная структура предприятия и экспликация помещений отделов.
3. Построение описания объекта информатизации. Перечень и характеристики информационных ресурсов.
4. Построение описания объекта информатизации. Список и характеристики персонала.
5. Проектирование корпоративной сети передачи данных. Список и характеристики средств хранения, обработки, передачи и представления информации.
6. Проектирование корпоративной сети передачи данных. Список и характеристики средств защиты информации.
7. Проектирование корпоративной сети передачи данных. Топология КСПД и схема адресации.
8. Разработка слоев «информационные ресурсы», «КСПД», «персонал», «уязвимости», «угрозы» на плане объекта.
9. Разработка слоев СЗИ на плане объекта.

Темы лабораторных работ 2 семестр

1. Разработка положения о службе безопасности предприятия (Устав службы безопасности);
2. Разработка положения «О защите информации от технических разведок и от ее утечки по техническим каналам на объекте»;
3. Разработка положения «О подразделениях инженерно-технической защиты информации на объекте»;
4. Разработка положения «О режимно-секретном подразделении на объекте»;
5. Разработка инструкции «Об осуществлении контрольно-пропускного и объектового режима на объекте»;
6. Разработка положения «О постоянно действующих технических комиссиях по защите государственной тайны»;
7. Разработка инструкции (положения, руководства) по защите государственной тайны (конфиденциальной информации) на объекте;
8. Разработка инструкции (положения, руководства) по защите государственной тайны (конфиденциальной информации) при ее обработке с помощью средств вычислительной техники на объекте;
9. Разработка инструкций по направлениям деятельности для обеспечения защиты информации на объекте (по вариантам);
10. Разработка должностных инструкций сотрудников СБ на объекте (по вариантам).

Темы для курсовой работы 2 семестр:

Тема проекта (работы): Разработка и оценка системы защиты информации на предприятии.

1. Исходные данные

- Планировки помещений объекта информатизации
- Описание организационной структуры

2. Объём работы

2.1. Разработать следующие вопросы

- Построить описание объекта информатизации.
- Спроектировать корпоративную сеть передачи данных. • Выполнить анализ угроз ИБ и защищённости ИС
- Построить и оценить СЗИ па предприятии.

2.2. Конструктивно разработать (вычертить)

- Слой «информационные ресурсы» на плане объекта.
- Слой «корпоративная сеть передачи данных» на плане объекта.
- Слой «персонал» на плане объекта.
- Слой «уязвимости» на плане объекта.
- Слой «угрозы» на плане объекта.

Вопросы и задания для самостоятельной работы студентов:

1. Прокомментируйте основные направления обеспечения ИБ
2. Что понимается под безопасностью информации? Что такое ЗИ?
3. Дайте определение понятиям «конфиденциальность», «целостность», «доступность».
4. Перечислите основные задачи системы информационной безопасности.
5. В чем заключается основная цель защиты информации?
6. Определите организационные проблемы информационной безопасности.
7. Сформулируйте технические проблемы информационной безопасности.
8. Раскройте общее содержание методологии проектирования системы ЗИ. Как понимается процесс создания оптимальной системы? Сформулируйте возможные постановки задачи оптимизации СЗИ.
9. Приведите наиболее распространенную на сегодняшний день классификацию средств ЗИ. Каковы, на ваш взгляд, преимущества и недостатки программных, аппаратных и организационных средств ЗИ?
10. Раскройте содержание функции ЗИ. Какие из функций образуют полное множество функций защиты?
11. Дайте определение системы ЗИ и сформулируйте основные концептуальные требования, предъявляемые к ней.
12. Приведите принятую методику построения системы ИБ предприятия
13. Почему, на ваш взгляд, действительно эффективная защита информации может быть обеспечена только при комплексном системном подходе к решению этой проблемы? В чем заключается комплексность?
14. Сформулируйте основные концептуальные положения теории ЗИ.
15. По каким аспектам экспертная комиссия предприятия рассматривает предварительный перечень конфиденциальных сведений?
16. Приведите типовой примерный перечень сведений, составляющих служебную или коммерческую тайну организации.
17. Перечислите степень секретности (гриф), который могут иметь сведения, составляющие служебную или коммерческую тайну предприятия 18. Что принято понимать под служебной или коммерческой тайной?
19. Каковы критерии отнесения организаций и частных лиц к потенциальным злоумышленникам (которые могут быть заинтересованы в доступе к охраняемой информации)?
20. Каким образом принимается и как оформляется решения о включении сведений в окончательный вариант Перечня?
21. Назовите основную цель планирования в обеспечении ИБ предприятия. Охарактеризуйте стратегическое (или перспективное) и тактическое (или текущее) планирование.

22. Из каких этапов состоит работа по формированию Перечня сведений, составляющих служебную или коммерческую тайну?
23. Определите составляющие информационно-логической модели объекта защиты.
24. Что понимают под Политикой информационной безопасности?
25. Что должна включать в себя в обобщенном виде Концепция обеспечения ИБ?
26. Перечислите основные элементы Концепции обеспечения ИБ на предприятии. Зачем необходим раздел с основными понятиями концепции?
27. Прокомментируйте разделы Концепции, касающиеся определения состава потенциально существующих угроз безопасности информации, описания каналов вторжения в ИС, требований к системе обеспечения ИБ и методов оценки ее эффективности.
28. Что понимают под концепцией ИБ?
29. Назовите причины необходимости разработки Концепции обеспечения ИБ на каждом предприятии.
30. Определите основную цель и комплекс мероприятий управления ИБ предприятия.

Приведите обобщенную схему процесса управления ИБ предприятия

31. Охарактеризуйте основные направления деятельности администратора безопасности 32. Охарактеризуйте этапы логической последовательности принятия решения в процессе управления ИБ
33. Приведите структуру АРМа администратора безопасности
34. Основные подразделения службы ИБ, их организационно-правовой статус.
35. Приведите основные особенности и принципы построения системы управления ИБ. Охарактеризуйте основные подсистемы СУИБ.
36. Приведите и прокомментируйте пакет планирующих документов по обеспечению ИБ
37. С какой целью разрабатывается план мероприятий по противодействию ЧС?
38. Какие мероприятия по работе с персоналом необходимо проводить для наиболее эффективного противодействия ЧС? Приведите основные методы реагирования на ЧС 39. Какие ситуации называют чрезвычайными? Приведите классификацию ЧС. Охарактеризуйте наиболее распространенные угрозы в условиях чрезвычайных ситуаций 40. Охарактеризуйте постоянно проводимые мероприятия защиты и мероприятия, проводимые по необходимости
41. Охарактеризуйте разовые и периодически проводимые мероприятия защиты 42.

Охарактеризуйте источники получения информации для администратора безопасности

43. Служба защиты информации как составная часть системы защиты и как орган управления защитой информации. Концепция построения системы безопасности предприятия;
44. Правовые основы деятельности службы безопасности предприятия. Организационнофункциональные документы системы безопасности предприятия. Виды нормативных документов;
45. Организационные задачи службы защиты информации. Функции службы защиты информации;
46. Взаимосвязь организационных, технологических, координационных задач и функций службы защиты информации. Факторы, влияющие на задачи и функции службы защиты информации;
47. Структурная схема службы защиты информации. Должностной состав сотрудников службы защиты информации. Виды и типы организационных структур службы защиты информации;
48. Задачи, функции, права и ответственность сотрудников службы защиты информации;
49. Порядок создания службы защиты информации;

50. Структура и содержание положения о службе защиты информации;
51. Организация взаимодействия службы защиты информации и подразделений и внешних служб защиты информации;
52. Требования, предъявляемые к сотрудникам службы защиты информации.

Особенности подбора кадров для службы защиты информации;

53. Формы повышения квалификации персонала и подготовка кадрового резерва;
54. Особенности деятельности сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации;
55. Структура и содержание должностных инструкций сотрудников службы защиты информации;
56. Принципы управления службой защиты информации. Система методов управления;
57. Виды планирования и их назначение. Содержание и структура планов;
58. Организация и технология планирования. Методы и формы контроля выполнения планов;
59. Методы оценки эффективности и качества службы защиты информации;
60. Выбор оборудования и технических средств для оснащения рабочих мест сотрудников службы безопасности и обеспечения их деятельности;
61. Организация взаимодействия и сотрудничества службы безопасности предприятия с силовыми структурами региона;
62. Направления развития методов и средств безопасности предприятия.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. ISBN 978-5-8199-0411-4 Режим доступа: http://znanium.com/catalog.php?bookinfo=402686
2. Интеллектуальные системы защиты информации: учеб. пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. - http://www.studentlibrary.ru/book/ISBN9785942756673.html 172 с.
3. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - http://www.studentlibrary.ru/book/ISBN9785940746478.html. 474 с.

б) Дополнительная литература:

1. Бизнес-безопасность / Кузнецов И.Н. - М. : Дашков и К, 2012. - http://www.studentlibrary.ru/book/ISBN9785394014383.html. 416 с.
2. Офисный шпионаж / Мелтон К., Пилиджан К., Сверчински Д. - М. : Альпина Паблишер, 2013. - http://www.studentlibrary.ru/book/ISBN9785916712070.html. 182 с.
3. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций / Ямалов И.У. - М. : БИНОМ, 2015. - http://www.studentlibrary.ru/book/ISBN9785996325627.html. 291 с.
4. Искусство управления информационными рисками / Астахов А.М. - М. : ДМК Пресс, 2010. - http://www.studentlibrary.ru/book/ISBN9785940745747.html. 312 с.

в) Периодические издания :

1. «Журнал сетевых решений/LAN» -Режим доступа: http://www.osp.ru/lan/current;
2. Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: http://www.delpress.ru/

г) Программное обеспечение и 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/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 10.04.01 «Информационная безопасность»

Рабочую программу составил зав. кафедрой ИЗИ д.т.н., профессор Монахов М.Ю.

Рецензент (представитель работодателя) к.т.н. Вертилевский Н.В. РАЦ ООО «ИнфоЦентр», заместитель руководителя

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 2018/2019 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.04.01 «Информационная безопасность»

Протокол № 1 от 2018/2019 года

Председатель комиссии д.т.н., профессор /М.Ю. Монахов/

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ

РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2019-2020 учебный год

Протокол заседания кафедры № 1 от 16.09.2019 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ

РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2020 - 2021 учебный год

Протокол заседания кафедры № 1 от 31.08.2020 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/