УП2013

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

УТВЕРЖДАЮ
Проректор
по образовательной деятельности
_____ А.А.Панфилов
«_29_» _12_____ 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

СЛУЖБА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

(наименование дисциплины)

Направление подготовки 10.03.01 Информационная безопасность

Профиль / программа подготовки Комплексная защита объектов информатизации

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоемкость зач. ед./ час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
7	3/108	18	18		72	Зачет
Итого	3/108	18	18		72	Зачет

Владимир 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Служба информационной безопасности на предприятии» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность», формирование у бакалавров знаний по современным проблемам организации и структурного построения службы безопасности на предприятии. В курсе рассматривается вопросы модели компонентов системы безопасности предприятия, организационного проектирования службы, организационно-штатные структуры СБ, их основные задачи и назначение.

Задачей изучения дисциплины «Служба информационной безопасности на предприятии» является изучение: -концепции построения системы безопасности предприятия; -правовых основ деятельности службы безопасности предприятия; организационного проектирования деятельности службы безопасности предприятия; - структуры и функций службы безопасности предприятия; - задач и назначений подразделений службы безопасности предприятия; - организации службы защиты информации; - управление службой безопасности предприятия; -подбор, расстановка и обучение сотрудников службы защиты информации.

Курс предусматривает овладение навыками практической деятельности в области построения, организации и управления службой безопасности предприятия. создания правоустанавливающих документов структурных подразделений службы безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО БАКАЛАВРИАТА

Данная дисциплина относится дисциплинам по выбору вариативной части Блока Б1 (код Б1.В.ДВ.1). В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций 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 курсу «Организационное и правовое обеспечение информационной безопасности» профессионального цикла по направлению подготовки 10.03.01 «Информационная безопасность», квалификации - бакалавр. Кроме того, для грамотного использования полученных знаний в профессиональной деятельности, требуется изучение курсов «Документоведение»; «Правоведение», «Основы управленческой деятельности».

Курс тесно взаимосвязан с другими дисциплинами данного цикла. Он является полезным для изучения таких дисциплин как «Актуальные вопросы информационного права», «Организационное и правовое обеспечение информационной безопасности», «Управление информационной безопасностью», «Система защиты информации на предприятии».

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

В результате освоения дисциплины бакалавр должен обладать следующими общепрофессиональными компетенциями:

ОПК-7- способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

профессиональными компетенциями:

ПК-4- способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;

ПСК-3.1- способностью проводить совместный анализ функционального процесса объекта защиты и применяемых информационных технологий и технических средств с целью определения возможных источников информационных угроз, их вероятных целей и тактики.

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1) Знать: основные понятия и методы в области управления службой безопасности предприятия; содержание управленческой работы руководителя подразделения службы безопасности предприятия; организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России. Знать понятия и виды защищаемой информации; виды основных угроз защищаемой информации; базовые понятия о методах и средствах защиты информации применяемых в деятельности службы безопасности предприятия; международные стандарты информационной безопасности (ОПК-7, ПК-4, ПСК-3.1);

2) Уметь: - определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; - выявлять уязвимости информационно-технологических ресурсов информационных систем; - определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем; - осуществлять планирование и организацию работы рабочего коллектива при выполнении поставленных задач. Уметь пользоваться научно- технической и справочной литературой для решения прикладных задач; осуществлять поиск информации в Интернет и выполнять аналитического исследования по определенной теме (ОПК-7, ПК-4, ПСК-3.1);

3) Владеть:- навыками анализа информационной инфраструктуры информационной системы и ее безопасности; - методами выявления угроз информационной безопасности информационных систем; -пользоваться нормативными документами по противодействию технической разведке; применять действующую законодательную базу в области обеспечения информационной безопасности; -применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности. Владеть основами процесса формирования структуры службы безопасности на предприятии, моделями проектирования службы защиты информации; системами защиты информации, применяемыми в практике обеспечения информационной безопасности; методами и средствами защиты информации, применяемыми в деятельности службы безопасности на предприятиях (ОПК-7, ПК-4, ПСК-3.1).

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

- способность разрабатывать основополагающие организационно-распорядительные документы службы безопасности на предприятии.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 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	Цель, задачи, содержание и структура дисциплины.	7	1-2	2	2			8		1/25%	
2	Служба защиты информации как орган управления защитой информации и составная часть системы защиты.	7	3-4	2	2			8		2/50%	
3	Виды и типы организационных структур службы защиты информации.	7	5-6	2	2			8		2/50%	Рейтинг контроль 1
4	Порядок создания службы защиты информации.	7	7-8	2	2			8		1/25%	
5	Принципы организации и деятельности службы защиты информации.	7	9-10	2	2			8		2/50%	
6	Условия и факторы, влияющие на организацию службы защиты информации.	7	11-12	2	2			8		3/75%	Рейтинг контроль 2
7	Организация взаимодействия службы защиты информации и подразделений и внешних служб защиты информации.	7	13-14	2	2			8		2/50%	
8	Технология управления службой защиты информации.	7	15-16	2	2			8		3/75%	Рейтинг контроль 3
9	Цели планирования. Виды планирования и их назначение	7	17-18	2	2			8		3/75%	
	Всего			18	18			72		19/53%	Зачет

Содержание дисциплины «Служба информационной безопасности на предприятии»

Раздел 1. Концепция построения системы безопасности предприятия. Определение и основные понятия системы безопасности. Защита информации в системе безопасности предприятия. Концептуальные модели компонентов системы безопасности предприятия. Принципы построения системы безопасности предприятия.

Раздел 2. Правовые основы деятельности службы безопасности предприятия. Организационно-функциональные документы системы безопасности предприятия. Виды нормативных документов. Лицензирование видов деятельности службы безопасности предприятия. Рекомендации по разработке уставных документов службы безопасности предприятия.

Раздел 3. Организационное проектирование деятельности службы безопасности предприятия. Основы организационного проектирования систем управления. Методика проектирования функционального содержания управленческой деятельности. Методика проектирования организационной структуры системы управления. Методика оформления основных документов организационного проекта системы управления

Раздел 4. Структура и функции службы безопасности предприятия. Состав службы безопасности предприятия. Основные функции службы безопасности предприятия. Построение структурной схемы управления службой безопасности предприятия.

Раздел 5. Подразделения службы безопасности предприятия. Подразделения режима и охраны. Специальный отдел. Подразделение информационно-аналитической деятельности. Подразделение инженерно-технической защиты. Подразделение разведки. Обеспечение контрольно-пропускного и объектового режимов.

Раздел 6. Организация службы защиты информации. Создание СЗИ. Структура СЗИ. Организационно-технические мероприятия СЗИ. Руководитель службы защиты информации. Разработка должностных инструкций для специалистов по защите информации.

Раздел 7. Управление службой безопасности предприятия (СБП). Методы управления СБП. Функции процессов управления СПБ. . Принципы управления СБП. Обеспечение деятельности службы безопасности. Управление безопасностью предприятия в кризисных ситуациях.

Раздел 8. Подбор, расстановка и обучение сотрудников службы защиты информации. Роль персонала в системе защиты информации. Набор и отбор персонала в СБП. Требования к специалистам по защите информации.

Раздел 9. Организация обучения специалистов по защите информации. Требования к начальнику службы безопасности предприятия. Новые подходы к кадровому обеспечению службы безопасности предприятия

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Изучение дисциплины предполагает не только запоминание и понимание, но и анализ, синтез, рефлексию, формирует универсальные умения и навыки, являющиеся основой становления бакалавра по направлению «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:

разбор конкретных ситуаций;

учебную дискуссию;

электронные средства обучения (слайд-лекции).

Лекционные занятия проводятся в аудитории, оборудованной проектором, что позволяет сочетать активные и интерактивные формы проведения занятий.

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 бакалаврами, а также интенсификация и диверсификация учебного процесса.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью ОПОП бакалавриата по направлению 10.03.01, 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 45 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 бакалавра в различных видах учебной деятельности, степень сформированности у бакалавра общекультурных и профессиональных компетенций.

Примерный перечень заданий для текущих контрольных мероприятий:

Вопросы рейтинг контроля №1

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.

Вопросы рейтинг контроля №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

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 зачету (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 практических работ

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 рефератов

1. Служба защиты информации как составная часть системы защиты и как орган управления защитой информации. Концепция построения системы безопасности предприятия
2. Правовые основы деятельности службы безопасности предприятия. Организационно-функциональные документы системы безопасности предприятия. Виды нормативных документов.
3. Организационные задачи службы защиты информации. Функции службы защиты информации.
4. Взаимосвязь организационных, технологических, координационных задач и функций службы защиты информации. Факторы, влияющие на задачи и функции службы защиты информации.
5. Структурная схема службы защиты информации. Должностной состав сотрудников службы защиты информации. Виды и типы организационных структур службы защиты информации.
6. Задачи, функции, права и ответственность сотрудников службы защиты информации.
7. Порядок создания службы защиты информации.
8. Структура и содержание положения о службе защиты информации.
9. Организация взаимодействия службы защиты информации и подразделений и внешних служб защиты информации.

10. Требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров для службы защиты информации.
11. Формы повышения квалификации персонала и подготовка кадрового резерва.
12. Особенности деятельности сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации.
13. Структура и содержание должностных инструкций сотрудников службы защиты информации.
14. Принципы управления службой защиты информации. Система методов управления.
15. Виды планирования и их назначение. Содержание и структура планов.
16. Организация и технология планирования. Методы и формы контроля выполнения планов.
17. Методы оценки эффективности и качества службы защиты информации.
18. Выбор оборудования и технических средств для оснащения рабочих мест сотрудников службы безопасности и обеспечения их деятельности
19. Организация взаимодействия и сотрудничества службы безопасности предприятия с силовыми структурами региона
20. Направления развития методов и средств безопасности предприятия

Вопросы и задания для самостоятельной работы студентов:

- Служба защиты информации как составная часть системы защиты и как орган управления защитой информации. Концепция построения системы безопасности предприятия;
- Правовые основы деятельности службы безопасности предприятия. Организационно-функциональные документы системы безопасности предприятия. Виды нормативных документов;
- Организационные задачи службы защиты информации. Функции службы защиты информации;
- Взаимосвязь организационных, технологических, координационных задач и функций службы защиты информации. Факторы, влияющие на задачи и функции службы защиты информации;
- Структурная схема службы защиты информации. Должностной состав сотрудников службы защиты информации. Виды и типы организационных структур службы защиты информации;
- Задачи, функции, права и ответственность сотрудников службы защиты информации;
- Порядок создания службы защиты информации;
- Структура и содержание положения о службе защиты информации;
- Организация взаимодействия службы защиты информации и подразделений и внешних служб защиты информации;
- Требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров для службы защиты информации;
- Формы повышения квалификации персонала и подготовка кадрового резерва;
- Особенности деятельности сотрудников службы защиты информации. Распределение обязанностей между сотрудниками службы защиты информации;
- Структура и содержание должностных инструкций сотрудников службы защиты информации;
- Принципы управления службой защиты информации. Система методов управления;
- Виды планирования и их назначение. Содержание и структура планов;
- Организация и технология планирования. Методы и формы контроля выполнения планов;
- Методы оценки эффективности и качества службы защиты информации;
- Выбор оборудования и технических средств для оснащения рабочих мест сотрудников службы безопасности и обеспечения их деятельности;
- Организация взаимодействия и сотрудничества службы безопасности предприятия с силовыми структурами региона;
- Направления развития методов и средств безопасности предприятия.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Основная литература:

1. Бизнес-безопасность / Кузнецов И.Н. - М. : Дашков и К, 2012. - http://www.studentlibrary.ru/book/ISBN9785394014383.html. - 3-е изд. - М.: - 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. Башлы, П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 Режим доступа: http://znanium.com/catalog.php?bookinfo=405000

б) Дополнительная литература:

1. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2015. - 322 с. ISBN 978-5-369-01450-9 Режим доступа: http://znanium.com/catalog.php?bookinfo=495249
2. Микрюков Т.В. Службы экономической безопасности и их функции / Вестник Удмуртского университета. Серия 2. Экономика и право, Вып. 1, 2010 Режим доступа: http://znanium.com/catalog.php?bookinfo=525174
3. Кузнецов, И. Н. Бизнес-безопасность / И. Н. Кузнецов. - 3-е изд. - М.: Дашков и К, 2013. - 416 с. - ISBN 978-5-394-01438-3. Режим доступа: http://znanium.com/catalog.php?bookinfo=430343

в) Периодические издания:

1. Журнал "Алгоритм безопасности» – Режим доступа: http://www.algoritm.org/index.php;
2. Электронный научный журнал «Проблемы безопасности» – Режим доступа: http://www.pb.littera-n.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 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»

Рабочую программу составил доцент кафедры ИЗИ к.т.н. Тельный А.В.
(ФИО, подпись)

Рецензент
(представитель работодателя) Заместитель руководителя РАЦ ООО «ИнфоЦентр»

к.т.н. Вертилевский Н.В.
(место работы, должность, ФИО, подпись)

Программа рассмотрена и одобрена на заседании кафедры ИЗИ
Протокол № 7 от 28.12.16 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность» профиль «Комплексная защита объектов информатизации»
Протокол № 4 от 28.12.16 года
Председатель комиссии д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на 2017/18 учебный год
Протокол заседания кафедры № 1 от 28.08.17 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на _____ учебный год
Протокол заседания кафедры № _____ от _____ года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Приложение

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

Институт _____

Кафедра _____

Актуализированная
рабочая программа
рассмотрена и одобрена
на заседании кафедры
протокол № ____ от ____ 20__г.

Заведующий кафедрой

_____
(подпись, ФИО)

Актуализация рабочей программы дисциплины

_____
(наименование дисциплины)

Направление подготовки

Профиль/программа подготовки

Уровень высшего образования

Форма обучения

Владимир 20__

Рабочая программа учебной дисциплины актуализирована в части рекомендуемой литературы.

Актуализация выполнена: _____
(подпись, должность, ФИО)

а) основная литература: _____

б) дополнительная литература: _____

в) периодические издания: _____

в) интернет-ресурсы: _____