

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## **ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ**

Направление подготовки 10.03.01 Информационная безопасность

Направленность «Организация и технология защиты информации»


Квалификация (степень) выпускника: Бакалавр

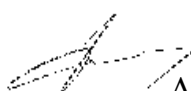
**Кострома**

Рабочая программа дисциплины «Основы управления информационной безопасностью» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность

Приказ Минобрнауки России от 1.12.2016 № 1515. Зарегистрировано в Минюсте России, регистрационный № 44821 от 20 декабря 2016 года.

Год начала подготовки 2016

Разработал:  Волков Антон Андреевич, доцент кафедры защиты информации, к.т.н.

Рецензент:  Алексеев Дмитрий Станиславович, доцент кафедры защиты информации, к.т.н.

УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания кафедры № 13 от 6 июля 2017 г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 12 от 27 июня 2018 г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 11 от 30.05.2019 \_\_\_\_\_ г.

Заведующий кафедрой защиты информации

 Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 8 от 6.04.2020 г.

Заведующий кафедрой защиты информации



Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 6 от 22.01.2021 г.

Заведующий кафедрой защиты информации



Щекочихин Олег Владимирович, к.т.н., доцент

## 1. Цели и задачи освоения дисциплины

**Целями дисциплины** «Основы управления информационной безопасностью» являются получение необходимых знаний о принципах и методах, инструментальных средств, нормативных документах регуляторах, позволяющих успешно управлять информационной безопасностью организации в условиях активного использования информационных технологий.

**Задачи дисциплины:**

- формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем;
  - ознакомление обучаемых с основными методами управления информационной безопасностью организаций, объектов и систем, обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации.
  - приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации и разграничения полномочий персонала, ответственного за информационную безопасность

## 2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

### **знать**

- современные подходы к управлению ИБ и направления их развития;
- основные стандарты, регламентирующие управление ИБ;
- принципы построения СУИБ; принципы разработки процессов управления ИБ;
- взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ;
- подходы к интеграции СУИБ в общую систему управления предприятием.

### **уметь**

- анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ;
- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;
- применять процессный подход к управлению ИБ в различных сферах деятельности;
- используя современные методы и средства разрабатывать процессы управления ИБ, учитывая особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;
- практически решать задачи формализации разрабатываемых процессов управления ИБ;
- разрабатывать и внедрять СУИБ и оценивать ее эффективность.

### **владеть**

- навыками управления информационной безопасностью простых объектов;
- терминологией и процессным подходом построения систем управления ИБ;
- навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
- навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом

### **Освоить компетенции:**

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 (ОПК-7)

способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3)

способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)

способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)

способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11)

способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14)

### 3. Место дисциплины в структуре ОП ВО

Дисциплина «Основы управления информационной безопасности» относится к циклу базовых дисциплин,

Дисциплина изучается на четвертом курсе, требования к входным знаниям, умениям и навыкам определяются требованиями к уровню подготовки по дисциплинам «Криптографические методы защиты информации», «Техническая защита информации».

Изучение дисциплины является основой для освоения последующих дисциплин/практик: «Комплексные системы защиты информации на предприятии», «Управление информационными ресурсами и проектами», «Организация и управление службой защиты информации на предприятии».

### 4. Объем дисциплины (модуля)

#### 4.1. Объем дисциплины в зачетных единицах с указанием академических (астрономических) часов и виды учебной работы

Виды учебной работы,	Очная форма
Общая трудоемкость в зачетных единицах	5
Общая трудоемкость в часах	180
Аудиторные занятия в часах, в том числе:	58
Лекции	28
Практические занятия	-
Лабораторные занятия	30
Самостоятельная работа в часах	86
Форма промежуточной аттестации	Экзамен 7 семестр

#### 4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	28
Практические занятия	-
Лабораторные занятия	30
Консультации	3,4
Зачет/зачеты	-
Экзамен/экзамены	0,35
Курсовые работы	-
Курсовые проекты	-
Всего	60,35

**5.Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий**

**5.1 Тематический план учебной дисциплины**

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лабораторные	
1.	Введение.	10	2	2	6
2.	Понятие национальной безопасности. Виды информации. Виды безопасности	10	2	2	6
3.	Информационная безопасность в системе национальной безопасности. Государственная информационная политика. Проблемы региональной информационной политики	10	2	2	6
4.	Основные понятия и общеметодологические принципы теории информационной безопасности. Анализ угроз информационной безопасности	10	2	2	6
5.	Информационная война, методы и средства её ведения	10	2	2	6
6.	Методы и средства обеспечения информационной безопасности	10	2	2	6
7.	Основы комплексного обеспечения информационной безопасности	10	2	2	6
8.	Модели, стратегии и системы обеспечения информационной безопасности	10	2	2	6
9.	Критерии и классы защищённости средств вычислительной техники и автоматизированных информационных систем	10	2	2	6
10.	Способы и методы защиты информации	10	2	2	6
11.	Модели информационной безопасности	10	2	2	6
12.	Уровни информационной безопасности	10	2	2	6
13.	Подходы к реализации и этапы построения систем защиты информации	10	2	2	6
14.	Принципы построения систем защиты информации	14	2	4	8
<b>Экзамен</b>		36			
<b>Всего:</b>		<b>216</b>	<b>28</b>	<b>30</b>	<b>86</b>

**5.2. Содержание:**

**ТЕМА 1. Введение.**

Роль и место дисциплины «Основы информационной безопасности» в подготовке специалистов по защите информации. Цели и задачи дисциплины. Рекомендации в изучении курса. Библиография.

**ТЕМА 2. Понятие национальной безопасности. Виды информации. Виды безопасности**

Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства: экономическая, внутривластная, социальная, международная, информационная, военная, экологическая и др.

Виды защищаемой информации. Информация как объект права собственности.

Особенности регулирования прав собственности на информацию. Информация как объект защиты: понятие информации, подлежащей защите, категории важности и ценности информации.

Этапы жизненного цикла информации. Информация как объект защиты. Уровни представления

информации (уровень носителей информации, уровень средств взаимодействия с носителем, уровень представления информации, уровень содержания информации). Роль и место системы обеспечения информационной безопасности в системе национальной безопасности государства.

### **ТЕМА 3. Информационная безопасность в системе национальной безопасности. Государственная информационная политика. Проблемы региональной информационной политики.**

Концепция национальной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации. Виды угроз. Источники угроз. Внешние источники угроз. Внутренние источники угроз.

### **ТЕМА 4. Основные понятия и общеметодологические принципы теории информационной безопасности. Анализ угроз информационной безопасности.**

Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе 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. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению. Принципы обеспечения информационной безопасности. Общие методы обеспечения информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности. Структуризация методов защиты информации, уровни обеспечения защиты. Основные принципы обеспечения информационной безопасности.

Угрозы конфиденциальности, целостности и доступности информации, угроза раскрытия параметров системы.

Причины и виды утечки информации. Каналы утечки информации: акустические (включая и акустопреобразовательные), визуально-оптические, электромагнитные, материально-вещественные, информационные.

### **ТЕМА 5. Информационная война, методы и средства её ведения**

Информационная безопасность и информационное противоборство. Субъекты информационного противоборства. Цели информационного противоборства.

Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности. Информационная война как результат столкновения интересов в условиях рынка. Моделирование информационных войн. меры противодействия вероятному противнику в условиях информационной войны.

### **ТЕМА 6. Методы и средства обеспечения информационной безопасности**

Построение систем обеспечения конфиденциальности информации. Организационно-правовые методы защиты. Технические методы защиты: идентификация и аутентификация, парольные системы, криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания. Построение систем защиты от угрозы нарушения целостности информации. Меры защиты целостности информации при её хранении, обработке и транспортировке. Цифровая подпись. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита от сбоев программно-аппаратной среды. Обеспече-

ние отказоустойчивости программного обеспечения. Защита актуальности информации. Построение систем защиты от угрозы раскрытия параметров информационной системы.

#### **ТЕМА 7. Основы комплексного обеспечения информационной безопасности**

Классификация объектов защиты информации. Особенности защиты информации в сосредоточенных и распределённых вычислительных системах. Технология защиты информации сосредоточенного вычислительного комплекса. Технология защиты информации распределённого вычислительного комплекса. Методы и средства обеспечения безопасности в каналах связи и телекоммуникаций Практические аспекты обеспечения информационной безопасности на предприятии. Методологические основы создания систем обеспечения информационной безопасности.

#### **ТЕМА 8. Модели, стратегии и системы обеспечения информационной безопасности**

Понятие политики безопасности. Основные типы политики безопасности. Разработка и реализация политики безопасности. Модели безопасности. Модель матрицы доступов HRU. Модель системы безопасности Белла-Лападула.

#### **ТЕМА 9. Критерии и классы защищённости средств вычислительной техники и автоматизированных информационных систем**

Критерии и классы защищённости СВТ и АС в соответствии с Руководящими документами ГТК России. Анализ стандартов информационной безопасности: Критерии оценки безопасности компьютерных систем Министерства обороны США; Европейские критерии безопасности информационных технологий; Федеральные критерии безопасности информационных технологий; Канадские критерии безопасности информационных технологий.

#### **ТЕМА 10. Способы и методы защиты информации**

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

#### **ТЕМА 11. Модели информационной безопасности**

Основными структурными элементами информационной безопасности компьютерных систем в данной модели являются:

1. Цели защиты информации.
2. Субъекты, участвующие в процессах информационного обмена.
3. Угрозы безопасности информационных систем.
4. Уровни уязвимости информации и информационной инфраструктуры.

Обеспечение безопасности состоит в достижении трех взаимосвязанных целей: конфиденциальность, целостность и доступность.

#### **ТЕМА 12. Уровни информационной безопасности**

Организационные основы как необходимые условия осуществления защиты информации. Условия, необходимые для обеспечения технологии защиты информации, а также сохранности и конфиденциальности информации. Значение методологических принципов защиты информации.

#### **ТЕМА 13. Подходы к реализации и этапы построения систем защиты информации**

Реализация системы защиты информации на основе встраиваемых и встроенных средств защиты. Организация безопасной среды для работы обработки конфиденциальной информации. Этапы проектирования и реализации систем защиты конфиденциальной информации.



## ТЕМА 14. Принципы построения систем защиты информации

Принципы, обусловленные принадлежностью, ценностью, конфиденциальностью, технологией защиты информации. Основные меры и архитектурные принципы обеспечения обслуживаемости ИС. Сервисы безопасности. Понятие и назначение технологического обеспечения защиты информации. Классификация организационно технологических документов по защите информации. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий. Значение и виды контрольных мероприятий.

### 6. Методические материалы для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы.

Обучающемуся важно помнить, что лекция эффективно помогает ему овладеть программным материалом благодаря расстановке преподавателем необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации. Кроме того, во время лекции имеет место прямой визуальный и эмоциональный контакт обучающегося с преподавателем, обеспечивающий более полную реализацию воспитательной компоненты обучения.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков применения методов формирования, организации и поддержки комплекса мер по обеспечению информационной безопасности объекта защиты;
- совершенствование навыков поиска публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации студента.

#### 6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

№ п/п	Раздел (тема) дисциплины	Задание	Методические рекомендации по выполнению задания	Форма контроля
1	2	3	4	5
1.	Тема № 1	Усвоить	1. Изучить значение и место курса в подготовке специалистов по защите информации. Литература основная [1-6], дополнительная [1-9]	Контрольный опрос
2.	Тема № 2	Усвоить	1. Изучить информационной безопасности с информатизацией общества. 2. Усвоить понятия "информационная	Контрольный опрос

			безопасность” Литература основная[1-6], дополнительная [1-9]	
3.	Тема № 3	Приобрести навык	1. Изучить свойства информации как предмета защиты. 2. Изучить понятие предмета защиты. Литература основная[1-6], дополнительная [1-9]	Проверка выполнения лабораторной работы
4.	Тема № 4	Усвоить	1. Изучить современную концепцию национальной безопасности. 2. Изучить виды состав угроз информационной безопасности. 3. Изучить общие методы обеспечения информационной безопасности. Литература основная[1-6], дополнительная [1-9]	Контрольный опрос
5.	Тема № 5	Усвоить	1. Изучить определение защищаемой информации. 2. Изучить основные признаки защищаемой информации Литература основная[1-6], дополнительная [1-9]	Проверка выполнения практического задания
6.	Тема № 6	Усвоить	1. Изучить основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации. Литература основная[1-6], дополнительная [1-9]	Контрольный опрос
7.	Тема № 7	Приобрести навык	1. Изучить основные виды конфиденциальной информации, нуждающейся в защите. 2. Изучить основные объекты профессиональной тайны. Литература основная[1-6], дополнительная [1-9]	Проверка выполнения
8.	Тема № 8	Приобрести навык	1. Изучить основные компоненты концептуальной модели ИБ. 2. Изучить основные источники угроз. Литература основная[1-6], дополнительная [1-9]	Проверка выполнения
9.	Тема № 9	Приобрести навык	1. Изучить способы несанкционированного доступа к конфиденциальной информации 2. Изучить обобщенную модель взаимодействия способов несанкционированного доступа и источников конфиденциальной информации. Литература основная[1-6], дополнительная [1-9]	Проверка выполнения
10.	Тема № 10	Усвоить	1. Изучить основные методы, используемые злоумышленниками для получения доступа к	Контрольный опрос

			конфиденциальной информации Литература основная[1-6], дополнительная [1-9]	
11.	Тема № 11	Приобрести навык	1. Изучить современные подходы к понятию угрозы защищаемой информации. 2. Усвоить связь угрозы защищаемой информации с уязвимостью информации. Литература основная[1-6], дополнительная [1-9]	Проверка выполнения
12.	Тема № 12	Усвоить	1.Изучить способы предупреждения возможных угроз. 2. Изучить основные защитные действия при реализации способов ЗИ. Литература основная[1-6], дополнительная [1-9]	Проверка выполнения
13.	Тема № 13	Приобрести навык	Изучить основные структурные элементы информационной безопасности Литература основная[1-6], дополнительная [1-9]	Проверка выполнения
14.	Тема № 14	Усвоить	Изучить организационные основы как необходимые условия осуществления защиты информации. Литература основная[1-6], дополнительная [1-9]	Контрольный опрос
15.	Тема № 15	Приобрести навык	Изучить этапы проектирования и реализации систем защиты конфиденциальной информации. Литература основная[1-6], дополнительная [1-9]	Контрольный опрос
16.	Тема № 16	Усвоить	Изучить принципы, обусловленные принадлежностью, ценностью, конфиденциальностью, технологией защиты информации. Литература основная[1-6], дополнительная [1-9]	Контрольный опрос

Формой отчетности по данной дисциплине является экзамен. Необходимые условия допуска к экзамену:

- Наличие полного конспекта лекций
- Сдача всех контрольных работ (3 шт) с положительным результатом

## **6.2. Тематика и задания для практических занятий (при наличии)**

*Не предусмотрены*

## **6.3. Тематика и задания для лабораторных занятий**

Темы лабораторных работ

Тема 1. Состав и классификация носителей защищаемой информации

Тема 2. Значение информационной безопасности и ее место в системе национальной безопасности. Современная доктрина информационной безопасности Российской Федерации

Тема 3. Критерии, условия и принципы отнесения информации к защищаемой. Классификация защищаемой информации по видам тайны и степеням конфиденциальности

- Тема 4. Классификация защищаемой информации по собственникам и владельцам
- Тема 5. Концептуальные основы защиты информации
- Тема 6. Каналы и методы несанкционированного доступа к конфиденциальной информации
- Тема 7. Понятие и структура угроз защищаемой информации. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию
- Тема 8. Классификация видов, методов и средств защиты информации
- Тема 9. Технологическое обеспечение защиты информации

## 7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

### а) основная

1. **Информационная безопасность конструкций ЭВМ и систем** : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — М. : ИНФРА-М, 2018. — 118 с. + Доп. материалы [Электронный ресурс; Режим доступа <http://www.znanium.com>]. — (Высшее образование: Бакалавриат). — <http://znanium.com/catalog.php?bookinfo=925825>
2. **Информационная безопасность и защита информации**: Учебное пособие. / Баранова Е.К., Бабаш А.В. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017. — 322 с. — (Высшее образование). — <http://znanium.com/catalog.php?bookinfo=763644>
3. **Загинайлов, Ю.Н.** Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - Москва ; Берлин : Директ-Медиа, 2015. - 253 с. : ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=276557>
4. **Нестеров, С.А.** Основы информационной безопасности : учебное пособие / С.А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - Санкт-Петербург. : Издательство Политехнического университета, 2014. - 322 с. : схем., табл., ил. - ISBN 978-5-7422-4331-1 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=363040>
5. **Информационная безопасность и защита информации** : учеб. пособие для вузов / Ю. Ю. Громов [и др.]. - Старый Оскол : ТНТ, 2010. - 384 с.: рис. - ISBN 978-5-94178-216-1 : 590.00.
6. **Бабаш, Александр Владимирович** . Информационная безопасность: Лабор. практикум+CD: учеб. пособие / Бабаш, Александр Владимирович . - 2-изд., стер. - Москва : КноРус, 2013. - 136 с.: рис. - (Бакалавриат). - СД. - осн. - ISBN 978-5-406-02760-8 : 303.00.

### б) дополнительная

1. **Информационная безопасность предприятия** : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). <http://znanium.com/catalog.php?bookinfo=612572>
2. **Информационная система предприятия**: Учебное пособие/Вдовенко Л. А., 2-е изд., пераб. и доп. - М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. - 304 с.: 60x90 1/16 (Переплёт 7БЦ) ISBN 978-5-9558-0329-6, 500 экз. <http://znanium.com/catalog.php?bookinfo=501089>
3. **Артемов, А.В.** Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=428605>
4. **Золотарев, В. В.** Управление информационной безопасностью. Ч. 1. Анализ информационных рисков [Электронный ресурс] : учеб. пособие/ В. В. Золотарев, Е. А.

- Данилова. - Красноярск :Сиб. гос. аэрокосмич. ун-т, 2010. - 144 с.  
<http://znanium.com/catalog.php?bookinfo=463037>
5. **Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности** [Электронный ресурс] : учеб. пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. гос. аэрокосмич. ун-т, 2012. - 100 с. <http://znanium.com/catalog.php?bookinfo=463061>
  6. **Бабаш, Александр Владимирович.**  
Информационная безопасность : лабораторный практикум : учеб. пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. - М. : КНОРУС, 2012. - 131 с. + 1 опт. диск. - Библиогр.: с. 131. - ISBN 978-5-406-01170-6 : 250.00.
  7. **Мельников, Владимир Павлович.**  
Информационная безопасность и защита информации : учеб. пособие для вузов спец. 230201 "Информац. системы и технологии" / Мельников Владимир Павлович, С. А. Клейменов, А. М. Петраков ; под ред. Клейменова С.А. - 3-е изд., стер. - Москва : Академия, 2008. - 336 с. - (Высш. проф. образов. Информат. и выч. техн.). - УМО. - ЕН, ОПД, СД. - ISBN 978-5-7695-4884-0 : 165.66.
  8. **Партыка, Татьяна Леонидовна.**  
Информационная безопасность : Учеб. пособие для сред. проф. образования, спец. информатики и выч. техники / Партыка Татьяна Леонидовна, Попов Игорь Иванович. - 2-е изд., испр. и доп. - Москва : ФОРУМ - ИЕФРА-М, 2007. - 368 с.: ил. - (Профессиональное образование). - МО РФ . - ОПД, СД. - ISBN 5-91134-095-X; 5-16-002849-8 : 288.00.
  9. **Филин, Сергей Александрович.**  
Информационная безопасность : учеб. пособие / Филин Сергей Александрович. - Москва : Альфа-Пресс, 2006. - 412 с. - ОПД, СД. - ISBN 5-94280-163-0 : 200.00.
  10. **Малюк, А. А.**  
Информационная безопасность: концептуальные и методологические основы защиты информации : Учеб. пособие для студ. высш. учеб. заведений / А. А. Малюк. - М. : Горячая линия-Телеком , 2004. - 280 с. : ил. - Библиогр.: с. 276-278. - ISBN 5-93517-197-X : 99.00.  
В прил.: Гос. образовательный стандарт высшего профессионального образования. - Допущено МО РФ

## **8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

Информационно-образовательные ресурсы:

1. [www.atlas.krasnodar.ru](http://www.atlas.krasnodar.ru) -КФ НТЦ «Атлас»: защита информации.

Электронные библиотечные системы:

1. Университетская библиотека онлайн <http://biblioclub.ru>
2. «Лань» <http://e.lanbook.com/>
3. ЭБС «Znanium»
4. Справочно-информационная система (СИС) «Гарант».
5. Справочно-информационная система «Консультант».
6. Электронно-библиотечная система (ЭБС) «Инфра-М».

## **9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Лекционная аудитория, оснащенная проектором, компьютером.

Компьютерный класс 9 персональных компьютеров