

МИНОБРНАУКИ РОССИИ



Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«Российский государственный гуманитарный университет»  
(ФГБОУ ВО «РГГУ»)**

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ

Факультет информационных систем и безопасности

Кафедра информационной безопасности

## **СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАРУБЕЖНЫХ СТРАНАХ**

### **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

По направлению подготовки 10.03.01 «Информационная безопасность»  
профиль: Организация и технология защиты информации (по отрасли  
или в сфере профессиональной деятельности)  
Уровень квалификации выпускника (*бакалавр*)

Форма обучения (*очная*)

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2021

Системы защиты информации в зарубежных странах  
Рабочая программа дисциплины  
Составитель:  
д.т.н., профессор В.В. Арутюнов

Ответственный редактор  
к.и.н., доцент, заведующая кафедрой  
информационной безопасности Г.А. Шевцова

УТВЕРЖДЕНО  
Протокол заседания кафедры  
№ 10 от 20.05.2021

## ОГЛАВЛЕНИЕ

### **1. Пояснительная записка**

1.1 Цель и задачи дисциплины (*модуля*)

1.2. Перечень планируемых результатов обучения по дисциплине (*модулю*), соотнесенных с индикаторами достижения компетенций

1.3. Место дисциплины в структуре образовательной программы

### **2. Структура дисциплины (*модуля*)**

### **3. Содержание дисциплины (*модуля*)**

### **4. Образовательные технологии**

### **5. Оценка планируемых результатов обучения**

5.1. Система оценивания

5.2. Критерии выставления оценок

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (*модулю*)

### **6. Учебно-методическое и информационное обеспечение дисциплины**

6.1. Список источников и литературы

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

### **7. Материально-техническое обеспечение дисциплины (*модуля*)**

### **8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов**

### **9. Методические материалы**

9.1. Планы практических занятий

9.2. Методические рекомендации по организации самостоятельной работы

## **Приложения**

Приложение 1. Аннотация дисциплины

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

### 1. Пояснительная записка

#### 1.1. Цель и задачи дисциплины (модуля)

Цель дисциплины (модуля): формирование знаний у обучающихся о закономерностях становления и тенденциях развития систем защиты информации в ведущих зарубежных странах, особенностях их современной организации и функционирования, перспективах развития и возможностях совершенствования зарубежного опыта в России.

Задачи дисциплины:

- изучение процесса формирования и развития систем защиты информации в ведущих зарубежных странах;
- анализ состава органов защиты информации и особенностей классификации защищаемой информации;
- освоение современного опыта организации систем защиты информации в ведущих зарубежных странах.

#### 1.2. Формируемые компетенции, соотнесённые с планируемыми результатами обучения по дисциплине (модулю):

Компетенция (код и название)	Индикаторы компетенций (код и наименование)	Результаты обучения
ОПК-13  Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	ОПК-13.1  Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире	Знать: состав, структуру и основные направления деятельности органов защиты информации в ведущих зарубежных странах; Уметь: применять полученные знания в научно-исследовательской и практической работе; Владеть: навыками критически переосмысливать и применять накопленный зарубежный опыт в области информационной безопасности
	ОПК-13.2  Умеет формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории	Знать: основные этапы развития цивилизации; Уметь: классифицировать основные периоды развития средств и методов защиты информации безопасности; Владеть: навыками построения типовой структуры системы защиты информации

	<p>ОПК-13.3</p> <p>Владеет навыками по соотнесению общих исторических процессов и отдельных фактов, выявлению существенных черт исторических процессов, явлений и событий</p>	<p>Знать: основные направления государственной политики в области защиты информации в ведущих зарубежных странах;</p> <p>Уметь: использовать зарубежный опыт при разработке комплексной системы защиты информации;</p> <p>Владеть: основными комплексами знаний о тенденциях и перспективах развития систем защиты информации в ведущих зарубежных странах</p>
<p>ПК-10</p> <p>Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности</p>	<p>ПК-10.1</p> <p>Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации</p>	<p>Знать: основные нормативно-правовые документы в профессиональной деятельности;</p> <p>Уметь: пользоваться нормативно-правовыми документами в области информационной безопасности;</p> <p>Владеть: навыками работы с нормативно-правовыми документами в профессиональной деятельности;</p>
	<p>ПК-10.2</p> <p>Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации</p>	<p>Знать: базовые международные и российские регуляторы по информационной безопасности;</p> <p>Уметь: работать со стандартами и нормативными документами в своей профессиональной деятельности</p> <p>Владеть: навыками использования международных и национальных стандартов в области информационной безопасности;</p>
	<p>ПК-10.3</p> <p>Владеет навыком разработки аналитического обоснования</p>	<p>Знать: требования к составу и содержанию информации при решении практических</p>

	необходимости создания системы защиты информации в организации	задач в сфере создания системы защиты информации; Уметь: определять информационные потребности для решения конкретной задачи при аналитическом обосновании необходимости создания системы защиты информации; Владеть: навыками профессиональной оценки информации, необходимой для создания системы защиты информации.
--	--	--

### 1.1. Место дисциплины в структуре основной образовательной программы

Дисциплина (модуль) «Системы защиты информации в зарубежных странах» относится к вариативной части блока дисциплин учебного плана (дисциплина по выбору).

Для освоения дисциплины (модуля) необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Основы профессиональной деятельности», «Основы информационной безопасности».

В результате освоения дисциплины (модуля) формируются знания, умения и владения, необходимые для прохождения преддипломной практик: Сети и системы передачи информации, Комплексное обеспечение безопасности объекта информатизации-Организационное проектирование систем защиты информации.

## 2. Структура дисциплины (модуля) для очной формы обучения

Общая трудоемкость дисциплины составляет 2 з. е., 76 ч., в том числе контактная работа обучающихся с преподавателем 40 ч., самостоятельная работа обучающихся 36 ч.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации (по семестрам)
			контактная					Самостоятель- ная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1	Противоборство в системе международных отношений в современном обществе	2	2					4	

2	Системы защиты информации в США	2	4		4			8	опрос
3	Системы защиты информации в странах Евросоюза	2	6		6			8	опрос, контрольная работа 1
4	Системы защиты информации в Китайской Народной Республике и Японии	2	2		6			6	опрос
5	Системы защиты информации в ведущих мировых компаниях	2	2		8			4	опрос, контрольная работа 2
	<b>Итого</b>		<b>16</b>		<b>24</b>			<b>36</b>	

### 3. Содержание дисциплины (модуля)

№	Наименование раздела дисциплины	Содержание
1	<b>Тема 1. Противоборство в системе международных отношений в современном обществе</b>	<p>Предмет и содержание дисциплины, методы изучения, основная литература, контроль освоения дисциплины.</p> <p>Основные стадии развития средств и методов защиты информации. Типовая структура системы защиты информации. Современная картина политических отношений в мире.</p> <p>Основы информационно-психологического воздействия. Основные формы информационной войны. Базовые виды современного информационного оружия.</p>
2	<b>Тема 2. Системы защиты информации в США</b>	<p>Правовое регулирование информационной безопасности (ИБ) в США. Современная концепция информационной войны в США и базовые уровни её реализации. Основные объекты применения информационного оружия.</p> <p>Государственные органы обеспечения безопасности США. Структура и функции АНБ США. Особенности системы "Эшелон".</p>

		<p>Основные директоры ЦРУ США. Подразделения Министерства обороны США, занимающиеся вопросами стратегии и тактики в сфере ИБ.</p> <p>Особенности подготовки кадров в области информационной безопасности в США.</p>
3	<p><b>Тема 3. Системы защиты информации в странах Евросоюза</b></p>	<p>Состояние системы информационной безопасности в странах Евросоюза.</p> <p>Системы защиты информации в Великобритании. Структура спецслужб Великобритании. Основные директоры разведывательной службы SIS (MI-6). Структура Контрразведывательной службы MI-5. Правовая база деятельности спецслужб Великобритании.</p> <p>Особенности системы защиты информации в Федеративной Республике Германии. Общая функции деятельности Федеральной службы безопасности в сфере информационной техники (BSI). Государственные органы обеспечения безопасности Германии.</p> <p>Характеристика системы защиты информации во Франции. Структура спецслужб Франции. Структура Генеральной дирекции внешней безопасности – главной военной разведки Франции. Состав Управления военной разведки Франции.</p> <p>Основные задачи системы контроля и управления средствами ведения информационной войны в Швеции. Особенности конкурентной разведки частных компаний в Швеции. Подготовка персонала в области ИБ в Швеции. Особенности работы промышленных служб безопасности.</p>



4	<b>Тема 4. Системы защиты информации в Китайской Народной Республике и Японии</b>	<p>Основные элементы правовой системы Китая в области защиты информации. Особенности уголовной ответственности за совершение компьютерных преступлений в Китае. Базовые уровни системы ведения кибервойны.</p> <p>Базовые функции Министерства государственной безопасности Китая в области ИБ. "Великая стена" информационной безопасности Китая.</p> <p>Основные направления деятельности по совершенствованию системы информационной безопасности Японии. Правовая база Японии по борьбе с правонарушениями в сфере информационных ресурсов. Мероприятия японских частных компаний по защите информационных ресурсов.</p>
5	<b>Тема 5. Системы защиты информации в ведущих мировых компаниях</b>	<p>Развитие международного сотрудничества в области обеспечения информационной безопасности. Международные организации в области информационной безопасности. Правовое регулирование сети Интернет.</p> <p>Практика компании IBM в области защиты информации. Практический опыт компании Cisco Systems в разработке сетевой политики безопасности.</p> <p>Практика работы компании Microsoft в области информационной безопасности.</p>

#### 4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебной работы	Информационные и образовательные технологии
1.	Противоборство в системе международных	Лекция 1	Вводная лекция с использованием видеоматериалов

	отношений в современном обществе		
2.	Системы защиты информации в США	Лекция 2 Практическое занятие 1	Лекция с использованием видеоматериалов опрос
3.	Системы защиты информации в странах Евросоюза	Лекция 3 Практическое занятие 2 Контрольная работа 1	Лекция с использованием видеоматериалов опрос Подготовка к контрольной с использованием материалов лекций и литературы
4.	Системы защиты информации в Китайской Народной Республике и Японии	Лекция 4 Практическое занятие 3	Лекция с использованием видеоматериалов опрос
5.	Системы защиты информации в ведущих мировых компаниях	Лекция 4 Практическое занятие 4 Контрольная работа 2	Лекция с использованием видеоматериалов опрос Подготовка к контрольной с использованием материалов лекций и литературы

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

## 5. Оценка планируемых результатов обучения

### 5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		

- опрос	5 баллов	20 баллов
- контрольная работа 1 (темы 1-2)	20 баллов	20 баллов
- контрольная работа 2 (темы 3-4)	20 баллов	20 баллов
Промежуточная аттестация (традиционная форм)		40 баллов
<b>Итого за семестр зачёт</b>		<b>100 баллов</b>

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

## 5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	зачтено	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	зачтено	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		<p>профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D, E	зачтено	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F, FX	не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)

#### Примерная тематика опросных заданий

1. Понятие информационной безопасности и защиты информации - ПК-10.
2. В чем состоит сущность информационного воздействия? - ОПК-13.

3. Какова роль ФБР в решении задач обеспечения ИБ США? - ПК-10.
4. Базовые проблемы, решаемые специалистами стран Евросоюза в условиях возможности применения информационного оружия - ПК-10.
5. Основные трудности создания системы коллективного контроля и обеспечения ИБ европейских стран - ОПК-13.
6. Базовые задачи системы контроля и управления средствами ведения информационной войны в Швеции - ОПК-13.
7. Что представляет собой концепция ИБ Китая? - ПК-10.
8. Какие услуги предоставляет Интернет-союз информационной безопасности? - ОПК-13.

### **Примерная тематика контрольной работы 1**

1. Основные элементы типовой системы защиты информации - ПК-10.
2. Базовые объекты применения информационного оружия - ОПК-13.
3. Основные формы информационной войны - ОПК-13.
4. Особенности системы ЭШЕЛОН - ПК-10.
5. Базовые структурные подразделения ЦРУ и задачи, решаемые ими - ПК-10.
6. Структура спецслужбы МИ-6 Великобритании - ПК-10.
7. Структура контрразведывательной службы МИ-5 Великобритании - ПК-10.
8. Особенности системы защиты информации в Германии - ОПК-13.
9. Основные спецслужбы Франции - ОПК-13.
10. Особенности деятельности служб безопасности шведских промышленных предприятий - ПК-10.

### **Примерная тематика контрольной работы 2**

1. Базовые мероприятия, осуществляемые руководством Китая, направленные на повышение уровня ИБ страны - ОПК-13.
2. Нормативно-правовая база Китая в сфере ИБ и ответственность за компьютерные преступления в Китае - ПК-10.
3. Задачи «Великой стены» информационной безопасности Китая - ОПК-13.
4. Основные направления совершенствования национальной системы информационной безопасности Японии - ПК-10.
5. Современные тенденции международного сотрудничества в области ИБ - ПК-10.
6. Основные направления деятельности Ассоциации аудита и контроля информационных систем - ОПК-13.
7. Особенности подхода компании IBM к построению корпоративных политик

безопасности - ПК-10.

8. Основные этапы реагирования на события безопасности в компании CISCO - ОПК-13.

9. Сущность «матрицы безопасности» компании CISCO - ПК-10.

10. Основные принципы обеспечения информационной безопасности в компании Microsoft - ОПК-13.

### **Промежуточная аттестация (примерные контрольные вопросы по курсу)**

1. Основные этапы развития методов и средств ЗИ в процессе эволюции человечества - ОПК-13.
2. Базовые элементы типовой системы защиты информации - ОПК-13.
3. Основные формы информационной войны - ОПК-13.
4. Базовые виды информационного оружия - ОПК-13.
5. Основные причины, вызывающие возникновение информационных войн - ОПК-13.
6. Цели реализации концепции информационной войны на государственном уровне в США - ПК-10.
7. Особенности радиоэлектронной борьбы - ОПК-13.
8. Основные объекты применения информационного оружия - ОПК-13.
9. Особенности системы ЭШЕЛОН - ПК-10.
10. Структура государственных органов обеспечения национальной ИБ США - ПК-10.
11. Особенности подготовки кадров в области ИБ в США - ОПК-13.
12. Характеристика государственной системы безопасности Великобритании - ПК-10.
13. Структура спецслужб Великобритании - ПК-10.
14. Основные государственные органы обеспечения безопасности Германии - ПК-10.
15. Характеристика системы защиты информации Франции - ПК-10.
16. Особенности системы защиты информации Швеции - ПК-10.
17. Основные мероприятия по обеспечению ИБ Китая, осуществляемые в процессе интеграции в глобальную сеть Интернет - ОПК-13.
18. Основные направления совершенствованию национальной системы ИБ Японии - ПК-10.
19. Схема процесса разработки политики безопасности в компании IBM - ОПК-13.
20. Матрица безопасности компании Cisco Systems - ПК-10.
21. Базовые компоненты стратегии безопасности в компании Microsoft - ОПК-13.

## **6. Учебно-методическое и информационное обеспечение дисциплины**

### **6.1. Список источников и литературы**

#### **Литература**

основная:

1. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах. - М.: ФЛИНТА, 2016. - 450 с. URL: <http://znanium.com/bookread2.php?book=453884>

2. Бабаш А.В., Ларин Д.А. История защиты информации в зарубежных странах: учебное пособие. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 283 с. URL: <http://znanium.com/catalog/product/492549>

дополнительная:

1. Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. URL: <http://znanium.com/bookread2.php?book=1013794>

2. Купрейчик Р.В. Совершенствование правовых и организационных основ защиты информации в Российской Федерации на основе опыта зарубежных государств // Научный аспект. 2020. Т. 4. № 2. - С. 489-497. — Режим доступа: URL: <https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv>

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Информационный портал в области защиты информации. URL: <http://www.securitylab.ru>

2. Обзор зарубежного законодательства в области информационной безопасности. URL: <https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4>

3. Центр исследования компьютерной преступности. Г. Маклаков. Научно-методологические аспекты подготовки специалистов в области информационной безопасности. URL: <http://www.crime-research.ru/>

### Перечень БД и ИСС

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru

4	Компьютерные справочные правовые системы Консультант Плюс, Гарант
---	---

### 7. Материально-техническое обеспечение дисциплины/модуля

Материально-техническая база включает учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Современный компьютерный класс оснащен Microsoft Office 2010, включающий наряду с компьютерами, подключёнными к сети Интернет, экран и проектор.

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

#### Состав программного обеспечения (ПО)

№п /п	Наименование ПО	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
10	ОС «Альт Образование» 8	ООО «Базальт СПО	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное
14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное
17	Zoom	Zoom	лицензионное

### 8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:



- для слепых и слабовидящих:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
  - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
  - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
  - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
  - письменные задания оформляются увеличенным шрифтом;
  - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих:
  - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
  - письменные задания выполняются на компьютере в письменной форме;
  - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата:
  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
  - письменные задания выполняются на компьютере со специализированным программным обеспечением;
  - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:
  - в печатной форме увеличенным шрифтом;
  - в форме электронного документа;
  - в форме аудиофайла.
- для глухих и слабослышащих:
  - в печатной форме;
  - в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - в печатной форме;
  - в форме электронного документа;
  - в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;
  - принтером Брайля EmBraille ViewPlus;
- для глухих и слабослышащих:
  - автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:
  - передвижными, регулируемые эргономическими партами СИ-1;
  - компьютерной техникой со специальным программным обеспечением.

## **9. Методические материалы**

### **9.1. Планы практических занятий**

Тема 1 (4 ч.). Государственные органы обеспечения безопасности США

Вопросы для обсуждения:

1. Типовая структура системы защиты информации - ПК-10.

2. Основные формы реализации концепции ИБ США на государственном уровне - ОПК-13.

3. Базовые нормативно-правовые акты, регулирующие правовое обеспечение ИБ в США - ОПК-13.

4. Структура государственных органов обеспечения национальной ИБ США - ПК-10.

5. Структура и функции АНБ США - ПК-10.

6. Особенности системы ЭШЕЛОН - ОПК-13.

7. Основные структурные подразделения ЦРУ и задачи, решаемые ими - ПК-10.

8. Особенности подготовки кадров в области ИБ в США - ОПК-13.

#### Список литературы

1. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах. - М.: ФЛИНТА, 2016. - 450 с. URL: <http://znanium.com/bookread2.php?book=453884>

2. Бабаш А.В., Ларин Д.А. История защиты информации в зарубежных странах: учебное пособие. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 283 с. URL: <http://znanium.com/catalog/product/492549>

3. Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. URL: <http://znanium.com/bookread2.php?book=1013794>

4. Купрейчик Р.В. Совершенствование правовых и организационных основ защиты информации в Российской Федерации на основе опыта зарубежных государств // Научный аспект. 2020. Т. 4. № 2. - С. 489-497. — Режим доступа: URL: <https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv>

5. Информационный портал в области защиты информации. URL: <http://www.securitylab.ru>

6. Обзор зарубежного законодательства в области информационной безопасности. URL: <https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4>

7. Центр исследования компьютерной преступности. Г. Маклаков. Научно-методологические аспекты подготовки специалистов в области информационной безопасности. URL: <http://www.crime-research.ru/>.

Тема 2 (6 ч.). Состояние системы информационной безопасности в странах Евросоюза

Вопросы для обсуждения:

1. Базовые проблемы, решаемые специалистами стран Евросоюза в условиях возможности применения информационного оружия - ОПК-13.

2. Основные трудности создания системы коллективного контроля и обеспечения ИБ европейских стран - ОПК-13.

3. Базовые цели создания системы коллективного контроля и обеспечения ИБ европейских стран- ОПК-13.

4. Характеристика государственной системы безопасности Великобритании - ОПК-13.

5. Задачи спецслужбы МИ-6 Великобритании - ПК-10.

6. Особенности системы защиты информации Германии - ПК-10.

7. Характеристика системы защиты информации Франции - ПК-10.

8. Особенности системы защиты информации Швеции - ПК-10.

#### Список литературы

1. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах. - М.: ФЛИНТА, 2016. - 450 с. URL: <http://znanium.com/bookread2.php?book=453884>

2. Бабаш А.В., Ларин Д.А. История защиты информации в зарубежных странах: учебное пособие. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 283 с. URL: <http://znanium.com/catalog/product/492549>

3. Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. URL: <http://znanium.com/bookread2.php?book=1013794>

4. Купрейчик Р.В. Совершенствование правовых и организационных основ защиты информации в российской федерации на основе опыта зарубежных государств // Научный аспект. 2020. Т. 4. № 2. - С. 489-497. — Режим доступа: URL: <https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv>

5. Информационный портал в области защиты информации. URL: <http://www.securitylab.ru>

6. Обзор зарубежного законодательства в области информационной безопасности. URL: <https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4>

7. Центр исследования компьютерной преступности. Г. Маклаков. Научно-методологические аспекты подготовки специалистов в области информационной безопасности. URL: <http://www.crime-research.ru/>.

Тема 3 (4 ч.). Особенности системы защиты информации в Китае

Вопросы для обсуждения:

1. Концепция ИБ Китая - ОПК-13.

2. Основные элементы правовой системы Китая в области защиты информации - ПК-10.

3. Особенности уголовной ответственности за совершение компьютерных преступлений в Китае - ОПК-13.

4. Базовые функции Министерства государственной безопасности Китая в области информационной безопасности- ПК-10.
5. "Великая стена" информационной безопасности Китая - ОПК-13.
6. Китайская система ведения кибервойн - ПК-10.
7. Структура разведки НОАК - ПК-10.
8. Основные мероприятия, осуществляемые руководством Китая, направленные на повышение ИБ страны - ОПК-13.

#### Список литературы

1. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах. - М.: ФЛИНТА, 2016. - 450 с. URL: <http://znanium.com/bookread2.php?book=453884>
2. Бабаш А.В., Ларин Д.А. История защиты информации в зарубежных странах: учебное пособие. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 283 с. URL: <http://znanium.com/catalog/product/492549>
3. Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. URL: <http://znanium.com/bookread2.php?book=1013794>
4. Купрейчик Р.В. Совершенствование правовых и организационных основ защиты информации в Российской Федерации на основе опыта зарубежных государств // Научный аспект. 2020. Т. 4. № 2. - С. 489-497. — Режим доступа: URL: <https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv>
5. Информационный портал в области защиты информации. URL: <http://www.securitylab.ru>
6. Обзор зарубежного законодательства в области информационной безопасности. URL: <https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4>
7. Центр исследования компьютерной преступности. Г. Маклаков. Научно-методологические аспекты подготовки специалистов в области информационной безопасности. URL: <http://www.crime-research.ru/>.

Тема 4 (4 ч.). Особенности системы защиты информации в ведущих мировых компаниях  
Вопросы для обсуждения:

1. Основные компоненты процесса разработки политики безопасности компании IBM - ОПК-13.
2. Базовые этапы разработки политики безопасности компании IBM - ПК-10.
3. Основные типы пользователей в компании Cisco, ответственные за обеспечение информационной безопасности - ПК-10.
4. Базовые этапы управления рисками, реализуемые в компании CISCO - ПК-10.

5. Классификация принципов ИБ в компании Microsoft - ОПК-13.
6. Основные компоненты стратегии ИБ в компании Microsoft - ОПК-13.

#### Список литературы

1. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах. - М.: ФЛИНТА, 2016. - 450 с. URL: <http://znanium.com/bookread2.php?book=453884>
2. Бабаш А.В., Ларин Д.А. История защиты информации в зарубежных странах: учебное пособие. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 283 с. URL: <http://znanium.com/catalog/product/492549>
3. Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. URL: <http://znanium.com/bookread2.php?book=1013794>
4. Купрейчик Р.В. Совершенствование правовых и организационных основ защиты информации в Российской Федерации на основе опыта зарубежных государств // Научный аспект. 2020. Т. 4. № 2. - С. 489-497. — Режим доступа: URL: <https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv>
5. Информационный портал в области защиты информации. URL: <http://www.securitylab.ru>
6. Обзор зарубежного законодательства в области информационной безопасности. URL: <https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4>
7. Центр исследования компьютерной преступности. Г. Маклаков. Научно-методологические аспекты подготовки специалистов в области информационной безопасности. URL: <http://www.crime-research.ru/>

#### 9.2. Методические рекомендации по организации самостоятельной работы

Вид работы	Содержание (перечень вопросов)	Трудоем- кость самостоя- тельной работы (в часах)	Рекомендации
Подготовка к практическому занятию Тема 1. Государственные органы обеспечения безопасности США	Типовая структура системы защиты информации  Основные формы реализации концепции ИБ США на государственном уровне  Базовые нормативно-	8	Проанализировать материал из законодательных, нормативных документов, учебников:  Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты

	<p>правовые акты, регулирующие правовое обеспечение ИБ в США</p> <p>Структура государственных органов обеспечения национальной ИБ США</p> <p>Структура и функции АНБ США</p> <p>Особенности системы ЭШЕЛОН</p> <p>Основные структурные подразделения ЦРУ и задачи, решаемые ими</p> <p>Особенности подготовки кадров в области ИБ в США</p>	<p>информации в ведущих зарубежных странах. - М.: ФЛИНТА, 2016. - 450 с. URL: <a href="http://znanium.com/bookread2.php?book=453884">http://znanium.com/bookread2.php?book=453884</a></p> <p>Бабаш А.В., Ларин Д.А. История защиты информации в зарубежных странах: учебное пособие. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 283 с. URL: <a href="http://znanium.com/catalog/product/492549">http://znanium.com/catalog/product/492549</a></p> <p>Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. URL: <a href="http://znanium.com/bookread2.php?book=1013794">http://znanium.com/bookread2.php?book=1013794</a></p> <p>Купрейчик Р.В. Совершенствование правовых и организационных основ защиты информации в Российской Федерации на основе опыта зарубежных государств // Научный аспект. 2020. Т. 4. № 2. - С. 489-497. — Режим доступа: URL: <a href="https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv">https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv</a></p> <p>Информационный портал в области защиты информации. URL: <a href="http://www.securitylab.ru">http://www.securitylab.ru</a></p> <p>Обзор зарубежного законодательства в области</p>
--	---	---

			<p>информационной безопасности. URL: <a href="https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4">https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4</a></p> <p>Центр исследования компьютерной преступности. Г. Маклаков. Научно-методологические аспекты подготовки специалистов в области информационной безопасности. URL: <a href="http://www.crime-research.ru/">http://www.crime-research.ru/</a></p>
<p>Подготовка к практическому занятию</p> <p>Тема 2. «Особенности семантического Web как разновидности семантических технологий»</p>	<p>Базовые проблемы, решаемые специалистами стран Евросоюза в условиях возможности применения информационного оружия</p> <p>Основные трудности создания системы коллективного контроля и обеспечения ИБ европейских стран</p> <p>Базовые цели создания системы коллективного контроля и обеспечения ИБ европейских стран</p> <p>Характеристика государственной системы безопасности Великобритании</p> <p>Задачи спецслужбы MI-6 Великобритании</p> <p>Особенности системы защиты информации Германии</p> <p>Характеристика системы защиты информации Франции</p> <p>Особенности системы</p>	8	<p>Проанализировать материал из законодательных, нормативных документов, учебников:</p> <p>Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах. - М.: ФЛИНТА, 2016. - 450 с. URL: <a href="http://znanium.com/bookread2.php?book=453884">http://znanium.com/bookread2.php?book=453884</a></p> <p>Бабаш А.В., Ларин Д.А. История защиты информации в зарубежных странах: учебное пособие. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 283 с. URL: <a href="http://znanium.com/catalog/product/492549">http://znanium.com/catalog/product/492549</a></p> <p>Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. URL: <a href="http://znanium.com/bookread2.php?book=1013794">http://znanium.com/bookread2.php?book=1013794</a></p>



	защиты информации Швеции		<p>Купрейчик Р.В. Совершенствование правовых и организационных основ защиты информации в Российской Федерации на основе опыта зарубежных государств // Научный аспект. 2020. Т. 4. № 2. - С. 489-497. — Режим доступа: URL: <a href="https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv">https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv</a></p> <p>Информационный портал в области защиты информации. URL: <a href="http://www.securitylab.ru">http://www.securitylab.ru</a></p> <p>Обзор зарубежного законодательства в области информационной безопасности. URL: <a href="https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4">https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4</a></p> <p>Центр исследования компьютерной преступности. Г. Маклаков. Научно-методологические аспекты подготовки специалистов в области информационной безопасности. URL: <a href="http://www.crime-research.ru/">http://www.crime-research.ru/</a></p>
Подготовка к практическому занятию  Тема 3. Особенности системы защиты информации в	<p>Концепция ИБ Китая - ОПК-13.</p> <p>Основные элементы правовой системы Китая в области защиты информации</p>	6	<p>Проанализировать материал из законодательных, нормативных документов, учебников:</p> <p>Аверченков В.И., Рытов М.Ю., Кондрашин Г.В.,</p>

Китае	<p>Особенности уголовной ответственности за совершение компьютерных преступлений в Китае</p> <p>Базовые функции Министерства государственной безопасности Китая в области информационной безопасности</p> <p>"Великая стена" информационной безопасности Китая</p> <p>Китайская система ведения кибервойн</p> <p>Структура разведки НОАК</p> <p>Основные мероприятия, осуществляемые руководством Китая, направленные на повышение ИБ страны</p>	<p>Рудановский М.В. Системы защиты информации в ведущих зарубежных странах. - М.: ФЛИНТА, 2016. - 450 с. URL: <a href="http://znanium.com/bookread2.php?book=453884">http://znanium.com/bookread2.php?book=453884</a></p> <p>Бабаш А.В., Ларин Д.А. История защиты информации в зарубежных странах: учебное пособие. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 283 с. URL: <a href="http://znanium.com/catalog/product/492549">http://znanium.com/catalog/product/492549</a></p> <p>Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. URL: <a href="http://znanium.com/bookread2.php?book=1013794">http://znanium.com/bookread2.php?book=1013794</a></p> <p>Купрейчик Р.В. Совершенствование правовых и организационных основ защиты информации в Российской Федерации на основе опыта зарубежных государств // Научный аспект. 2020. Т. 4. № 2. - С. 489-497. — Режим доступа: URL: <a href="https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv">https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv</a></p> <p>Информационный портал в области защиты информации. URL:</p>
-------	--	---

			<a href="http://www.securitylab.ru">http://www.securitylab.ru</a>  Обзор зарубежного законодательства в области информационной безопасности. URL: <a href="https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4">https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4</a>
Подготовка к практическому занятию  Тема 4. Особенности системы защиты информации в ведущих мировых компаниях	Основные компоненты процесса разработки политики безопасности компании IBM  Базовые этапы разработки политики безопасности компании IBM  Основные типы пользователей в компании Cisco, ответственные за обеспечение информационной безопасности  Базовые этапы управления рисками, реализуемые в компании CISCO  Классификация принципов ИБ в компании Microsoft  Основные компоненты стратегии ИБ в компании Microsoft	4	Проанализировать материал из законодательных, нормативных документов, учебников:  Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В. Системы защиты информации в ведущих зарубежных странах. - М.: ФЛИНТА, 2016. - 450 с. URL: <a href="http://znanium.com/bookread2.php?book=453884">http://znanium.com/bookread2.php?book=453884</a>  Бабаш А.В., Ларин Д.А. История защиты информации в зарубежных странах: учебное пособие. М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 283 с. URL: <a href="http://znanium.com/catalog/product/492549">http://znanium.com/catalog/product/492549</a> Шариков П.А. Проблемы информационной безопасности в полицентричном мире. - М.: Весь Мир, 2015. - 320 с. URL: <a href="http://znanium.com/bookread2.php?book=1013794">http://znanium.com/bookread2.php?book=1013794</a>  Купрейчик Р.В. Совершенствование правовых и организационных основ защиты информации в Российской Федерации на основе опыта зарубежных

		<p>государств // Научный аспект. 2020. Т. 4. № 2. - С. 489-497. — Режим доступа: URL: <a href="https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv">https://na-journal.ru/2-2020-pravo-obshchestvo/2213-sovershenstvovanie-pravovyh-i-organizacionnyh-osnov-zashchity-informacii-v-rossijskoj-federacii-na-osnove-opyta-zarubezhnyh-gosudarstv</a></p> <p>Информационный портал в области защиты информации. URL: <a href="http://www.securitylab.ru">http://www.securitylab.ru</a></p> <p>Обзор зарубежного законодательства в области информационной безопасности. URL: <a href="https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4">https://www.intuit.ru/studies/courses/10/10/lecture/302?page=4</a></p> <p>Центр исследования компьютерной преступности. Г. Маклаков. Научно-методологические аспекты подготовки специалистов в области информационной безопасности. URL: <a href="http://www.crime-research.ru/">http://www.crime-research.ru/</a></p>
--	--	--

## АННОТАЦИЯ

Дисциплина (модуль) «Системы защиты информации в зарубежных странах» реализуется на факультете информационных систем и безопасности Института информационных наук и технологий безопасности кафедрой информационной безопасности.

Цель дисциплины (модуля): формирование знаний у обучающихся о закономерностях становления и тенденциях развития систем защиты информации в ведущих зарубежных странах, особенностях их современной организации и функционирования, перспективах развития и возможностях совершенствования зарубежного опыта в России.

Задачи дисциплины:

- изучение процесса формирования и развития систем защиты информации в ведущих зарубежных странах;
- анализ состава органов защиты информации и особенностей классификации защищаемой информации;
- освоение современного опыта организации систем защиты информации в ведущих зарубежных странах.

Дисциплина (модуль) направлена на формирование следующих компетенций:

- ОПК-13 - способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма;

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире
- Умеет формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории
- Владеет навыками по соотнесению общих исторических процессов и отдельных фактов, выявлению существенных черт исторических процессов, явлений и событий

- ПК-10 - способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

В результате освоения дисциплины (модуля) обучающийся должен:

- Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации
- Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации
- Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации

По дисциплине (модулю) предусмотрена промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины (модуля) составляет 2 зачетные единицы.