

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

**СОВРЕМЕННЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ  
В ВЕДУЩИХ ЗАРУБЕЖНЫХ СТРАНАХ**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

01.04.04 Прикладная математика

---

*Код и наименование направления подготовки/специальности*

**Математические методы и модели обработки  
и защиты информации в социотехнических системах**

---

*Наименование направленности (профиля)/ специализации*

Уровень высшего образования: *магистратура*

Форма обучения: *очная, заочная*

РПД адаптирована для лиц  
с ограниченными возможностями  
здоровья и инвалидов

Москва 2024

**СОВРЕМЕННЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ВЕДУЩИХ  
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  
Информационной безопасности  
№ 11 от 18.03.2024

## ОГЛАВЛЕНИЕ

1. Пояснительная записка .....	4
1.1. Цель и задачи дисциплины .....	4
1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций .....	4
1.3. Место дисциплины в структуре образовательной программы .....	4
2. Структура дисциплины .....	4
3. Содержание дисциплины .....	5
4. Образовательные технологии .....	6
5. Оценка планируемых результатов обучения .....	7
5.1 Система оценивания .....	7
5.2 Критерии выставления оценки по дисциплине .....	8
5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине .....	9
6. Учебно-методическое и информационное обеспечение дисциплины .....	10
6.1 Список источников и литературы .....	10
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет». ....	10
6.3 Профессиональные базы данных и информационно-справочные системы .....	11
7. Материально-техническое обеспечение дисциплины .....	11
8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов .....	11
9. Методические материалы .....	12
9.1 Планы практических занятий .....	12
Приложение 1. Аннотация рабочей программы дисциплины .....	14

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

Цель дисциплины: формирование у обучающихся знаний в области построения систем защиты информации в ведущих зарубежных странах, изучение и освоение опыта разработки систем защиты информации в этих странах, включая США, основные страны Евросоюза, Китай и Японию.

Задачи дисциплины: анализ особенностей построения систем защиты информации (СЗИ) в ведущих зарубежных странах; выявление состояния проблемы информационной безопасности в этих странах; освоение основных методологий создания СЗИ.

### 1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
ПК-1. Способен проводить систематизацию, алгоритмизацию конкретных информационных потоков по месту научных исследований, производственной деятельности	ПК-1.2. Выделяет динамические, статистические структуры для представления их математическими моделями	Знать: основные стадии развития средств и методов защиты информации; типовую структуру системы защиты информации; компоненты информационного противоборства и виды современного информационного оружия; концепции информационной безопасности в ведущих зарубежных странах; Уметь: анализировать структуру систем защиты информации в ведущих зарубежных странах, правовое регулирование в этих странах вопросов в сфере информационной безопасности, особенности подготовки кадров в области защиты информации; применять полученные знания в научно-исследовательской и практической работе; Владеть: опытом разработки и реализации концепции информационной безопасности в ведущих зарубежных странах, формирования в них систем защиты информации.

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Современные системы защиты информации в ведущих зарубежных странах» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин: "Криптографические приложения в социотехнических системах".

## 2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часа(ов).

### Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	8
2	Практические занятия	22
Всего:		30

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 78 академических часа(ов).

### Структура дисциплины для заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	4
2	Практические занятия	8
Всего:		12

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 96 академических часа(ов).

### 3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	Информационное противоборство в системе международных отношений в современном обществе	Предмет и содержание дисциплины, методы изучения, основная литература, контроль освоения дисциплины. Основные стадии развития средств и методов защиты информации. Типовая структура системы защиты информации. Современная картина политических отношений в мире. Основы информационно-психологического воздействия. Основные формы информационной войны. Базовые виды современного информационного оружия.
2	Системы защиты информации в США	Правовое регулирование информационной безопасности (ИБ) в США. Современная концепция информационной войны в США и базовые уровни её реализации. Основные объекты применения информационного оружия. Государственные органы обеспечения безопасности США. Структура и функции АНБ США. Особенности системы "Эшелон". Основные директораты ЦРУ США. Подразделения Министерства обороны США, занимающиеся вопросами стратегии и тактики в сфере ИБ. Особенности подготовки кадров в области информационной безопасности в США.
3	Системы защиты информации в странах	Состояние системы информационной безопасности в странах Евросоюза.

	Евросоюза	<p>Системы защиты информации в Великобритании. Структура спецслужб Великобритании. Основные директораты 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.</p> <p>Основные задачи системы контроля и управления средствами ведения информационной войны в Швеции.</p> <p>Особенности конкурентной разведки частных компаний в Швеции. Подготовка персонала в области ИБ в Швеции. Особенности работы промышленных служб безопасности.</p>
4	Системы защиты информации в Китайской Народной Республике и Японии	<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>

#### 4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1.	Информационное противоборство в системе международных отношений в современном обществе	<p>Лекция 1</p> <p>Практическое занятие 1</p> <p>Самостоятельная работа</p>	<p>Вводная лекция с использованием видеопроектора</p> <p>дискуссия</p> <p>Подготовка к занятию с использованием электронного курса лекций</p>
2.	Системы защиты информации в США	<p>Лекция 2</p> <p>Практическое занятие 2</p> <p>Самостоятельная работа</p>	<p>Лекция с использованием видеопроектора</p> <p>дискуссия</p> <p>Подготовка к занятию с использованием электронного курса лекций</p>

3.	Системы защиты информации в странах Евросоюза	Лекция 3	Лекция с использованием видеопроектора
		Практическое занятие 3	дискуссия
		Самостоятельная работа	Подготовка к занятию с использованием электронного курса лекций
4.	Системы защиты информации в Китайской Народной Республике и Японии	Лекция 4	Лекция с использованием видеопроектора
		Практическое занятие 4	дискуссия
		Самостоятельная работа	Подготовка к занятиям с использованием электронного курса лекций

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 - контрольная работа (темы 3-4)	10 баллов 20 баллов	40 баллов 20 баллов
Промежуточная аттестация - экзамен (экзамен по билетам)		40 баллов
<b>Итого за семестр</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	отлично/ 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.</p> <p>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	хорошо/ 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 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	удовлетво- рительно/ 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	неудовлет- ворительно/ 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**

#### **Текущий контроль**

##### ***Примерные вопросы к дискуссии***

1. Понятие информационной войны и информационного оружия.
2. Охарактеризуйте эпоху Интернет-2 в России.
3. Основные цели информационной войны.
4. Роль ФБР в решении задач обеспечения ИБ США.
5. Основные формы реализации концепции информационной войны на государственном уровне в США.
6. Базовые проблемы, решаемые специалистами стран Евросоюза в условиях возможности применения информационного оружия.
7. Основные трудности создания системы коллективного контроля и обеспечения ИБ европейских стран.
8. Основные задачи системы контроля и управления средствами ведения информационной войны в Швеции.
9. Концепция ИБ Китая.

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

1. Структура спецслужбы MI-6 Великобритании.
2. Структура Контрразведывательной службы MI-5 Великобритании.
3. Особенности системы защиты информации Германии.
4. Особенности системы защиты информации Германии.
5. Структура федерального бюро защиты конституции VfV Германии.
6. Основные спецслужбы Франции.
7. Особенности деятельности служб безопасности шведских промышленных предприятий.
8. Основные элементы правовой системы ИБ Китая в области защиты информации.
9. Базовые виды компьютерных преступлений в Китае, за совершение которых предусмотрена уголовная ответственность.
10. Основные направления совершенствованию национальной системы ИБ Японии.

#### **Промежуточная аттестация**

##### ***Примерная тематика вопросов для экзамена***

1. Основные этапы развития методов и средств ЗИ в процессе эволюции человечества.
2. Базовые элементы типовой системы защиты информации.
3. Основные виды информационного оружия.
4. Цели реализации концепции информационной войны на государственном уровне в США.
5. Особенности системы ЭШЕЛОН.

6. Особенности радиоэлектронной борьбы.
7. Основные объекты применения информационного оружия.
8. Структура государственных органов обеспечения национальной ИБ США.
9. Особенности подготовки кадров в области ИБ в США.
10. Характеристика государственной системы безопасности Великобритании.
11. Структура спецслужб Великобритании.
12. Основные государственные органы обеспечения безопасности Германии.
13. Характеристика системы защиты информации Франции.
14. Методы работы иностранных государственных спецслужб и частных разведывательно-информационных органов в Швеции.
15. Структура министерства государственной безопасности Китая.
16. Структура системы спецслужб Японии.

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

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

#### Литература

##### *Основная*

1. Шариков, П. А. Проблемы информационной безопасности в полицентричном мире / П.А. Шариков. - М.: Весь Мир, 2015. - 320 с. ISBN 978-5-7777-0601-0. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1013794>
2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/537247>.
3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542340>.

##### *Дополнительная*

1. Бабаш А. В. История защиты информации в зарубежных странах: Учебное пособие / Бабаш А. В., Ларин Д. А. - Москва : ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 283 с. - ISBN 978-5-369-01214-7. - Текст: электронный. - URL: <https://znanium.com/catalog/product/492549>

### **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. Режим доступа: 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. Режим доступа: URL: <http://www.crime-research.ru/>

Национальная электронная библиотека (НЭБ) [www.rusneb.ru](http://www.rusneb.ru)  
 ELibrary.ru Научная электронная библиотека [www.elibrary.ru](http://www.elibrary.ru)  
 Электронная библиотека Grebennikon.ru [www.grebennikon.ru](http://www.grebennikon.ru)

Cambridge University Press  
 ProQuest Dissertation & Theses Global  
 SAGE Journals  
 Taylor and Francis  
 JSTOR

### 6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

## 7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимы:

*Для лекций:*

- учебная аудитория,
- доска,
- проектор (стационарный или переносной),
- компьютер или ноутбук,
- программное обеспечение (ПО).

*Для практических занятий:*

- лаборатория или компьютерный класс,
- доска,
- проектор (стационарный или переносной),
- компьютер или ноутбук для преподавателя,
- компьютеры для обучающихся,
- выход в Интернет,
- программное обеспечение (ПО).

Состав программного обеспечения:

1. Windows
2. Microsoft Office
3. Kaspersky Endpoint Security

## 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 их 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 SE; 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. Типовая структура системы защиты информации**

*Задания:*

1. Основные элементы системы защиты информации (СЗИ)
2. Содержание элемента СЗИ "Правовая защита информации".
3. Методы, реализуемые в организационной защите информации при создании СЗИ.

4. Особенности страховой защиты информации.
5. Средства и методы, реализуемые при использовании криптографической защиты информации.
6. Сущность психологической защиты информации.

## **Тема 2. Государственные органы обеспечения безопасности США**

*Задания:*

1. Типовая структура системы защиты информации.
2. Основные формы реализации концепции ИБ США на государственном уровне.
3. Базовые нормативно-правовые акты, регулирующие правовое обеспечение ИБ в США.
4. Структура государственных органов обеспечения национальной ИБ США.
5. Структура и функции Агенства национальной безопасности США.
6. Особенности системы ЭШЕЛОН.
7. Основные структурные подразделения ЦРУ и задачи, решаемые ими.
8. Особенности подготовки кадров в области ИБ в США.

## **Тема 3. Состояние системы информационной безопасности в странах Евросоюза**

*Задания:*

1. Базовые проблемы, решаемые специалистами стран Евросоюза в условиях возможности применения информационного оружия.
2. Основные трудности создания системы коллективного контроля и обеспечения ИБ европейских стран.
3. Базовые цели идеи создания системы коллективного контроля и обеспечения ИБ европейских стран.
4. Характеристика государственной системы безопасности Великобритании.
5. Задачи спецслужбы MI-6 Великобритании.
6. Особенности системы защиты информации Германии.
7. Характеристика системы защиты информации Франции.
8. Особенности системы защиты информации Швеции.

## **Тема 4. Особенности системы защиты информации в Китае**

*Задания:*

1. Концепция ИБ Китая.
2. Основные элементы правовой системы Китая в области защиты информации.
3. Особенности уголовной ответственности за совершение компьютерных преступлений в Китае.
4. Базовые функции Министерства государственной безопасности Китая в области информационной безопасности.
5. "Великая стена" информационной безопасности Китая.
6. Китайская система ведения кибервойны.
7. Структура разведки НОАК.
8. Основные мероприятия, осуществляемые руководством Китая, направленные на повышение ИБ страны.

## АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Современные системы защиты информации в ведущих зарубежных странах» реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.

Цель дисциплины: формирование у обучающихся знаний в области построения систем защиты информации в ведущих зарубежных странах, изучение и освоение опыта разработки систем защиты информации в этих странах, включая США, основные страны Евросоюза, Китай и Японию.

Задачи дисциплины: анализ особенностей построения систем защиты информации (СЗИ) в ведущих зарубежных странах; выявление состояния проблемы информационной безопасности в этих странах; освоение основных методологий создания СЗИ.

Дисциплина направлена на формирование следующих компетенций:

ПК-1. Способен проводить систематизацию, алгоритмизацию конкретных информационных потоков по месту научных исследований, производственной деятельности

В результате освоения дисциплины обучающийся должен:

*Знать:* основные стадии развития средств и методов защиты информации; типовую структуру системы защиты информации; компоненты информационного противоборства и виды современного информационного оружия; концепции информационной безопасности в ведущих зарубежных странах;

*Уметь:* анализировать структуру систем защиты информации в ведущих зарубежных странах, правовое регулирование в этих странах вопросов в сфере информационной безопасности, особенности подготовки кадров в области защиты информации; применять полученные знания в научно-исследовательской и практической работе;

*Владеть:* опытом разработки и реализации концепции информационной безопасности в ведущих зарубежных странах, формирования в них систем защиты информации.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы.