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 комплексной защиты информации

# ТЕХНОЛОГИЯ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность
*Код и наименование направления подготовки*

Организация и технологии защиты государственной тайны
*Наименование направленности (профиля)*

Уровень высшего образования: *магистратура*

Форма обучения: *очная, очно-заочная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2024

Технология построения защищенных систем обработки информации
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
№ 11 от 18.03.2024

**ОГЛАВЛЕНИЕ**

## 1. Пояснительная записка

### 1.1. Цель и задачи дисциплины

Цель дисциплины: формирование у обучающихся знаний и навыков в сфере обеспечения защиты информации на объекте информатизации, способности оценивать эффективность защиты, а также принимать эффективные управленческие решения при выборе проектов построения защищённых систем обработки информации.

Задачи дисциплины: освоение основных понятий и терминологии в области построения защищённых систем обработки информации, анализ угроз информационной безопасности, приобретение навыков в системном подходе к построению защищенных систем обработки информации.

### 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 анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений | ПК-1.1 Знает разработку концепции средств и систем информатизации в защищенном исполнении, разработку технического задания на средство и/или систему информатизации в защищенном исполнении | Знать: нормативно-правовые акты, национальные и зарубежные стандарты в области информационной безопасности;<br>Уметь: работать с нормативно-правовыми актами и стандартами в области защиты информации;<br>Владеть: навыками использования международных и национальных стандартов в области информационной безопасности; |
| | ПК-1.2 Умеет разрабатывать конструкторскую и технологическую документацию на средство и/или систему информатизации в защищенном исполнении | Знать: условия функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации;<br>Уметь: анализировать данные о функциях и условиях функционирования объектов и систем обработки информации ограниченного доступа;<br>Владеть: опытом применения полученных знаний в научно-исследовательской и практической работе; |
| | ПК-1.3 Владеет навыками разработки рабочей и эксплуатационной документации на средства и системы информатизации в защищенном исполнении | Знать: основы аналитического обоснования необходимости создания системы защиты информации в организации;<br>Уметь: пользоваться методами установления причинно-следственных связей и определения наиболее значимых среди них при построении системы защиты информации в организации;<br>Владеть: навыком аналитического обоснования необходимости создания системы защиты |

| | | |
|---|---|---|
| | | информации на предприятии; |
| ПК-2 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов | ПК-2.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа, проектирования средств защиты информации, сертификации средств защиты информации на соответствие требованиям по безопасности информации и аттестации объектов информатизации на соответствие требованиям по защите информации, стандарты ЕСКД, ЕСТД и ЕСПД | Знать: основные разделы технического задания на разработку защищенной системы обработки информации;<br>Уметь: реализовать технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами;<br>Владеть: навыками использования действующих нормативно-правовых и методических документов в области построения защищенной системы обработки информации; |
| | ПК-2.2 Умеет оформлять рабочую и эксплуатационную документацию на средства и системы информатизации в защищенном исполнении | Знать: основные стадии проектирования защищенной системы обработки информации;<br>Уметь: применять основные национальные и зарубежные стандарты в области обеспечения информационной безопасности;<br>Владеть: навыками проектирования защищенной системы обработки информации; |
| | ПК-2.3 Владеет навыками разработки технического проекта средства и/или системы информатизации в защищенном исполнении | Знать: основные разделы технического задания на построение защищенной системы обработки информации;<br>Уметь: пользоваться приобретёнными знаниями для формирования проекта технического задания на создание защищенной системы обработки информации;<br>Владеть: навыками по контролю над соблюдением порядка построения защищённой системы обработки информации и законодательства России при решении вопросов в сфере информационной безопасности |

### 1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Технология построения защищенных систем обработки информации» относится к вариативной части блока дисциплин учебного плана, изучается в 4-ом семестре.

Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплин: "Технологии обеспечения информационной безопасности", "Защищенные информационные системы ".

В результате освоения дисциплины формируются знания, умения и владения, необходимые для прохождения преддипломной практики.

## 2. Структура дисциплины

Общая трудоемкость дисциплины составляет 4 з. е., 144 академических часа.

**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 |
|---|---|---|
| 4 | Лекции | 32 |
| 4 | Практические работы | 46 |
| | Всего: | 78 |

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет _66__ академических часа.

**Структура дисциплины для очно-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 |
|---|---|---|
| 4 | Лекции | 16 |
| 4 | Практические работы | 16 |
| | Всего: | 32 |

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 112 академических часа(ов).

## 3. Содержание дисциплины

| № | Наименование раздела дисциплины | Содержание |
|---|---|---|
| 1 | Основные понятия, определения и проблемы в области построения защищённых систем обработки информации | Предмет и содержание дисциплины, основная литература, контроль освоения дисциплины. Термины, определяющие научную основу информационной безопасности. Основные термины, определяющие предметную основу информационной безопасности. Термины, определяющие характер деятельности по обеспечению информационной безопасности. |
| 2 | Анализ угроз информационной безопасности | Особенности классы угроз информационной безопасности систем. Классификация случайных угроз. Классификация преднамеренных угроз. Возможности несанкционированного доступа к информации. Классификация вредоносных программ. Модели нарушителя информационной безопасности. |
| 3 | Концептуальная модель | Основные уровни обеспечения информационной безопасности. Особенности правового уровня обеспечения информационной |

| | | |
|---|---|---|
| | информационной безопасности | безопасности. Основные элементы административного уровня. Базовые группы процедурных мер защиты информации. Основные механизмы программно-технического уровня обеспечения информационной безопасности. |
| 4 | Системный подход к построению защищенных систем обработки информации | Базовые принципы построения системы защиты. Основные методы защиты информации. Особенности оптимизации взаимодействия пользователей и обслуживающего персонала. Методы и средства защиты информации от традиционного шпионажа и инсайдерства. Методы и средства защиты от электромагнитных излучений и наводок. |

## 4. Образовательные технологии

| № п/п | Наименование раздела | Виды учебной работы | Информационные и образовательные технологии |
|---|---|---|---|
| 1. | Основные понятия, определения и проблемы в области построения защищённых систем обработки информации | Лекция 1 | Вводная лекция с использованием видеопроектора |
| | | Практическое занятие 1 | опрос |
| | | Самостоятельная работа | Подготовка к занятию с использованием электронного курса лекций |
| 2. | Анализ угроз информационной безопасности | Лекция 2 | Лекция с использованием видеопроектора |
| | | Практическое занятие 2 | опрос |
| | | Самостоятельная работа | Подготовка к занятию с использованием электронного курса лекций |
| 3. | Концептуальная модель информационной безопасности | Лекция 3 | Лекция с использованием видеопроектора |
| | | Практическое занятие 3 | опрос |
| | | Самостоятельная работа | Подготовка к занятию с использованием электронного курса лекций |
| 4. | Системный подход к построению защищенных систем обработки информации | Лекция 4 | Лекция с использованием видеопроектора |
| | | Практическое занятие 4 | опрос |
| | | Контрольная работа | Подготовка к контрольной с использованием электронного курса лекций |
| | | Самостоятельная работа | Подготовка к занятию 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:<br>*- опрос*<br>*- контрольная работа (темы 3-4)* | <br>*10 баллов*<br>*20 баллов* | <br>*40 баллов*<br>*20 баллов* |
| Промежуточная аттестация<br>*(зачёт с оценкой по билетам)* | | *40 баллов* |
| **Итого за семестр**<br>*зачёт с оценкой* | | *100 баллов* |

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 оценок

| Баллы/ Шкала ECTS | Оценка по дисциплине | Критерии оценки результатов обучения по дисциплине |
|---|---|---|
| 100-83/ A, B | отлично | Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.<br>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.<br>Свободно ориентируется в учебной и профессиональной литературе. |

| Баллы/ Шкала ECTS | Оценка по дисциплине | Критерии оценки результатов обучения по дисциплине |
|---|---|---|
| | | Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий». |
| 82-68/ C | хорошо | 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. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший». |
| 67-50/ D, E | удовлетворительно | 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. 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. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный». |
| 49-0/ F, FX | неудовлетворительно | 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. 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. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы. |

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

**Текущий контроль**

**Примерные вопросы к опросу - ПК-1; ПК-2**

1. Современные проблемы развития теории и практики информационной безопасности.
2. Основные элементы, определяющие меры безопасности системы.
3. Классификация угроз информационной безопасности систем.
4. Основные уровни обеспечения информационной безопасности.
5. В каком нормативно-правовом документе России даётся определение информации как товара?
6. Понятие объекта защиты.
7. В чём заключается системный подход к обеспечению информационной безопасности объекта защиты?
8. Особенности биометрической системы защиты информации.

**Примерная тематика контрольной работы - ПК-1; ПК-2**

1. Основные термины, определяющие характер деятельности по обеспечению информационной безопасности.
2. Обобщённая схема обеспечения информационной безопасности системы.
3. Основные субъекты информационных отношений при построении защищённых систем обработки информации.
4. Базовые свойства систем обработки информации, подлежащие защите.
5. Основные трудности обеспечения конфиденциальности для современных информационных систем в России.
6. Концептуальные правовые документы федерального уровня по обеспечению информационной безопасности в России.
7. Основные органы - регуляторы правовых актов в области информационной безопасности в России.
8. Базовые мероприятия на административном уровне обеспечения информационной безопасности.
9. Основные виды тайн, содержащихся в информации и подлежащих защите.
10. Понятие государственной тайны и основные уровни секретности в России.
11. Классификация вредоносных программ.
12. Особенности административного уровня обеспечения информационной безопасности.

.

**Промежуточная аттестация**

**Примерная тематика вопросов для зачёта с оценкой - ПК-1; ПК-2**

1. Понятие объекта защиты.
2. Основные подходы к измерению количества информации.
3. Понятие информационной системы.
4. Основные принципы построения защищённых систем обработки информации.
5. Характеристика случайных угроз информационной безопасности.
6. Классификация преднамеренных угроз информационной безопасности.
7. Основные методы шпионажа и инсайдерства.
8. Базовые мотивы нарушений информационной безопасности.
9. Классификация нарушителей информационной безопасности.
10. Основные методы разграничения доступа.
11. Базовые методы идентификации и аутентификации.
12. Основные алгоритмы криптографической защиты информации.
13. Особенности протоколирования и аудита.

14. Базовые группы процедурных мер для обеспечения защиты автоматизированных систем.
15. Основные механизмы программно-технического уровня обеспечения защиты автоматизированных систем.
16. Классификация межсетевых экранов.

## 6. Учебно-методическое и информационное обеспечение дисциплины

### 6.1 Список источников и литературы

Литература

*Основная*

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — Москва : ИД «ФОРУМ» ; ИНФРА-М, 2016. — 416 с. - Режим доступа: URL: http://znanium.com/catalog/product/549989

3. Баранов В.В., Горошко И.В., Торопов Б.А., Лебедев В.Н., Петрова В.Ю., Макаров В.Ф. Информационные технологии управления и организация защиты информации (учебное пособие) - М.: Академия управления МВД России, 2018. - 456 с. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=44544096

4. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации (учебное пособие). СПб: Национальный исследовательский университет ИТМО, 2018. - 100 с. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=44449457

5. Методика оценки угроз безопасности информации (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.). - Режим доступа: URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g

*Дополнительная*

1. Защита информации в компьютерных системах / под ред. Е.В. Стельмашонок, И.Н. Васильевой. – СПб: Изд-во СПбГЭУ, 2017. – 163 с. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=32254007

2. Корякин С.В. Разработка концепции построения программно-аппаратного ядра универсальной среды проектирования автоматизированных систем защищенного исполнения // Проблемы автоматики и управления. 2020, №1 (38). - С. 60-69. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=43980501

### 6.2. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Информационный портал в области защиты информации. - Режим доступа: URL: http://www.securitylab.ru
2. Национальный открытый университет ИНТУИТ. - Режим доступа: URL:

http://www.intuit.ru

3. Информационный портал ФСТЭК России. - Режим доступа: URL: http://www.fstec.ru

4. Перечень современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС)

### 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

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 оснащён 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.

Средства вычислительной техники, сетевое оборудование, техническое, программное и программно-аппаратные средства защиты информации и средствами контроля защищенности информации.

**Состав программного обеспечения (ПО)**

| № п/п | Наименование ПО | Производитель | Способ распространения (*лицензионное или свободно распространяемое*) |
|---|---|---|---|
| 1. | Microsoft Office 2013 | Microsoft | лицензионное |
| 2. | Windows 10 Pro | Microsoft | лицензионное |
| 3. | Kaspersky Endpoint Security | Kaspersky | лицензионное |
| 4. | Microsoft Office 2016 | Microsoft | 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;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа;

- письменные задания выполняются на компьютере в письменной форме;

- экзамен и зачёт проводятся в письменной форме на компьютере;

- 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.

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:

- специальные устройства для сканирования и чтения;

- 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:
- компьютерной техникой со специальным программным обеспечением.

## 9. Методические материалы

### 9.1. Планы практических занятий - ПК-1; ПК-2

**Тема 1. Доктрина информационной безопасности Российской Федерации**

*Задания:*

1. Термины, определяющие научную основу информационной безопасности.
2. Термины, определяющие предметную основу информационной безопасности.
3. Термины, определяющие характер деятельности по обеспечению информационной безопасности.
4. Национальные интересы России в информационной сфере.
5. Основные информационные угрозы РФ.
6. Основные направления обеспечения информационной безопасности.
7. Организационная основа системы обеспечения информационной безопасности РФ.
8. Участники системы обеспечения информационной безопасности РФ.

**Тема 2. Классификация преднамеренных угроз информационной безопасности.**

*Задания:*

1. Базовые методы шпионажа и инсайдерства.
2. Основные причины несанкционированного доступа к информации;.
3. Особенности прослушивания объекта защиты.
4. Классификация нарушителей безопасности информационных систем.
5. Особенности инсайдеров и аутсайдеров.
6. Основные классы вредоносных программ.
7. Особенности побочных электромагнитных излучений и наводок (ПЭМИН).
8. Основные виды компьютерных вирусов.

**Тема 3. Национальные стандарты России, созданные на основе международной серии стандартов ISO/IEC 27000**

*Задания:*

1. ГОСТ Р ИСО/МЭК 27000-2012 как глоссарий терминов в области системы менеджмента информационной безопасности (СМИБ).

2. Нормативные требования для создания, внедрения и эксплуатации СМИБ (ГОСТ Р ИСО/МЭК 27001-2006).

3. Руководство по внедрению средств управления защитой информации (ГОСТ Р ИСО/МЭК 27002-2012).

4. Описание процессного подхода к внедрению СМИБ (ГОСТ Р ИСО/МЭК 27003-2012).

5. Система измерений, позволяющая оценивать эффективность СМИБ (ГОСТ Р ИСО/МЭК 27004-2011).

6. Руководство по внедрению процессного подхода к управлению рисками (ГОСТ Р ИСО/МЭК 27005-2010).

7. Руководство для органов, проводящих аудит и сертификацию СМИБ (ГОСТ Р 27006-2008).

8. Руководство для организаций, реализующих внутренний или внешний аудит СМИБ (ГОСТ Р 27007-2014).

**Тема 4. Методы и средства защиты информации от шпионажа и инсайдерства**

*Задания:*

1. Основные задачи защиты информации от шпионажа и инсайдерства.
2. Базовые рубежи защиты объекта от шпионажа и инсайдерства.
3. Состав системы охраны защищаемого объекта.
4. Основные требования к системам охранной сигнализации.
5. Базовые виды датчиков для выявления злоумышленников.
6. Основные элементы телевизионной системы видеоконтроля.
7. Основные методы борьбы с подслушиванием.
8. Методы и средства защиты от электромагнитных излучений и наводок.

Приложение1Аннотация рабочей программы дисциплины

# АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина "Технологии построения защищённых систем обработки информации" реализуется на факультете информационных систем и безопасности кафедрой информационной безопасности.

Цель дисциплины: формирование у обучающихся знаний и навыков в сфере обеспечения защиты информации на объекте информатизации, способности оценивать эффективность защиты, а также принимать эффективные управленческие решения при выборе проектов построения защищённых систем обработки информации.

Задачи дисциплины: освоение основных понятий и терминологии в области построения защищённых систем обработки информации, анализ угроз информационной безопасности, приобретение навыков в системном подходе к построению защищенных систем обработки информации.

Дисциплина направлена на формирование следующих компетенций:

ПК-1 Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

ПК-2 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

В результате освоения дисциплины обучающийся должен:

*Знать:* нормативно-правовые акты, национальные и зарубежные стандарты в области информационной безопасности; условия функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации; основы аналитического обоснования необходимости создания системы защиты информации в организации; основные разделы технического задания на разработку защищенной системы обработки информации; основные стадии проектирования защищенной системы обработки информации; основные разделы технического задания на построение защищенной системы обработки информации;

*Уметь:* работать с нормативно-правовыми актами и стандартами в области защиты информации; анализировать данные о функциях и условиях функционирования объектов и систем обработки информации ограниченного доступа; пользоваться методами установления причинно-следственных связей и определения наиболее значимых среди них при построении системы защиты информации в организации; реализовать технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами; применять основные национальные и зарубежные стандарты в области обеспечения информационной безопасности; пользоваться приобретёнными знаниями для формирования проекта технического задания на создание защищенной системы обработки информации;

*Владеть:* навыками использования международных и национальных стандартов в области информационной безопасности; опытом применения полученных знаний в научно-исследовательской и практической работе; навыком аналитического обоснования необходимости создания системы защиты информации на предприятии; навыками использования действующих нормативно-правовых и методических документов в области построения защищенной системы обработки информации; навыками проектирования защищенной системы обработки информации; навыками по контролю над соблюдением порядка построения защищённой системы обработки информации и законодательства России при решении вопросов в сфере информационной безопасности.

По дисциплине предусмотрена промежуточная аттестация в форме зачёта с оценкой.

Общая трудоемкость освоения дисциплины составляет 4 зачетные единицы.