**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**
**ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ**
**ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ**

УТВЕРЖДАЮ
Декан факультета
_____ Л.Р. Фионова
«15» февраля 2016 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

## Б1.2.9 Защита информации

Направление подготовки 09.03.01 «Информатика и вычислительная техника»

Профиль подготовки «Вычислительные машины, комплексы, системы и сети»

Квалификация (степень) выпускника – бакалавр

Форма обучения _ очная

Пенза, 2016

## 1. Цели освоения дисциплины

**Целью изучения дисциплины** является формирование у студентов профессиональных знаний и навыков выбирать и применять адекватные меры, направленные на обеспечение целостности и сохранности информации, а также использовать современные средства обнаружения и предотвращения угроз информационной безопасности. Приобретаются навыки разработки защищенных информационных систем с использованием криптографических библиотек.

## 2. Место дисциплины в структуре ОПОП

2.1. Дисциплина относится к вариативной части блока Б1 программы бакалавриата по направлению 09.03.01 «Информатика и ВТ». Изучение данной дисциплины базируется на следующих курсах: «Программирование», «ЭВМ и периферийные устройства», «Операционные системы».

2.2. Минимальные требования к «входным» знаниям, необходимым для успешного усвоения данной дисциплины - удовлетворительное усвоение программ по следующим разделам указанных выше дисциплин:

- «Программирование» - практика программирование на языке высокого уровня;
- «ЭВМ и периферийные устройства» в полном объеме;
- «Операционные системы» в полном объеме.

## 3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

| Коды компетенции | Наименование компетенции | Структурные элементы компетенции (в результате освоения дисциплины обучающийся должен знать, уметь, владеть) |
|---|---|---|
| 1 | 2 | 3 |
| ПК-2 | способность разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструмен-тальные средства и технологии программи-рования (проектно-технологическая деятельность) | Знать: принципы и модели, положенные в основу построения защищённых информационных систем.<br>Уметь: выбирать и использовать адекватные методы и средства защиты информации для решения задач обеспечения безопасности систем обработки информации и управления; решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; разрабатывать компоненты аппаратно-программных комплексов и баз данных, используя современные инструментальные средства и технологии программирования.<br>Владеть: языками процедурного и объектно-ориентированного программирования; навыками использования методов и средств защиты информации для решения широкого круга задач. |

| | | |
|---|---|---|
| ОПК-5 | способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (научно-исследовательская деятельность) | Знать: концептуальные и теоретические модели классических проблем и задач.<br>Уметь: анализировать новые возникающие проблемы и находить пути их решения.<br>Владеть: современными математическими и информационными методами работы с информацией. |

## 4. Структура и содержание дисциплины (модуля)

### 4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

| № п/п | Наименование разделов и тем дисциплины (модуля) | Семестр | Недели семестра | Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах) | | | | | | | | | Формы текущего контроля успеваемости *(по неделям семестра)* | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Аудиторная работа | | | | Самостоятельная работа | | | | | | | | | | | | |
| | | | | Всего | Лекция | Практические занятия | Лабораторные занятия | Всего | Подготовка к аудиторным занятиям | Реферат, эссе и др. | Курсовая работа (проект) | Подготовка к экзамену | Собеседование | Коллоквиум | Проверка тестов | Проверка контрольн. | Проверка реферата | Проверка эссе и иных творческих работ | курсовая работа (проект) | др. |
| 1. | Введение в дисциплину | 6 | | | 2 | | | | 14 | | | | 1 | | | | | | | |
| 2. | Основные понятия и теоретические основы криптографии | 6 | | | 6 | | 16 | | 18 | | | | 1 | | | | | | | |
| 3. | Протоколы | 6 | | | 8 | | 6 | | 14 | | | | 1 | | | | | | | |
| 4. | Модели политики безопасности | 6 | | | 6 | | 6 | | 14 | | | | 5 | | | | | | | |
| 5. | Стандарты информационной безопасности | 6 | | | 5 | | | | 14 | | | | 1 | | | | | | | |
| 6. | Системы обнаружения вторжений | 6 | | | 4 | | 6 | | 14 | | | | 1 | | | | | | | |
| 7. | Заключение | 6 | | | 3 | | | | | | | | 1 | | | | | | | |
| | *Курсовая работа (проект)* | | | | | | | | | | | | | | | | | | | |
| | *Подготовка к экзамену* | 6 | | | | | | | | | | *24* | | | | | | | | |
| | Общая трудоемкость, в часах | | | 68 | 34 | | 34 | 112 | 88 | | | 24 | Промежуточная аттестация | | | | | | | |
| | | | | | | | | | | | | | Форма | | | Семестр | | | | |
| | | | | | | | | | | | | | Зачет | | | | | | | |
| | | | | | | | | | | | | | Экзамен | | | *6* | | | | |

## 4.2. Содержание дисциплины

### 4.2.1 Содержание лекционного курса

| № п/п | № темы | Наименование тем лекционных занятий | Кол. Часов |
|---|---|---|---|
| 1 | 1 | Цели и задачи курса и его место в подготовке специалиста. Этапы и перспективы развития средств защиты информации. Определения и термины. Современные тенденции в области защиты информации | 2 |
| 2 | 2 | Способы защиты информационных систем. Абсолютная система защиты. Символьные шифры. Одноразовые блокноты. Компьютерные алгоритмы. Генераторы псевдослучайных чисел. | 6 |
| 3 | 3 | Введение в протоколы. Протоколы с посредником. Арбитражные протоколы. Самодостаточные протоколы. Попытки вскрытия протоколов. Однонаправленные функции. Однонаправленные функции с лазейкой. Симметричная криптография. Криптография с открытым ключом. Цифровые подписи. | 8 |
| 4 | 4 | Дискреционная модель. Мандатная модель. Ролевая модель. | 6 |
| 5 | 5 | Обзор стандартов информационной безопасности. Оранжевая книга. Европейские критерии информационной безопасности. Руководящие документы Гостехкомиссии России. | 5 |
| 6 | 6 | Обзор современных средств обнаружения вторжений. Состав и принципы функционирования системы обнаружения вторжений. Проблемы современных систем обнаружения вторжений. | 4 |
| 7 | 7 | Перспективы развития средств защиты информации. Обзор курса. | 3 |

### 4.2.2 Перечень и содержание лабораторных занятий

| № п/п | № темы | Наименование лабораторных работ | Кол. Часов |
|---|---|---|---|
| 1 | 1 | Символьные шифры. Перестановочный шифр. | 4 |
| 2 | 2 | Символьные шифры. Подстановочный шифр. | 4 |
| 3 | 3 | Генераторы псевдослучайных последовательностей. | 6 |
| 4 | 4 | Стеганография. | 8 |
| 5 | 5 | Управление атрибутами безопасности ОС. | 8 |
| 6 | 6 | Защита программ с использованием ключевой информации. | 4 |

## 5. Образовательные технологии

5.1 Чтение лекций по дисциплине проводится с использованием мультимедийного компьютерного проектора с раздачей демонстрируемых слайдов комментарий.

5.2 При изучении материалов лабораторного практикума использовать ресурсы с сайта кафедры ВТ (alice.pnzgu.ru и titan.vt).

5.3 При самостоятельной работе используются материалы сайта «Интернет-Университет Информационных Технологий (www.intuit.ru) и д.р.

5.3 Лабораторные занятия носят исследовательский и проектный характер.

5.4 Образовательные технологии сочетаются с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В частности, рекомендуются встречи студентов с представителями российских компаний - работодателей, посвященных обсуждению перспектив развития области информатики и вычислительной техники и её использованием в промышленности.

5.5 В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по собственной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы со студентами, в том числе в электронной образовательной среде с использованием соответствующего программного обеспечения, дистанционных форм обучения, возможностей интернет-ресурсов, индивидуальных консультаций и т.д.

## 6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

### 6.1. План самостоятельной работы студентов

| № нед. | Тема | Вид самостоятельной работы | Задание | Рекомендуемая литература | Кол. часов |
|---|---|---|---|---|---|
| 1-3 | Введение в дисциплину | Подготовка к аудиторным занятиям | Ознакомиться с этапами развития средств защиты информации и современными тенденциями в этой области. | Учебно-методические материалы и электронные учебные пособия по дисциплине с сервера кафедры ВТ. Основная и дополнительная литература. | 14 |
| 4-6 | Основные понятия и теоретические основы криптографии | Подготовка к аудиторным занятиям | Изучить способы защиты информационных систем. Изучить подстановочные и перестановочные шифры. Изучить принципы работы генераторов псевдослучайных чисел. Самостоятельная подготовка к лекциям и лабораторным занятиям | Учебно-методические материалы и электронные учебные пособия по дисциплине с сервера кафедры ВТ. Основная и дополнительная литература. | 18 |
| 7-9 | Протоколы | Подготовка к аудиторным занятиям | Изучить принципы построения и функционирования протоколов, а также возможные атаки на них. Самостоятельная подготовка к лабораторным занятиям | Учебно-методические материалы и электронные учебные пособия по дисциплине с сервера кафедры ВТ. Основная и дополнительная литература. | 14 |
| 10-11 | Модели политики безопасности | Подготовка к аудиторным занятиям | Изучить классические модели политик безопасности. Самостоятельная подготовка к лабораторным занятиям | Учебно-методические материалы и электронные учебные пособия по дисциплине с сервера кафедры | 14 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | ВТ. Основная и дополнительная литература. | |
| 12-14 | Стандарты информационной безопасности | Подготовка к аудиторным занятиям | Изучить общемировые и отечественные стандарты информационной безопасности. Самостоятельная подготовка к лекциям и лабораторным занятиям | Учебно-методические материалы и электронные учебные пособия по дисциплине с сервера кафедры ВТ. Основная и дополнительная литература. | 14 |
| 15-17 | Системы обнаружения вторжений | Подготовка к аудиторным занятиям | Изучить принципы функционирования современных систем обнаружения вторжений. Самостоятельная подготовка к лекциям и лабораторным занятиям | Учебно-методические материалы и электронные учебные пособия по дисциплине с сервера кафедры ВТ. Основная и дополнительная литература. | 14 |
| 18 | Подготовка к экзамену | Подготовка к экзамену | Подготовиться к экзамену. | Учебно-методические материалы и электронные учебные пособия по дисциплине с сервера кафедры ВТ. Основная и дополнительная литература. | 24 |

### 6.2. Методические указания по организации самостоятельной работы студентов

Каждый студент должен вести самостоятельную работу по основным разделам дисциплины в объемах, не меньших, чем указано в программе.

1. **Самостоятельная подготовка к лабораторным работам**. Контроль производится во время выполнения и сдачи лабораторных работ.

### 6.3. Материалы для проведения текущего и промежуточного контроля знаний студентов

1. Для проведения промежуточного и текущего контроля знаний использовать блоки контрольных заданий.

***Контроль освоения компетенций***

| № п\п | Вид контроля | Контролируемые темы (разделы) | Компетенции, компоненты которых контролируются |
|---|---|---|---|
| 1 | Текущий: собеседование при защите лаб. заданий. Промежуточный: зачет по результатам сдачи | Основные понятия и теоретические основы криптографии; Протоколы | ПК-2, ОПК-5 |

| | | | |
|---|---|---|---|
| | лабораторных работ. | | |
| 2 | Текущий: собеседование при защите лаб. заданий. Промежуточный: зачет по результатам сдачи лабораторных работ. | Модели политики безопасности; Системы обнаружения вторжений | ПК-2, ОПК-5 |

Контроль освоения компетенции выполняется:

– для компетенции ПК-2 - путем оценки способности студента использовать специальное и стандартное ПО для решения практических задач разработки компонентов программного обеспечения при выполнении лабораторных работ.

– для компетенции ОПК-5 - путем оценки способности студента решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

**Вопросы к экзамену**

1. Информация и способы ее защиты. Основные понятия и определения.
2. Однонаправленные функции. Однонаправленные функции с лазейкой.
3. Способы защиты информационных систем. Абсолютная система защиты.
4. Головоломки Меркла.
5. Основные понятия криптографии.
6. Однонаправленные хэш-функции. Цифровые подписи.
7. Символьные шифры. Подстановочные шифры.
8. Подпись документа. Содержимое подписи и метки времени.
9. Перестановочные шифры. Одноразовые блокноты.
10. Модели политики безопасности. Дискреционная модель.
11. Генерация случайных и псевдослучайных последовательностей.
12. Модели политики безопасности. Мандатная модель.
13. Физические ГСЧ.
14. Модели политики безопасности. Ролевая модель.
15. Табличные ГСЧ.
16. Стандарты информационной безопасности. «Оранжевая книга».
17. Алгоритмические ГСЧ.
18. Стандарты информационной безопасности. Европейские критерии безопасности информационных технологий.
19. Проверка качества работы ГСЧ.
20. Стандарты информационной безопасности. Руководящие документы Гостехкомиссии России.
21. Протоколы. Попытки вскрытия протоколов. Элементы протоколов.
22. Атаки на информационные системы. Уровни сетевых атак согласно модели OSI.
23. Симметричная криптография.
24. Протокол SSL. Алгоритм установления соединения.
25. Асимметричная криптография.
26. Виртуальные частные сети. Проблемы безопасности беспроводных соединений.

## 7. Учебно-методическое и информационное обеспечение дисциплины

### 7.1. Основная литература:

1. Бескид П.П. Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс]: Учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— СПб.: Российский государственный гидрометеорологический университет, 2010.— 95 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=17925.— «БИБЛИОКОМПЛЕКТАТОР», по паролю
2. Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс]: Учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— СПб.: Российский государственный гидрометеорологический университет, 2010.— 104 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=17926.— «БИБЛИОКОМПЛЕКТАТОР», по паролю

### 7.2. Дополнительная литература:

1. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=10677.— «БИБЛИОКОМПЛЕКТАТОР», по паролю

### 7.3. Интернет-ресурсы

1. Материалы раздела Учебные пособия» сайта «Кафедра ВТ» http://alice.pnzgu.ru
2. Материалы раздела «Программирование» сайта «Интернет-Университет Информационных Технологий» http://www.intuit.ru/

### 7.4 Программное обеспечение:

1. Среда разработки ПО для выполнения обязательных лабораторных работ: MS Visual Studio 2005;
2. Среда разработки отчетов по выполненным лабораторным работам: пакет Open Office;

## 8. Материально-техническое обеспечение дисциплины

Перечень специализированных аудиторий с указанием используемого в учебном процессе основного учебно-лабораторного оборудования, технических средств обучения и контроля.

Лабораторные занятия проводятся в классе, оснащенным ПЭВМ, с операционной системой Windows 7 или более современной версии.

Для лиц с ограниченными возможностями здоровья по ходатайству заведующего кафедрой устанавливается специальный индивидуальный набор программного обеспечения (Scype, Viber и т.д.) на вычислительную технику, выделенную для освоения дисциплины для лица с ограниченными возможностями здоровья.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.01 «Информатика и вычислительная техника»

Программу составил:
1. Дубравин Алексей Викторович, доцент



Программа одобрена на заседании кафедры «Вычислительная техника»

Протокол № ___ от «____» _____ 2016 года

Зав. кафедрой ВТ _____ Д.В. Пащенко

Программа одобрена методической комиссией ФВТ

Протокол № ___ от «____» _____ 2016 года

Председатель методической комиссии ФВТ _____Н.Н.Коннов

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.03.01 «Информатика и вычислительная техника»

Программу составил:
1. Дубравин Алексей Викторович, доцент _____



Программа одобрена на заседании кафедры «Вычислительная техника»

Протокол № 7 от «15» 02 2016 года

Зав. кафедрой ВТ _____ Д.В. Пащенко

Программа одобрена методической комиссией ФВТ

Протокол № 4 от «15» 02 2016 года

Председатель методической комиссии ФВТ _____ Н.Н.Коннов