МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Декан факультета
вычислительной техники
_____ Фионова Л.Р.

«15» июня 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.2.20.1 Информационная безопасность

Направление подготовки: 010302 Прикладная математика и информатика

Профиль подготовки: Системное программирование и компьютерные технологии

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Пенза, 2015

1. Цели освоения дисциплины

Целью изучения дисциплины «Информационная безопасность» является ознакомление студентов с основными понятиями и определениями информационной безопасности; источниками, рисками и формами атак на информацию; угрозами, которым подвергается информация; вредоносными программами; защитой от компьютерных вирусов и других вредоносных программ; методами и средствами защиты информации; политикой безопасности компании в области информационной безопасности; стандартами информационной безопасности; криптографическими методами и алгоритмами шифрования информации; алгоритмами аутентификации пользователей; защитой информации в сетях; требованиями к системам защиты информации.

Задачи изучаемой дисциплины:

Исходя из общих целей подготовки бакалавра:

- содействовать средствами дисциплины «Информационная безопасность» развитию у студентов мотивации к профессиональной деятельности, творческого мышления, коммуникативной готовности, общей культуры;
- научить студентов ясно, точно, грамотно излагать свои мысли в устной и письменной речи.

Исходя из конкретного содержания дисциплины:

- изучение правовых актов в области информационной безопасности в конкретной сфере деятельности, защиты государственной тайны, коммерческой тайны, интеллектуальной собственности;
- рассмотреть вопросы информационной безопасности в компьютерных сетях и системах.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Информационная безопасность» относится к вариативной части дисциплин по выбору.

Для освоения дисциплины обучающиеся используют знания, умения, сформированные в ходе изучения дисциплин бакалавриата.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Информационная безопасность»

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
ОПК-1	способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с прикладной математикой и информатикой	Знать: основы безопасности компьютерных систем и сетей
		Уметь: использовать средства обеспечения безопасности в компьютерных системах и сетях
		Владеть: навыками обеспечения безопасности в компьютерных системах и сетях
ОПК-3	способностью к разработке алгоритмических и программных решений в области системного и	Знать: требования к разработке приложений, обеспечивающий информационную безопасность

	прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям	Уметь: разрабатывать приложения для обеспечения информационной безопасности
		Владеть: навыками разработки приложений в области информационной безопасности
ОПК-4	способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Знать: законы и стандарты, обеспечивающие информационную безопасность
		Уметь: применять законодательную базу
		Владеть: навыками применения стандартов и законов в области информационной безопасности для решения стандартных задач профессиональной деятельности
ПК-7	способностью к разработке и применению алгоритмических и программных решений в области системного и прикладного программного обеспечения	Знать: основы безопасности компьютерных сетей
		Уметь: использовать средства обеспечения безопасности в сетях
		Владеть: навыками обеспечения безопасности в локальных и глобальных компьютерных сетях

4. Структура и содержание дисциплины «Информационная безопасность»

4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет _3_ зачетных единицы _108_ 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	Лабораторные занятия	Всего	Подготовка к лекциям	Подготовка к лаб. работе	Подготовка к контрольной работе	Опрос на лабораторных занятиях	Проверка отчетов о выполнении лабораторных работ	Контрольная работа
1.	**Раздел 1. Теоретические аспекты информационной безопасности**			**26**	**10**	**16**	**31**	**14**	**16**	**1**			
1.1.	Тема 1.1. Введение	8	1	6	2	4	2	2			1	1	
1.2.	Тема 1.2. Угроза информационной безопасности	8	2	4	2	2	6	2	4		2	2	
1.3.	Тема 1.3. Организационно-правовые методы информационной безопасности	8	3	6	2	4	8	4	4		3	3	
1.4.	Тема 1.4. Роль стандартов в обеспечении информационной безопасности	8	4-5	10	4	6	15	6	8	1	4-5	5	5

2.	**Раздел 2. Основные методы реализации защиты информации в компьютерных системах**			**19**	**8**	**11**	**32**	**16**	**16**				
2.1.	Тема 2.1. Программно-технические методы защиты	8	6	4	2	2	8	4	4		6	6	
2.2.	Тема 2.2. Криптографические методы защиты	8	7	6	2	4	8	4	4		7	7	
2.3.	Тема 2.3. Основные понятия теории информационной безопасности	8	8	4	2	2	8	4	4		8	8	
2.4.	Тема 2.4. Технологии построения защищенных систем	8	9	5	2	3	8	4	4		9	9	
	Общая трудоемкость, в часах			**45**	**18**	**27**	**63**	**30**	**32**	**1**	Промежуточная аттестация		
											Форма		Семестр
											Зачет		*8*

4.2. Содержание дисциплины

4.2.1. Содержание лекционных занятий

Раздел 1. Теоретические аспекты информационной безопасности

Тема 1.1. Введение в предмет

Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем.

Тема 1.2. Угрозы информационной безопасности

Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).

Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности.

Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.

Тема 1.3. Организационно-правовые методы информационной безопасности

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

Тема 1.4. Роль стандартов в обеспечении информационной безопасности

Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности.

Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности.

Руководящие документы Гостехкомиссии России. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем.

Международные стандарты информационной безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»). Основные положения Единых критериев. Функциональные требования и требования доверия. Понятие Профиля защиты и Проекта защиты.

Раздел 2. Основные методы реализации защиты информации в компьютерных системах

Тема 2.1. Программно-технические методы защиты

Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы, влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.

Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-

карты, их применение. Использование биометрических данных при аутентификации пользователей.

Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.

Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.

Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах.

Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.

Тема 2.2. Криптографические методы защиты

Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации.

Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа совместно с другими программами).

Использование криптографических средств для решения задач идентификация и аутентификация.

Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы.

Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.

Тема 2.3. Основные понятия теории информационной безопасности

Основные положения теории информационной безопасности информационных систем. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности.

Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности.

Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Тема 2.4. Технологии построения защищенных систем

Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования.

Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе.

Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

4.2.2. Темы лабораторных работ

1. Изучение программной реализации комплекса криптоалгоритмов Pretty Good Privacy (PGP 6.02).
2. Тестирование усвоения студентом принципов построения комплекса криптоалгоритмов PGP
3. Эксплуатация комплекса криптоалгоритмов PGP

4. Введение в криптографию (шифры простой замены)
5. Асимметричный алгоритм шифрования RSA
6. Оформление и защита отчетов

5. Образовательные технологии

В ходе освоения дисциплины «Информационная безопасность», при проведении аудиторных занятий, используются технологии традиционных учебных занятий.

Технология традиционного обучения предусматривает такие методы и формы изучения материала как лекция, лабораторные занятия.

- Проведение интерактивной лекции, демонстрирующей работу антивирусных программ (Тема 1.3 Использование антивирусных программ).
- Проведение проблемной лекции (Тема 2.1 Противодействие методам социальной инженерии).

Занятия, проводимые в интерактивной форме, в том числе с использованием интерактивных технологий составляют 25% от общего количества аудиторных занятий.

Самостоятельная работа студентов подразумевает индивидуальную работу студента, выполняемую, в том числе, в компьютерном классе с выходом в сеть «Интернет».

При реализации образовательных технологий используются следующие виды самостоятельной работы:

- работа с конспектом лекции и литературой;
- подготовка к лабораторной работе: изучение теоретического материала, разработка и отладка программ заданий по лабораторным работам;
- обработка результатов лабораторных работ и подготовка письменных отчетов;
- поиск информации в сети «Интернет» и дополнительной и справочной литературе;
- подготовка к сдаче лабораторных работ;
- подготовка к контрольной работе;
- подготовка к сдаче зачёта.

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 оборудования, 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	Количество часов
1	**2**	**3**	**4**	**5**	**6**
1	**1.1**	Подготовка к лекции. Подготовка к лабораторной работе. Оформление отчета по лабораторной работе	Ознакомиться с рекомендуемой литературой. Знать основные определения. Познакомиться с почтовой программой TheBat. Знать ее основные возможности.	**1-8**	**2**

2	**1.2**	Подготовка к лекции. Подготовка к лабораторной работе. Оформление отчета по лабораторной работе	Ознакомиться с рекомендуемой литературой. Знать основные определения. Уметь настраивать TheBat для работы с почтой по сети	**1-8**	**2** **4**
3	**1.3**	Подготовка к лекции. Подготовка к лабораторной работе. Оформление отчета по лабораторной работе	Ознакомиться с рекомендуемой литературой. Знать основные определения. Познакомиться с программой Putty. Знать ее сетевые настройки	**1-8, 9, 10, 11,12, 13**	**4** **4**
4-5	**1.4**	Подготовка к лекции. Подготовка к лабораторной работе. Оформление отчета по лабораторной работе Подготовка к контрольной работе	Ознакомиться с рекомендуемой литературой. Знать основные определения. Знать принцип работы комплекса PGP, его основные настройки.	**1-8, 14**	**6** **8** **1**
6	**2.1**	Подготовка к лекции. Подготовка к лабораторной работе. Оформление отчета по лабораторной работе	Ознакомиться с рекомендуемой литературой. Знать основные определения. Знать понятия шифрования закрытым и открытым ключом.	**1-8**	**4** **4**
7	**2.2**	Подготовка к лекции. Подготовка к лабораторной работе. Оформление отчета по лабораторной работе	Ознакомиться с рекомендуемой литературой. Знать основные определения. Определение цифровой подписи. Хэш-функции.	**1-8**	**4** **4**
8	**2.3**	Подготовка к лекции. Подготовка к лабораторной работе. Оформление отчета по лабораторной работе	Ознакомиться с рекомендуемой литературой. Знать основные определения. Удаленное подключение через TelNet и SSH.	**1-8**	**4** **4**
9	**2.4**	Подготовка к лекции. Подготовка к лабораторной работе. Оформление отчета по лабораторной работе	Ознакомиться с рекомендуемой литературой. Знать основные определения. Шифры простой замены, перестановки, решетка Кардано.	**1-8**	**4** **4**

6.2 Методические указания по организации самостоятельной работы студентов

Планируются следующие виды самостоятельной работы:

- подготовка к лабораторным и лекционным занятиям,
- подготовка к контрольной работе;
- подготовка к зачету.

6.3 Материалы для проведения текущего и промежуточного контроля знаний студентов

Контроль освоения компетенций

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются

1	Текущий: собеседование при защите лабораторных работ	Разделы 1 – 8	ОПК-1, 3, 4; ПК-7.
2	Текущий: проверка контрольной работы	Разделы 1 – 4	ОПК-1, 3, 4; ПК-7.
3	Промежуточный: Зачет	Разделы 1 – 8	ОПК-1, 3, 4; ПК-7.

Примерный вариант контрольной работы
Вариант 1

Вопрос №1. Дайте определение информации и носителя информации.

Вопрос №2. Перечислите основные аспекты обеспечения информационной безопасности и дайте их определения.

Вопрос №3. Раскройте историческое развитие вопросов обеспечения конфиденциальности и целостности информации.

Вопрос №4. Приведите примеры угроз, которые являются нарушением целостности и доступности.

Вопросы для зачета (очная форма обучения)

1. Понятие информационной безопасности (ИБ). Основные составляющие ИБ.
2. Определения угроз. Классификация угроз.
3. Вредоносное программное обеспечение.
4. Примеры угроз.
5. Российское законодательство в области ИБ.
6. Закон «Об информации, информатизации, защите информации».
7. Закон «О лицензировании».
8. Закон «О цифровой подписи».
9. Понятия стандартов и спецификаций («Оранжевая книга»). Механизмы безопасности. Классы безопасности.
10. Сетевые сервисы и механизмы безопасности. Администрирование средств безопасности.
11. Функциональные требования.
12. Требования доверия безопасности.
13. Документы Гостехкомиссии.
14. Административный уровень ИБ. Основные понятия. Политика безопасности.
15. Административный уровень ИБ. Программа безопасности. Синхронизация программы с жизненным циклом системы.
16. Идентификация и аутентификация. Основные понятия. Парольная аутентификация. Одноразовые пароли.
17. Сервер Kerberos.
18. Идентификация и аутентификация с помощью биометрических данных.
19. Управление доступом. Основные понятия.
20. Ролевое управление доступом.
21. Шифрование данных.
22. Контроль целостности.
23. Основные понятия управления рисками.

24. Подготовительные этапы управления рисками.

25. Основные этапы управления рисками.

26. Управление персоналом.

27. Физическая защита.

28. Поддержание работоспособности.

29. Реагирование на нарушение режима безопасности.

30. Планирование восстановительных работ.

31. Основные понятия программно-технического уровня информационной безопасности.

32. Особенности современных информационных систем, существенные с точки зрения безопасности.

33. Архитектурная безопасность.

7. Учебно-методическое и информационное обеспечение дисциплины «Информационная безопасность»

а) основная литература:

1. Фороузан, Бехроуз А. Криптография и безопасность сетей [Текст]: учебное пособие / Б. А. Фороузан; пер. с англ. А. Н. Берлина. - М.: Интернет - Ун-т Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. - 784 ил. - (Основы информационных технологий). - ISBN 978-5-9963-0242-0 http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=14842
2. Аникин, Д.В. Информационная безопасность и защита информации. [Электронный ресурс]: учеб. пособие — Электрон. дан. — СПб.: ИЭО СПбУТУиЭ, 2011. — 269 с. — Режим доступа: http://e.lanbook.com/book/63950 — Загл. с экрана.
3. Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс]: учеб. пособие — Электрон. дан. — СПб.: СПбГПУ, 2014. — 322 с. — Режим доступа: http://e.lanbook.com/book/64809 — Загл. с экрана.
4. Прохорова, О.В. Информационная безопасность и защита информации. [Электронный ресурс]: учеб. — Электрон. дан. — Самара: АСИ СамГТУ, 2014. — 114 с. — Режим доступа: http://e.lanbook.com/book/73915 — Загл. с экрана.
5. Артемов, А.В. Информационная безопасность: курс лекций. [Электронный ресурс] : учеб. пособие — Электрон. дан. — Орел : , 2014. — 257 с. — Режим доступа: http://e.lanbook.com/book/97695 — Загл. с экрана.
6. Шаньгин, В.Ф. Информационная безопасность. [Электронный ресурс] : учеб. пособие — Электрон. дан. — М. : ДМК Пресс, 2014. — 702 с. — Режим доступа: http://e.lanbook.com/book/50578 — Загл. с экрана.
7. Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] : учеб. пособие — Электрон. дан. — СПб. : Лань, 2017. — 324 с. — Режим доступа: http://e.lanbook.com/book/90153 — Загл. с экрана.
8. Малюк, А.А. Введение в информационную безопасность. [Электронный ресурс] : учеб. пособие / А.А. Малюк, В.С. Горбатов, В.И. Королев. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 288 с. — Режим доступа: http://e.lanbook.com/book/5171 — Загл. с экрана.
9. Ханипова, Л.Ю. Информационная безопасность и защита информации. [Электронный ресурс] : учеб. пособие / Л.Ю. Ханипова, Г.Р. Кутлова. — Электрон. дан. — Уфа : БГПУ имени М. Акмуллы, 2010. — 112 с. — Режим доступа: http://e.lanbook.com/book/49513 — Загл. с экрана.
10. Титова, Л.Н. Информационная безопасность и защита информации: учебно-методическое пособие. [Электронный ресурс] : учеб.-метод. пособие — Электрон. дан.

— Уфа : БГПУ имени М. Акмуллы, 2013. — 108 с. — Режим доступа: http://e.lanbook.com/book/56704 — Загл. с экрана.
11. Ерохин, В.В. Безопасность информационных систем. [Электронный ресурс] : учеб. пособие / В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко. — Электрон. дан. — М. : ФЛИНТА, 2015. — 182 с. — Режим доступа: http://e.lanbook.com/book/62972 — Загл. с экрана.
12. Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.: 60x90 1/16. - (Высшее образование) (Переплёт) ISBN 978-5-369-01450-9 http://znanium.com/catalog.php?bookinfo=495249
13. Лапонина, Ольга Робертовна. Основы сетевой безопасности : криптографические алгоритмы и протоколы взаимодействия : курс лекций / О. Р. Лапонина ; под ред. В. А. Сухомлина. - М. : Интернет - Ун-т Информационных Технологий, 2005. - 608 с. : ил. - (Основы информационных технологий). - ISBN 5-9556-0020-5 http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=7124
14. Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - М. : Академия, 2006. - 336 с. : ил. - (Высшее профессиональное образование). - ISBN 5-7695-2592-4 http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=7125
15. Информационная безопасность открытых систем. В 2-х т. : учебник. Т. 1. Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников [и др.]. - М. : Горячая линия - Телеком, 2006. - 536 с. : ил. - ISBN 5-93517-291-1(Т.1) http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=7122
16. Введение в защиту информации [Текст] : [учеб. пособие] / Байбурин В.Б. [и др.]. - М. : ФОРУМ : ИНФРА-М , 2004. - 128 с. - (Профессиональное образование). - 681.3(075) аб-3, чз2-2. - ISBN 5-8199-0130-4. - ISBN 5-16-001942-1 http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=3156
17. Основы информационной безопасности : учебное пособие / Е. Б. Белов [и др.]. - М. : Горячая линия - Телеком, 2006. - 544 с. : ил. - ISBN 5-93517-292-5 http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=8540
18. Оценка защищенности информационной системы организации : методические указания к практическим занятиям / Пенз. гос. ун-т ; сост. В. М. Алексеев. - Пенза : Изд-во Пенз. гос. ун-та, 2007. - 48 с. http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=8217
19. Алексеев, Владимир Михайлович. Обеспечение информационной безопасности на жизненном цикле автоматизированных систем [Текст] : учебное пособие / В. М. Алексеев, А. Г. Фатеев, М. Ю. Лупанов ; Пенз. гос. ун-т. - Пенза : Изд-во Пенз. гос. ун-та, 2009. - 292 с. http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=8382
20. Закон РФ от 21 июля 1993 г. N 5485-I "О государственной тайне".
21. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

22. Гражданский Кодекс РФ 2016 (ГК РФ).
23. Конституция РФ, (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ).
24. Уголовный кодекс РФ от 13.06.1996 N 63-ФЗ (ред. от 19.12.2016).
25. Критерии оценки надежных компьютерных систем ("Оранжевая книга" Министерства обороны США) (от 08.1983 г.).

б) дополнительная литература:

1. Галатенко, Владимир Антонович. Основы информационной безопасности: учебное пособие / В. А. Галатенко; под ред. В. Б. Бетелина. - 4-е изд. - М.: Интернет - Ун-т Информационных Технологий: БИНОМ. Лаборатория знаний, 2012. - 205 с.: ил. - (Основы информационных технологий). - ISBN 978-5-94774-821-5 http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=14831
2. Шаньгин, Владимир Федорович. Защита компьютерной информации. Эффективные методы и средства [Текст]: учебное пособие / В. Ф. Шаньгин. - М.: ДМК Пресс, 2008. - 544 с.: ил. - ISBN 5-94074-383-8 http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=11504
3. Бабаш, Александр Владимирович. Криптография [Текст] / А. В. Бабаш, Г. П. Шанкин ; под ред. В. П. Шерстюка, Э. А. Применко. - М.: СОЛОН-Пресс, 2007. - 512 с. - (Аспекты защиты). - ISBN 5-93455-135-3 http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=17397
4. Прохорова, Ольга Витольдовна. Информационная безопасность и защита информации [Текст]: учебник / О. В. Прохорова; Самарский государственный архитектурно-строительный университет. - Самара: СГАСУ, 2014. - 112 с.: ил. - ISBN 978-5-9585-0603-3 http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=17979
5. Лучник, А. И. Учебный курс AMS-120 "Базовые технологии информационной безопасности (CompTIA Security+) [Текст]: конспект лекций и практические работы (ver. 3.00) / А. И. Лучник, Д. В. Зырянов; Учебный центр ВМК МГУ & Softline Academy. - М. : Б. и., 2007. - 135 с. http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=18548
6. Лапонина, Ольга Робертовна. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия [Текст]: учебное пособие / О. Р. Лапонина; под ред. В. А. Сухомлина. - 2-е изд., испр. - М.: Интернет - Ун-т Информационных Технологий; М.: БИНОМ. Лаборатория знаний, 2007. - 531 с.: ил. - (Основы информационных технологий). - ISBN 978-5-9556-0102-1 http://kleopatra.pnzgu.ru/cgi-bin/irbis64r_91/cgiirbis_64.exe?P21DBN=KATL&I21DBN=KATL_PRINT&S21FMT=fullw_print&C21COM=F&Z21MFN=17364

в) программное обеспечение: программная реализация криптоалгоритма RSA, комплекс криптоалгоритмов Pretty Good Privacy (PGP 6.02.) **и Интернет-ресурсы**

№	Название	Электронный адрес	Содержание
1	**Санкт-Петербургский центр защиты информации**	http://www.ssl.stu.neva.ru	

2	**Курс лекций по информационной безопасности Ускова А.В.**	http://uskov.info	Лекции по информационной безопасности преподавателя ННГУ им. Н.И. Лобачевского, включают 20 вопросов
3	**Средства защиты информации**	http://www.analitika.info/main.php	

8. Материально-техническое обеспечение дисциплины

В целях оптимизации учебного процесса студенты используют рабочие места в компьютерном классе, оборудованном локальной сетью и выходом в Internet, имеющиеся в библиотеке учебники. Все работы выполняются на персональных компьютерах.

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки "Прикладная математика и информатика" и профилю подготовки "Системное программирование и компьютерные технологии".

Программу составил:

1. Артюхин В.В., доцент, к.т.н. _____
(подпись)

Настоящая программа не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.

Программа одобрена на заседании кафедры «Компьютерные технологии»

Протокол № 10 от «10» июня 2015 года

Зав. кафедрой «Компьютерные технологии» _____ В. И. Горбаченко

Программа одобрена методической комиссией факультета вычислительной техники

Протокол № 6 от «15» июня 2015 года

Председатель методической комиссии
Факультета вычислительной техники _____ Коннов Н. Н.
(подпись) (Ф.И.О.)

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата, подпись зав. кафедрой)	Внесенные изменения	Номера листов		
			заменен-ных	новых	аннулиро-ванных
2016/2017	№1 от 31.08.2016	Внесены изменения в п.5	8	—	—
2017/2018	№1 от 30.08.2017	Не изменений	—	—	—