

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г. ШУХОВА»
(БГТУ им. В.Г. Шухова)

УТВЕРЖДАЮ
Директор института

Рубанов В.Г.

« 23 »

2015 г.



РАБОЧАЯ ПРОГРАММА
дисциплины (модуля)

**ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ АВТОМАТИЗАЦИИ И
УПРАВЛЕНИЯ**

направление подготовки (специальность):

15.04.04 – Автоматизация технологических процессов и производств

Направленность программы (профиль, специализация):

**Автоматизация технологических процессов и производств
(промышленность)**

Квалификация

магистр

Форма обучения

очная

Институт: Информационных технологий и управляющих систем

Кафедра: Техническая кибернетика

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств (уровень магистратуры), утвержденного приказом №1484 от 21.11.2014,
- плана учебного процесса БГТУ им. В.Г. Шухова, введенного в действие в 2015 году по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств (магистратура).

Составитель (составители): к.т.н.  (Бажанов А.Г.)

Рабочая программа согласована с выпускающей кафедрой
«Техническая кибернетика»

Заведующий кафедрой: д.т.н., проф.  (Рубанов В.Г.)

« 11 » марта 2015 г.

Рабочая программа обсуждена на заседании кафедры

« 13 » марта 2015 г., протокол № 8

Заведующий кафедрой: д.т.н., проф.  (Рубанов В.Г.)

Рабочая программа одобрена методической комиссией института

« 14 » апреля 2015 г., протокол № 9

Председатель: к.т.н., доц.  (Солопов Ю.И.)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Формируемые компетенции			Требования к результатам обучения
№	Код компетенции	Компетенция	
Профессиональные			
1	ПК-16	Способность проводить математическое моделирование процессов, оборудования, средств и систем автоматизации, контроля, диагностики, испытаний и управления с использованием современных технологий научных исследований, разрабатывать алгоритмическое и программное обеспечение средств и систем автоматизации и управления	<p>В результате освоения дисциплины обучающийся должен:</p> <p>Знать: методы и средства хранения и защиты компьютерной информации, методики построения систем защиты компьютерной информации и их иерархию.</p> <p>Уметь: применять методы и средства хранения и защиты компьютерной информации, анализировать угрозы информации и проектировать политики безопасности для их предотвращения, защищать объекты интеллектуальной собственности, распределять нагрузку на подсистемы хранения информационных систем.</p> <p>Владеть: навыками практической охраны интеллектуальной собственности, хранения и защиты компьютерной информации, навыками построения подсистем безопасности информационных систем.</p>

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Содержание дисциплины основывается и является логическим продолжением следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Информационные технологии
2	Программирование и основы алгоритмизации
3	Цифровые системы управления

Содержание дисциплины служит основой для изучения следующих дисциплин:

№	Наименование дисциплины (модуля)
1	Теория и практика научных исследований
2	НИР по направлению

3.ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зач. единиц, 180 часов.

Вид учебной работы	Всего часов	Семестр № 3
Общая трудоемкость дисциплины, час	180	180
Контактная работа (аудиторные занятия), в т.ч.:	68	68
лекции	17	17
лабораторные	34	34
практические	17	17
Самостоятельная работа студентов, в том числе:	112	112
Курсовой проект		
Курсовая работа		
Расчетно-графическое задания		
Индивидуальное домашнее задание		
<i>Другие виды самостоятельной работы</i>	112	112
Самостоятельная работа при подготовке к экзамену	36	36
Самостоятельная работа при подготовке к практическим занятиям	22	22
Самостоятельная работа при подготовке к лабораторным занятиям	34	34
Самостоятельная работа при подготовке к лекциям	20	20
Форма промежуточная аттестация (зачет, экзамен)	экзамен	экзамен

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Наименование тем, их содержание и объем

Курс 2 Семестр 3

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Практические занятия	Лабораторные занятия	Самостоятельная работа
1. Основы защиты информации					
	Основные понятия: угрозы вычислительной системе, идентификация и аутентификация, авторизация, построение политик безопасности.	1			2
	Реализация угроз вычислительной системе. Действия злоумышленника. Модели безопасности.	2		4	6
	Симметричная криптография. Шифры замены и перестановки. Алгоритм ГОСТ 28147-89. Обзор алгоритмов блочного и поточного шифрования. Криптостойкость и длина ключа шифрования	1	4		8
	Асимметричная криптография (криптография с открытым ключом). Публичный и закрытый ключи. Концепции. Алгоритмы RSA и Эль-Гамаль. Функции хэширования, обзор алгоритмов. Электронная подпись. Цифровые сертификаты. Центры сертификатов. Использование сертификатов для аутентификации пользователей и обмена сеансовыми ключами.	2	2		6
	Основы асимметричного шифрования данных	1	3	8	12
2. Защита информации в операционных и информационных системах					
	Угрозы безопасности операционной системе. Построение системы безопасности в системах с дискреционным доступом. Механизмы разграничения доступа в операционных системах. Идентификация, аутентификация и авторизация субъектов доступа. Аудит доступа. Реализация мандатного доступа в операционных системах.	2			3
	Типовые сценарии атак на операционные системы. Перебор паролей. Атаки, основанные на переполнении буфера. Атаки на доверие. Использование разрушающих программных средств (РПС). Вирусы, сетевые черви, троянские программы. Защита информации в компьютерных сетях. Классификация удаленных атак. Методы защиты от них.	2		6	8
	Использования технологий криптографии для передачи конфиденциального трафика. Технологии VPN. Шифрование данных на сетевом уровне. Применение технологий шифрования данных совместно с межсетевыми экранами. Защищенные протоколы прикладных уровней.	1	4	8	14

	Генерация и проверка электронной цифровой подписи. Исследование модели безопасности современной операционной системы. Настройка политики безопасности операционной системы	1		8	9
3. Правовые основы защиты информации и интеллектуальных прав					
	Правовые основы интеллектуальной собственности. Охрана интеллектуальной собственности авторским правом. Системы патентования объектов интеллектуальной собственности. Виды лицензий на программное обеспечение. Правовое обеспечение защиты информации. Обзор международного и Российского законодательства в области защиты информации.	4	4		8
	ВСЕГО	17	17	34	76

4.2. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема практического (семинарского) занятия	К-во часов	К-во часов СРС
семестр №3				
1	Основы защиты информации	Разработка алгоритма симметричного и ассиметричного шифрования	4	6
2	Основы защиты информации	Обзор существующих программных и аппаратных систем, реализующих предложенную технологию защиты информации	2	4
3	Основы защиты информации	Расчет криптостойкости и надежности шифрования	3	3
4	Защита информации в операционных и информационных системах	Разработка программы защищенной передачи данных	4	4
5	Правовые основы защиты информации и интеллектуальных прав	Практическая реализация мер по обеспечению защиты или хранения информации	4	5
ИТОГО:			17	22
ВСЕГО:				39

4.3. Содержание лабораторных занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К-во часов	К-во часов СРС
семестр №3				
1	Основы защиты информации.	Разработка модели представления системы защиты информации	4	4
2	Основы защиты информации	Разработка модуля шифрования	8	8
3	Защита информации в операционных и информационных	Создание системы шифрования и дешифровки	6	6

	системах			
4	Защита информации в операционных информационных системах	и	Реализация прикладного обеспечения с защитой данных	8 8
5	Защита информации в операционных информационных системах	и	Разработка защищенной системы хранения и передачи информации	8 8
ИТОГО:				34 34
ВСЕГО:				68

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

5.1. Перечень контрольных вопросов (типовых заданий)

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1.	Основы защиты информации	<ol style="list-style-type: none"> 1. Компьютерная информация: определение, основные категории с точки зрения безопасности. 2. Основные категории безопасности информационных систем. Регламентирующие документы и стандарты в области компьютерной безопасности. Критерии надежности систем, классы безопасности. 3. Правовые основы защиты информации в РФ, Обзор законов РФ в области информационной безопасности. 4. Дискреционная и мандатная модель доступа к объектам информационных систем. 5. Классификация угроз информационным системам. Фундаментальные, базовые и первичные угрозы. 6. Механизмы реализации услуг безопасности в информационных системах. 7. Классификация криптографических алгоритмов. 8. Структурная схема симметричной криптосистемы. 9. Структурная схема асимметричной криптосистемы.
2.	Защита информации в операционных и информационных системах	<ol style="list-style-type: none"> 10. Математические определения шифра, процедур шифрования и дешифрации. 11. История развития криптоалгоритмов: шифр Цезаря, аффинная криптосистема, шифры Виженера и Вернома. 12. Частотный криптоанализ одно- и многопоточных шифров. 13. Понятие секретности криптоалгоритма. Разновидности атак на криптоалгоритмы. 14. Блочное симметричное шифрование, обратимые и необратимые, линейные и нелинейные преобразования. 15. Принцип итерирования как основной принцип построения современных блочных шифров. SP-сеть, сеть Фейштеля. 16. Алгоритм шифрования TEA: структура, достоинства и недостатки. 17. Режимы шифрования блочных шифров ECB, CBC, CFB, OFB.

		<p>18. Методы криптоанализа блочных шифров.</p> <p>19. Поточные шифры: принципы функционирования, структура.</p> <p>20. Методы построения нелинейных поточных шифров.</p> <p>21. Асимметричные криптосистемы: принципы функционирования, трудновычислимые математические задачи, определяющие криптостойкость асимметричных криптоалгоритмов.</p> <p>22. RSA: структура криптоалгоритма.</p> <p>23. Метод ключевого обмена Диффи-Хелмана.</p> <p>24. Хэш-функции: назначение и основные свойства.</p> <p>25. Итеративно-последовательная схема построения хэш-функций. Хэш-функции на основе блочных шифров.</p> <p>26. Электронная цифровая подпись: назначение, структура системы ЭЦП на основе алгоритма RSA.</p> <p>27. Инфраструктура PKI. Сертификация ключей асимметричных систем шифрования. Структура сертификата.</p> <p>28. Иерархическая и сетевая модель сертификации ключей асимметричных систем шифрования.</p> <p>29. Обзор современных защищенных сетевых протоколов.</p> <p>30. Угрозы безопасности в глобальных сетях.</p> <p>31. Межсетевые экраны: назначение, основные функции, состав</p> <p>32. Пакетные фильтры: назначение, основные принципы формирования правил фильтрации, достоинства и недостатки.</p> <p>33. Прокси-сервера: назначение, основные функции, достоинства и недостатки.</p> <p>34. Архитектура современных межсетевых экранов: двухканальный компьютер, экранированный узел, демилитаризованная зона.</p> <p>35. Определение вредоносной программы. Классификация вредоносных программ.</p> <p>36. Компьютерные вирусы: разновидности, используемые методы заражения.</p> <p>37. Сетевые черви: определение, способы распространения.</p> <p>38. Троянская программа: назначение, классификация, руткиты как средство маскировки.</p> <p>39. Методики защиты от вредоносных программ.</p>
3.	Правовые основы защиты информации и интеллектуальных прав	<p>40. Модель безопасности ОС Windows. Реализация дискреционной модели защиты доступа к ресурсам системы.</p> <p>41. Аудит событий безопасности современных операционных систем.</p> <p>42. Модель безопасности ОС Windows. Идентификация пользователей: идентификатор безопасности и маркер доступа субъекта, привилегии.</p> <p>43. Шифрующая файловая система (EFS): принцип работы, структура зашифрованного файла, роль агентов восстановления.</p>

**5.2. Перечень тем курсовых проектов, курсовых работ,
их краткое содержание и объем
(Не предусмотрены)**

**5.3. Перечень индивидуальных домашних заданий,
расчетно-графических заданий
(Не предусмотрены)**

**5.4. Перечень контрольных работ
(Не предусмотрены)**

6. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

6.1. Перечень основной литературы

- 1) Меньшаков, Ю. К. Защита объектов и информации от технических средств разведки: учеб. пособие / Ю. К. Меньшаков. – М.: РГГУ, 2002. – 399 с. – ISBN 5-7281-0487-8
- 2) Ярочкин, В. И. Информационная безопасность: учебник / В. И. Ярочкин. – 4-е изд. – М.: Академический Проект, 2006. – 543 с. – ISBN 5-8291-0740-6.
- 3) Полянская, О. Ю. Инфраструктуры открытых ключей: учеб. пособие / О. Ю. Полянская, В. С. Горбатов. – М.: Бином. Лаборатория знаний, 2007. – 367 с. – ISBN 978-5-94774-6 02-0.
- 4) Мельников, В.В. Защита информации в компьютерных системах / В. В. Мельников. – М: Финансы и статистика: Электронинформ, 1997. – 368 с.
- 5) Мельников, В.В. Безопасность информации в автоматизированных системах / В. В. Мельников. – М: Финансы и статистика, 2003. – 367 с.
- 6) 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.iprbookshop.ru/10677.html>.
- 7) Васильев, В.И. Интеллектуальные системы защиты информации [Электронный ресурс]: учебное пособие / Васильев В.И. – Электрон. текстовые данные. – М: Машиностроение, 2013. – 172 с. – Режим доступа: <http://www.iprbookshop.ru/18519.html>.
- 8) Малюк, А.А. Теория защиты информации [Электронный ресурс]: монография/ Малюк А.А. – Электрон. текстовые данные. – М: Горячая линия - Телеком, 2012. – 184 с. – Режим доступа: <http://www.iprbookshop.ru/12048.html>.

6.2. Перечень дополнительной литературы

- 1) Каторин, Ю.Ф. Энциклопедия промышленного шпионажа / сост. Ю. Ф. Каторин [и др.]; ред. Е. В. Куренков. – СПб: Полигон, 2000. – 512 с.
- 2) Баричев, С.Г. Основы современной криптографии: учеб. курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. – 2-е изд., перераб. и доп. – М: Горячая линия - Телеком, 2002. – 175 с.
- 3) Никифоров, С.В. Введение в сетевые технологии: Элементы применения и администрирования сетей: учеб. пособие / С. В. Никифоров. – М: Финансы и

статистика, 2003. – 224 с.

- 4) Бабаш, А.В. Криптография: учеб. пособие / А. В. Бабаш, Г. П. Шанкин. – М: СОЛОН-Р, 2002. – 511 с.
- 5) Харин, Ю.С. Математические и компьютерные основы криптологии : учеб. пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Минск: Новое знание, 2003. – 381 с.
- 6) Аверченков, В.И. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.]. – Электрон. текстовые данные. – Брянск: Брянский государственный технический университет, 2012. – 187 с. – Режим доступа: <http://www.iprbookshop.ru/7000.html>.
- 7) Соколов, В.П. Кодирование в системах защиты информации [Электронный ресурс]: учебное пособие/ Соколов В.П., Тарасова Н.П. – Электрон. текстовые данные. – М: Московский технический университет связи и информатики, 2016. – 94 с. – Режим доступа: <http://www.iprbookshop.ru/61485.html>.
- 8) Коваленко, Ю.И. Методика защиты информации в организациях [Электронный ресурс]: монография / Коваленко Ю.И., Москвитин Г.И., Тараскин М.М. – Электрон. текстовые данные. – М.: Русайнс, 2016. – 162 с. – Режим доступа: <http://www.iprbookshop.ru/61625.html>.

6.3. Перечень интернет ресурсов

<http://www.elibrary.ru/>- Научная электронная библиотека

<http://www.gpntb.ru/>- Государственная публичная научно-техническая библиотека России

<http://elibrary.bmstu.ru> – Библиотека МГТУ им. Н.Баумана

<http://www.viniti.ru> – Всероссийский институт научной информации по техническим наукам(ВИНИТИ)

<http://www.unilib.neva.ru/rus/>- Фундаментальная библиотека Санкт-Петербургского государственного политехнического университета

<http://elibrary.eltech.ru> – Библиотека Санкт-Петербургского государственного электротехнического университета

<http://www.ntb.bstu.ru> и [переход к системе NormaCS](#) - Электронно-библиотечная система БГТУ им В.Г.Шухова

http://re.mipt.ru/infsec/2004/essay/2004_PGP_Keys_Web_of_Trust_Lukjanchenko.htm - Открытые источники сайта МФТИ.

7.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Преподавание дисциплины «Защита информации в системах автоматизации и управления» осуществляется в следующих аудиториях:

1) специализированный компьютерный класс МК229: 15 персональных компьютеров с выходом в интернет, проектор, 10 комплектов оборудования для моделирования систем Matlab;

при активном использовании ИКТ, используя в учебном процессе для улучшения наглядности и доступности следующее обеспечение:

- мультимедиа и анимационный материал поясняющее работу элементов и устройств;
- презентационное программное обеспечение для демонстрации презентаций по разнообразным темам;
- MathWorks Individual Licenses (per License): MATLAB 2016b, Simulink, Neural Networks Toolbox, Fuzzy Logic Toolbox, Control System Toolbox 10 бессрочная лиц. №1145851;
- MathWorks Individual Licenses (per License): MATLAB 2014b, Simulink, Neural Networks Toolbox, Statistics and Machine Learning Toolbox10 бессрочная лиц. №362444;
- Microsoft Windows 7 64x MSDN подписка БГТУ;

Microsoft Office 2013 лицензия БГТУ.

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений
Рабочая программа без изменений утверждена на 2016/2017 учебный год.
Протокол № 10 заседания кафедры от «16» 05 2016г.

Заведующий кафедрой _____  _____ Рубанов В.Г.
подпись, ФИО

Директор института _____  _____ Белоусов А.В.
подпись, ФИО

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений

Рабочая программа без изменений утверждена на 2017/2018 учебный год.
Протокол № 11 заседания кафедры от «15» 05 2017г.

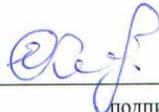
Заведующий кафедрой _____ Рубанов В.Г.
подпись, ФИО

Директор института _____ Белоусов А.В.
подпись, ФИО

8. УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Утверждение рабочей программы без изменений
Рабочая программа без изменений утверждена на 2018/2019 учебный год.
Протокол № 13 заседания кафедры от «01» 06 2018г.

Заведующий кафедрой  Рубанов В.Г.
подпись, ФИО

Директор института  Белоусов А.В.
подпись, ФИО

ПРИЛОЖЕНИЯ

Приложение №1. Методические указания для обучающегося по освоению дисциплины (включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине).

Данный курс состоит из лекций, лабораторных работ и практических занятий. Основой является модульный метод обучения, сущность которого состоит в том, что содержание обучения структурируется в автономные организационно-методические блоки – модули, содержание и объём которых могут варьировать в зависимости от дидактических целей. Сами модули формируются в виде разделов, объединяемых по тематическому признаку.

Информационные технологии предполагают использование электронных материалов, системных и программных средств. Применение персональных компьютеров при изучении дисциплины активизирует познавательную деятельность студентов в области современных информационных технологий.

Самостоятельная работа студентов предполагает активное, последовательное и подробное освоение ими соответствующих учебных материалов дисциплины по всем ее структурным разделам с использованием рекомендуемой основной и дополнительной литературы и интернет источников. При рассмотрении всех разделов дисциплины рекомендуется постоянная работа с Интернет-ресурсами, с вебинарами проводимыми на русском и английском языках. Итоговый контроль осуществляется в форме экзамена после изучения всех частей курса.