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

СОГЛАСОВАНО
Директор института магистратуры
_____ И. В. Ярмоленко
«20» 05 2021 г.

УТВЕРЖДАЮ
Директор института ЭИТУС
_____ А. В. Белоусов
«20» 05 2021 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 Магистратуры

Кафедра Технической кибернетики

Белгород 2021

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта высшего образования 15.04.04 Автоматизация технологических процессов и производств (уровень магистратуры), утвержденного приказом Министерства науки и высшего образования Российской Федерации № 1452 от 25 ноября 2020 г.
- учебного плана, утвержденного ученым советом БГТУ им. В. Г. Шухова в 2021 году.

Составитель (составители):

| канд. техн. наук | | А. Г. Бажанов |
|---|---|---|
| (ученая степень и звание) | (подпись) | (инициалы, фамилия) |

Рабочая программа обсуждена на заседании кафедры
«14» 05 2021 г., протокол № 9

Заведующий кафедрой:

| д-р техн. наук, проф. | | В. Г. Рубанов |
|---|---|---|
| (ученая степень и звание) | (подпись) | (инициалы, фамилия) |

Рабочая программа согласована с выпускающей(ими) кафедрой(ами)
Технической кибернетики
(наименование кафедры/кафедр)

Заведующий кафедрой:

| д-р техн. наук, проф. | | В. Г. Рубанов |
|---|---|---|
| (ученая степень и звание) | (подпись) | (инициалы, фамилия) |

«14» 05 2021 г.

Рабочая программа одобрена методической комиссией института
«20» 05 2021 г., протокол № 9

Председатель:

| канд. техн. наук, доц. | | А. Н. Семернин |
|---|---|---|
| (ученая степень и звание) | (подпись) | (инициалы, фамилия) |

# 1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

| Категория (группа) компетенций | Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Наименование показателя оценивания результата обучения по дисциплине |
|---|---|---|---|
| Профессиональные компетенции | ПК-2. Способен проводить математическое моделирование процессов, оборудования, средств и систем автоматизации, контроля, диагностики и управления с использованием современных технологий научных исследований, разрабатывать алгоритмическое и программное обеспечение средств и систем автоматизации и управления | ПК-2.5. Использует методы и средства хранения и защиты компьютерной информации при разработке алгоритмического и программного обеспечения средств и систем автоматизации и управления<br>ПК-2.6. Разрабатывает математические модели для обеспечения информационной безопасности автоматизированных систем управления | **Знать:** методы и средства хранения и защиты компьютерной информации, методики построения систем защиты компьютерной информации и их иерархию.<br>**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.<br>**Владеть:** навыками практической охраны интеллектуальной собственности, хранения и защиты компьютерной информации, навыками построения подсистем безопасности информационных систем. |

# 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

**1. Компетенция** ПК-2. Способен проводить математическое моделирование процессов, оборудования, средств и систем автоматизации, контроля, диагностики и управления с использованием современных технологий научных исследований, разрабатывать алгоритмическое и программное обеспечение средств и систем автоматизации и управления

Данная компетенция формируется следующими дисциплинами.

| Стадия | Наименования дисциплины |
|---|---|
| 1 | Теория матриц |
| 2 | Метод пространства состояния в теории управления |
| 3 | Web-технологии |
| 4 | Защита информации в системах автоматизации и управления |
| 5 | Производственная преддипломная практика |
| 6 | Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы |

## 3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зач. единиц, 180 часов.
Форма промежуточной аттестации экзамен.

| Вид учебной работы | Всего часов | Семестр № 3 |
|---|---|---|
| Общая трудоемкость дисциплины, час | 180 | 180 |
| **Контактная работа (аудиторные занятия), в том числе:** | **72** | **72** |
| лекции | 17 | 17 |
| лабораторные | 34 | 34 |
| практические | 17 | 17 |
| групповые консультации в период теоретического обучения и промежуточной аттестации | 4 | 4 |
| контроль самостоятельных работ | 0 | 0 |
| **Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:** | **108** | **108** |
| курсовой проект | 0 | 0 |
| курсовая работа | 0 | 0 |
| расчетно-графическое задание | 0 | 0 |
| индивидуальное домашнее задание | 0 | 0 |
| самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия) | 72 | 72 |
| экзамен | 36 | 36 |

# 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 на подготовку к аудиторным занятиям |
| 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 | | 6 |
| | 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 | | 4 |
| | 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 | | | 2 |
| | 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 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| 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 | 72 |

## 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 | 4 |
| 2 | Основы защиты информации | Обзор существующих программных и аппаратных систем, реализующих предложенную технологию защиты информации | 2 | 2 |
| 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 | 17 |
| ВСЕГО: | | | | 34 |

## 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 системах | Создание системы шифрования и дешифровки | 6 | 6 |
| 4 | Защита информации в операционных и информационных системах | Реализация прикладного обеспечения с защитой данных | 8 | 8 |
| 5 | Защита информации в | Разработка защищенной системы | 8 | 8 |

| | | | | |
|---|---|---|---|---|
| | операционных и информационных системах | хранения и передачи информации | | |
| ИТОГО: | | | 34 | 34 |
| ВСЕГО: | | | | 68 |

### 4.4. Содержание курсового проекта/курсовой работы

Не предусмотрено учебным планом.

### 4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Не предусмотрено учебным планом.

## 5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### 5.1. Реализация компетенций

**1. Компетенция** ПК-2. Способен проводить математическое моделирование процессов, оборудования, средств и систем автоматизации, контроля, диагностики и управления с использованием современных технологий научных исследований, разрабатывать алгоритмическое и программное обеспечение средств и систем автоматизации и управления.

| Наименование индикатора достижения компетенции | Используемые средства оценивания |
|---|---|
| ПК-2.5. Использует методы и средства хранения и защиты компьютерной информации при разработке алгоритмического и программного обеспечения средств и систем автоматизации и управления | Защита лабораторных работ, решение практических задач, экзамен |
| ПК-2.6. Разрабатывает математические модели для обеспечения информационной безопасности автоматизированных систем управления | |

### 5.2. Типовые контрольные задания для промежуточной аттестации

### 5.2.1. Перечень контрольных вопросов (типовых заданий) для экзамена / дифференцированного зачета / зачета

| № п/п | Наименование раздела дисциплины | Содержание вопросов (типовых заданий) |
|---|---|---|
| 1. | Основы защиты информации | 1. Компьютерная информация: определение, основные категории с точки зрения безопасности.<br>2. Основные категории безопасности информационных систем. Регламентирующие документы и стандарты в области компьютерной безопасности. Критерии надежности систем, классы безопасности.<br>3. Правовые основы защиты информации в РФ, Обзор законов РФ в области информационной безопасности.<br>4. Дискреционная и мандатная модель доступа к объектам |

| | | |
|---|---|---|
| | | информационных систем.<br>5. Классификация угроз информационным системам. Фундаментальные, базовые и первичные угрозы.<br>6. Механизмы реализации услуг безопасности в информационных системах.<br>7. Классификация криптографических алгоритмов.<br>8. Структурная схема симметричной криптосистемы.<br>9. Структурная схема асимметричной криптосистемы. |
| 2. | Защита информации в операционных и информационных системах | 10. Математические определения шифра, процедур шифрования и дешифрации.<br>11. История развития криптоалгоритмов: шифр Цезаря, аффинная криптосистема, шифры Виженера и Вернома.<br>12. Частотный криптоанализ одно- и многопоточных шифров.<br>13. Понятие секретности криптоалгоритма. Разновидности атак на криптоалгоритмы.<br>14. Блочное симметричное шифрование, обратимые и необратимые, линейные и нелинейные преобразования.<br>15. Принцип итерирования как основной принцип построения современных блочных шифров. SP-сеть, сеть Фейштеля.<br>16. Алгоритм шифрования TEA: структура, достоинства и недостатки.<br>17. Режимы шифрования блочных шифров ECB, CBC, CFB, OFB.<br>18. Методы криптоанализа блочных шифров.<br>19. Поточные шифры: принципы функционирования, структура.<br>20. Методы построения нелинейных поточных шифров.<br>21. Асимметричные криптосистемы: принципы функционирования, трудновычислимые математические задачи, определяющие криптостойкость асимметричных криптоалгоритмов.<br>22. RSA: структура криптоалгоритма.<br>23. Метод ключевого обмена Диффи-Хелмана.<br>24. Хэш-функции: назначение и основные свойства.<br>25. Итеративно-последовательная схема построения хэш-функций. Хэш-функции на основе блочных шифров.<br>26. Электронная цифровая подпись: назначение, структура системы ЭЦП на основе алгоритма RSA.<br>27. Инфраструктура PKI. Сертификация ключей асимметричных систем шифрования. Структура сертификата.<br>28. Иерархическая и сетевая модель сертификации ключей асимметричных систем шифрования.<br>29. Обзор современных защищенных сетевых протоколов.<br>30. Угрозы безопасности в глобальных сетях.<br>31. Межсетевые экраны: назначение, основные функции, состав<br>32. Пакетные фильтры: назначение, основные принципы формирования правил фильтрации, достоинства и недостатки.<br>33. Proxy-сервера: назначение, основные функции, достоинства и недостатки. |

| | | |
|---|---|---|
| | | 34. Архитектура современных межсетевых экранов: двухканальный компьютер, экранированный узел, демилитаризованная зона.<br>35. Определение вредоносной программы. Классификация вредоносных программ.<br>36. Компьютерные вирусы: разновидности, используемые методы заражения.<br>37. Сетевые черви: определение, способы распространения.<br>38. Троянская программа: назначение, классификация, руткиты как средство маскировки.<br>39. Методики защиты от вредоносных программ. |
| 3. | Правовые основы защиты информации и интеллектуальных прав | 40. Модель безопасности ОС Windows. Реализация дискреционной модели защиты доступа к ресурсам системы.<br>41. Аудит событий безопасности современных операционных систем.<br>42. Модель безопасности ОС Windows. Идентификация пользователей: идентификатор безопасности и маркер доступа субъекта, привилегии.<br>43. Шифрующая файловая система (EFS): принцип работы, структура зашифрованного файла, роль агентов восстановления. |

## 5.3. Типовые контрольные задания (материалы) для текущего контроля в семестре

**Лабораторные работы**. В лабораторном практикуме по дисциплине представлен перечень лабораторных работ, обозначены цель и задачи, необходимые теоретические и методические указания работе, рассмотрен практический пример, даны варианты выполнения и перечень контрольных вопросов.

Защита лабораторных работ возможна после проверки правильности выполнения задания, оформления отчета. Защита проводится в форме собеседования преподавателя со студентом по теме лабораторной работы. Примерный перечень контрольных вопросов для защиты лабораторных работ представлен в таблице

| № | Тема лабораторной работы | Контрольные вопросы |
|---|---|---|
| 1. | Лабораторная работа №1. Разработка модели представления системы защиты информации. | 1. Какие виды систем защиты информации вы знаете?<br>2. Какие алгоритмы защиты информации вы знаете? |
| 2. | Лабораторная работа №2. Разработка модуля шифрования. | 1. В чем заключается суть шифрования?<br>2. Какие методы являются наиболее эффективными при шифровании больших объемов информации? |

| № | Тема лабораторной работы | Контрольные вопросы |
|---|---|---|
| 3. | Лабораторная работа №3. Создание системы шифрования и дешифровки. | 1. Опишите алгоритмы шифрования данных.<br>2. Опишите способы дешифровки посылок и взлома кодированной информации. |
| 4. | Лабораторная работа №4. Реализация прикладного обеспечения с защитой данных. | 1. Какие алгоритмы вы применяли для защиты данных?<br>2. Какие нюансы необходимо учитывать при разработки системы защиты данных? |
| 5. | Лабораторная работа №5. Разработка защищенной системы хранения и передачи информации. | 1. Какие методы хранения информации могут относиться к системам защиты?<br>2. Какие основные эффективные пути передачи защищенной информации вы знаете? |

## 5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме экзамена, используется следующая шкала оценивания: 2 – неудовлетворительно, 3 – удовлетворительно, 4 – хорошо, 5 – отлично.

Критериями оценивания достижений показателей являются:

| Наименование показателя оценивания результата обучения по дисциплине | Критерий оценивания |
|---|---|
| Знания | Знание терминов, классификаций, основных принципов, видов регуляторов |
| | Объем освоенного материала |
| | Полнота ответов на вопросы |
| | Четкость изложения и интерпретации знаний |
| Умения | Умение применять методы и средства хранения и защиты компьютерной информации |
| | Умение анализировать угрозы информации и проектировать политики безопасности для их предотвращения |
| | Умение защищать объекты интеллектуальной собственности |
| | Умение распределять нагрузку на подсистемы хранения информационных систем |
| Навыки | Владение навыками практической охраны интеллектуальной собственности |
| | Владение навыками хранения и защиты компьютерной информации |

| | |
|---|---|
| | Владение навыками построения подсистем безопасности информационных систем |

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

| Критерий | Уровень освоения и оценка | | | |
|---|---|---|---|---|
| | 2 | 3 | 4 | 5 |
| Знание терминов, классификаций, основных принципов | Не знает терминов классификаций, основных принципов | Знает термины классификации, основные принципы, но допускает неточности формулировок | Знает термины классификации, основные принципы | Знает термины классификации, основные принципы, может корректно сформулировать их самостоятельно |
| Объем освоенного материала | Не знает значительной части материала дисциплины | Знает только основной материал дисциплины, не усвоил его деталей | Знает материал дисциплины в достаточном объеме | Обладает твердым и полным знанием материала дисциплины, владеет дополнительным и знаниями |
| Полнота ответов на вопросы | Не дает ответы на большинство вопросов | Дает неполные ответы на все вопросы | Дает ответы на вопросы, но не все – полные | Дает полные, развернутые ответы на поставленные вопросы |
| Четкость изложения и интерпретации знаний | Излагает знания без логической последовательности | Излагает знания с нарушениями в логической последовательности | Излагает знания без нарушений в логической последовательности | Излагает знания в логической последовательности, самостоятельно их интерпретируя и анализируя |
| | Не иллюстрирует изложение поясняющими схемами, рисунками и примерами | Выполняет поясняющие схемы и рисунки небрежно и с ошибками | Выполняет поясняющие рисунки и схемы корректно и понятно | Выполняет поясняющие рисунки и схемы точно и аккуратно, раскрывая полноту усвоенных знаний |
| | Неверно излагает и интерпретирует знания | Допускает неточности в изложении и интерпретации знаний | Грамотно и по существу излагает знания | Грамотно и точно излагает знания, делает самостоятельные выводы |

Оценка сформированности компетенций по показателю Умения.

| Критерий | Уровень освоения и оценка | | | |
|---|---|---|---|---|
| | 2 | 3 | 4 | 5 |
| Умение применять методы и средства хранения и защиты компьютерной информации | Обучающий не умеет применять методы и средства хранения и защиты компьютерной информации | Обучающий умеет применять методы и средства хранения и защиты компьютерной информации, но допускает при решении этих вопросов много ошибок | Обучающий умеет применять методы и средства хранения и защиты компьютерной информации с небольшими ошибками | Обучающийся умеет применять методы и средства хранения и защиты компьютерной информации |
| Умение анализировать угрозы информации и проектировать политики безопасности для их предотвращения | Обучающий не умеет анализировать угрозы информации и проектировать политики безопасности для их предотвращения | Обучающий умеет анализировать угрозы информации и проектировать политики безопасности для их предотвращения, но допускает при решении этих вопросов много ошибок | Обучающий умеет анализировать угрозы информации и проектировать политики безопасности для их предотвращения с небольшими ошибками | Обучающийся умеет анализировать угрозы информации и проектировать политики безопасности для их предотвращения |
| Умение защищать объекты интеллектуальной собственности | Обучающий не умеет защищать объекты интеллектуальной собственности | Обучающий умеет защищать объекты интеллектуальной собственности, но допускает при решении этих вопросов много ошибок | Обучающий умеет защищать объекты интеллектуальной собственности с небольшими ошибками | Обучающийся умеет защищать объекты интеллектуальной собственности |
| Умение распределять нагрузку на подсистемы хранения информационных систем | Обучающий не умеет распределять нагрузку на подсистемы хранения информационных систем | Обучающий умеет распределять нагрузку на подсистемы хранения информационных систем, но допускает при решении этих вопросов много ошибок | Обучающий умеет распределять нагрузку на подсистемы хранения информационных систем с небольшими ошибками | Обучающийся умеет распределять нагрузку на подсистемы хранения информационных систем |

Оценка сформированности компетенций по показателю Навыки.

| Критерий | Уровень освоения и оценка | | | |
|---|---|---|---|---|
| | 2 | 3 | 4 | 5 |
| Владеть навыками практической охраны интеллектуальной собственности | Обучающийся не имеет навыков практической охраны интеллектуальной собственности | Обучающийся демонстрирует слабые навыки практической охраны интеллектуальной собственности | Обучающийся демонстрирует необходимые навыки практической охраны интеллектуальной собственности | Обучающийся успешно применяет навыки практической охраны интеллектуальной собственности |
| Владеть навыками хранения и защиты компьютерной информации | Обучающийся не владеет навыками хранения и защиты компьютерной информации | Обучающийся демонстрирует слабые навыки хранения и защиты компьютерной информации | Обучающийся демонстрирует необходимые навыки хранения и защиты компьютерной информации | Обучающийся успешно применяет навыки хранения и защиты компьютерной информации |
| Владеть навыками построения подсистем безопасности информационных систем | Обучающийся не владеет навыками построения подсистем безопасности информационных систем | Обучающийся демонстрирует слабое владение навыками построения подсистем безопасности информационных систем | Обучающийся демонстрирует необходимое владение навыками построения подсистем безопасности информационных систем | Обучающийся успешно применяет навыки построения подсистем безопасности информационных систем |

# 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

## 6.1. Материально-техническое обеспечение

| № | Наименование специальных помещений и помещений для самостоятельной работы | Оснащенность специальных помещений и помещений для самостоятельной работы |
|---|---|---|
| 1 | Специализированный компьютерный класс МК229 | Мультимедийный проектор, экран, ноутбук; 15 персональных компьютеров с выходом в интернет, проектор, 10 комплектов оборудования для моделирования систем NI Elvis II и Matlab |
| 2 | Лаборатория теории автоматического управления и моделирования средств управления МК231 | Аналоговые вычислительные комплексы АВК 6, аналоговые вычислительные комплексы АВК 31, аналоговые вычислительные комплексы АВК 32, 6 высокопроизводительных компьютеров, проектор, 3D-принтер, 3D-сканер, стенд для исследования мобильных роботов |
| 3 | Специализированная лаборатория «Микроконтроллеры в системах автоматизации» МК208 | микроконтроллеры и стенды на основе микропроцессоров (5 стендов), промышленные контроллеры VIPA, Segnetics, ОВЕН, Siemens S7-200, 300, 400, 1200, 1500, LOGO!, 32-х разрядные |

| | | |
|---|---|---|
| | | микроконтроллеры 1986ВЕ93У производства АО «ПКК Миландр» с отладочными платами (8 комплектов) |
| 4 | Читальный зал библиотеки для самостоятельной работы | Компьютерная техника, подключенная к сети «Интернет» и имеющая доступ в электронно-информационную образовательную среду; специализированная мебель |
| 5 | Методический кабинет | Специализированная мебель; мультимедийный проектор, переносной экран, ноутбук |

## 6.2. Лицензионное и свободно распространяемое программное обеспечение

| № | Перечень лицензионного программного обеспечения | Реквизиты подтверждающего документа |
|---|---|---|
| 1 | Microsoft Windows 10 Корпоративная | Соглашение Microsoft Open Value Subscription V6328633. Соглашение действительно с 02.10.2017 по 31.10.2023). Договор поставки ПО 0326100004117000038-0003147-01 от 06.10.2017 |
| 2 | Microsoft Office Professional Plus 2016 | Соглашение Microsoft Open Value Subscription V6328633. Соглашение действительно с 02.10.2017 по 31.10.2023 |
| 3 | Kaspersky Endpoint Security «Стандартный Russian Edition» | Сублицензионный договор № 102 от 24.05.2018. Срок действия лицензии до 19.08.2020<br>Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования (лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2022г. |
| 4 | Matlab Simulink | Лицензия №1145851 бессрочная |
| 5 | MSC Easy5, Patran, Nastran, Adams | Соглашение RE008959BST-1 от 26.11.2018 |
| 6 | Google Chrome | Свободно распространяемое ПО согласно условиям лицензионного соглашения |
| 7 | Mozilla Firefox | Свободно распространяемое ПО согласно условиям лицензионного соглашения |
| 8 | Master SCADA 4D | Свободно распространяемое ПО согласно условиям лицензионного соглашения |
| 9 | MasterSCADA v. 3.4 | 16410414_3193 (1 компьютер, HASP-ключ) бессрочная |

## 6.3. Перечень учебных изданий и учебно-методических материалов


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.
9. Каторин, Ю.Ф. Энциклопедия промышленного шпионажа / сост. Ю. Ф. Каторин [и др.]; ред. Е. В. Куренков. – СПб: Полигон, 2000. – 512 с.
10. 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.
11. Никифоров, С.В. Введение в сетевые технологии: Элементы применения и администрирования сетей: учеб. пособие / С. В. Никифоров. – М: Финансы и статистика, 2003. – 224 с.
12. Бабаш, А.В. Криптография: учеб. пособие / А. В. Бабаш, Г. П. Шанкин. – М: СОЛОН-Р, 2002. – 511 с.
13. 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.
14. 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.
15. 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.
16. 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.

### 6.4. Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем

1. http://www.elibrary.ru- Научная электронная библиотека
2. http://www.gpntb.ru/- Государственная публичная научно-техническая библиотека Росии
3. http://elibrary. bmstu./ru – Библиотека МГТУ им. Н.Баумана
4. http://www.viniti.ru – Всероссийский институт научной информации по техническим наукам(ВИНИТИ)
5. http://www.unilib.neva.ru/rus/- Фундаментальная библиотека Санкт-Петербургского государственного политехнического университета
6. http://elibrary.eltech.ru – Библиотека Санкт-Петербургского государственного электротехнического университета
7. http://www.ntb.bstu.ru и переход к системе NormaCS - Электронно-библиотечная система БГТУ им В.Г.Шухова
8. http://scholar.google.com/ – научный Google, со всеми его гигантскими достоинствами и определенными маркетинговыми особенностями.

## УТВЕРЖДЕНИЕ РАБОЧЕЙ ПРОГРАММЫ

Рабочая программа утверждена на 20_____ / 20_____ учебный год без изменений.

Протокол № _____ заседания кафедры от «____» _____ 20____ г.

Зав. кафедрой _____ В. Г. Рубанов
подпись ФИО

Директор института _____ И. В. Ярмоленко
подпись ФИО