ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Петербургский государственный университет путей сообщения

Императора Александра I»

(ФГБОУ ВО ПГУПС)

Кафедра «Информатика и информационная безопасность»

**РАБОЧАЯ ПРОГРАММА**

*дисциплины*

«БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ» (Б1.Б.8)

для специальности

10.05.03 «Информационная безопасность автоматизированных систем»

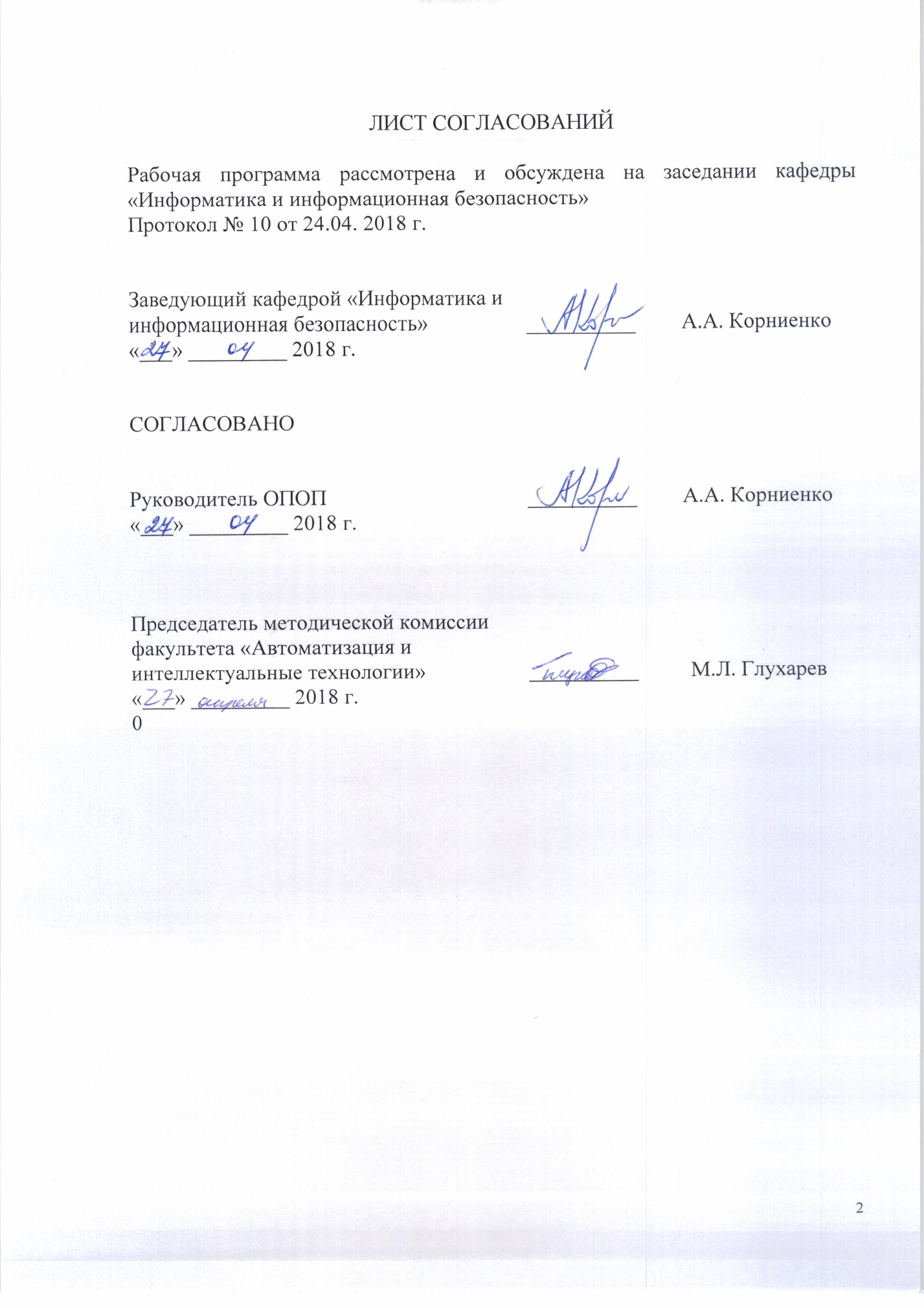
по специализации

«Информационная безопасность автоматизированных системна транспорте»

Форма обучения – очная

Санкт-Петербург

2018



**1. Цели и задачи дисциплины**

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным от 01.12.2016, приказ № 1509по специальности 10.05.03 «Информационная безопасность автоматизированных систем» по специализации «Информационная безопасность автоматизированных систем на транспорте» по дисциплине «Безопасность операционных систем» (Б1.Б.8).

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других базовых дисциплин профессионального цикла в соответствии с требованиями, установленными федеральным государственным образовательным стандартом для формирования у выпускника профессиональных компетенций, способствующих решению профессиональных задач в соответствии с видами профессиональной деятельности: научно-исследовательская, проектная, контрольно-аналитическая,организационно-управленческая, эксплуатационная и специализацией «Информационная безопасность автоматизированных систем на транспорте».

Для достижения поставленной цели определены следующие задачи изучения дисциплины:

* подготовка студента по разработанной в университете основной образовательной программе к успешной аттестации планируемых конечных результатов освоения дисциплины;
* подготовка студента к изучению дисциплин, определённых учебным планом в соответствии с указанными компетенциями;
* развитие социально-воспитательного компонента учебного процесса.

При изучении дисциплины решаются следующие конкретные задачи:

* изучение основных принципов построения, назначения и функций операционных систем;
* изучение управления задачами и ресурсами в операционных системах;
* изучение требований к защите операционных систем;
* изучение разграничения доступа в операционных системах;
* изучение аудита в операционных системах.

**2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы**

Планируемыми результатами обучения по дисциплине являются: приобретение знаний, умений, навыков и/или опыта деятельности.

В результате освоения дисциплины обучающийся должен:

**ЗНАТЬ:**

– принципы построения и функционирования, примеры реализаций современных операционных систем;

– функции операционных систем, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;

– критерии оценки эффективности и надежности средств защиты операционных систем;

– принципы организации и структуру подсистем защиты операционных систем семейств UNIX и Windows;

**УМЕТЬ:**

– использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;

– оценивать эффективность и надежность защиты операционных систем;

– планировать политику безопасности операционных систем;

**ВЛАДЕТЬ:**

– навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;

– навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности;

– навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности.

Приобретенные знания, умения, навыки и/или опыт деятельности, характеризующие формирование компетенций, осваиваемые в данной дисциплине, позволяют решать профессиональные задачи, приведенные в соответствующем перечне по видам профессиональной деятельности в п. 2.4 основной профессиональной образовательной программы (ОПОП).

Изучение дисциплины направлено на формирование следующих **профессиональных компетенций (ПК)**, соответствующих видам профессиональной деятельности, на которые ориентирована программа специалитета:

*научно-исследовательская деятельность:*

– способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

– способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ (ПК-7);

*эксплуатационная деятельность:*

– способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-26).

Область профессиональной деятельности обучающихся, освоивших данную дисциплину, приведена в п. 2.1 ОПОП.

Объекты профессиональной деятельности обучающихся, освоивших данную дисциплину, приведены в п. 2.2 ОПОП.

**3. Место дисциплины в структуре основной профессиональной образовательной программы**

Дисциплина «Безопасность операционных систем» (Б1.Б.8) относится к базовой части и является обязательной.

**4. Объем дисциплины и виды учебной работы**

|  |  |  |  |
| --- | --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестр** | |
| **5** | **6** |
| Контактная работа (по видам учебных занятий)  В том числе:   * лекции (Л) * практические занятия (ПЗ) * лабораторные работы (ЛР) | 148  66  16  66 | 64  32  32 | 84  34  16  34 |
| Самостоятельная работа (СРС) (всего) | 95 | 26 | 69 |
| Контроль | 45 | 36 | 9 |
| Форма контроля знаний | Э,З,КР | Э | З, КР |
| Общая трудоемкость: час / з.е. | 288/8 | 126/3,5 | 162/4,5 |

**5. Содержание и структура дисциплины**

5.1 Содержание дисциплины

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
|  | Модуль 1 | |
| 1 | Введение в операционные системы | Понятие операционной системы (ОС). Функции ОС. Эволюция ОС. Виды ОС.  Многозадачность. Понятие многозадачности. Виды многозадачности. |
| 2 | Процессы и потоки | Мультипроцессирование: определение, примеры.  Мультипрограммирование (Многозадачность). Планирование. Понятие процесса. Состояние процессов. Виртуальная память.  Создание процессов и потоков. Описатель процесса. Потоки-потомки.  Очереди процессов. Алгоритмы планирования на основе квантования. Алгоритмы планирования на основе приоритетов. Абсолютные и относительные приоритеты. Смешанные алгоритмы планирования.  Планирование в системах реального времени. Виды систем реального времени. Типы запросов в системах реального времени.  Моменты перепланировки. Перепланировка потоков.  Механизм прерываний. Назначение и типы прерываний. Способы прерываний. Программные прерывания. Диспетчеризация и приоритезация прерываний в ОС. Функции централизованного диспетчера прерываний. Обработка прерываний. Процедуры обработки прерываний и текущий процесс.  Синхронизация процессов и потоков. Цели и средства синхронизации. Необходимость синхронизации и гонки. Гонка условий или гонка данных. Критические секции: блокировка. Семафоры. Тупики. Синхронизирующие объекты ОС. Сигналы.  Требования к реализации системных вызовов. Виды системных вызовов. |
| 3 | Управление памятью | Функции ОС по управлению памятью. Типы адресов. Типы виртуальных адресных пространств.  Алгоритмы распределения памяти. Распределение памяти фиксированными разделами. Распределение памяти динамическими разделами. Распределение памяти перемещаемыми разделами.  Свопинг и виртуальная память. Страничное распределение памяти. Сегментное распределение памяти.  Хранение данных. Кэш-память. Типы запоминающих устройств. ПЗУ.  ОЗУ. Иерархия запоминающих устройств.  Кэш-память. Определение. Принцип действия. Схема функционирования. Время доступа. Проблема согласования данных. Способы отображения основной памяти на кэш. Уровни кэш-памяти процессора. |
| 4 | Файловая система | Файл и файловая система. Виды логической организации файловой системы. Монтирование файловых систем  Типы файловых систем. Физическая организация файловой системы и адресация файла. Файловые операции  Организация контроля доступа к файлам. Модели доступа к файлам. Механизм проверки прав доступа. |
| 5 | Концепции распределенной обработки в сетевых ОС | Буферизация в примитивах передачи сообщений.Буферизация в блокирующих примитивах.Буферизация в неблокирующих примитивах.Надежные и ненадежные примитивы: виды и отличия.  Передача сообщений.Механизм Sockets ОС UNIX. Определение. Требования к реализации. Системные вызовы. |
|  | Модуль 2 | |
| 6 | Угрозы безопасности ОС | Классификация угроз информационной безопасности ОС. Основные угрозы безопасности для ОС.  Понятие безопасной ОС. Подходы к организации защиты. Административные меры. Этапы построения защиты. Требования к подсистеме аудита. Политика аудита ОС. |
| 7 | Типовая архитектура подсистемы защиты ОС | Идентификация и аутентификация пользователей. Идентификация и аутентификация на основе многоразового пароля.Идентификация и аутентификацияс помощью внешних носителей ключевой информации.Аутентификация на основе цифрового сертификата. Идентификация и аутентификация с помощью биометрических характеристик пользователей.  Управление доступом. Избирательное и полномочное разграничение доступа. Изолированная программная среда.  Аудит безопасности ОС. |
| 8 | Особенности защиты в операционных системах семейства UNIX | Подсистема идентификации и аутентификации Пользовательский идентификатор. Файлы паролей пользователя. Групповой идентификатор.  Подсистема разграничения доступа. Объекты и субъекты доступа. Механизм разграничения доступа к ресурсам. Изменение прав доступа к ресурсам системы.  Подсистема аудита. |
| 9 | Особенности защиты в операционных системах семейства WINDOWS | Подсистема идентификации и аутентификации. Архитектура подсистемы аутентификации. Параметры аутентификации.  Подсистема разграничения доступа. Объекты и субъекты доступа. Атрибуты безопасности пользователя.  Подсистема аудита. |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1 | Введение в операционные системы | 4 |  |  | 2 |
| 2 | Процессы и потоки | 10 |  | 10 | 8 |
| 3 | Управление памятью | 8 |  | 10 | 8 |
| 4 | Файловая система | 4 |  | 6 | 4 |
| 5 | Концепции распределенной обработки в сетевых ОС | 6 |  | 6 | 4 |
| 6 | Угрозы безопасности ОС | 4 | 4 |  | 10 |
| 7 | Типовая архитектура подсистемы защиты ОС | 8 | 12 |  | 11 |
| 8 | Особенности защиты в операционных системах семейства UNIX | 10 |  | 34 | 24 |
| 9 | Особенности защиты в операционных системах семейства WINDOWS | 12 |  |  | 24 |
| **Итого** | | 66 | 16 | 66 | 95 |

**6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Наименование раздела дисциплины** | **Перечень учебно-методического обеспечения** |
| 1 | Введение в операционные системы | Стащук, П.В. Краткое введение в операционные системы. М. : ФЛИНТА, 2014. 124 с. |
| 2 | Процессы и потоки | Стащук, П.В. Краткое введение в операционные системы. М. : ФЛИНТА, 2014. 124 с. |
| 3 | Управление памятью | Стащук, П.В. Краткое введение в операционные системы. М. : ФЛИНТА, 2014. 124 с. |
| 4 | Файловая система | Стащук, П.В. Краткое введение в операционные системы. М. : ФЛИНТА, 2014. 124 с. |
| 5 | Концепции распределенной обработки в сетевых ОС | Стащук, П.В. Краткое введение в операционные системы. М. : ФЛИНТА, 2014. 124 с. |
| 6 | Угрозы безопасности ОС | 1. Диасамидзе С. В.Безопасность операционных систем: учебное пособие. – СПб: ПГУПС, 2018. – 75 с.  2. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях.— М. : ДМК Пресс, 2012. — 592 с. |
| 7 | Типовая архитектура подсистемы защиты ОС | 1. Диасамидзе С. В.Безопасность операционных систем: учебное пособие. – СПб: ПГУПС, 2018. – 75 с.  2. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. — М. : ДМК Пресс, 2012. — 592 с. |
| 8 | Особенности защиты в операционных системах семейства UNIX | 1. Диасамидзе С. В.Безопасность операционных систем: учебное пособие. – СПб: ПГУПС, 2018. – 75 с.  2. Войтов, Н.М. Основы работы с Linux. Учебный курс.— М. : ДМК Пресс, 2010. — 216 с. |
| 9 | Особенности защиты в операционных системах семейства WINDOWS | 1. Диасамидзе С. В.Безопасность операционных систем: учебное пособие. – СПб: ПГУПС, 2018. – 75 с.  2. Нортон, П. Полное руководство по MicrosoftWindows XP.— М. : ДМК Пресс, 2009. — 733 с. |

**7. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине**

Фонд оценочных средств по дисциплине является неотъемлемой частью рабочей программы и представлен отдельным документом, рассмотренным на заседании кафедры и утвержденным заведующим кафедрой.

**8. Перечень основной и дополнительной учебной литературы, нормативно-правовой документации и других изданий, необходимых для освоения дисциплины**

8.1 Перечень основной учебной литературы, необходимой для освоения дисциплины

1. Стащук, П.В. Краткое введение в операционные системы. [Электронный ресурс] — Электрон. дан. — М. : ФЛИНТА, 2014. — 124 с. — Режим доступа: <http://e.lanbook.com/book/63042>

2. Диасамидзе С. В.Безопасность операционных систем: учебное пособие. – СПб: ПГУПС, 2018. – 75 с.

3. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. [Электронный ресурс] — Электрон.дан. — М. : ДМК Пресс, 2012. — 592 с. — Режим доступа: <http://e.lanbook.com/book/3032>

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Войтов, Н.М. Основы работы с Linux. Учебный курс. [Электронный ресурс] — Электрон.дан. — М. : ДМК Пресс, 2010. — 216 с. — Режим доступа: <http://e.lanbook.com/book/1198>

2. Нортон, П. Полное руководство по MicrosoftWindows XP. [Электронный ресурс] / П. Нортон, Д. Мюллер. — Электрон.дан. — М. : ДМК Пресс, 2009. — 733 с. — Режим доступа: <http://e.lanbook.com/book/1195>

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

При освоении данной дисциплины нормативно-правовая документация не используется.

8.4 Другие издания, необходимые для освоения дисциплины

При освоении данной дисциплины другие издания не используются.

**9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

1. Сайт научно-технической библиотеки университета: <http://library.pgups.ru/jirbis/index.php?option=com_irbis&Itemid=300>
2. Проект «Информационная безопасность». <http://www.itsec.ru/>
3. Проект IT <http://citforum.ru/>
4. Проект «Национальный Открытый Университет «ИНТУИТ»http://www.intuit.ru/

**10. Методические указания для обучающихся по освоению дисциплины**

Порядок изучения дисциплины следующий:

1. Освоение разделов дисциплины производится в порядке, приведенном в разделе 5 «Содержание и структура дисциплины». Обучающийся должен освоить все разделы дисциплины с помощью учебно-методического обеспечения, приведенного в разделах 6, 8 и 9 рабочей программы.
2. Для формирования компетенций обучающийся должен представить выполненные типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, предусмотренные текущим контролем (см. фонд оценочных средств по дисциплине).
3. По итогам текущего контроля по дисциплине, обучающийся должен пройти промежуточную аттестацию (см. фонд оценочных средств по дисциплине).

**11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем**

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине:

* технические средства (компьютерная техника и средства связи(персональные компьютеры, проектор, интерактивная доска,видеокамеры, акустическая система и т.д.);
* методы обучения с использованием информационных технологий(компьютерное тестирование, демонстрация мультимедийныхматериалов, компьютерный лабораторный практикум и т.д.);
* перечень Интернет-сервисов и электронных ресурсов (поисковыесистемы, электронная почта, профессиональные, тематические чаты ифорумы, системы аудио и видео конференций, онлайн-энциклопедии исправочники, электронные учебные и учебно-методические материалы).

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:

* Microsoft Windows 7;
* Microsoft Word 2010;
* MicrosoftExcel 2010;
* MicrosoftPowerPoint 2010;
* VirtualBox (бесплатное, свободно распространяемое программное обеспечение, режим доступа <https://www.virtualbox.org>).
* Lunix Ubuntu (бесплатное, свободно распространяемое программное обеспечение, режим доступа <http://ubuntu.ru>).
* WireShark (бесплатное, свободно распространяемое программное обеспечение, режим доступа <https://www.wireshark.org/download.html>).
* SpyNet (бесплатное, свободно распространяемое программное обеспечение, режим доступа <http://laurentiu-nicula.software.informer.com>).
* перечень прикладного программного обеспечения (системы тестирования, профессиональные пакеты прикладных программ, программы-тренажеры, программы-симуляторы) перечень информационных справочных систем.

**12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Материально-техническая база обеспечивает проведение всех видов учебных занятий, предусмотренных учебным планом по даннойспециальности и соответствует действующим санитарным и противопожарным нормам и правилам.

Она содержит:

* помещения для проведения лабораторных работ, укомплектованных специальной учебно-лабораторной мебелью, лабораторным оборудованием, лабораторными стендами, специализированными измерительными средствами в соответствии с перечнем лабораторных работ.
* помещения для проведения лекционных и практических (семинарских) занятий, укомплектованных специализированной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (настенным экраном с дистанционным управлением, подвижной маркерной доской, считывающим устройством для передачи информации в компьютер, мультимедийным проектором и другими информационно-демонстрационными средствами).

|  |  |  |
| --- | --- | --- |
| Разработчик программы, доцент  «23» апреля 2018 г. |  | С.В. Диасамидзе |