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*

«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» (Б1.Б.17)

для специальности

10.05.03 «Информационная безопасность автоматизированных систем»

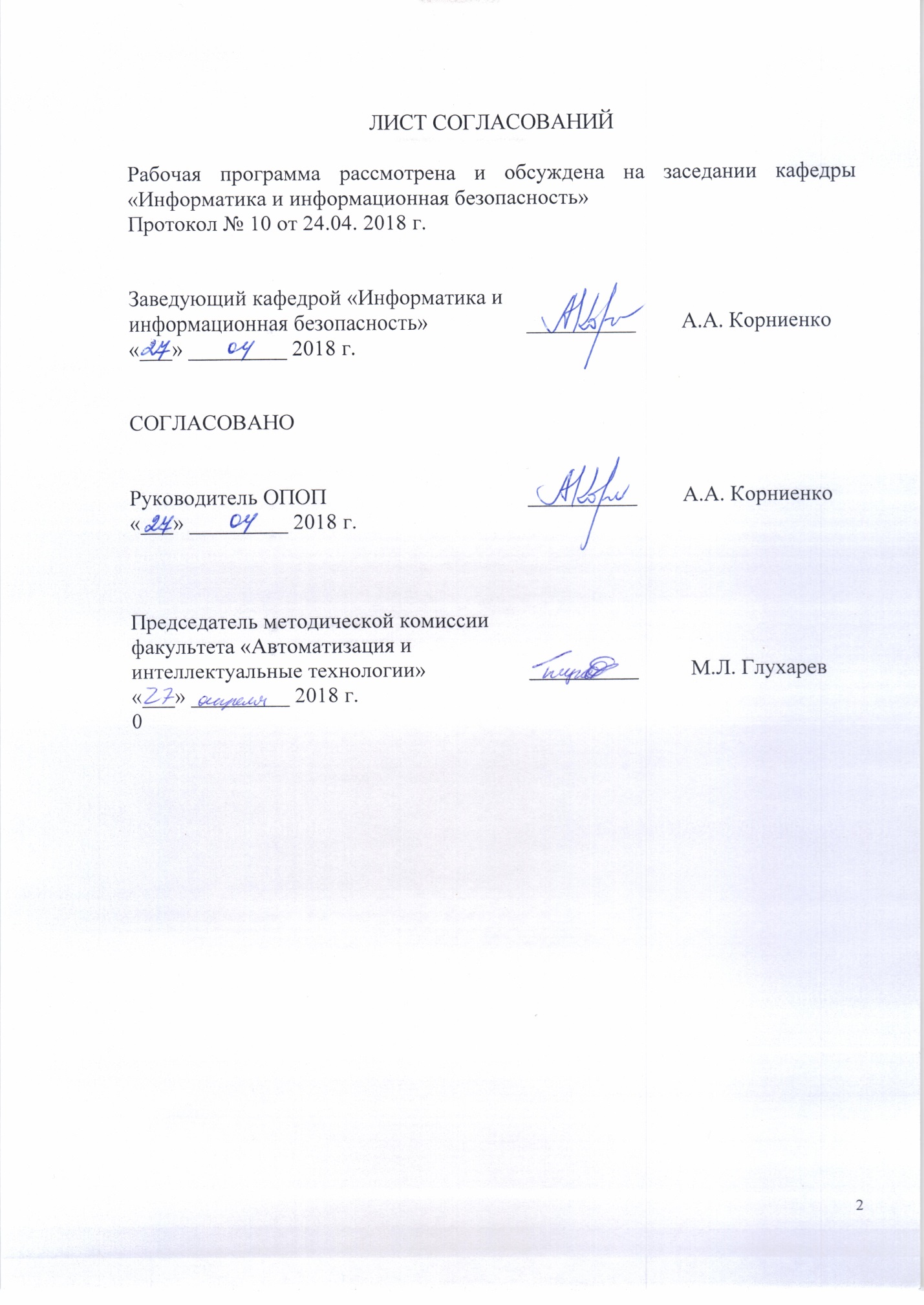
по специализации

«Информационная безопасность автоматизированных систем на транспорте»

Форма обучения – очная

Санкт-Петербург

2018



**1. Цели и задачи дисциплины**

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным «01» декабря 2016 г., приказ № 1509 по направлению 10.05.03 «Информационная безопасность автоматизированных систем», по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности».

Цель изучения дисциплины «Программно-аппаратные средства обеспечения информационной безопасности» состоит в изучении основных принципов создания программно-аппаратных средств обеспечения информационной безопасности, концепции диспетчера доступа; программно-аппаратных средств, реализующих отдельные функциональные требования по защите, их принципов действия и технологических особенностей, взаимодействия с общесистемными компонентами вычислительных систем; методов и средств ограничения доступа к компонентам вычислительных систем; методов и средств привязки программного обеспечения к аппаратному окружению и физическим носителям; методов и средств хранения ключевой информации; защиты программ от изучения, способов встраивания средств защиты в программное обеспечение; защиты от разрушающих программных воздействий, защиты программ от изменения и контроль целостности, построения изолированной программной среды; задач и технологии сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основных категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратных средств защиты информации в сетях передачи данных..

Для достижения поставленной цели решаются следующие задачи:

* Знакомство с основами создания программно-аппаратных средств обеспечения информационной безопасности;
* Изучение концепций построения диспетчеров доступа;
* Изучение взаимодействия программно-аппаратных средств обеспечения информационной безопасности с общесистемными компонентами вычислительных систем;
* Изучение методов и средств ограничения доступа к компонентам вычислительных систем.

**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 опыта деятельности в области производства и эксплуатации программно-аппаратных средств обеспечения информационной безопасности.

В результате освоения дисциплины обучающийся должен:

**ЗНАТЬ:**

* основные принципы создания программно-аппаратных средств обеспечения информационной безопасности;
* концепции построения диспетчера доступа;
* методы и средства ограничения доступа к компонентам вычислительных систем;
* методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям;
* методы и средства хранения ключевой информации;
* способы встраивания средств защиты в программное обеспечение;
* основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.

**УМЕТЬ*:***

* использовать на практике, основные, представленные на рынке, аппаратно-программные средства обеспечения информационной безопасности;
* выполнять привязку программного обеспечения системы защиты информации к аппаратному окружению и физическим носителям;
* использоватьтехническую документацию для корректной и непротиворечивой настройки механизмов безопасности программно-аппаратных средств обеспечения информационной безопасности;
* использовать средства хранения ключевой информации и способы встраивания аппаратных компонентов средств защиты в программное обеспечение;
* оценивать эффективность и надежность функционирования программно-аппаратных средств обеспечения информационной безопасности;
* выявлять уязвимости защиты программно-аппаратных средств обеспечения информационной безопасности и предотвращать их использование для взлома защиты;
* разрабатывать предложения по совершенствованиюприменения программно-аппаратных средств обеспечения информационной безопасности на предприятии.

**ВЛАДЕТЬ:**

* навыками администрирования программно-аппаратных средств обеспечения информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте;
* профессиональной терминологией в области программно-аппаратных средств обеспечения информационной безопасности;
* навыками корректного использования программно-аппаратных средств обеспечения 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 **общепрофессиональных компетенций (ОПК)**:

* способности к освоению новых образцов программных, технических средств и информационных технологий(ОПК-8).

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

**научно-исследовательская деятельность:**

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

**эксплуатационная деятельность:**

* способности 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 образовательной программы**

Дисциплина «Программно-аппаратные средства информационной безопасности» (Б1.Б.17) относится к базовой части профессионального цикла и является обязательной дисциплиной.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестр** | |
| **VII** | **VIII** |
| Контактная работа (по видам учебных занятий)  В том числе:   * лекции (Л) * практические занятия (ПЗ) * лабораторные работы (ЛР) | 80  32  16  32 | 32  16  16 | 48  16  16  16 |
| Самостоятельная работа (СРС) (всего) | 55 | 40 | 15 |
| Контроль | 45 | 36 | 9 |
| Форма контроля знаний | Э,З | Э | З |
| Общая трудоемкость: час / з.е. | 180/5 | 108/3 | 72/2 |

**5. Содержание и структура дисциплины**

5.1 Содержание дисциплины

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Архитектура систем защиты информации | Требования к защите компьютерной информации  Анализ защищенности современных ОС  Подходы к проектированию СЗИ  Оценивание эффективности СЗИ при их проектировании  Проектирование СЗИ  Системный подход к проектированию систем защиты  Архитектура СЗИ  Особенности архитектуры сетевой СЗИ  Анализ эффективности СЗИ |
| 2 | Авторизация и управление доступом | Авторизация и ее задачи  Добавочные механизмы парольной защиты  Классификация объектов и субъектов доступа |
| 3 | Модели управления доступом | Канонические модели управления доступом  Реализация моделей доступа.  Общие положения по реализации управления доступом  Особенности настройки механизмов управления доступом  Субъект доступа «Процесс»  Особенности разграничения доступа к разным ресурсам  Локализация прав доступа и практические примеры управления доступом  Особенности использования субъекта «процесс» и организация замкнутой программной среды  Формальная модель диспетчера доступа |
| 4 | Реализация механизмов защиты | Моделирование рабочей станции без системы защиты  Моделирование рабочей станции с системой защиты  Влияние добавочных средств на загрузку вычислительной системы  Механизм контроля целостности  Использование аппаратных средств защиты  Противодействие переводу программного обеспечения СЗИ в пассивное состояние |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | Архитектура систем защиты информации | 10 | - | 10 | 15 |
| 2 | Авторизация и управление доступом | 6 | - | 6 | 15 |
| 3 | Модели управления доступом | 8 | - | 16 | 15 |
| 4 | Реализация механизмов защиты | 8 | 16 | - | 10 |
| **Итого** | | 32 | 16 | 32 | 55 |

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

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела** | **Перечень учебно-методического обеспечения** |
| 1 | Архитектура систем защиты информации | Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. 448 с.  РД Гостехкомиссии: Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. – М.:1992.  РД Гостехкомиссии: Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. – М.:1992. |
| 2 | Авторизация и управление доступом | Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. 448 с.  РД Гостехкомиссии: Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. – М.:1992. |
| 3 | Модели управления доступом | Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. 448 с.  РД Гостехкомиссии: Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. – М.:1992. |
| 4 | Реализация механизмов защиты | Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. 448 с.  РД Гостехкомиссии: Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. – М.:1992.  РД Гостехкомиссии: Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. – М.:1992. |

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

Фонд оценочных средств по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» является неотъемлемой частью рабочей программы и представлен отдельным документом, рассмотренным на заседании кафедры «Информатика и информационная безопасность» 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. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. 448 с.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. А.А. Корниенко, С. Е. Ададуров, А.П. Глухов . Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: / под ред. А. А. Корниенко. – Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. 440 с.
2. Технические средства и методы защиты информации : учебное пособие / под ред. А. П. Зайцева и А. А. Шелупанова. - [4-е изд., испр. и доп.]. - Москва : Горячая линия - Телеком, 2012. - 615 с.
3. Технические средства и методы защиты информации : учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. - 7-е изд. - Москва : Горячая линия - Телеком, 2012. - 442 с.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. РД Гостехкомиссии: Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации. – М.:1992 г.
2. РД Гостехкомиссии: Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации. – М.:1992 г.

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

1. Личный кабинет обучающегося и электронная информационно-образовательная среда [Электронный ресурс]. – Режим доступа: [http://sdo.pgups.ru/](https://clck.yandex.ru/redir/nWO_r1F33ck?data=NnBZTWRhdFZKOHQxUjhzSWFYVGhXU3JfTEdTY2JPeVRZR0xKdjAzQkRCSko1NlJTd2UxVnRZOWJ3NkhNSG5nRGFZbGdOVmE4T194clZwME1VcDhFOU5VcjlaUDk0MWF3QWMzZU9idjVRajA&b64e=2&sign=5a9122886b8d18119545f9ca08079cfb&keyno=17) (для доступа к полнотекстовым документам требуется авторизация).

2. Научно-техническая библиотека университета [Электронный ресурс]. – Режим доступа: [http://library.pgups.ru/](https://clck.yandex.ru/redir/nWO_r1F33ck?data=NnBZTWRhdFZKOHQxUjhzSWFYVGhXZDVCOHVPSVNvZHd3VEZ4ZVFxVlJnRm1UVG9fYjAzVWJ2S1NkUlQ1Tld6ZjFCRFZ6dDFvd2FLU2k0Unh3T0ZkYmFtcXE5X2prQmdiRlgyaGVtejFSUmNldVBOc3ZjdnFfcktNb3haSDJNZlRJYzA1bEE0NS1fWVlSRlBoeU53dVFPeDNXN3drUE9WWDVHYUFKNkctQ29aOXZwYkxFNEQwM1E&b64e=2&sign=70e725131d005c182709ee9e58f210d4&keyno=17) (свободный доступ).

3. Гарант Информационно-правовой портал [Электронный ресурс]– Режим доступа: <http://www.garant.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;
* Блокпост-Экран 2000/ХР - Лицензия ООО “Газинформсервис» от 17.05.2017;
* Блокпост-2000/ХР - Лицензия ООО “Газинформсервис» от 17.05.2017;
* Блокхост-Сеть К - Лицензия ООО “Газинформсервис» от 17.05.2017;
* Блокхост-МДЗ - Лицензия ООО “Газинформсервис» от 17.05.2017;
* Litoria Desktop - Лицензия ООО “Газинформсервис» от 17.05.2017; .

**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 данной специальности и соответствует действующим санитарным и противопожарным нормам и правилам.

Она содержит:

* помещение для проведения лабораторных работ (ауд. 2-110), укомплектованное специальной учебно-лабораторной мебелью, лабораторным оборудованием, лабораторными стендами, специализированными измерительными средствами в соответствии с перечнем лабораторных работ (требования к помещениям в соответствии с ФГОС).
* помещение для проведения лекционных занятий (ауд. 2-113), укомплектованное 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) (требования к помещениям в соответствии с ФГОС).
* помещение для проведения групповых и индивидуальных консультаций (ауд. 2-110) (требования к помещениям в соответствии с ФГОС).
* помещение для проведения текущего контроля и промежуточной аттестации (ауд. 2-110) (требования к помещениям в соответствии с ФГОС).
* помещения для самостоятельной работы (ауд. 2-110) (требования к помещениям в соответствии с ФГОС).



|  |  |  |
| --- | --- | --- |
| Разработчик программы, профессор | \_\_\_\_\_\_\_\_\_\_\_\_ | В.Н. Кустов |
| |  | | --- | | 12.04.2018 г. | |  |  |