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*

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ ТРАНСПОРТНЫХ СИСТЕМ» (Б1.Б.38)

для специальности

10.05.03 «Информационная безопасность автоматизированных систем»

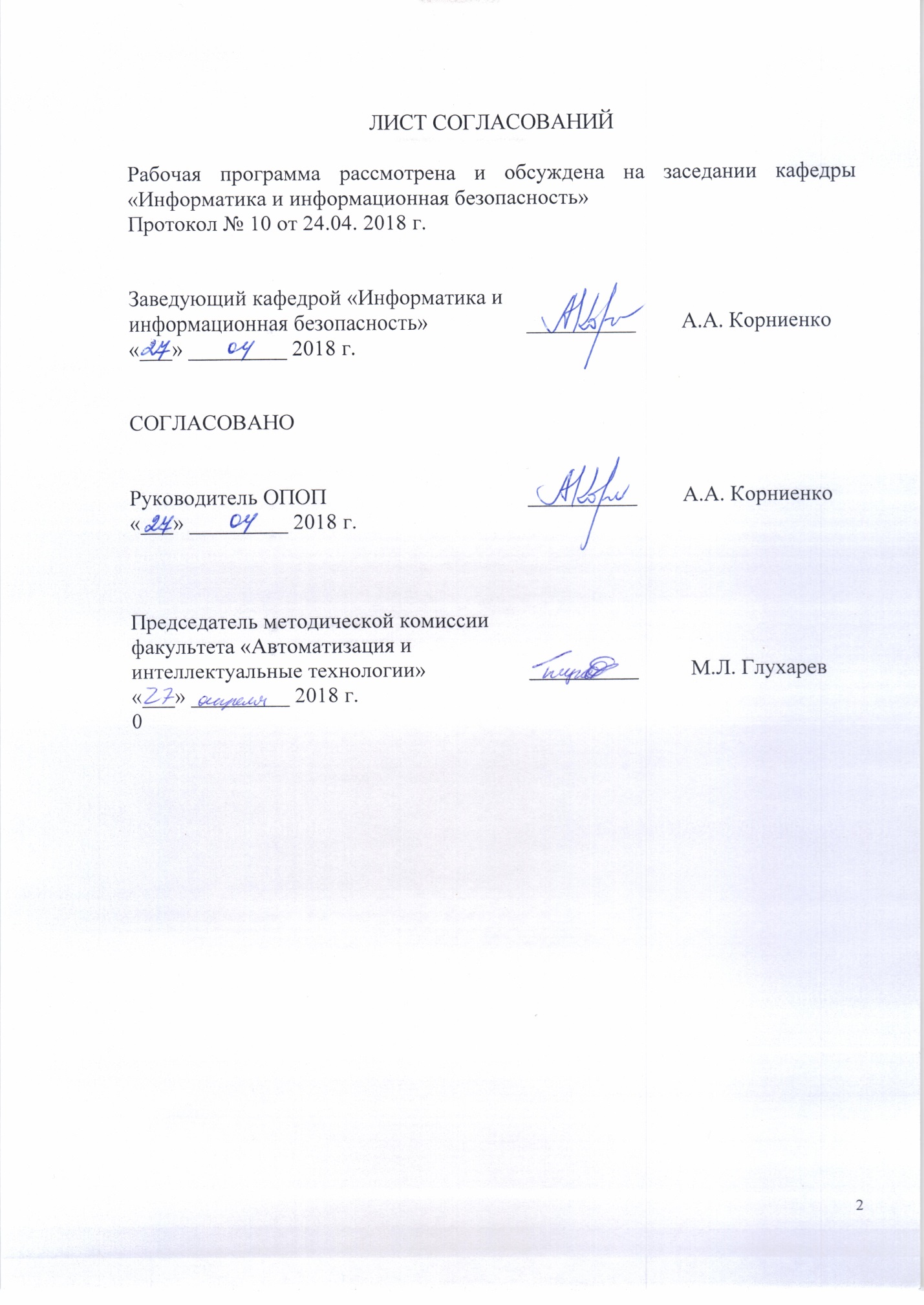
по специализации

«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 от 01.12.2016, приказ № 1509 по специальности 10.05.03 «Информационная безопасность автоматизированных систем» по специализации «Информационная безопасность автоматизированных систем на транспорте» по дисциплине «Информационная безопасность автоматизированных транспортных систем» (Б1.Б.38).

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 методологии проведения комплексного анализа защищенности и ин­ст­ру­мен­таль­ного мо­ни­то­рин­га автоматизированных транспортных систем;

- изучение принципов проектирования и оценивания надежности результатов разработки программных элементов автоматизированных транспортных систем;

- анализ возможностей эксплуатации программно-аппаратных средств защиты автоматизированных транспортных систем с учетом специфики угроз информации в них.

**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 применения и построения ERP-систем (систем управления ресурсами предприятия) и PLM-технологий (технологий поддержки жизненного цикла), методы и средства обеспечения их информационной безопасности;

**УМЕТЬ:**

– используя современные методы и средства, разрабатывать и оценивать модели и политики безопасности автоматизированных и информационно-управляющих систем на транспорте;

– анализировать, оценивать и исключать уязвимости информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте, применять автоматизированные средства мониторинга, аудита и анализа защищенности данных систем;

**ВЛАДЕТЬ:**

– навыками анализа угроз и уязвимостей информационной безопасности в автоматизированных и информационно-управляющих системах на транспорте;

– методами эксплуатации средств защиты информации.

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

*профессионально-специализированными компетенциями, соответствующими специализации программы специалитета:*

* способность участвовать в разработке защищенных автоматизированных, информационно-управляющих и информационно-логистических систем на транспорте (по видам) с использованием программных, программно-аппаратных и технических методов и средств защиты информации (ПСК-10.1).

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 «Информационная безопасность автоматизированных транспортных систем» (Б1.Б.38) относится базовой части и является обязательной дисциплиной.

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

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестр** |
| **9** |
| Контактная работа (по видам учебных занятий)  В том числе:   * лекции (Л) * практические занятия (ПЗ) * лабораторные работы (ЛР) | 48  32  16 | 48  32  16 |
| Самостоятельная работа (СРС) (всего) | 51 | 51 |
| Контроль | 9 | 9 |
| Форма контроля знаний | З, КП | З, КП |
| Общая трудоемкость: час / з.е. | 108/3 | 108/3 |

**5. Содержание и структура дисциплины**

5.1 Содержание дисциплины

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Система обеспечения информационной безопасности на железнодорожном транспорте | Цели, задачи и объекты обеспечения информационной безопасности  Архитектура, назначение и компоненты системы обеспечения информационной безопасности  Принципы построения и функционирования системы управления информационной безопасностью  Организационная структура и нормативная база обеспечения и управления информационной безопасностью  Корпоративные политики информатизации и информационной безопасности  Методики оценки значимости информационных ресурсов и безопасности информации  Система оценки защищенности автоматизированных информационных и телекоммуникационных систем ОАО «РЖД» |
| 2 | Информационная безопасность ERP-систем | Автоматизированные системы управления ресурсами предприятия (ERP-системы).  ERP-система компании SAP AG. Структура системы SAP Business Suit. Функциональность систем SAP. Структура программных средств системы SAP. Управление рабочими потоками и транзакции SAP. Основы администрирования SAP.  Общая характеристика ERP-систем российских железных дорог как объектов информационной безопасности.  Профиль защиты ЕК АСУФР. Задание по безопасности ЕК АСУФР. |
| 3 | Информационная безопасность информационных транспортных систем | Основные сервисы безопасности и методы защиты информации в корпоративных информационных системах и сетях.  Системы обеспечения информационной безопасности и защиты информации корпоративного уровня. Системы управления доступом. Системы антивирусной защиты. Защищенный сегмент электронной почтовой системы. Инфраструктура открытых ключей.  Система обеспечения информационной безопасности АСУ «Экспресс-3»  Автоматизированная система ЭТРАН как объект информационной безопасности.  Кибербезопасность и защита от компьютерных атак на железнодорожном транспорте. Характеристика информационной инфраструктуры железнодорожного транспорта как объекта, потенциально подверженного компьютерным атакам. Основные принципы и меры защиты информационной инфраструктуры железнодорожного транспорта от компьютерных атак.  Основы построения интеллектуальных систем защиты информации. |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1 | Система обеспечения информационной безопасности на железнодорожном транспорте | 12 |  | 8 | 27 |
| 2 | Информационная безопасность ERP-систем | 10 |  | 8 | 12 |
| 3 | Информационная безопасность информационных транспортных систем | 10 |  |  | 12 |
| **Итого** | | 32 |  | 16 | 51 |

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

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Наименование раздела дисциплины** | **Перечень учебно-методического обеспечения** |
| 1 | Система обеспечения информационной безопасности на железнодорожном транспорте | 1. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 440 с. 2. Автоматизированные средства поддержки системы управления информационной безопасностью на железнодорожном транспорте: учебное пособие. – СПб: ПГУПС, 2016. – 45 с. |
| 2 | Информационная безопасность ERP-систем | 1. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 440 с. 2. Корпоративные информационные системы на железнодорожном транспорте. — М. : УМЦ ЖДТ, 2013. — 256 с.   3. Профили защиты и задания по безопасности корпоративных информационных систем и сетей железнодорожного транспорта: учебное пособие. – СПб: ПГУПС, 2014. – 94 с. |
| 3 | Информационная безопасность интеллектуальных транспортных систем | 1. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 440 с. 2. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 448 с. 3. Кибербезопасность и защита от компьютерных атак на железнодорожном транспорте: учебное пособие. – СПб: ПГУПС, 2015. – 50 с. 4. Васильев, В.И. Интеллектуальные системы защиты информации. — М. : Машиностроение, 2013. — 172 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. Информационная безопасность и защита информации на железнодорожном транспорте. В 2-х частях. Часть 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. — М. : УМЦ ЖДТ, 2014. — 440 с.

2. Информационная безопасность и защита информации на железнодорожном транспорте. Ч. 2: Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. - М.: УМЦ ЖДТ, 2014. – 448 с.

3. Кибербезопасность и защита от компьютерных атак на железнодорожном транспорте: учебное пособие. – СПб: ПГУПС, 2015. – 50 с.

4. Васильев, В.И. Интеллектуальные системы защиты информации. [Электронный ресурс] — Электрон. дан. — М. : Машиностроение, 2013. — 172 с. — Режим доступа: http://e.lanbook.com/book/5792

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Корниенко А.А., Поляничко М.А. Стандарты информационной безопасности (учебное пособие). – СПб.: ПГУПС, 2011. – 72 с.
2. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. - М.: Горячая линия–Телеком, 2014. - 244 с.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646);
2. Федеральные законы:
   * + - «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006;
       - «О коммерческой тайне» № 119-ФЗ от 29.07.2004;
       - «О персональных данных» № 152-ФЗ от 27.07.2006.
3. Сборник Руководящих документов Гостехкомиссии России по защите информации от несанкционированного доступа – М: Гостехкомиссия, 1998. – 120 с.
4. ГОСТ Р ИСО/МЭК 15408-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. - М.: ИПК Издательство стандартов, 2008.
5. ГОСТ Р ИСО/МЭК 27001-2013. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
6. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
7. Порядок задания требований защиты информации в АСУ ОАО «РЖД» // ОАО «РЖД», 2015.
8. Стратегия развития холдинга «РЖД» на период до 2030 года и основные приоритеты его развития на среднесрочный период до 2015 года // ОАО «РЖД», 2010.
9. СТО РЖД 1.18.002-2009 «Управление информационной безопасностью. Общие положения» // ОАО «РЖД», 2009.

8.4 Другие издания, необходимые для освоения дисциплины

1. Корниенко А.А., Диасамидзе С.В. Управление информационной безопасностью (методические указания к лабораторным работам). - СПб: ПГУПС, 2016. – 48 с.

**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. Официальный портал Росстандарта <http://www.gost.ru/wps/portal/>, портал по стандартизации <http://standard.gost.ru/wps/portal/>
3. Официальный сайт ФСТЭК России <http://www.fstec.ru/>
4. Проект «Информационная безопасность». <http://www.itsec.ru/>
5. 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;
* 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 данной специальности 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, заведующий кафедрой, проф. | \_\_\_\_\_\_\_\_\_\_\_\_ | А.А. Корниенко |
| 12.04.2018 г. |  |  |