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*

«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» (Б1.Б.16)

для специальности

10.05.03 «Информационная безопасность автоматизированных систем»

по специализации

«Информационная безопасность автоматизированных систем на транспорте»

Форма обучения – очная

Санкт-Петербург

2018



1. Цель и задачи государственной итоговой аттестации

Рабочая программа составлена в соответствии с ФГОС ВО, утвержденным «1» декабря 2016г. №1509 по направлению 10.00.00 «Информационная безопасность», по дисциплине «Организационное и правое обеспечение информационной безопасности».

Целью изучения дисциплины является расширение и углубление профессиональной подготовки в составе других базовых дисциплин вариативной части первого блока в соответствии с требованиями, установленными федеральным государственным образовательным стандартом (приказ Минобрнауки России от 1.12.2016 № 1509 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 решаются следующие задачи:

* подготовка обучающегося по разработанной в университете основной образовательной программе к успешной аттестации планируемых конечных результатов освоения дисциплины;
* подготовка обучающегося к написанию и защите «Выпускной квалификационной работы»;
* развитие социально-воспитательного компонента учебного процесса.

1. Перечень планируемых результатов 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:

* основы российской правовой системы и законодательства;
* основы правового статуса личности;
* характеристику основных отраслей российского права, правовые основы обеспечения национальной безопасности РФ;
* основные меры по защите информации в АС (организационные, правовые);
* методы аттестации уровня защищенности АС;
* нормативно-правовую базу обеспечения ИБ;
* основные отечественные и зарубежные стандарты в области ИБ;
* принципы формирования политики ИБ;основные понятия и содержание организационного обеспечения ИБ АС;
* основы комплексного обеспечения информационной безопасности автоматизированных систем на железнодорожном транспорте;
* акты в области обеспечения информационной безопасности и нормативные, методические документы ФСБ России и ФСТЭК России в области защиты информации;
* правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;
* организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
* основные угрозы безопасности информации и модели нарушителя в автоматизированных системах;
* основные методы управления информационной безопасностью;
* принципы формирования политики информационной безопасности в автоматизированных системах.

УМЕТЬ:

* использовать в практической деятельности правовые знания;
* анализировать правовые акты и осуществлять правовую оценку информации;
* предпринимать необходимые меры по восстановлению нарушенных прав;
* определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
* разрабатывать модели угроз и нарушителей ИБ АС;
* разрабатывать предложения по совершенствованию системы управления ИБ АС;
* разрабатывать проекты нормативных и методических документов, регламентирующих работы по обеспечению ИБ АС;
* используя современные методы и средства, разрабатывать и оценивать модели и политики безопасности автоматизированных и информационно-управляющих систем на железнодорожном транспорте;
* проводить мониторинг угроз безопасности компьютерных сетей;
* реализовывать политику безопасности баз данных;
* применять средства обеспечения безопасности данных;
* классифицировать защищаемую информацию по видам и грифам секретности (конфиденциальности);
* анализировать и оценивать угрозы информационной безопасности объекта;
* определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;
* разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем;
* выявлять уязвимости информационно-технологических ресурсов автоматизированных систем, проводить мониторинг угроз безопасности автоматизированных систем;
* оценивать информационные риски в автоматизированных системах;
* определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем;
* составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем;
* разрабатывать частные политики информационной безопасности автоматизированных систем;
* контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем;
* разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем.

ВЛАДЕТЬ:

* навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
* методами оценки информационных рисков;
* навыками анализа угроз и уязвимостей информационной безопасности в автоматизированных и информационно-управляющих системах на железнодорожном транспорте;
* навыками анализа угроз и навыками построения политик безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем железнодорожного транспорта;
* профессиональной терминологией в области информационной безопасности;
* навыками безопасного использования технических средств в профессиональной деятельности;
* навыками работы с нормативными правовыми актами;
* навыками организации и обеспечения режима секретности;
* методами организации и управления деятельностью служб защиты информации на предприятии;
* методами формирования требований по защите информации.

Освоение ОПОП направлено на формирование следующих общепрофессиональных компетенций (ОПК):

способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6).

Освоение ОПОП направлено на формирование следующих профессиональных компетенций (ПК), соответствующих видам профессиональной деятельности, на которые ориентирована программа специалитета:

* **научно-исследовательская деятельность:**

способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4).

* **контрольно-аналитическая деятельность:**

способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16).

* **эксплуатационная деятельность:**

способностью разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

Сформированность компетенций у обучающихся проверяется на различных этапах их формирования в соответствии с Фондами оценочных средств по дисциплинам и практикам учебного плана. Государственная итоговая аттестация направлена на проверку сформированности у обучающегося следующих компетенций: ОПК-6, ПК-1, ПК-4, ПК-9, ПК-16, ПК-21, ПК-23.

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

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

1. Место дисциплины в структуре основной профессиональной образовательной программы

«Организационное и правовое обеспечение информационной безопасности» (Б1.Б.16) относится к базовой части Блока 1 и является обязательной.

1. Объем дисциплины и виды учебной работы

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего**  **часов** | **Семестр** |
| **IV** |
| Контактная работа (по видам учебных занятий)  В том числе:   * лекции (Л) * практические занятия (ПЗ) * лабораторные работы (ЛР) | 48  16  32 | 48  16  32 |
| Самостоятельная работа (СРС) (всего) | 60 | 60 |
| Контроль | 36 | 36 |
| Форма контроля знаний | экзамен | экзамен |
| Общая трудоемкость: час / з.е. | 144 / 4 | 144 / 4 |

1. Содержание и структура дисциплины

**5.1 Содержание дисциплины**

|  |  |  |
| --- | --- | --- |
| №  п/п | Наименование раздела дисциплины | Содержание раздела |
| 1. | Российское законодательство в области информационной безопасности | Основы законодательства Российской Федерации в области информационной безопасности и защиты информации Понятие и виды информации, защищаемой законодательством Российской Федерации |
| 2. | Защита информации с ограниченным доступом | Государственная тайна и система ее защиты  Конфиденциальная информация и ее защита |
| 3. | Правовые режимы защиты информации | Правовой режим защиты государственной тайны Правовые режимы защиты конфиденциальной информации |
| 4. | Защита интеллектуальной собственности | Международное право в сфере защиты информации Защита авторских и смежных прав в законодательстве Российской Федерации |
| 5. | Организационные системы обеспечения безопасности информации | Организационные структуры государственной системы обеспечения информационной безопасности федеральных органов исполнительной власти Физическая зашита |
| 6. | Корпоративное нормативное регулирование | Корпоративная нормативная база по защите информации Политика безопасности |
| 7. | Организация объектовых режимов безопасности | Организация пропускного режима Организация внутриобъектового режима  Порядок проведения служебных расследований |
| 8. | Система подготовки кадров в области информационной безопасности в Российской Федерации | Структура системы подготовки кадров в области информационной безопасности  Состав учебно-методического обеспечения системы и ее подсистема управления Основные направления учебной деятельности |

**5.2 Разделы дисциплины и виды занятий**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Наименование раздела дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1. | Понятие национальной безопасности | 1 | 2 | - | 4 |
| 2. | Информационная безопасность в системе национальной безопасности Российской Федерации | 1 | 2 | - | 4 |
| 3. | Государственная информационная политика | 2 | 4 | - | 4 |
| 4. | Информация - наиболее ценный ресурс современного общества | 1 | 2 | - | 4 |
| 5. | Угрозы информации | 2 | 4 | - | 6 |
| 6. | Проблемы информационной войны | 1 | 2 | - | 4 |
| 7. | Проблемы информационной безопасности в сфере государственного и муниципального управления | 1 | 2 | - | 4 |
| 8. | Система подготовки кадров в области информационной безопасности в Российской Федерации | 1 | 2 | - | 4 |
| 9. | Анализ существующих методик определения требований к защите информации | 2 | 4 | - | 10 |
| 10. | Способы и средства защиты информации | 2 | 4 | - | 10 |
| 11. | Методы и модели оценки уязвимости информации | 2 | 4 | - | 6 |
| **Итого** | | 16 | 32 | - | 60 |

1. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по прохождению государственной итоговой аттестации

|  |  |  |
| --- | --- | --- |
| №  п/п | Наименование раздела дисциплины | Перечень учебно-методического обеспечения |
| 1. | Российское законодательство в области  информационной  безопасности | Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", ГОСТ Р 50922-2006 С истема ГАРАНТ: [http://base.garant.rU/12148555 /#ixzz3Q6X8uNT J](http://base.garant.rU/12148555%20/#ixzz3Q6X8uNT J) |
| 2. | Защита информации с ограниченным доступом | Доктрина информационной безопасности; Стратегия национальной безопасности; Закон РФ от 21.07.1993 № 5485-1 (ред. от 21.12.2013) "О государственной тайне" (21 июля 1993 г.) Система Консультант Плюс [httD://www.consultant.ru /document/cons doc LAW 156018/](http://www.consultant.ru/document/cons_doc_LAW_156018/)  А. Тихонов, В.В. Райх Информационная безопасность: концептуальные , правовые, организационные и технические аспекты: Учебное пособие. М.: Гелиос АРВ, 2012. 528с., ил.  Н. Семкин, А.Н. Семкин Основы правового обеспечения защиты информации: Учебное пособие для ВУЗов. - М.: Горячая линия-Телеком, 2010. М.: «Гелиос- АРВ», 2010. -239 с.: ил.  А.А. [Малюк,](http://www.techbook.ru/book_list.php?str_author=%d0%a0%d1%9a%d0%a0%c2%b0%d0%a0%c2%bb%d0%a1%d0%8b%d0%a0%d1%94%20%d0%a0%d1%92.%20%d0%a0%d1%92.) В.С. [Горбатов,](http://www.techbook.ru/book_list.php?str_author=%d0%a0%e2%80%9c%d0%a0%d1%95%d0%a1%d0%82%d0%a0%c2%b1%d0%a0%c2%b0%d0%a1%e2%80%9a%d0%a0%d1%95%d0%a0%d0%86%20%d0%a0%e2%80%99.%20%d0%a0%d0%8e.) В.И. [Королев и](http://www.techbook.ru/book_list.php?str_author=%d0%a0%d1%99%d0%a0%d1%95%d0%a1%d0%82%d0%a0%d1%95%d0%a0%c2%bb%d0%a0%c2%b5%d0%a0%d0%86%20%d0%a0%e2%80%99.%20%d0%a0%c2%98.) др. Введение в информационную безопасность: Учебное пособие для вузов. М.: Научно-техническое издательство «Горячая линия - Телеком», 2014. 288 с. |
| 3. | Правовые режимы защиты информации |
| 4. | Защита интеллектуальной собственности | Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Основы информационной безопасности. Учебное пособие для вузов / - М.: Горячая линия - Телеком, 2006. - 544 с.: ил.  [http://www.1variant.ru/2011-10-27-22-57-07/175-2014-02-10- 10-02-40A870--4-4-2014-43.html](http://www.1variant.ru/2011-10-27-22-57-07/175-2014-02-10-10-02-40/1870--4-4-2014-43.html) |
| 5. | Организационные системы обеспечения безопасности информации | В.А. Тихонов, В.В. Райх Информационная безопасность: концептуальные , правовые, организационные и технические аспекты: Учебное пособие. М.: Гелиос АРВ, 2012. 528с., ил. |
| 6. | Корпоративное нормативное регулирование | Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" С истема ГАРАНТ: [http://base.garant.ru/12148555/#ixzz3Q6X8uNT J](http://base.garant.ru/12148555/%23ixzz3Q6X8uNTJ) |
| 7. | Организация объектовых режимов безопасности | Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" С истема ГАРАНТ: [http://base.garant.ru/12148555/#ixzz3Q6X8uNT J](http://base.garant.ru/12148555/%23ixzz3Q6X8uNTJ) |
| 8. | Система подготовки кадров | Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Основы информационной безопасности. Учебное пособие для вузов / - М.: Горячая линия - в области информационной безопасности в Российской Федерации Телеком, 2006. - 544 с.: ил.  [http://www.1variant.ru/2011-10-27-22-57-07/175-2014-02-10-10-02-40/1870--4-4-2014-43.htm](http://www.1variant.ru/2011-10-27-22-57-07/175-2014-02-10-10-02-40/1870--4-4-2014-43.html) |

1. Фонд оценочных средств для прохождения государственной итоговой аттестации

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

1. Перечень основной и дополнительной учебной литературы, нормативно-правовой документации и других изданий, необходимых для прохождения государственной итоговой аттестации
   1. **Перечень основной учебной литературы, необходимой для прохождения государственной итоговой аттестации**
2. А.А. Стрельцов, В.С. Горбатов, Т.А. Полякова и др. Организационное и правовое обеспечение информационной безопасности. Учебное пособие для вузов / - М.: Издательский Центр - «Академия», 2008. - 242 с.: ил.
3. В.А. Тихонов, В.В. Райх Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. М.: Гелиос АРВ, 2012. 528с., ил.
4. С.Н. Семкин, А.Н. Семкин Основы правового обеспечения защиты информации: Учебное пособие для ВУЗов. - М.: Горячая линия- Телеком, 2008. М.: «Гелиос-АРВ», 2010. -239 с.: ил.
5. А.А. [Малюк,](http://www.techbook.ru/book_list.php?str_author=%d0%a0%d1%9a%d0%a0%c2%b0%d0%a0%c2%bb%d0%a1%d0%8b%d0%a0%d1%94%20%d0%a0%d1%92.%20%d0%a0%d1%92.) В.С. [Горбатов,](http://www.techbook.ru/book_list.php?str_author=%d0%a0%e2%80%9c%d0%a0%d1%95%d0%a1%d0%82%d0%a0%c2%b1%d0%a0%c2%b0%d0%a1%e2%80%9a%d0%a0%d1%95%d0%a0%d0%86%20%d0%a0%e2%80%99.%20%d0%a0%d0%8e.) В.И. [Королев и](http://www.techbook.ru/book_list.php?str_author=%d0%a0%d1%99%d0%a0%d1%95%d0%a1%d0%82%d0%a0%d1%95%d0%a0%c2%bb%d0%a0%c2%b5%d0%a0%d0%86%20%d0%a0%e2%80%99.%20%d0%a0%c2%98.) др. Введение в информационную безопасность: Учебное пособие для вузов. М.: Научно­техническое издательство «Горячая линия - Телеком», 2014. 288 с.
   1. **Перечень дополнительной учебной литературы, необходимой для освоения дисциплины**
6. Конституция Российской Федерации. // Российская газета № 7 от 22.12.2008г.
7. Закон Российской Федерации № 2446-1 от 5.03.1992г. «О безопасности». // Российская газета от 22.02.1995г.
8. Стратегия национальной безопасности Российской Федерации. // Российская газета от 31.12.2015г.
9. Доктрина информационной безопасности Российской Федерации. // Российская газета от 05.12.2016г.
10. В.А. Кулишкин Краткий курс лекций по дисциплине «Основы информационной безопасности»: Учебное пособие. - СПб.: ПГУПС, 2008.­232 с.
    1. **Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**
11. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) - [Электронный ресурс] - Режим доступа: [(http://fstec.ru/)](http://fstec.ru/);
12. Электронный фонд нормативно-правовой документации. [Электронный ресурс] – Режим доступа: ([http://docs.cntd.ru/search/intellectual?q= %D0%93%D0%9E%D0%A1 %D0%A2](http://docs.cntd.ru/search/intellectual?q=%20%D0%93%D0%9E%D0%A1%20%D0%A2)[+%D0%A0+56205-2014+&itemtype);](http://docs.cntd.ru/search/intellectual?q=%D0%93%D0%9E%D0%A1%D0%A2+%D0%A0+56205-2014+&itemtype)
13. Официальный сайт информационной сети ТЕХЭКСПЕРТ [Электронный ресурс] - Режим доступа: <http://www.cntd.ru/>**,** свободный;
14. Официальный сайт технического комитета по разработке ГОСТов по информационной безопасности - [Электронный ресурс] - Режим доступа: [(http://tk.gost.ru/wps/portal/tk362)](http://tk.gost.ru/wps/portal/tk362);
15. Информационно-поисковая система «МИМОЗА» (База данных о изобретениях и полезных моделях с 1994 г. по н.в.) (Установлена на компьютере преподавателя в ауд. 2/110);
16. Базу данных «Система ГОСТов по обеспечению информационной безопасности» (Свидетельство о государственной регистрации базы данных №2014621325 от 18.09.2014
    1. **Методические указания для обучающихся по освоению дисциплины**
17. В.А. Кулишкин Аттестация объектов информатизации по требованиям безопасности конфиденциальной информации: Учебное пособие (Методические указания по выполнению лабораторных работ). - СПб.: ПГУПС, 2006, 40 с.;
18. В.А. Кулишкин Организационное обеспечение информационной безопасности: Методические указания для выполнения лабораторных работ. - СПб.: ПГУПС, 2009, 87 с.;
19. В.А. Кулишкин Разработка организационно-распорядительных документов: Учебное пособие (Методические указания по выполнению лабораторных работ). - СПб.: ПГУПС, 2010, 65 с.;
20. В.А. Кулишкин Разработка должностных инструкций: Учебное пособие. - СПб.: ПГУПС, 2014, 100 с. Электронный вариант. База данных менеджмент образовательного процесса на кафедре;
21. В.А. Кулишкин Деловая игра «Аттестация объектов информатизации»: Учебное пособие. - СПб.: ПГУПС, 2012, 29 с
22. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения государственнойитоговой аттестации
23. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) - [Электронный ресурс] - Режим доступа: [(http://fstec.ru/)](http://fstec.ru/);
24. Официальный сайт технического комитета по разработке ГОСТов по информационной безопасности - [Электронный ресурс] - Режим доступа: [(http://tk.gost.ru/wps/portal/tk362)](http://tk.gost.ru/wps/portal/tk362);
25. Электронный фонд нормативно-правовой документации.

[Электронный ресурс] - Режим доступа:

(<http://docs.cntd.ru/search/intellectual?q=%D0%93%D0%9E%D0%A1%D0%A2> [+ %D0%A0+56205-2014+&itemtype);](http://docs.cntd.ru/search/intellectual?q=%D0%93%D0%9E%D0%A1%D0%A2+%D0%A0+56205-2014+&itemtype)

1. Система ГАРАНТ: [http: //base.garant.ru/12148555/#ixzz3 Q6X8uNT J;](http://base.garant.ru/12148555/%23ixzz3Q6X8uNTJ)
2. Система Консультант Плюс [http://www.consultant.ru/document/ cons doc LAW 156018/.](http://www.consultant.ru/document/%20cons%20doc%20LAW%20156018/.)
3. Методические указания для обучающихся по прохождению государственной итоговой аттестации

Методические указания для обучающихся по прохождению государственной итоговой аттестации являются неотъемлемой частью рабочей программы и представлены отдельным документом, рассмотренным на заседании кафедры и утвержденными заведующим кафедрой.

1. Перечень информационных технологий, используемых при прохождении государственной итоговой аттестации, включая перечень программного обеспечения и информационных справочных систем

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

* персональные компьютеры, локальная вычислительная сеть кафедры, проектор;
* методы обучения с использованием информационных технологий: компьютерный лабораторный практикум, демонстрация мультимедийных материалов;
* лабораторное программное обеспечение, разрабатываемое в ходе учебного процесса студентами совместно с преподавателем;
* Интернет-сервисы и электронные ресурсы: сайты, перечисленные в разделе 9 рабочей программы; электронные учебно-методические материалы, доступные через личный кабинет обучающегося на сайте sdo.pgups.ru; на выбор обучающегося - поисковые системы, профессиональные, тематические чаты и форумы, системы аудио и видео конференций, онлайн-энциклопедии и справочники.

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:

* операционная система Windows, MS Office, Антивирус Касперский;
* Adobe Acrobat Reader DC (бесплатное, свободно распространяемое программное обеспечение; режим доступа https://get.adobe.com/ru/reader/).

1. Описание материально-технической базы, необходимой для  
   прохождения государственной итоговой аттестации

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 специальные помещения, укомплектованных специализированной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Материально-техническая база дисциплины включает:

* + - * помещения для проведения лекционных занятий, укомплектованные наборами демонстрационного оборудования (стационарными или переносными персональными компьютерами, настенными или переносными экранами, мультимедийными проекторами с дистанционным управлением и другими информационно-демонстрационными средствами) и учебно-наглядными пособиями (презентациями), обеспечивающими тематические иллюстрации в соответствии с рабочей программой дисциплины;
      * лабораторию информационной безопасности информационно-коммуникационных систем (ауд. 2-104), оснащенную программно-аппаратными средствами защиты информации в соответствии с требованиями ФГОС ВО; лаборатория также оборудована современной вычислительной техникой, комплектом проекционного оборудования для преподавателя;
      * помещения для выполнения курсовой работы, оснащенные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых для выполнения индивидуального задания программных средств (см. раздел 11), а также комплектом оборудования для печати;
      * помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации;
      * помещения для проведения групповых и индивидуальных консультаций, укомплектованные рабочими местами на базе вычислительной техники с установленным офисным пакетом и набором необходимых программных средств (см. раздел 11);
      * помещения для проведения текущего контроля и промежуточной аттестации.

