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*

«Техническая защита информации»  
(Б1.Б.14)

для специальности  
10.05.03 «Информационная безопасность автоматизированных систем»  
по специализации  
«Информационная безопасность автоматизированных систем на транспорте»

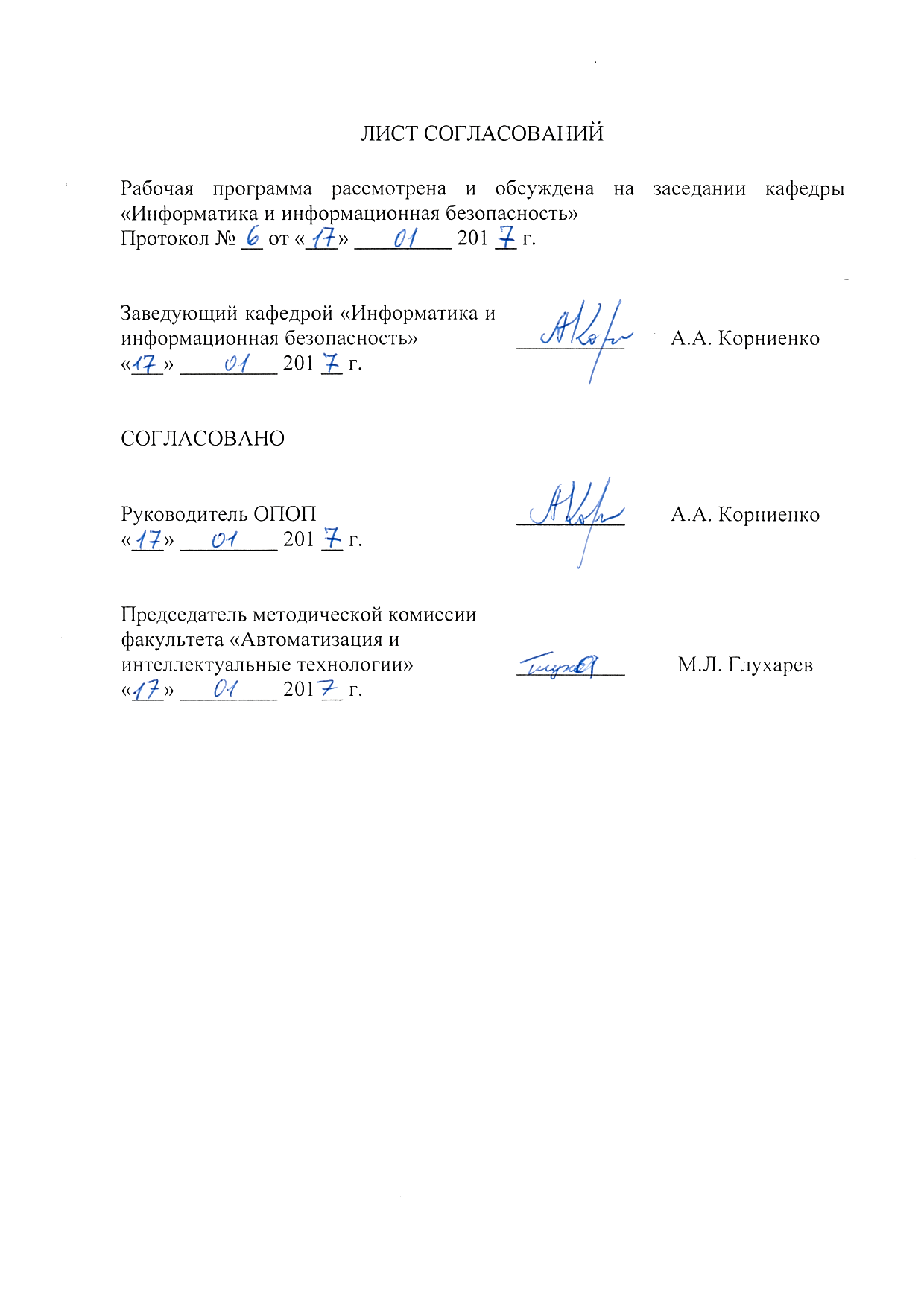
форма обучения - очная

Санкт-Петербург

2017



**1 Цели и задачи дисциплины**



Рабочая программа составлена в соответствие с ФГОС ВО, утвержденным «01» декабря 2016 г., приказ № 1509 по специальности 10.05.03 «Информационная безопасность автоматизированных систем», по дисциплине по дисциплине «Техническая защита информации».

Целью дисциплины «Техническая защита информации» является теоретическая и практическая подготовленность студента к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях.

Для достижения поставленной цели решаются следующие задачи:

* ознакомление студента с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
* ознакомление студента с техническими каналами утечки акустической (речевой) информации;
* ознакомление студента с техническими средствами защиты;
* изучение способов и средств защиты информации, обрабатываемой техническими средствами;
* изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
* изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
* обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

**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:**

* технические каналы утечки информации;
* возможности технических средств перехвата информации;
* способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
* организацию защиты информации от утечки по техническим каналам на объектах информатизации;
* основы физической защиты объектов информатизации.

**УМЕТЬ:**

* пользоваться нормативными документами по противодействию технической разведке;
* анализировать и оценивать угрозы информационной безопасности объекта.

**ВЛАДЕТЬ:**

* методами и средствами технической защиты информации;
* методами расчета и инструментального контроля показателей технической защиты информации.
* навыками рационального выбора средств и методов защиты информации объектов информатизации.

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)**:

* *способность 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:

**организационно-управленческая деятельность:**

* *способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа* (ПК-23).

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 «Техническая защита информации» (Б1.Б.14) относится к базовой части и является обязательной для изучения.

**4 Объем дисциплины и виды учебной работы**

Общая трудоемкость дисциплины ‑ 4 зачетных единицы.

|  |  |  |
| --- | --- | --- |
| **Вид учебной работы** | **Всего часов** | **Семестры** |
| **8** |
| Контактная работа (по видам учебных занятий) В том числе: | 72 | 72 |
| ‑ лекции (Л) | 36 | 36 |
| ‑ практические занятия (ПЗ) | - | - |
| ‑ лабораторные работы (ЛР) | 36 | 36 |
| Самостоятельная работа (СРС) (всего) | 27 | 27 |
| Контроль | 45 | 45 |
| Форма контроля знаний | Экзамен | Экзамен |
| Общая трудоемкость: час /з.е. | 144 / 4 | 144 / 4 |

**5 Содержание и структура дисциплины**

5.1 Содержание дисциплины

|  |  |  |
| --- | --- | --- |
| **№ П/П** | **Наименование раздела дисциплины** | **Содержание раздела** |
| 1 | Источники угрозы безопасности информации | Вводная лекция: цели и задачи, основные понятия и определения;  Основные направления защиты информации. Система показателей защищенности. Объекты защиты информации. Классификация объектов. Демаскирующие признаки. Источники опасных сигналов.  Системный подход к защите информации. Основные концептуальные положения инженерно-технической защиты информации. Основные проблемы инженерно-технической защиты информации  Общая характеристика технической разведки. Классификация методов разведки. |
| 2 | Классификация технических каналов утечки информации | Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Классификация ТКУИ. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика и возможности.  Основы методологии защиты информации. Общая характеристика методов защиты информации. Методы скрытия. Методы технической дезинформации.  Методы и средства защиты информации от утечки по техническим каналам. Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Способы и средства защиты выделенных помещений от утечки речевой информации по техническим каналам. Классификация и характеристика методов и средств поиска устройств перехвата информации.  Особенности защиты акустической информации. Каналы утечки акустической информации. Методы и средства защиты информации от утечки по АКУИ. |
| 3 | Техническое противодействие техническим средствам разведки | Методы и средства добывания информации. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки. Возможности видов технической разведки. Основные направления развития технической разведки. Средства перехвата информации. Средства перехвата информации по ТКУИ. Средства обеспечения технической защиты информации. |
| 4 | Основы контроля эффективности мер защиты информации | Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации.  Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам.  Методы и средства выявления электронных устройств перехвата информации. |
| 5 | Правовое и организационное обеспечение информационной безопасности | Основы нормативно-правового обеспечения защиты информации. Государственная система защиты информации: организационная структура и структура НМД. Закон «О государственной тайне». ФЗ «Об информации, информационных технологиях и защите информации». ФЗ «О персональных данных». Понятие защищаемой информации.  Основы организации ЗИ на объектах информатизации. Система НМД в части конфиденциальной информации (СТРК, Гост). Проведение аттестация ВП, аттестация ОИ, спец.исследования и контроль эффективности. |

5.2 Разделы дисциплины и виды занятий

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование разделов дисциплины** | **Л** | **ПЗ** | **ЛР** | **СРС** |
| 1 | Источники угрозы безопасности информации | 4 | - | 0 | 5 |
| 2 | Классификация технических каналов утечки информации | 12 | - | 14 | 6 |
| 3 | Техническое противодействие техническим средствам разведки | 6 | - | 14 | 6 |
| 4 | Основы контроля эффективности мер защиты информации | 8 | - | 8 | 4 |
| 5 | Правовое и организационное обеспечение информационной безопасности | 6 | - | - | 6 |
| **Итого** | | 36 | - | 36 | 27 |

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

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование раздела дисциплины** | **Перечень учебно-методического обеспечения** |
| 1 | Источники угрозы безопасности информации | Основная литература: [1], [3]  Дополнительная литература: [1] |
| 2 | Классификация технических каналов утечки информации | Основная литература: [1], [2]  Интернет-ресурсы: [1], [4] |
| 3 | Техническое противодействие техническим средствам разведки | Основная литература [1]  Дополнительная литература: [2]  Интернет-ресурсы: [1], [3] |
| 4 | Основы контроля эффективности мер защиты информации | Основная литература [1]  Дополнительная литература: [2]  Интернет-ресурсы: [1], [3], [4] |
| 5 | Правовое и организационное обеспечение информационной безопасности | Основная литература: [3]  Нормативно-правовая документация [1], [2], [3]  Интернет-ресурсы: [2] |

**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. Исаева М.Ф. Техническая защита информации / М.Ф. Исаева – СПб: ФГБОУ ВО ПГУПС, 2017. – 48 с.
2. Беляков И.А. Технические каналы утечки информации / И.А. Беляков – СПб: ФГБОУ ВО ПГУПС, 2017. – 33 с.
3. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / 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. – 439 с.

8.2 Перечень дополнительной учебной литературы, необходимой для освоения дисциплины

1. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / 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. – 447 с.
2. Меньшаков Ю.К. Основы защиты от технических разведок: учеб. пособие / Ю.К. Меньшаков; под общ. ред. М.П. Сычева. – М.: Изд-во МГТУ им. Н.Э.Баумана, 2011. – 478 с.

8.3 Перечень нормативно-правовой документации, необходимой для освоения дисциплины

1. Закон «О государственной тайне» №5485-1 от 21.07.1993.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» №149­ФЗ от 27.07.2006.
3. Федеральный Закон «О персональных данных» №152­ФЗ от 27.07.2006.

**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. Электронно-библиотечная система «Лань». Режим доступа: <https://e.lanbook.com/> (для доступа к полнотекстовым документам требуется авторизация).

**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, персональные компьютеры, средства связи, средства визуализации и презентации);
* методы обучения с использованием информационных технологий (демонстрация мультимедийных материалов, компьютерный лабораторный практикум);
* перечень Интернет-сервисов и электронных ресурсов: сайты, перечисленные в разделе 9 рабочей программы; электронные учебно-методические материалы, доступные через личный кабинет обучающегося на сайте sdo.pgups.ru; на выбор обучающегося – поисковыесистемы, профессиональные, тематические чаты ифорумы, системы аудио и видео конференций, онлайн-энциклопедии исправочники.

Кафедра обеспечена необходимым комплектом лицензионного программного обеспечения:  операционная система Windows, MS Office, Антивирус Касперский.

**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 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;
* помещение для проведения лабораторных работ – лабораторию технической защиты информации (ауд. 2-112), оснащенную специализированным оборудованием по защите информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок, технические средства контроля эффективности защиты информации от утечки по указанным каналам;
* 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.

